

Leitfaden

Amazon EKS



Amazon EKS: Leitfaden

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, Kunden irrezuführen oder Amazon in irgendeiner Weise herabzusetzen oder zu diskreditieren. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

.....	xxii
.....	xxiii
Was ist Amazon EKS?	1
Amazon EKS: Vereinfachtes Kubernetes-Management	1
Features von Amazon EKS	2
Zugehörige Services	4
Amazon EKS — Preisgestaltung	4
Häufige Anwendungsfälle	5
Architektur	6
Steuerebene	7
Datenverarbeitung	7
Kubernetes-Konzepte	9
Warum Kubernetes?	10
Cluster	15
Workloads	20
Nächste Schritte	26
Optionen für die Bereitstellung	27
Verstehen Sie die Bereitstellungsoptionen von Amazon EKS	27
Amazon EKS in der Cloud	27
Amazon EKS in Ihren Rechenzentren oder Edge-Umgebungen	28
Amazon EKS Anywhere für Air-Gap-Umgebungen	29
Amazon EKS-Tools	30
Einrichten	31
Nächste Schritte	31
AWS CLI einrichten	31
So erstellen Sie einen Zugriffsschlüssel	32
Um die AWS CLI zu konfigurieren	32
So rufen Sie ein Sicherheitstoken ab	33
So überprüfen Sie die Benutzeridentität	33
Nächste Schritte	34
Richten Sie kubectl und eksctl ein	34
Installieren oder aktualisieren kubectl	34
Schritt 1: Überprüfen Sie, ob kubectl es installiert ist	35
Schritt 2: Installation oder Aktualisierung kubectl	35

Installieren eksctl	49
Nächste Schritte	49
Quickstart	50
In diesem Tutorial	50
Voraussetzungen	51
Konfigurieren Sie den Cluster	51
Erstellen IngressClass	52
Stellen Sie die Beispielanwendung für das Spiel 2048 bereit	52
Daten im automatischen Modus von Amazon EKS dauerhaft speichern	56
Löschen Sie Ihren Cluster und Ihre Knoten	58
Lernen Sie Amazon EKS kennen	59
Übersicht	59
Workshop zu Amazon EKS	59
Praktische Anleitungen zur Einrichtung von Amazon EKS-Clustern	61
Amazon EKS-Beispiele	62
AWS Tutorials	62
Workshop für Entwickler	63
Terraform-Workshop	63
AWS Amazon EKS-Schulung	63
Erste Schritte	65
Cluster erstellen (EKS-Automatikmodus)	65
Cluster erstellen (eksctl)	66
Voraussetzungen	67
Schritt 1: Erstellen Sie Ihre Amazon-EKS-Cluster und -Knoten	67
Schritt 2: Anzeigen von Kubernetes-Ressourcen	69
Schritt 3: Löschen Ihrer Cluster und Knoten	71
Nächste Schritte	71
Cluster erstellen (Konsole und CLI)	71
Voraussetzungen	72
Schritt 1: Erstellen Sie Ihre Amazon-EKS-Cluster	73
Schritt 2: Konfigurieren Sie Ihren Computer für die Kommunikation mit Ihrem Cluster	76
Schritt 3: Erstellen von Knoten	77
Schritt 4: Ressourcen anzeigen	79
Schritt 5: Löschen von Ressourcen	79
Nächste Schritte	80
Automatischer EKS-Modus	82

Features	82
Automatisierte Komponenten	83
Konfiguration	85
Cluster erstellen	86
eksctl CLI	87
AWS CLI	89
Verwaltungskonsole	97
Aktivieren Sie vorhandene Cluster	99
Referenz zur Migration	100
Migration von EBS-Volumes	101
Load Balancer migrieren	102
Auf dem Cluster aktivieren	102
Migrieren Sie von Karpenter	106
Migrieren Sie von MNGs	110
Von Fargate migrieren	111
Workloads ausführen	117
Stellen Sie einen aufgeblasenen Workload bereit	118
Stellen Sie den Load Balancer bereit	121
Stellen Sie einen statusbehafteten Work	126
Konfiguration	132
Erstellen Sie eine Knotenklasse	135
Erstellen Sie einen Knotenpool	143
Ingress-Klasse erstellen	149
Service erstellen	157
Erstellen StorageClass	163
Deaktivieren Sie den EKS-Automatikmodus	172
Aktualisieren Sie die Kubernetes-Version	174
Überprüfen Sie die integrierten Knotenpools	175
Steuern Sie die Bereitstellung	177
Führen Sie wichtige Add-Ons aus	179
Verwenden Sie Netzwerkrichtlinien	181
Taggen Sie Subnetze	183
Stellen Sie beschleunigte Arbeitslasten bereit	185
CIS-Bericht generieren	192
Verschlüsseln Sie Root-Volumes	195
AMI-Steuerelemente aktualisieren	199

Steuern Sie den ODCR-Einsatz	202
Funktionsweise	203
Verwaltete Instances	203
Identität und Zugriff	208
Netzwerk	214
Fehlerbehebung	217
Agent zur Knotenüberwachung	218
Rufen Sie mithilfe der AWS EC2 CLI die Konsolenausgabe von einer EC2 verwalteten Instanz ab	218
Rufen Sie Knotenprotokolle mithilfe von Debug-Containern und der CLI ab kubectl1	219
Zeigen Sie die mit dem automatischen Modus von EKS verknüpften Ressourcen in der AWS Konsole an	220
IAM-Fehler in Ihrem AWS Konto anzeigen	221
Beheben Sie die Fehlerbehebung, wenn der Pod nicht auf den Automodus-Knoten zugreifen kann	221
Problembehandlung für den Knoten, der dem Cluster nicht beitrifft	222
Volumes auf mehreren Pods teilen	224
Beheben Sie Fehler bei mitgelieferten Controllern im Automatikmodus	225
Versionshinweise	225
30. Juni 2025	225
20. Juni 2025	226
13. Juni 2025	226
30. April 2025	226
18. April 2025	226
11. April 2025	226
4. April 2025	227
31. März 2025	227
21. März 2025	227
14. März 2025	227
Cluster	228
Autocluster erstellen	229
Voraussetzungen	51
Cluster erstellen — Konsole AWS	231
Cluster erstellen — AWS CLI	236
Nächste Schritte	97
Erstellen eines -Clusters	242

Voraussetzungen	51
Schritt 1: Cluster-IAM-Rolle erstellen	243
Schritt 2: Cluster erstellen	245
Schritt 3: Kubeconfig aktualisieren	255
Schritt 4: Cluster-Setup	255
Nächste Schritte	97
Cluster-Erkenntnisse	257
Bereiten Sie sich mit Cluster-Erkenntnissen auf Kubernetes-Versionsupgrades vor	258
Beheben Sie Fehlkonfigurationen mit Cluster-Erkenntnissen	259
Cluster-Einblicke anzeigen	259
Kubernetes-Version aktualisieren	265
Überlegungen zum Amazon EKS Auto Mode	267
Übersicht	267
Schritt 1: Bereiten Sie das Upgrade vor	268
Schritt 2: Überprüfen Sie die Überlegungen zum Upgrade	269
Schritt 3: Aktualisieren Sie die Cluster-Steuerebene	270
Schritt 4: Clusterkomponenten aktualisieren	273
Downgrade der Kubernetes-Version für einen Amazon EKS-Cluster	274
Einen Cluster löschen	275
Überlegungen	101
Cluster löschen (eksctl)	275
Cluster löschen (AWS Konsole)	276
Cluster löschen (AWS CLI)	278
Cluster-Endpointzugriff	279
IPv6Format des Cluster-Endpunkts	280
IPv4Cluster-Endpointformat	280
Privater Cluster-Endpoint	281
Ändern des Cluster-Endpointzugriffs	282
Zugriff auf einen privaten API-Server	285
Konfigurieren Sie den Endpointzugriff	286
Aktivieren Sie die Windows-Unterstützung	290
Überlegungen	101
Voraussetzungen	51
Aktivieren Sie die Windows-Unterstützung	292
Stellen Sie Windows-Pods bereit	294
Support eine höhere Pod-Dichte auf Windows-Knoten	294

Windows-Unterstützung deaktivieren	295
Private Cluster	296
Kubernetes-Versionen	300
Verfügbare Versionen mit Standard-Support	300
Verfügbare Versionen mit verlängertem Support	301
Amazon-EKS-Kubernetes-Veröffentlichungskalender	301
Versionsinformationen mit AWS CLI abrufen	302
Amazon EKS-Version FAQs	303
Erweiterter Support für Amazon EKS FAQs	306
Standard-Supportversionen	308
Versionen mit verlängerten Support	314
Supportzeitraum anzeigen	318
Upgrade-Richtlinie anzeigen	319
Aktivieren Sie den erweiterten Support	321
Deaktivieren Sie den erweiterten Support	322
Plattformversionen	323
Kubernetes-Version 1.33	325
Kubernetes-Version 1.32	326
Kubernetes-Version 1.31	328
Kubernetes-Version 1.30	331
Kubernetes-Version 1.29	334
Kubernetes-Version 1.28	339
Kubernetes-Version 1.27	344
Kubernetes-Version 1.26	350
Holen Sie sich die aktuelle Plattformversion	355
Plattformversion ändern	356
Auto Scaling	356
Automatischer EKS-Modus	356
Zusätzliche Lösungen	357
Erfahren Sie mehr über Zonal Shift	358
Grundlegendes zum Ost-West-Netzwerkdatenverkehr zwischen Pods	358
Anforderungen an EKS Zonal Shift	363
Häufig gestellte Fragen	372
Weitere Ressourcen	375
Aktivieren Sie Zonal Shift	375
Überlegungen	376

Was ist Amazon Application Recovery Controller?	376
Was ist Zonenverschiebung?	377
Was ist Zonal Autoshift?	377
Was macht EKS während eines Autoshifts?	377
Registrieren Sie den EKS-Cluster beim Amazon Application Recovery Controller (ARC) (AWS Konsole)	377
Nächste Schritte	97
Zugriff verwalten	379
Allgemeine Aufgaben	379
Hintergrund	183
Überlegungen zum EKS-Automatikmodus	275
Kubernetes-API-Zugriff	381
Verknüpfen Sie IAM-Identitäten mit Kubernetes-Berechtigungen	382
Stellen Sie den Cluster-Authentifizierungsmodus ein	383
Erteilen Sie Berechtigungen	384
aws-auth ConfigMap	427
OIDC-Anbieter verknüpfen	438
Verknüpfung mit dem OIDC-Anbieter aufheben	443
Auf Cluster-Ressourcen zugreifen	443
Erforderliche Berechtigungen	444
Greifen Sie mit kubectl auf den Cluster zu	450
kubeconfig-Datei automatisch erstellen	452
Workload-Zugriff auf AWS	453
Servicekonto-Tokens	453
Cluster-Add-ons	455
Erteilen von AWS Identity and Access Management Zugriffsverwaltungsberechtigungen für Workloads auf Amazon Elastic Kubernetes Service Service-Clustern	455
Referenzen bei IRSA	460
Pod-Identität	486
Rechenleistung verwalten	521
Vergleichen Sie die Rechenoptionen	521
Verwaltete Knotengruppen	528
Konzepte für verwaltete Knotengruppen	529
Kapazitätstypen für verwaltete Knotengruppen	532
Erstellen	535
Aktualisierung	548

Verhaltensdetails aktualisieren	553
Startvorlagen	557
Löschen	575
Selbstverwaltete Knoten	577
Amazon Linux	579
Bottlerocket	589
Windows	593
Ubuntu Linux	603
Update-Methoden	606
AWS Fargate	620
AWS Überlegungen zu Fargate	620
Fargate-Vergleichstabelle	623
Erste Schritte	626
Definieren Sie Profile	632
Profile löschen	637
Einzelheiten zur Pod-Konfiguration	638
Betriebssystem-Patch-Ereignisse	641
Erfassen Sie Messwerte	644
Protokollierung	647
EC2 Amazon-Instance-Typen	658
Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen	661
Überlegungen zum automatischen EKS-Modus	275
Vorgefertigt, optimiert AMIs	663
AL2 AMI-Abwertung	663
Amazon Linux	669
Bottlerocket	678
Ubuntu Linux	685
Windows	685
Zustand des Knotens	788
Agent zur Knotenüberwachung	788
auto Knotenreparatur	789
Probleme mit dem Zustand des Knotens	790
Zustand des Knotens anzeigen	803
Holen Sie sich Knotenprotokolle	805
Hybridknoten	808

Features	809
Einschränkungen	810
Überlegungen	810
Weitere Ressourcen	811
Voraussetzungen	811
Führen Sie Hybridknoten aus	881
Konfiguration	903
Funktionsweise	943
Hybridknoten nodeadm	988
Fehlerbehebung	1005
App-Datenspeicher	1028
Amazon EBS	1028
Überlegungen	1029
Voraussetzungen	1029
Schritt 1: Erstellen einer IAM-Rolle	1030
Schritt 2: Holen Sie sich den Amazon EBS CSI-Treiber	1038
Schritt 3: Stellen Sie eine Beispielanwendung bereit	1038
Amazon EFS	1039
Überlegungen	1039
Voraussetzungen	1039
Schritt 1: Erstellen einer IAM-Rolle	1040
Schritt 2: Holen Sie sich den Amazon EFS CSI-Treiber	1047
Schritt 3: Erstellen eines Amazon EFS-Dateisystems	1047
Schritt 4: Stellen Sie eine Beispielanwendung bereit	1047
Amazon FSx für Lustre	1048
Stellen Sie den Treiber bereit	1048
Optimieren (EFA)	1056
Optimieren (ohne EFA)	1072
Amazon FSx für NetApp ONTAP	1080
Amazon FSx für OpenZFS	1081
Amazon-Datei-Cache	1081
Mountpoint für Amazon S3	1082
Überlegungen	1082
Stellen Sie den Treiber bereit	1083
Entfernen Sie den Treiber	1093
CSI-Snapshot-Controller	1095

Netzwerk konfigurieren	1097
Fügen Sie über die Managementkonsole ein vorhandenes VPC-Subnetz zu einem Amazon EKS-Cluster hinzu	1097
VPC- und Subnetz-Anforderungen	1098
VPC-Anforderungen und -Überlegungen	1098
Subnetz-Anforderungen und -Überlegungen	1100
Anforderungen und Überlegungen für gemeinsam genutzte Subnetze	1106
Erstellen einer VPC	1107
Voraussetzungen	51
Öffentliche und private Subnetze	1108
Nur öffentliche Subnetze	1111
Nur private Subnetze	1113
Anforderungen an Sicherheitsgruppen	1115
Standardmäßige Cluster-Sicherheitsgruppe	1115
Einschränken des Clusterverkehrs	1117
Gemeinsam genutzte Sicherheitsgruppen	1118
Netzwerk-Add-Ons verwalten	1119
Integrierte Add-Ons	1119
Optionale AWS Netzwerk-Add-Ons	1120
Amazon VPC CNI	1121
Alternative CNI-Plugins	1240
AWS Load Balancer Balancer-Controller	1242
CoreDNS	1260
kube-proxy	1279
Workloads	1286
Beispielbereitstellung (Linux)	1286
Voraussetzungen	51
Namespaces erstellen	1287
Erstellen Sie eine Kubernetes-Bereitstellung	1287
Einen Service erstellen	1289
Überprüfen Sie die erstellten Ressourcen	1290
Führen Sie eine Shell auf einem Pod aus	1293
Nächste Schritte	1294
Beispielbereitstellung (Windows)	1294
Voraussetzungen	51
Namespaces erstellen	1287

Erstellen Sie eine Kubernetes-Bereitstellung	1287
Einen Service erstellen	1289
Überprüfen Sie die erstellten Ressourcen	1298
Führen Sie eine Shell auf einem Pod aus	1293
Nächste Schritte	1302
Vertical Pod Autoscaler	1302
Bereitstellen des Vertical Pod Autoscalers	1302
Testen der Installation von Vertical Pod Autoscaler	1304
Horizontal Pod Autoscaler	1308
Ausführen einer Horizontal Pod Autoscaler-Testanwendung	1309
Netzwerk-Load-Balancer	1311
Voraussetzungen	51
Überlegungen	101
Erstellen eines Network Load Balancers	1315
(Optional) Bereitstellen einer Beispielanwendung	1318
Application Load Balancing	1322
Voraussetzungen	51
Wiederverwendung mit Ingress-Gruppen ALBs	1325
(Optional) Bereitstellen einer Beispielanwendung	1327
Schränken Sie den externen Dienst ein IPs	1330
Kopieren eines Images in ein Repository	1333
Amazon-Bildregister anzeigen	1336
Amazon-EKS-Add-ons	1340
Überlegungen	1341
Überlegungen zum Amazon EKS Auto Mode	1342
Support	1343
AWS Add-Ons	1345
Community-Erweiterungen	1363
Marketplace-Add-ons	1369
Erstellen Sie ein Add-on	1385
Aktualisieren Sie ein Add-on	1399
Überprüfen Sie die Kompatibilität	1407
Entfernen Sie ein Add-On	1409
IAM-Rollen	1413
Felder, die Sie anpassen können	1420
Überprüfen von Container-Images	1424

Clusterverwaltung	1425
Kostenüberwachung	1425
Kosten nach Pod anzeigen	1426
Installieren Sie Kubecost	1427
Greifen Sie auf das Kubecost Dashboard zu	1428
Erfahre mehr über Kubecost	1429
Kennzahlen-Server	1440
Überlegungen	101
Als Community-Add-on mit Amazon EKS Add-ons bereitstellen	1440
Mit Manifest bereitstellen	1441
Stellen Sie Apps mit Helm bereit	1442
Markieren Ihrer -Ressourcen	1444
Grundlagen zu Tags (Markierungen)	1444
Markieren Ihrer -Ressourcen	1445
Tag-Einschränkungen	1446
Markieren von Ressourcen für die Fakturierung	1447
Arbeiten mit Tags über die Konsole	1448
Arbeiten mit Tags mittels CLI, API oder eksctl	1449
Servicekontingente	1450
EKS-Servicekontingente finden Sie in der AWS Management Console	1451
EKS-Dienstkontingente mit der AWS CLI anzeigen	1451
Amazon-EKS-Service-Quotas	1452
AWS Fargate-Servicekontingente	1453
Sicherheit	1454
Bewährte Methoden	1455
Analysieren Sie Schwachstellen	1455
Der Benchmark des Center for Internet Security (CIS) für Amazon EKS	1456
Amazon-EKS-Plattformversionen	1456
Liste der Sicherheitslücken im Betriebssystem	1457
Knotenerkennung mit Amazon Inspector	1457
Cluster- und Knotenerkennung mit Amazon GuardDuty	1457
Überprüfen Sie die Konformität	1457
Überlegungen zu EKS	1459
Sicherheit der Infrastruktur	1459
Ausfallsicherheit	1464
Überlegungen zu Kubernetes	1465

Zertifikatsignierung	1465
-Standardrollen und Benutzer	1468
Aktivieren Sie die geheime Verschlüsselung	1473
AWS Secrets Manager	1478
Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten	1478
Überlegungen zu EKS Auto	1487
API-Sicherheit und Authentifizierung	1487
Netzwerksicherheit	1488
EC2 Sicherheit verwalteter Instanzen	1488
Automatisiertes Ressourcenmanagement	1490
Bewährte Methoden für die Gewährleistung der Sicherheit	1490
IAM-Referenz	1491
Zielgruppe	1491
Authentifizierung mit Identitäten	1492
Verwalten des Zugriffs mit Richtlinien	1495
Amazon EKS und IAM	1498
Identitätsbasierte Richtlinien	1503
Service-verknüpfte Rollen	1511
IAM-Rolle zur Pod-Ausführung	1528
Konnektor-IAM-Rolle	1533
AWS verwaltete Richtlinien	1538
Fehlerbehebung	1567
Cluster-IAM-Rolle	1569
Knoten-IAM-Rolle	1573
Cluster-IAM-Rolle im automatischen Modus	1579
IAM-Rolle für Knoten im automatischen Modus	1583
Überwachen Sie Cluster	1587
Überwachung und Protokollierung auf Amazon EKS	1588
Überwachungs- und Protokollierungstools von Amazon EKS	1589
Beobachtungs-Dashboard	1593
Übersicht	1593
Zustand des Clusters	1593
Überwachung der Steuerungsebene	1594
Cluster-Erkenntnisse	1596
Probleme mit dem Zustand des Knotens	1596
Prometheus-Metriken	1597

Schritt 1: Prometheus-Metriken aktivieren	1598
Schritt 2: Verwenden Sie die Prometheus-Metriken	1600
Schritt 3: Prometheus-Scraper verwalten	1600
Mit Helm bereitstellen	1601
Steuerebene	1604
Amazon CloudWatch	1612
Grundlegende Kennzahlen in Amazon CloudWatch	1612
Amazon CloudWatch Observability-Betreiber	1621
Protokolle der Kontrollebene	1622
Aktivieren oder deaktivieren Sie die Protokolle der Kontrollebene	1623
Protokolle der Cluster-Steuerungsebene anzeigen	1626
AWS CloudTrail	1627
Referenzen	1628
Einträge in der Protokolldatei protokollieren	1629
Metriken zu Auto-Scaling-Gruppen	1632
ADOT Operator	1632
Amazon EKS-Übersicht	1633
Was ist das Amazon EKS Dashboard?	1633
Wie verwendet das Dashboard AWS Organizations?	1633
Aktivieren Sie das EKS-Dashboard über die Konsole AWS	1635
Sehen Sie sich das EKS-Dashboard an	1636
Konfigurieren Sie das Dashboard	1636
Deaktivieren Sie das EKS-Dashboard über die AWS Konsole	1637
Beheben Sie Fehler im EKS-Dashboard	1638
Organisationen konfigurieren	1638
Arbeiten mit anderen -Services	1645
AWS CloudFormation	1645
Amazon EKS und AWS CloudFormation Vorlagen	1645
Erfahren Sie mehr über AWS CloudFormation	1646
Amazon Detective	1646
Verwenden Sie Amazon Detective mit Amazon EKS	1647
Amazon GuardDuty	1647
AWS Resilience Hub	1649
Amazon Security Lake	1649
Vorteile der Verwendung von Security Lake mit Amazon Amazon EKS	1650
Security Lake für Amazon EKS aktivieren	1650

Analysieren von EKS-Protokollen in Security Lake	1651
Amazon VPC Lattice	1651
AWS Local Zones	1651
Fehlerbehebung	1653
Unzureichende Kapazität	1653
Knoten können nicht mit dem Cluster verknüpft werden	1653
Nicht autorisiert oder Zugriff verweigert (kubectl)	1655
hostname doesn't match	1656
getsockopt: no route to host	1657
Instances failed to join the Kubernetes cluster	1657
Fehlercodes bei verwalteten Knotengruppen	1657
Not authorized for images	1662
Der Knoten befindet sich im NotReady Status	1663
EKS Log Collector	1663
Container-Laufzeitnetzwerk nicht bereit	1664
TLS-Handshake-Zeitüberschreitung	1666
InvalidClientTokenId	1666
Die Knotengruppen müssen mit der Kubernetes-Version übereinstimmen, bevor die Kontrollebene aktualisiert wird	1667
Beim Starten vieler Knoten gibt es Too Many Requests-Fehler	1667
Unautorisierte Fehlerantwort (HTTP 401) bei Kubernetes-API-Serveranfragen	1668
Die Amazon-EKS-Plattformversion liegt mehr als zwei Versionen hinter der aktuellen Plattformversion	1668
FAQs Cluster-Integritäts- und Fehlercodes mit Lösungspfaden	1671
Amazon-EKS-Anschluss	1678
Überlegungen zum Amazon EKS Connector	1678
Erforderliche IAM-Rollen für Amazon EKS Connector	1679
Einen Cluster Connect	1679
Überlegungen	1680
Voraussetzungen	1680
Schritt 1: Registrieren des Clusters	1680
Schritt 2: Installieren des eks-connector-Agents	1683
Nächste Schritte	1685
Gewähren Sie Zugriff auf Cluster	1685
Voraussetzungen	1686
Einen Cluster abmelden	1687

Den Kubernetes-Cluster deregistrieren	1688
Bereinigen Sie die Ressourcen in Ihrem Kubernetes-Cluster	1689
Problembehandlung beim EKS-Connector	1689
Grundlegende Fehlersuche	1689
Helm-Ausgabe: 403 Forbidden	1691
Konsolenfehler: Der Cluster steckt im Status „Ausstehend“ fest	1692
Konsolenfehler: Der Benutzer system:serviceaccount:eks-connector:eks-connector kann sich nicht als Ressourcenbenutzer in der API-Gruppe im Clusterbereich ausgeben	1692
Konsolenfehler: [...] ist verboten: Der Benutzer [...] kann die Ressource [...] in der API-Gruppe im Clusterbereich nicht auflisten	1693
Konsolenfehler: Amazon EKS kann nicht mit Ihrem Kubernetes-Cluster-API-Server kommunizieren. Der Cluster muss sich im ACTIVE-Status befinden, um eine erfolgreiche Verbindung zu erreichen. Try again in few minutes. (Versuchen Sie es in ein paar Minuten erneut.)	1693
Die Pods des Amazon EKS-Connectors stürzen in einer Schleife ab	1694
EKS-Connector konnte nicht initiiert werden: InvalidActivation	1694
Im Cluster-Knoten fehlt die ausgehende Konnektivität	1696
Die Amazon EKS-Connector-Pods befinden sich im ImagePullBackOff Status	1696
Häufig gestellte Fragen	1696
Sicherheitsüberlegungen	1697
AWS Verantwortlichkeiten	1698
Pflichten des Kunden	1698
Amazon EKS auf AWS Outposts	1700
Wann die einzelnen Bereitstellungsoptionen verwendet werden sollten	1700
Vergleich der Optionen für die Bereitstellung	1701
Führen Sie lokale Cluster aus	1703
Unterstützte Regionen AWS	1704
Stellen Sie einen lokalen Cluster bereit	1704
Versionen der EKS-Plattform	1716
Erstellen von VPC und Subnetzen	1729
Bereiten Sie sich auf Verbindungsabbrüche vor	1733
Überlegungen zur Kapazität	1738
Fehlersuche bei Clustern	1741
Knoten	1754
eksctl	1755
AWS Management Console	1757

Machine Learning auf EKS	1764
Warum sollten Sie sich für EKS für KI/ML entscheiden?	1764
Wichtige Anwendungsfälle	1765
Fallstudien	1766
Beginnen Sie mit der Nutzung von Machine Learning auf EKS	1767
Fangen Sie mit ML an	1767
Weiter mit ML auf EKS	1768
Bereiten Sie sich auf ML vor	1769
Führen Sie Linux GPU aus AMIs	1770
Führen Sie Windows GPU aus AMIs	1772
Reservieren Sie GPUs für MNG	1778
Reservieren Sie GPUs für SMN	1781
Verfälschen Sie GPU-Knoten	1785
Trainingscluster mit EFA	1787
Bereiten Sie Inferentia-Cluster vor	1799
Probieren Sie Tutorials für ML auf EKS aus	1805
Erstellen Sie generative KI-Plattformen auf EKS	1805
Führen Sie spezielle generative KI-Frameworks auf EKS aus	1805
Maximieren Sie die NVIDIA-GPU-Leistung für ML auf EKS	1806
Führen Sie Videokodierungs-Workloads auf EKS aus	1806
Beschleunigen Sie das Laden von Bildern für Inferenz-Workloads	1806
Überwachung von ML-Workloads	1806
Ankündigungen für ML auf EKS	1806
Projekte im Zusammenhang mit Amazon EKS	1808
Support für Software, die auf EKS bereitgestellt wird	1808
Verwaltungs-Tools	1809
eksctl	1809
AWS Controller für Kubernetes	1809
Flux CD	1810
CDK für Kubernetes	1810
Netzwerk	1810
Amazon-VPC-CNI-Plug-In für Kubernetes	1810
AWS Load Balancer Controller für Kubernetes	1810
ExternalDNS	1811
Machine Learning	1811
Kubeflow	1811

Auto Scaling	1811
Cluster Autoscaler	1811
Karpenter	1812
Escalator	1812
Überwachung	1812
Prometheus	1812
Fortlaufende Integration/Fortlaufende Bereitstellung	1812
Jenkins X	1812
Neue Funktionen und Roadmap	1814
Dokumentverlauf	1815
Tragen Sie bei	1875
Einzelne Seite bearbeiten	1875
Voraussetzungen	51
Verfahren	105
Überblick über die Pull-Anfrage	1877
Bearbeiten Sie Dateien mit GitHub	1878
Voraussetzungen	51
Verfahren	105
Stil-Feedback anzeigen	1880
Installieren Sie Vale	1881
Installieren Sie die VS Code Vale-Erweiterung	1881
Vale synchronisieren	1881
Stil-Feedback in VS Code anzeigen	1881
Seite erstellen	1882
Seite erstellen	1882
Seite zur Navigation hinzufügen	1882
Link einfügen	1883
Link zu einer Seite oder einem Abschnitt im EKS-Benutzerhandbuch	1883
Link zu einem anderen Leitfaden in den AWS Dokumenten	1883
Link zu einer externen Webseite	1884
Mit Amazon Q erstellen	1884
Installieren Sie Amazon Q mit VS Code	1885
Melden Sie sich bei Amazon Q an	1885
Verwenden Sie Amazon Q, um Inhalte zu erstellen	1886
Tipps	1886
PR-Vorschau anzeigen	1886

Vorschau ansehen	1887
Einschränkungen in der Vorschau	1888
AsciiDoc Syntax	1888
Neue Seite	1889
Überschriften	1889
Formatierung von Text	1889
Listen	1889
Links	1890
Codebeispiele	1890
Bilder	1890
Tabellen	1891
Callouts	1891
Einschließlich anderer Dateien	1891
Attribute (ähnlich wie Entitäten)	1892
Verfahren	1892

Hilf mit, diese Seite zu verbessern

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

Wenn Sie zu diesem Benutzerhandbuch beitragen möchten, wählen Sie den GitHub Link Diese Seite bearbeiten auf, der sich im rechten Bereich jeder Seite befindet.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

Was ist Amazon EKS?

Amazon EKS: Vereinfachtes Kubernetes-Management

Amazon Elastic Kubernetes Service (EKS) bietet einen vollständig verwalteten Kubernetes-Service, der den Betrieb von Kubernetes-Clustern überflüssig macht. Mit EKS können Sie:

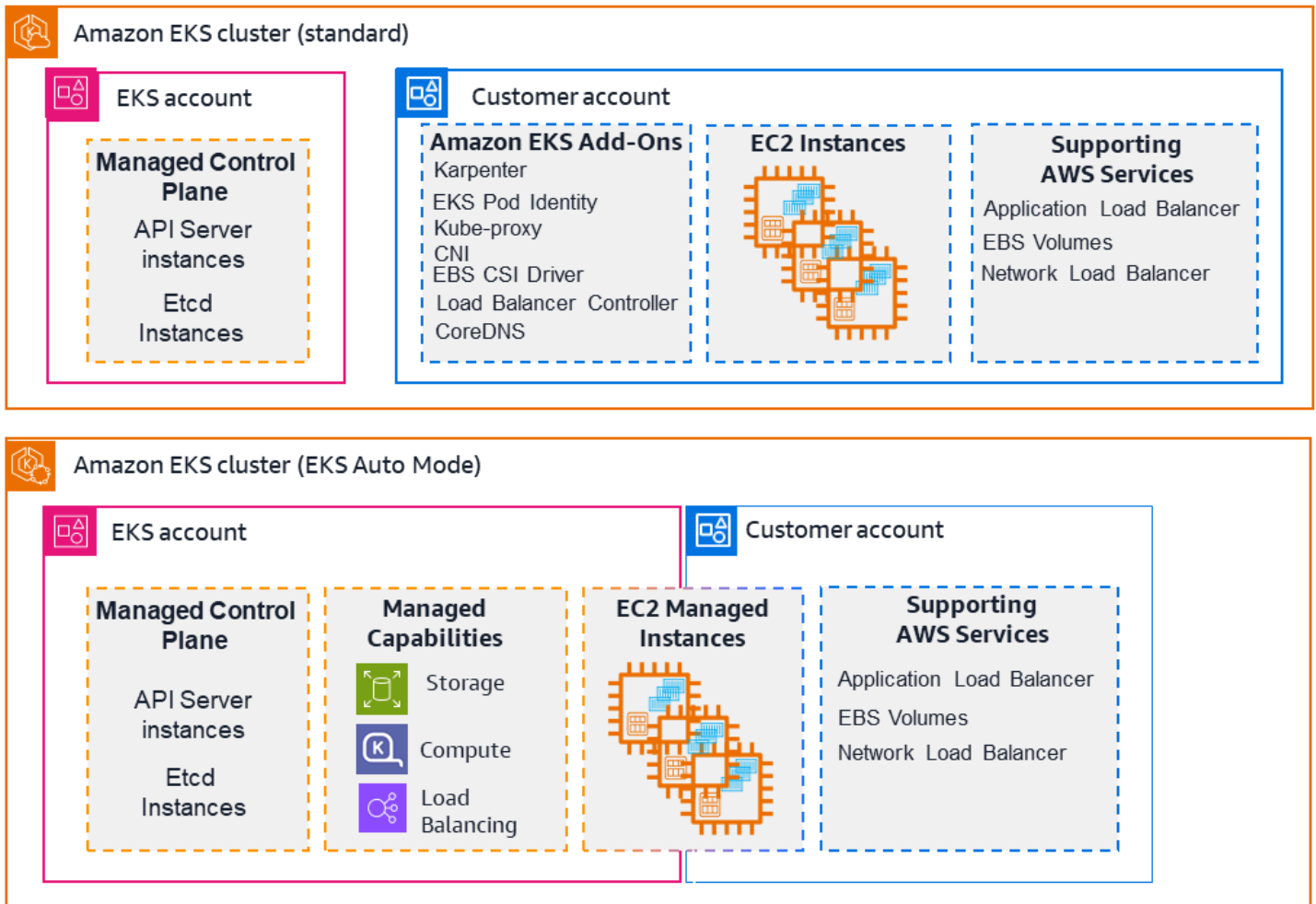
- Schnellere Bereitstellung von Anwendungen bei geringerem Betriebsaufwand
- Skalieren Sie nahtlos, um wechselnden Workload-Anforderungen gerecht zu werden
- Verbessern Sie die Sicherheit durch AWS Integration und automatisierte Updates
- Wählen Sie zwischen dem Standard-EKS- oder dem vollautomatischen EKS-Automatikmodus

Amazon Elastic Kubernetes Service (Amazon EKS) ist die führende Plattform für den Betrieb von [Kubernetes-Clustern](#), sowohl in der Amazon Web Services (AWS) -Cloud als auch in Ihren eigenen Rechenzentren ([EKS Anywhere und Amazon EKS Hybrid](#) Nodes).

Amazon EKS vereinfacht den Aufbau, die Sicherung und die Wartung von Kubernetes-Clustern. Es kann kostengünstiger sein, wenn es darum geht, genügend Ressourcen bereitzustellen, um Spitzennachfragen zu decken, als wenn es darum geht, Ihre eigenen Rechenzentren zu verwalten. Zwei der wichtigsten Ansätze für die Verwendung von Amazon EKS lauten wie folgt:

- EKS-Standard: AWS verwaltet die [Kubernetes-Steuerebene](#), wenn Sie einen Cluster mit EKS erstellen. Komponenten, die Knoten verwalten, Workloads planen, in die AWS Cloud integrieren und Informationen zur Kontrollebene speichern und skalieren, damit Ihre Cluster am Laufen bleiben, werden automatisch für Sie verwaltet.
- EKS-Automatikmodus: Mithilfe der Funktion [EKS Auto Mode](#) erweitert EKS seine Kontrolle auch auf die Verwaltung von [Knoten](#) (Kubernetes-Datenebene). Es vereinfacht das Kubernetes-Management durch die automatische Bereitstellung der Infrastruktur, die Auswahl optimaler Recheninstanzen, die dynamische Skalierung von Ressourcen, die kontinuierliche Optimierung der Kosten, das Patchen von Betriebssystemen und die Integration in Sicherheitsdienste. AWS

Das folgende Diagramm zeigt, wie Amazon EKS Ihre Kubernetes-Cluster in die AWS Cloud integriert, je nachdem, welche Methode der Clustererstellung Sie wählen:



Amazon EKS hilft Ihnen dabei, die Produktionszeit zu verkürzen, die Leistung, Verfügbarkeit und Stabilität zu verbessern und die Systemsicherheit zu verbessern. Weitere Informationen finden Sie unter [Amazon Elastic Kubernetes Service](#).

Features von Amazon EKS

Amazon EKS bietet die folgenden Funktionen auf hoher Ebene:

Verwaltungsschnittstellen

EKS bietet mehrere Schnittstellen zur Bereitstellung, Verwaltung und Wartung von Clustern: AWS Management Console, darunter Amazon EKS API/SDKs, CDK, AWS CLI, eksctl CLI und Terraform. AWS CloudFormation. Weitere Informationen erhalten Sie unter [Erste Schritte](#) und [Cluster](#).

Tools zur Zugriffskontrolle

EKS stützt sich sowohl auf Kubernetes- als auch auf AWS Identity and Access Management (AWS IAM) -Funktionen, um den [Zugriff von Benutzern und Workloads zu verwalten](#). Weitere Informationen erhalten Sie unter [the section called “Kubernetes-API-Zugriff”](#) und [the section called “Workload-Zugriff auf AWS”](#).

Ressourcen berechnen

Für [Rechenressourcen](#) ermöglicht EKS die gesamte Palette der EC2 Amazon-Instance-Typen und AWS Innovationen wie Nitro und Graviton mit Amazon EKS, sodass Sie die Rechenleistung für Ihre Workloads optimieren können. Weitere Informationen finden Sie unter [Rechenleistung verwalten](#).

Speicherung

[Der automatische Modus von EKS erstellt automatisch Speicherklassen mithilfe von EBS-Volumes](#). Mithilfe von Container Storage Interface (CSI) -Treibern können Sie auch Amazon S3, Amazon EFS, Amazon FSX und Amazon File Cache für Ihre Anwendungsspeicheranforderungen verwenden. Weitere Informationen finden Sie unter [App-Datenspeicher](#).

Sicherheit

Das Modell der gemeinsamen Verantwortung wird in Bezug auf die [Sicherheit in Amazon EKS](#) verwendet. Weitere Informationen finden Sie unter [Bewährte Methoden zur Sicherheit](#), [Infrastruktursicherheit](#) und [Kubernetes-Sicherheit](#).

Tools zur Überwachung

Verwenden Sie das [Observability-Dashboard](#), um Amazon EKS-Cluster zu überwachen. [Zu den Überwachungstools gehören Prometheus CloudWatch, Cloudtrail und ADOT Operator. Weitere Informationen zu Dashboards, Metrikservern und anderen Tools finden Sie unter EKS-Clusterkosten und Kubernetes Metrics Server.](#)

Kubernetes-Kompatibilität und Support

Amazon EKS ist Kubernetes-konform zertifiziert, sodass Sie Kubernetes-kompatible Anwendungen ohne Refactoring bereitstellen und Tools und Plug-ins der Kubernetes-Community verwenden können. EKS [bietet sowohl Standardsupport](#) als auch erweiterten Support für Kubernetes. Weitere Informationen finden Sie unter [the section called “Kubernetes-Versionen”](#).

Zugehörige Services

Services zur Verwendung mit Amazon EKS

Sie können andere AWS Services mit den Clustern verwenden, die Sie mit Amazon EKS bereitstellen:

Amazon EC2

Besorgen Sie sich skalierbare Rechenkapazität auf Abruf mit [Amazon EC2](#).

Amazon EBS

Fügen Sie skalierbare, leistungsstarke Blockspeicherressourcen mit [Amazon EBS](#) hinzu.

Amazon ECR

Speichern Sie Container-Images sicher mit [Amazon ECR](#).

Amazon CloudWatch

Überwachen Sie AWS Ressourcen und Anwendungen in Echtzeit mit [Amazon CloudWatch](#).

Amazon Prometheus

Verfolgen Sie Metriken für containerisierte Anwendungen mit [Amazon Managed Service for Prometheus](#).

Elastic Load Balancing

Verteilen Sie mit [Elastic Load Balancing](#) eingehenden Traffic auf mehrere Ziele.

Amazon GuardDuty

Erkennen Sie mit [Amazon](#) Bedrohungen für EKS-Cluster GuardDuty.

AWS Zentrum für Resilienz

Bewerten Sie die Widerstandsfähigkeit von EKS-Clustern mit [AWS Resilience Hub](#).

Amazon EKS — Preisgestaltung

Amazon EKS bietet Preise pro Cluster, die auf der Unterstützung der Kubernetes-Cluster-Version, den Preisen für den Amazon EKS Auto Mode und den Preis pro vCPU für Amazon EKS-Hybridknoten basieren.

Wenn Sie Amazon EKS verwenden, zahlen Sie separat für die AWS Ressourcen, die Sie für die Ausführung Ihrer Anwendungen auf Kubernetes-Worker-Knoten verwenden. Wenn Sie beispielsweise Kubernetes-Worker-Knoten als EC2 Amazon-Instances mit Amazon EBS-Volumes und öffentlichen IPv4 Adressen ausführen, werden Ihnen die Instance-Kapazität über Amazon EC2, die Volume-Kapazität über Amazon EBS und die IPv4 Adresse über Amazon VPC in Rechnung gestellt.

Detaillierte Preisinformationen finden Sie auf den jeweiligen Preisseiten der AWS Services, die Sie mit Ihren Kubernetes-Anwendungen nutzen.

- Die Preise für Amazon EKS-Cluster, Amazon EKS Auto Mode und Amazon EKS Hybrid Nodes finden Sie unter [Amazon EKS-Preise](#).
- EC2 Die Amazon-Preise finden Sie unter [Amazon EC2 On-Demand-Preise](#) und [Amazon EC2 Spot-Preise](#).
- Informationen zu AWS Fargate-Preisen finden Sie unter [AWS Fargate-Preise](#).
- Sie können Ihre Sparpläne für Rechenleistung verwenden, die in Amazon EKS-Clustern verwendet wird. Weitere Informationen finden Sie unter [Preise und Savings Plans](#).

Häufige Anwendungsfälle in Amazon EKS

Amazon EKS bietet robuste verwaltete Kubernetes-Services, die darauf ausgelegt sind AWS, containerisierte Anwendungen zu optimieren. Im Folgenden finden Sie einige der häufigsten Anwendungsfälle von Amazon EKS, die Ihnen dabei helfen, die Stärken von Amazon EKS für Ihre spezifischen Anforderungen zu nutzen.

Bereitstellung von Anwendungen mit hoher Verfügbarkeit

Mit [Elastic Load Balancing](#) können Sie sicherstellen, dass Ihre Anwendungen über mehrere [Availability Zones](#) hinweg hochverfügbar sind.

Aufbau von Microservices-Architekturen

Verwenden Sie die Funktionen zur Serviceerkennung von Kubernetes mit [AWS Cloud Map](#) oder [Amazon VPC Lattice](#), um belastbare Systeme aufzubauen.

Automatisierung des Softwareveröffentlichungsprozesses

Verwalten Sie Pipelines für fortlaufende Integration und fortlaufende Bereitstellung (Continuous Integration and Continuous Deployment, CI/CD), die den Prozess der automatisierten Erstellung, Prüfung und Bereitstellung von Anwendungen vereinfachen.

Serverlose Anwendungen ausführen

Verwenden Sie [AWS Fargate](#) mit Amazon EKS, um serverlose Anwendungen auszuführen. Das bedeutet, dass Sie sich ausschließlich auf die Anwendungsentwicklung konzentrieren können, während Amazon EKS und Fargate die zugrunde liegende Infrastruktur verwalten.

Workloads für maschinelles Lernen ausführen

Amazon EKS ist mit gängigen Machine-Learning-Frameworks wie [TensorFlow](#), [MXNet](#) und [PyTorch](#) kompatibel. Mit GPU-Unterstützung können Sie selbst komplexe Machine-Learning-Aufgaben effektiv bewältigen.

Konsistente Bereitstellung vor Ort und in der Cloud

Um die Ausführung von Kubernetes in lokalen Umgebungen zu vereinfachen, können Sie dieselben Amazon EKS-Cluster, Funktionen und Tools verwenden, um selbstverwaltete Knoten auf [AWS Outposts](#) auszuführen, oder Sie können [Amazon EKS-Hybridknoten](#) mit Ihrer eigenen Infrastruktur verwenden. Für eigenständige Air-Gap-Umgebungen können Sie [Amazon EKS Anywhere](#) verwenden, um das Kubernetes-Cluster-Lebenszyklusmanagement in Ihrer eigenen Infrastruktur zu automatisieren.

Ausführung kostengünstiger Batch-Verarbeitungs- und Big-Data-Workloads

Nutzen Sie [Spot-Instances](#), um Ihre Batch-Verarbeitungs- und Big-Data-Workloads wie [Apache Hadoop](#) und [Spark](#) zu einem Bruchteil der Kosten auszuführen. Auf diese Weise können Sie ungenutzte EC2 Amazon-Kapazitäten zu ermäßigten Preisen nutzen.

Sicherung der Anwendung und Sicherstellung der Einhaltung von Vorschriften

Implementieren Sie strenge Sicherheitspraktiken und sorgen Sie für die Einhaltung der Vorschriften mit Amazon EKS, das in AWS Sicherheitsservices wie [AWS Identity and Access Management](#) (IAM), [Amazon Virtual Private Cloud](#) (Amazon VPC) und [AWS Key Management Service](#) (AWS KMS) integriert ist. Dadurch werden der Datenschutz und die Datensicherheit gemäß den Branchenstandards gewährleistet.

Amazon-EKS-Architektur

Amazon EKS entspricht der allgemeinen Cluster-Architektur von Kubernetes. Weitere Informationen finden Sie unter [Kubernetes-Komponenten in der Kubernetes-Dokumentation](#). In den folgenden Abschnitten werden einige zusätzliche Architekturdetails für Amazon EKS zusammengefasst.

Steuerebene

Amazon EKS stellt sicher, dass jeder Cluster über eine eigene einzigartige Kubernetes-Steuerebene verfügt. Durch dieses Design wird die Infrastruktur jedes Clusters getrennt, sodass es keine Überschneidungen zwischen Clustern oder Konten gibt. AWS Das Setup beinhaltet:

Verteilte Komponenten

Die Kontrollebene positioniert mindestens zwei API-Serverinstanzen und drei [etcd-Instanzen](#) in drei AWS Availability Zones innerhalb einer AWS Region.

Optimale Leistung

Amazon EKS überwacht und passt die Instances der Steuerebene aktiv an, um eine Spitzenleistung aufrechtzuerhalten.

Ausfallsicherheit

Wenn eine Instance der Steuerebene ausfällt, wird sie von Amazon EKS schnell ersetzt, wobei bei Bedarf eine andere Availability Zone verwendet wird.

Konsistente Verfügbarkeit

Durch den Betrieb von Clustern in mehreren Availability Zones wird ein zuverlässiges [Service Level Agreement \(SLA\) für die Verfügbarkeit von API-Server-Endpunkten](#) erzielt.

Amazon EKS verwendet Amazon Virtual Private Cloud (Amazon VPC), um den Datenverkehr zwischen Komponenten der Steuerebene innerhalb eines einzelnen Clusters zu begrenzen. Clusterkomponenten können keine Kommunikation von anderen Clustern oder AWS Konten anzeigen oder empfangen, es sei denn, dies ist durch die Richtlinien für die rollenbasierte Zugriffskontrolle (RBAC) von Kubernetes autorisiert.

Datenverarbeitung

Zusätzlich zur Steuerebene verfügt ein Amazon-EKS-Cluster über eine Reihe von Worker-Computern, die als Knoten bezeichnet werden. Die Auswahl des geeigneten Amazon-EKS-Cluster-Knotentyps ist entscheidend, um Ihre spezifischen Anforderungen zu erfüllen und die Ressourcennutzung zu optimieren. Amazon EKS bietet die folgenden Primärknotentypen:

Automatischer EKS-Modus

Der [EKS-Automatikmodus](#) erweitert das AWS Management über die Steuerungsebene hinaus auf die Datenebene und automatisiert so die Verwaltung der Cluster-Infrastruktur. Er integriert die Kernfunktionen von Kubernetes als integrierte Komponenten, darunter automatische Rechenskalierung, Netzwerke, Lastenausgleich, DNS, Speicher und GPU-Unterstützung. Der automatische Modus von EKS verwaltet Knoten dynamisch auf der Grundlage der Workload-Anforderungen und verwendet unveränderliche Knoten AMIs mit erweiterten Sicherheitsfunktionen. Es automatisiert Updates und Upgrades unter Einhaltung der Pod-Disruption-Budgets und umfasst verwaltete Komponenten, für die andernfalls eine zusätzliche Verwaltung erforderlich wäre. Diese Option ist ideal für Benutzer, die AWS Fachwissen für den day-to-day Betrieb nutzen, den Betriebsaufwand minimieren und sich auf die Anwendungsentwicklung statt auf das Infrastrukturmanagement konzentrieren möchten.

AWS Fargate

[Fargate](#) ist eine Serverless-Compute-Engine für Container, die die Verwaltung der zugrunde liegenden Instances überflüssig macht. Mit Fargate spezifizieren Sie den Ressourcenbedarf Ihrer Anwendung und stellen die Infrastruktur AWS automatisch bereit, skalieren und warten. Diese Option ist ideal für Benutzer, die Prioritäten setzen ease-of-use und sich auf die Anwendungsentwicklung und -bereitstellung konzentrieren möchten, anstatt die Infrastruktur zu verwalten.

Karpenter

[Karpenter ist ein](#) flexibler, leistungsstarker Kubernetes-Cluster-Autoscaler, der zur Verbesserung der Anwendungsverfügbarkeit und Clustereffizienz beiträgt. Karpenter führt als Reaktion auf die sich ändernde Anwendungslast Rechenressourcen in der richtigen Größe ein. Mit dieser Option können just-in-time Rechenressourcen bereitgestellt werden, die den Anforderungen Ihrer Arbeitslast entsprechen.

Verwaltete Knotengruppen

[Verwaltete Knotengruppen](#) sind eine Mischung aus Automatisierung und Anpassung für die Verwaltung einer Sammlung von EC2 Amazon-Instances innerhalb eines Amazon EKS-Clusters. AWS kümmert sich um Aufgaben wie das Patchen, Aktualisieren und Skalieren von Knoten und vereinfacht so betriebliche Aspekte. Gleichzeitig werden benutzerdefinierte kubernetes-Argumente unterstützt, die Möglichkeiten für erweiterte CPU- und Speicherverwaltungsrichtlinien eröffnen. Darüber hinaus verbessern sie die Sicherheit durch AWS Identity and Access Management (IAM) -Rollen für Dienstkonten und reduzieren gleichzeitig den Bedarf an separaten Berechtigungen pro Cluster.

Selbstverwaltete Knoten

[Selbstverwaltete Knoten](#) bieten die volle Kontrolle über Ihre EC2 Amazon-Instances innerhalb eines Amazon EKS-Clusters. Sie sind für die Verwaltung, Skalierung und Wartung der Knoten zuständig und haben somit die volle Kontrolle über die zugrunde liegende Infrastruktur. Diese Option eignet sich für Benutzer, die eine differenzierte Kontrolle und Anpassung ihrer Knoten benötigen und bereit sind, Zeit in die Verwaltung und Wartung ihrer Infrastruktur zu investieren.

Amazon EKS-Hybridknoten

Mit [Amazon EKS Hybrid Nodes](#) können Sie Ihre lokale Infrastruktur und Ihre Edge-Infrastruktur als Knoten in Amazon EKS-Clustern verwenden. Amazon EKS Hybrid Nodes vereinheitlicht das Kubernetes-Management in allen Umgebungen und verlagert die Verwaltung der Kubernetes-Steuerungsebene auf AWS Ihre lokalen und Edge-Anwendungen.

Kubernetes-Konzepte

Amazon Elastic Kubernetes Service (Amazon EKS) ist ein AWS verwalteter Service, der auf dem [Open-Source-Kubernetes-Projekt](#) basiert. Es gibt zwar Dinge, die Sie darüber wissen müssen, wie der Amazon EKS-Service in die AWS Cloud integriert wird (insbesondere, wenn Sie zum ersten Mal einen Amazon EKS-Cluster erstellen), aber sobald er betriebsbereit ist, verwenden Sie Ihren Amazon EKS-Cluster auf die gleiche Weise wie jeden anderen Kubernetes-Cluster. Um also mit der Verwaltung von Kubernetes-Clustern und der Bereitstellung von Workloads zu beginnen, benötigen Sie zumindest ein grundlegendes Verständnis der Kubernetes-Konzepte.

Auf dieser Seite sind die Kubernetes-Konzepte in drei Abschnitte unterteilt:, und. [the section called “Warum Kubernetes?”](#) [the section called “Cluster”](#) [the section called “Workloads”](#) Der erste Abschnitt beschreibt den Wert der Ausführung eines Kubernetes-Service, insbesondere als verwalteter Service wie Amazon EKS. Im Abschnitt Workloads wird beschrieben, wie Kubernetes-Anwendungen erstellt, gespeichert, ausgeführt und verwaltet werden. Im Abschnitt Cluster werden die verschiedenen Komponenten beschrieben, aus denen Kubernetes-Cluster bestehen, und Ihre Aufgaben für die Erstellung und Wartung von Kubernetes-Clustern.

Themen

- [Warum Kubernetes?](#)
- [Cluster](#)
- [Workloads](#)
- [Nächste Schritte](#)

Wenn Sie diesen Inhalt durchgehen, führen Sie Links zu weiteren Beschreibungen der Kubernetes-Konzepte sowohl in der Amazon EKS- als auch in der Kubernetes-Dokumentation, falls Sie sich eingehend mit einem der hier behandelten Themen befassen möchten. Einzelheiten darüber, wie Amazon EKS die Steuerungsebene und die Rechenfunktionen von Kubernetes implementiert, finden Sie unter [the section called “Architektur”](#)

Warum Kubernetes?

Kubernetes wurde entwickelt, um die Verfügbarkeit und Skalierbarkeit bei der Ausführung geschäftskritischer containerisierter Anwendungen in Produktionsqualität zu verbessern. Anstatt Kubernetes nur auf einem einzigen Computer auszuführen (obwohl das möglich ist), erreicht Kubernetes diese Ziele, indem es Ihnen ermöglicht, Anwendungen auf mehreren Computern auszuführen, die je nach Bedarf erweitert oder verkleinert werden können. Kubernetes umfasst Funktionen, die Ihnen Folgendes erleichtern:

- Stellen Sie Anwendungen auf mehreren Maschinen bereit (mithilfe von Containern, die in Pods bereitgestellt werden)
- Überwachen Sie den Zustand der Container und starten Sie ausgefallene Container neu
- Skalieren Sie Container je nach Auslastung nach oben oder unten
- Aktualisieren Sie Container mit neuen Versionen
- Ordnen Sie Ressourcen zwischen Containern zu
- Gleichen Sie den Verkehr zwischen den Maschinen aus

Wenn Kubernetes diese Art von komplexen Aufgaben automatisiert, kann sich ein Anwendungsentwickler auf den Aufbau und die Verbesserung seiner Anwendungs-Workloads konzentrieren, anstatt sich Gedanken über die Infrastruktur machen zu müssen. Der Entwickler erstellt in der Regel als YAML-Dateien formatierte Konfigurationsdateien, die den gewünschten Status der Anwendung beschreiben. Dies kann beinhalten, welche Container ausgeführt werden sollen, Ressourcenlimits, Anzahl der Pod-Replikate, CPU-/Speicherzuweisung, Affinitätsregeln und mehr.

Eigenschaften von Kubernetes

Um seine Ziele zu erreichen, verfügt Kubernetes über die folgenden Eigenschaften:

- Containerisiert — Kubernetes ist ein Tool zur Container-Orchestrierung. Um Kubernetes verwenden zu können, müssen Sie Ihre Anwendungen zunächst containerisiert haben. Je

nach Art der Anwendung kann es sich dabei um eine Reihe von Microservices, als Batch-Jobs oder in anderen Formen handeln. [Anschließend können Ihre Anwendungen einen Kubernetes-Workflow nutzen, der ein riesiges Ökosystem von Tools umfasst, in dem Container als Images in einer Container-Registry gespeichert, in einem Kubernetes-Cluster bereitgestellt und auf einem verfügbaren Knoten ausgeführt werden können.](#) Sie können einzelne Container auf Ihrem lokalen Computer mit Docker oder einer anderen [Container-Runtime](#) erstellen und testen, bevor Sie sie in Ihrem Kubernetes-Cluster bereitstellen.

- **Skalierbar** — Wenn die Nachfrage nach Ihren Anwendungen die Kapazität der laufenden Instanzen dieser Anwendungen übersteigt, ist Kubernetes in der Lage, nach oben zu skalieren. Bei Bedarf kann Kubernetes erkennen, ob Anwendungen mehr CPU oder Speicher benötigen, und darauf reagieren, indem entweder die verfügbare Kapazität automatisch erweitert oder mehr der vorhandenen Kapazität genutzt wird. [Die Skalierung kann auf Pod-Ebene erfolgen, wenn genügend Rechenleistung zur Verfügung steht, um einfach mehr Instanzen der Anwendung auszuführen \(horizontale Pod-Autoskalierung\), oder auf Knotenebene, wenn mehr Knoten eingerichtet werden müssen, um die erhöhte Kapazität zu bewältigen \(Cluster Autoscaler oder Karpenter\).](#) Da keine Kapazität mehr benötigt wird, können diese Dienste nicht benötigte Pods löschen und nicht benötigte Knoten herunterfahren.
- **Verfügbar** — Wenn eine Anwendung oder ein Knoten fehlerhaft oder nicht verfügbar ist, kann Kubernetes laufende Workloads auf einen anderen verfügbaren Knoten verschieben. Sie können das Problem erzwingen, indem Sie einfach eine laufende Instanz eines Workloads oder Knotens löschen, auf dem Ihre Workloads ausgeführt werden. Die Quintessenz dabei ist, dass Workloads an anderen Standorten geladen werden können, wenn sie nicht mehr dort ausgeführt werden können, wo sie sich befinden.
- **Deklarativ** — Kubernetes verwendet aktiven Abgleich, um ständig zu überprüfen, ob der Status, den Sie für Ihren Cluster deklarieren, dem tatsächlichen Status entspricht. Indem Sie [Kubernetes-Objekte](#) auf einen Cluster anwenden, in der Regel mithilfe von Konfigurationsdateien im YAML-Format, können Sie beispielsweise darum bitten, die Workloads zu starten, die Sie auf Ihrem Cluster ausführen möchten. Sie können die Konfigurationen später ändern, um beispielsweise eine neuere Version eines Containers zu verwenden oder mehr Speicher zuzuweisen. Kubernetes wird alles Notwendige tun, um den gewünschten Status herzustellen. Dies kann das Hoch- oder Herunterfahren von Knoten, das Stoppen und Neustarten von Workloads oder das Abrufen aktualisierter Container beinhalten.
- **Zusammensetzbar** — Da eine Anwendung in der Regel aus mehreren Komponenten besteht, möchten Sie in der Lage sein, einen Satz dieser Komponenten (häufig dargestellt durch mehrere Container) gemeinsam zu verwalten. Docker Compose bietet zwar eine Möglichkeit, dies direkt mit Docker zu tun, aber der Befehl Kubernetes [Kompose](#) kann Ihnen dabei helfen, dies mit Kubernetes

zu tun. [Ein Beispiel dafür finden Sie unter Translate einer Docker-Compose-Datei in Kubernetes-Ressourcen.](#)

- **Erweiterbar** — Im Gegensatz zu proprietärer Software ist das Open-Source-Kubernetes-Projekt so konzipiert, dass Sie Kubernetes nach Belieben erweitern können, um Ihren Bedürfnissen gerecht zu werden. APIs und Konfigurationsdateien können direkt geändert werden. Drittanbieter werden ermutigt, ihre eigenen [Controller](#) zu schreiben, um sowohl die Infrastruktur als auch die Kubernetes-Funktionen für Endbenutzer zu erweitern. Mit [Webhooks](#) können Sie Cluster-Regeln einrichten, um Richtlinien durchzusetzen und sich an sich ändernde Bedingungen anzupassen. [Weitere Ideen zur Erweiterung von Kubernetes-Clustern finden Sie unter Erweiterung von Kubernetes.](#)
- **Portierbar** — Viele Unternehmen haben ihren Betrieb auf Kubernetes standardisiert, da sie damit alle ihre Anwendungsanforderungen auf dieselbe Weise verwalten können. Entwickler können dieselben Pipelines verwenden, um containerisierte Anwendungen zu erstellen und zu speichern. Diese Anwendungen können dann auf Kubernetes-Clustern bereitgestellt werden, die vor Ort, in Clouds, auf point-of-sales Terminals in Restaurants oder auf IOT-Geräten laufen, die über die Remote-Standorte des Unternehmens verteilt sind. Aufgrund seines Open-Source-Charakters können Benutzer diese speziellen Kubernetes-Distributionen zusammen mit den zu ihrer Verwaltung benötigten Tools entwickeln.

Verwaltung von Kubernetes

Der Kubernetes-Quellcode ist frei verfügbar, sodass Sie Kubernetes mit Ihren eigenen Geräten selbst installieren und verwalten können. Die Selbstverwaltung von Kubernetes erfordert jedoch fundiertes operatives Fachwissen und erfordert Zeit und Mühe bei der Wartung. Aus diesen Gründen entscheiden sich die meisten Anwender, die Produktionsworkloads bereitstellen, für einen Cloud-Anbieter (wie Amazon EKS) oder einen lokalen Anbieter (wie Amazon EKS Anywhere) mit eigener getesteter Kubernetes-Distribution und Support durch Kubernetes-Experten. Auf diese Weise können Sie einen Großteil der undifferenzierten Schwerarbeit entlasten, die für die Wartung Ihrer Cluster erforderlich sind, darunter:

- **Hardware** — Wenn Sie keine Hardware zur Verfügung haben, um Kubernetes gemäß Ihren Anforderungen auszuführen, kann Ihnen ein Cloud-Anbieter wie AWS Amazon EKS Vorabkosten sparen. Mit Amazon EKS bedeutet dies, dass Sie die besten Cloud-Ressourcen nutzen können, die Ihnen zur Verfügung stehen AWS, darunter Computer-Instances (Amazon Elastic Compute Cloud), Ihre eigene private Umgebung (Amazon VPC), zentrales Identitäts- und Berechtigungsmanagement (IAM) und Speicher (Amazon EBS). AWS verwaltet die Computer,

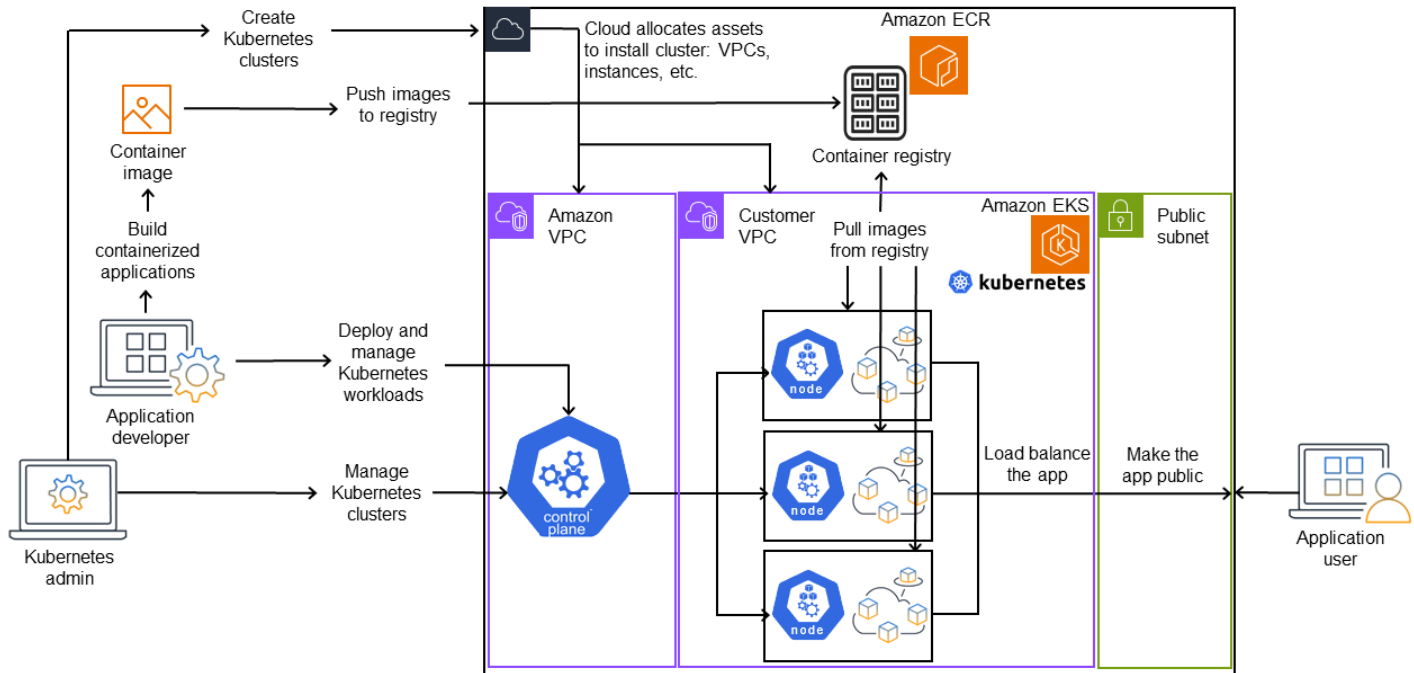
Netzwerke, Rechenzentren und alle anderen physischen Komponenten, die für den Betrieb von Kubernetes erforderlich sind. Ebenso müssen Sie Ihr Rechenzentrum nicht so planen, dass es die maximale Kapazität an den Tagen mit der höchsten Nachfrage bewältigen kann. Bei Amazon EKS Anywhere oder anderen lokalen Kubernetes-Clustern sind Sie für die Verwaltung der Infrastruktur verantwortlich, die in Ihren Kubernetes-Bereitstellungen verwendet wird, aber Sie können sich trotzdem darauf verlassen, dass wir Sie dabei unterstützen, Kubernetes auf dem AWS neuesten Stand zu halten.

- **Verwaltung der Kontrollebene** — Amazon EKS verwaltet die Sicherheit und Verfügbarkeit der AWS gehosteten Kubernetes-Steuerebene, die für die Planung von Containern, die Verwaltung der Verfügbarkeit von Anwendungen und andere wichtige Aufgaben verantwortlich ist, sodass Sie sich auf Ihre Anwendungs-Workloads konzentrieren können. Sollte Ihr Cluster ausfallen, AWS sollten Sie über die Mittel verfügen, Ihren Cluster wieder in den Betriebszustand zu versetzen. Für Amazon EKS Anywhere würden Sie die Steuerungsebene selbst verwalten.
- **Getestete Upgrades** — Wenn Sie Ihre Cluster aktualisieren, können Sie sich darauf verlassen, dass Amazon EKS oder Amazon EKS Anywhere getestete Versionen ihrer Kubernetes-Distributionen bereitstellen.
- **Add-Ons** — Es gibt Hunderte von Projekten, die für die Erweiterung und Nutzung von Kubernetes konzipiert wurden und die Sie der Infrastruktur Ihres Clusters hinzufügen oder zur Unterstützung der Ausführung Ihrer Workloads verwenden können. Anstatt diese Add-Ons selbst zu erstellen und zu verwalten, können AWS Sie [the section called “Amazon-EKS-Add-ons”](#) diese mit Ihren Clustern verwenden. Amazon EKS Anywhere bietet [kuratierte Pakete](#), die Builds vieler beliebter Open-Source-Projekte enthalten. Sie müssen die Software also nicht selbst erstellen oder wichtige Sicherheitspatches, Bugfixes oder Upgrades verwalten. Wenn die Standardeinstellungen Ihren Anforderungen entsprechen, ist es ebenfalls typisch, dass nur eine sehr geringe Konfiguration dieser Add-Ons erforderlich ist. Einzelheiten [the section called “Erweitern Sie Cluster”](#) zur Erweiterung Ihres Clusters mit Add-Ons finden Sie unter.

Kubernetes in Aktion

Das folgende Diagramm zeigt die wichtigsten Aktivitäten, die Sie als Kubernetes-Administrator oder Anwendungsentwickler durchführen würden, um einen Kubernetes-Cluster zu erstellen und zu verwenden. Dabei wird veranschaulicht, wie Kubernetes-Komponenten miteinander interagieren, wobei die AWS Cloud als Beispiel für den zugrunde liegenden Cloud-Anbieter verwendet wird.

A Kubernetes cluster in action



Ein Kubernetes-Administrator erstellt den Kubernetes-Cluster mithilfe eines Tools, das für den Anbietertyp spezifisch ist, auf dem der Cluster aufgebaut werden soll. In diesem Beispiel wird die AWS Cloud als Anbieter verwendet, der den verwalteten Kubernetes-Dienst namens Amazon EKS anbietet. Der verwaltete Service weist automatisch die Ressourcen zu, die für die Erstellung des Clusters benötigt werden, einschließlich der Erstellung von zwei neuen Virtual Private Clouds (Amazon VPCs) für den Cluster, der Einrichtung von Netzwerken und der direkten Zuordnung von Kubernetes-Berechtigungen zu den neuen VPCs für Cloud Asset Management. Der verwaltete Service erkennt auch, dass die Dienste der Kontrollebene über Ausführungsplätze verfügen, und weist null oder mehr EC2 Amazon-Instances als Kubernetes-Knoten für die Ausführung von Workloads zu. AWS verwaltet eine Amazon-VPC selbst für die Kontrollebene, während die andere Amazon-VPC die Kundenknoten enthält, die Workloads ausführen.

Viele der zukünftigen Aufgaben des Kubernetes-Administrators werden mithilfe von Kubernetes-Tools wie z. `kubectl`. Dieses Tool sendet Anfragen für Dienste direkt an die Steuerungsebene des Clusters. Die Art und Weise, wie Abfragen und Änderungen am Cluster vorgenommen werden, ist dann der Art und Weise, wie Sie sie in jedem Kubernetes-Cluster vornehmen würden, sehr ähnlich.

Ein Anwendungsentwickler, der Workloads für diesen Cluster bereitstellen möchte, kann mehrere Aufgaben ausführen. Der Entwickler muss die Anwendung in ein oder mehrere Container-Images

integrieren und diese Images dann in eine Container-Registry übertragen, auf die der Kubernetes-Cluster zugreifen kann. AWS bietet zu diesem Zweck das Amazon Elastic Container Registry (Amazon ECR) an.

Um die Anwendung auszuführen, kann der Entwickler Konfigurationsdateien im YAML-Format erstellen, die dem Cluster mitteilen, wie die Anwendung ausgeführt werden soll, einschließlich der Container, die aus der Registrierung abgerufen werden sollen und wie diese Container in Pods verpackt werden sollen. Die Steuerungsebene (Scheduler) plant die Container für einen oder mehrere Knoten, und die Container-Laufzeit auf jedem Knoten ruft die benötigten Container ab und führt sie aus. Der Entwickler kann auch einen Application Load Balancer einrichten, der den Datenverkehr auf die verfügbaren Container verteilt, die auf jedem Knoten ausgeführt werden, und die Anwendung so verfügbar macht, dass sie in einem öffentlichen Netzwerk für die Außenwelt verfügbar ist. Wenn das alles erledigt ist, kann sich jemand, der die Anwendung verwenden möchte, mit dem Anwendungsendpunkt verbinden, um darauf zuzugreifen.

In den folgenden Abschnitten werden die einzelnen Funktionen aus der Sicht von Kubernetes-Clustern und -Workloads detailliert beschrieben.

Cluster

Wenn Ihre Aufgabe darin besteht, Kubernetes-Cluster zu starten und zu verwalten, sollten Sie wissen, wie Kubernetes-Cluster erstellt, erweitert, verwaltet und gelöscht werden. Sie sollten auch wissen, aus welchen Komponenten ein Cluster besteht und was Sie tun müssen, um diese Komponenten zu verwalten.

Tools für die Verwaltung von Clustern bewältigen die Überschneidung zwischen den Kubernetes-Diensten und dem zugrunde liegenden Hardwareanbieter. Aus diesem Grund erfolgt die Automatisierung dieser Aufgaben in der Regel durch den Kubernetes-Anbieter (wie Amazon EKS oder Amazon EKS Anywhere) mithilfe von anbieterspezifischen Tools. Um beispielsweise einen Amazon EKS-Cluster zu starten, können Sie ihn verwenden `eksctl create cluster`, während Sie Amazon EKS Anywhere verwenden können `eksctl anywhere create cluster`. Beachten Sie, dass diese Befehle zwar einen Kubernetes-Cluster erstellen, aber spezifisch für den Anbieter sind und nicht Teil des Kubernetes-Projekts selbst sind.

Tools zur Clustererstellung und -verwaltung

Das Kubernetes-Projekt bietet Tools zum manuellen Erstellen eines Kubernetes-Clusters. [Wenn Sie also Kubernetes auf einem einzelnen Computer installieren oder die Steuerungsebene auf](#)

einem Computer ausführen und Knoten manuell hinzufügen möchten, können Sie CLI-Tools wie [kind](#), [minikube](#) oder [kubeadm](#) verwenden, die unter [Kubernetes Install Tools](#) aufgeführt sind.

Um den gesamten Lebenszyklus der Clustererstellung und -verwaltung zu vereinfachen und zu automatisieren, ist es viel einfacher, Tools zu verwenden, die von einem etablierten Kubernetes-Anbieter wie Amazon EKS oder Amazon EKS Anywhere unterstützt werden.

In AWS Cloud können Sie [Amazon EKS-Cluster](#) mithilfe von CLI-Tools wie [eksctl](#) oder deklarativen Tools wie Terraform erstellen (siehe [Amazon EKS Blueprints for Terraform](#)). Sie können auch einen Cluster aus dem erstellen. AWS Management Console Eine Liste der Vorteile von [Amazon EKS](#) [finden Sie unter Amazon EKS-Funktionen](#). Zu den Aufgaben von Kubernetes, die Amazon EKS für Sie übernimmt, gehören:

- **Verwaltete Kontrollebene** — AWS stellt sicher, dass der Amazon EKS-Cluster verfügbar und skalierbar ist, da er die Kontrollebene für Sie verwaltet und sie in allen AWS Availability Zones verfügbar macht.
- **Knotenverwaltung** — Anstatt Knoten manuell hinzuzufügen, können Sie Amazon EKS mithilfe von Managed Node Groups (siehe [the section called “Verwaltete Knotengruppen”](#)) oder [Karpenter](#) bei Bedarf automatisch Knoten erstellen lassen. [Verwaltete Knotengruppen sind in Kubernetes Cluster Autoscaling integriert](#). Mithilfe von Knotenmanagement-Tools können Sie Kosteneinsparungen wie [Spot-Instances](#) und Knotenkonsolidierung und Verfügbarkeit nutzen. Mithilfe von [Planungsfunktionen](#) können Sie festlegen, wie Workloads bereitgestellt und Knoten ausgewählt werden.
- **Cluster-Netzwerke** — Richten Sie mithilfe von `eksctl` von CloudFormation Vorlagen die Vernetzung zwischen Komponenten der Steuerungsebene und der Datenebene (Knoten) im Kubernetes-Cluster ein. Außerdem werden Endpunkte eingerichtet, über die interne und externe Kommunikation stattfinden kann. Einzelheiten finden Sie unter [Entmystifying Cluster Networking for Amazon EKS Worker Nodes](#). Die Kommunikation zwischen Pods in Amazon EKS erfolgt über Amazon EKS Pod Identities (siehe [the section called “Pod-Identität”](#)), wodurch Pods AWS Cloud-Methoden zur Verwaltung von Anmeldeinformationen und Berechtigungen nutzen können.
- **Add-Ons** — Amazon EKS erspart Ihnen das Erstellen und Hinzufügen von Softwarekomponenten, die üblicherweise zur Unterstützung von Kubernetes-Clustern verwendet werden. Wenn Sie beispielsweise einen Amazon EKS-Cluster aus dem erstellen AWS Management Console, werden automatisch die Amazon EKS kube-proxy ([the section called “kube-proxy”](#)), das Amazon VPC CNI-Plug-In für Kubernetes ([the section called “Amazon VPC CNI”](#)) und CoreDNS ([the section called “CoreDNS”](#)) hinzugefügt. [the section called “Amazon-EKS-Add-ons”](#) Weitere Informationen zu diesen Add-Ons, einschließlich einer Liste der verfügbaren, finden Sie unter.

Um Ihre Cluster auf Ihren eigenen lokalen Computern und Netzwerken auszuführen, bietet Amazon [Amazon EKS Anywhere an](#). Anstatt dass die AWS Cloud der Anbieter ist, haben Sie die Wahl, Amazon EKS Anywhere auf [VMWare vSphere](#) -, [Bare Metal](#)- ([Tinkerbell-Anbieter](#)), [Snow](#) - oder [Nutanix-Plattformen CloudStack](#) mit Ihren eigenen Geräten auszuführen.

Amazon EKS Anywhere basiert auf derselben [Amazon EKS Distro-Software](#), die auch von Amazon EKS verwendet wird. [Amazon EKS Anywhere stützt sich jedoch auf verschiedene Implementierungen der Kubernetes Cluster API \(CAPI\) -Schnittstelle, um den gesamten Lebenszyklus der Maschinen in einem Amazon EKS Anywhere Anywhere-Cluster zu verwalten \(wie CAPV für vSphere und CAPC für\)](#). CloudStack Da der gesamte Cluster auf Ihren Geräten läuft, übernehmen Sie zusätzlich die Verantwortung für die Verwaltung der Steuerungsebene und die Sicherung ihrer Daten (siehe weiter unten in diesem Dokument). `etcd`

Cluster-Komponenten

Die Kubernetes-Clusterkomponenten sind in zwei Hauptbereiche unterteilt: Kontrollebene und Worker-Knoten. [Komponenten der Steuerungsebene](#) verwalten den Cluster und bieten Zugriff auf seinen APIs. Worker-Knoten (manchmal auch einfach als Knoten bezeichnet) stellen die Orte dar, an denen die eigentlichen Workloads ausgeführt werden. [Knotenkomponenten](#) bestehen aus Diensten, die auf jedem Knoten ausgeführt werden, um mit der Steuerungsebene zu kommunizieren und Container auszuführen. Die Gruppe von Worker-Knoten für Ihren Cluster wird als Datenebene bezeichnet.

Steuerebene

Die Steuerungsebene besteht aus einer Reihe von Diensten, die den Cluster verwalten. Diese Dienste können alle auf einem einzigen Computer ausgeführt werden oder auf mehrere Computer verteilt sein. Intern werden diese als Control Plane Instances (CPIs) bezeichnet. Wie CPIs sie ausgeführt werden, hängt von der Größe des Clusters und den Anforderungen an die Hochverfügbarkeit ab. Wenn die Nachfrage im Cluster steigt, kann ein Service auf der Steuerungsebene skaliert werden, um mehr Instanzen dieses Dienstes bereitzustellen, wobei die Anforderungen zwischen den Instanzen ausbalanciert werden.

Zu den Aufgaben, die Komponenten der Kubernetes-Steuerebene ausführen, gehören:

- Kommunikation mit Cluster-Komponenten (API-Server) — Der API-Server ([kube-apiserver](#)) [macht die Kubernetes-API](#) verfügbar, sodass Anfragen an den Cluster sowohl innerhalb als auch außerhalb des Clusters gestellt werden können. Mit anderen Worten, Anfragen zum Hinzufügen oder Ändern von Objekten eines Clusters (Pods, Dienste, Knoten usw.) können von externen

Befehlen stammen, z. B. von Anfragen zum Ausführen eines Pods. `kubectl` Ebenso können Anfragen vom API-Server an Komponenten innerhalb des Clusters gestellt werden, z. B. eine Abfrage des Status eines Pods an den `kubelet` Dienst.

- Daten über den Cluster speichern (**etcd**Schlüsselwertspeicher) — Der `etcd` Dienst hat die entscheidende Rolle, den aktuellen Status des Clusters zu verfolgen. Wenn auf den `etcd` Dienst nicht mehr zugegriffen werden könnte, könnten Sie den Status des Clusters nicht aktualisieren oder abfragen, obwohl die Workloads noch eine Weile laufen würden. Aus diesem Grund werden in kritischen Clustern in der Regel mehrere Instanzen des `etcd` Dienstes mit Lastenausgleich gleichzeitig ausgeführt und es werden regelmäßig Backups des `etcd` Key-Value-Speichers erstellt, falls Daten verloren gehen oder beschädigt werden. Denken Sie daran, dass in Amazon EKS dies alles standardmäßig automatisch für Sie erledigt wird. Amazon EKS Anywhere bietet Anweisungen für die [Sicherung und Wiederherstellung von etcd](#). Sehen Sie sich das [etcd-Datenmodell](#) an, um zu erfahren, wie Daten `etcd` verwaltet werden.
- Pods für Knoten planen (Scheduler) — [Anfragen zum Starten oder Stoppen eines Pods in Kubernetes werden an den Kubernetes Scheduler \(kube-scheduler\) weitergeleitet](#). Da ein Cluster mehrere Knoten haben kann, die den Pod ausführen können, ist es Sache des Schedulers, auszuwählen, auf welchem Knoten (oder auf welchen Knoten, im Fall von Replikaten) der Pod ausgeführt werden soll. Wenn nicht genügend Kapazität verfügbar ist, um den angeforderten Pod auf einem vorhandenen Knoten auszuführen, schlägt die Anfrage fehl, sofern Sie keine anderen Vorkehrungen getroffen haben. Diese Bestimmungen könnten die Aktivierung von Diensten wie Managed Node Groups ([the section called “Verwaltete Knotengruppen”](#)) oder [Karpenter](#) beinhalten, die automatisch neue Knoten starten können, um die Workloads zu bewältigen.
- Komponenten im gewünschten Zustand belassen (Controller Manager) — Der Kubernetes Controller Manager wird als Daemon-Prozess ([kube-controller-manager](#)) ausgeführt, um den Status des Clusters zu beobachten und Änderungen am Cluster vorzunehmen, um die erwarteten Zustände wiederherzustellen. Insbesondere gibt es mehrere Controller, die verschiedene Kubernetes-Objekte überwachen, darunter `statefulset-controller`,, und andere. `endpoint-controller` `cronjob-controller` `node-controller`
- Cloud-Ressourcen verwalten (Cloud Controller Manager) — Interaktionen zwischen Kubernetes und dem Cloud-Anbieter, der Anfragen für die zugrunde liegenden Rechenzentrumsressourcen ausführt, werden vom [Cloud Controller](#) Manager () abgewickelt. [cloud-controller-manager](#) Controller, die vom Cloud Controller Manager verwaltet werden, können einen Route-Controller (zum Einrichten von Cloud-Netzwerkrouuten), einen Service-Controller (für die Nutzung von Cloud-Load-Balancing-Diensten) und einen Node-Lifecycle-Controller (um die Knoten während ihres gesamten Lebenszyklus mit Kubernetes synchron zu halten) umfassen.

Worker-Knoten (Datenebene)

Bei einem Kubernetes-Cluster mit einem Knoten laufen die Workloads auf derselben Maschine wie die Steuerungsebene. Eine Standardkonfiguration besteht jedoch darin, über ein oder mehrere separate Computersysteme ([Knoten](#)) zu verfügen, die für die Ausführung von Kubernetes-Workloads vorgesehen sind.

Wenn Sie zum ersten Mal einen Kubernetes-Cluster erstellen, können Sie mit einigen Tools zur Clustererstellung eine bestimmte Anzahl von Knoten konfigurieren, die dem Cluster hinzugefügt werden sollen (entweder indem Sie vorhandene Computersysteme identifizieren oder den Anbieter neue erstellen lassen). Bevor Workloads zu diesen Systemen hinzugefügt werden, werden jedem Knoten Dienste hinzugefügt, um die folgenden Funktionen zu implementieren:

- Jeden Knoten verwalten (**kubelet**) — Der API-Server kommuniziert mit dem [Kubelet-Dienst](#), der auf jedem Knoten ausgeführt wird, um sicherzustellen, dass der Knoten ordnungsgemäß registriert ist und die vom Scheduler angeforderten Pods ausgeführt werden. Das Kubelet kann die Pod-Manifeste lesen und Speichervolumes oder andere Funktionen einrichten, die von den Pods auf dem lokalen System benötigt werden. Es kann auch den Zustand der lokal laufenden Container überprüfen.
- Container auf einem Knoten ausführen (Container-Laufzeit) — Die [Container-Runtime](#) auf jedem Knoten verwaltet die Container, die für jeden dem Knoten zugewiesenen Pod angefordert werden. Das bedeutet, dass sie Container-Images aus der entsprechenden Registry abrufen, den Container ausführen, stoppen und auf Anfragen zum Container antworten kann. Die Standard-Container-Laufzeit ist [containerd](#). Ab Kubernetes 1.24 wurde die spezielle Integration von Docker (dockershim), die als Container-Laufzeit verwendet werden konnte, aus Kubernetes entfernt. Sie können Docker zwar weiterhin verwenden, um Container auf Ihrem lokalen System zu testen und auszuführen, aber um Docker mit Kubernetes zu verwenden, müssten Sie jetzt Docker Engine auf jedem Knoten [installieren](#), um sie mit Kubernetes verwenden zu können.
- Netzwerke zwischen Containern verwalten (**kube-proxy**) — Um die Kommunikation zwischen Pods zu unterstützen, verwendet Kubernetes eine als [Service](#) bezeichnete Funktion, um Pod-Netzwerke einzurichten, die IP-Adressen und Ports verfolgen, die diesen Pods zugeordnet sind. Der [Kube-Proxy-Service](#) wird auf jedem Knoten ausgeführt, um die Kommunikation zwischen Pods zu ermöglichen.

Erweitern Sie Cluster

Es gibt einige Dienste, die Sie zu Kubernetes hinzufügen können, um den Cluster zu unterstützen, die jedoch nicht in der Steuerungsebene ausgeführt werden. Diese Dienste werden oft direkt auf Knoten im Kube-System-Namespace oder in einem eigenen Namespace ausgeführt (wie dies häufig bei Drittanbietern der Fall ist). Ein gängiges Beispiel ist der CoreDNS-Dienst, der DNS-Dienste für den Cluster bereitstellt. Informationen darüber, wie Sie feststellen [können, welche Clusterdienste im Kube-System auf Ihrem Cluster ausgeführt werden, finden Sie unter Entdecken integrierter](#) Dienste.

Es gibt verschiedene Arten von Add-Ons, die Sie in Betracht ziehen können, Ihren Clustern hinzuzufügen. Um die Funktionsfähigkeit Ihrer Cluster zu gewährleisten, können Sie Observability-Funktionen (siehe [Überwachen Sie Cluster](#)) hinzufügen, mit denen Sie beispielsweise Logging, Auditing und Metriken durchführen können. Mit diesen Informationen können Sie auftretende Probleme beheben, häufig über dieselben Observability-Schnittstellen. [Beispiele für diese Arten von Diensten sind Amazon CloudWatch \(siehe the section called “Amazon CloudWatch”\) GuardDuty, AWS Distro for OpenTelemetry, das Amazon VPC CNI-Plugin für Kubernetes \(siehe the section called “Amazon VPC CNI”\) und Grafana Kubernetes Monitoring.](#) Für Speicher (siehe [App-Datenspeicher](#)) gehören zu den Add-Ons für Amazon EKS der Amazon Elastic Block Store CSI Driver (siehe [the section called “Amazon EBS”](#)), der Amazon Elastic File System CSI Driver (siehe [the section called “Amazon EFS”](#)) und mehrere Speicher-Add-Ons von Drittanbietern (z. B. der Amazon FSx for NetApp ONTAP CSI-Treiber [the section called “Amazon FSx für NetApp ONTAP”](#)).

Eine vollständigere Liste der verfügbaren Amazon EKS-Add-Ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

Workloads

Kubernetes definiert einen [Workload](#) als „eine Anwendung, die auf Kubernetes läuft“. Diese Anwendung kann aus einer Reihe von Microservices bestehen, die als [Container](#) in [Pods](#) ausgeführt werden, oder sie kann als Batch-Job oder andere Arten von Anwendungen ausgeführt werden. Die Aufgabe von Kubernetes besteht darin, sicherzustellen, dass die Anfragen, die Sie für die Einrichtung oder Bereitstellung dieser Objekte stellen, ausgeführt werden. Als jemand, der Anwendungen bereitstellt, sollten Sie lernen, wie Container gebaut werden, wie Pods definiert werden und welche Methoden Sie für deren Bereitstellung verwenden können.

Container

[Das grundlegendste Element eines Anwendungs-Workloads, den Sie in Kubernetes bereitstellen und verwalten, ist ein Pod.](#) Ein Pod stellt eine Möglichkeit dar, die Komponenten einer Anwendung zu

speichern und Spezifikationen zu definieren, die die Attribute des Pods beschreiben. Vergleichen Sie das mit etwas wie einem RPM- oder Deb-Paket, das Software für ein Linux-System zusammenpackt, aber selbst nicht als Einheit läuft.

Da der Pod die kleinste bereitstellbare Einheit ist, enthält er in der Regel einen einzelnen Container. In Fällen, in denen die Container eng miteinander verbunden sind, können sich jedoch mehrere Container in einem Pod befinden. Beispielsweise kann ein Webserver-Container in einem Pod mit einem Container vom Typ [Sidecar](#) verpackt sein, der Protokollierung, Überwachung oder andere Dienste bereitstellen kann, die eng mit dem Webserver-Container verknüpft sind. In diesem Fall stellt die Tatsache, dass sie sich im selben Pod befinden, sicher, dass für jede laufende Instanz des Pods beide Container immer auf demselben Knoten ausgeführt werden. Ebenso teilen sich alle Container in einem Pod dieselbe Umgebung, wobei die Container in einem Pod so ausgeführt werden, als ob sie sich auf demselben isolierten Host befinden würden. Dies hat zur Folge, dass sich die Container eine einzige IP-Adresse teilen, die den Zugriff auf den Pod ermöglicht, und dass die Container miteinander kommunizieren können, als würden sie auf ihrem eigenen lokalen Host laufen.

Die Pod-Spezifikationen ([PodSpec](#)) definieren den gewünschten Status des Pods. Sie können einen einzelnen Pod oder mehrere Pods bereitstellen, indem Sie Workload-Ressourcen zur Verwaltung von [Pod-Vorlagen](#) verwenden. Zu den Workload-Ressourcen gehören [Bereitstellungen](#) (zur Verwaltung mehrerer Pod-Repliken), [StatefulSets](#) (zur Bereitstellung von Pods, die einzigartig sein müssen, z. B. Datenbank-Pods) und [DaemonSets](#) (bei denen ein Pod kontinuierlich auf jedem Knoten ausgeführt werden muss). Dazu später mehr.

Während ein Pod die kleinste Einheit ist, die Sie einsetzen, ist ein Container die kleinste Einheit, die Sie erstellen und verwalten.

Container bauen

Der Pod ist eigentlich nur eine Struktur rund um einen oder mehrere Container, wobei jeder Container selbst das Dateisystem, die ausführbaren Dateien, Konfigurationsdateien, Bibliotheken und andere Komponenten enthält, um die Anwendung tatsächlich auszuführen. Da ein Unternehmen namens Docker Inc. Container zuerst populär gemacht hat, bezeichnen manche Leute Container als Docker-Container. Seitdem hat die [Open Container Initiative](#) jedoch Container-Laufzeiten, Images und Distributionsmethoden für die Branche definiert. Hinzu kommt die Tatsache, dass Container auf der Grundlage vieler vorhandener Linux-Funktionen erstellt wurden. Andere bezeichnen Container oft als OCI-Container, Linux-Container oder einfach Container.

Wenn Sie einen Container erstellen, beginnen Sie normalerweise mit einem Dockerfile (wörtlich so genannt). In diesem Dockerfile identifizieren Sie:

- Ein Basis-Image — Ein Basis-Container-Image ist ein Container, der in der Regel entweder aus einer Minimalversion des Dateisystems eines Betriebssystems (wie [Red Hat Enterprise Linux](#) oder [Ubuntu](#)) oder aus einem Minimalsystem erstellt wird, das erweitert wurde, um Software für die Ausführung bestimmter Arten von Anwendungen (wie [nodejs](#) - oder [Python-Apps](#)) bereitzustellen.
- Anwendungssoftware — Sie können Ihre Anwendungssoftware auf die gleiche Weise zu Ihrem Container hinzufügen, wie Sie sie einem Linux-System hinzufügen würden. In Ihrem Dockerfile können Sie beispielsweise eine Java-Anwendung ausführen npm und yarn installieren oder yum dnf RPM-Pakete installieren. Mit anderen Worten, mit einem RUN-Befehl in einem Dockerfile können Sie jeden Befehl ausführen, der im Dateisystem Ihres Basis-Images verfügbar ist, um Software zu installieren oder Software innerhalb des resultierenden Container-Images zu konfigurieren.
- Anweisungen — Die [Dockerfile-Referenz](#) beschreibt die Anweisungen, die Sie einer Dockerfile hinzufügen können, wenn Sie sie konfigurieren. Dazu gehören Anweisungen, die verwendet werden, um den Inhalt des Containers selbst (ADD oder COPY Dateien aus dem lokalen System) zu erstellen, Befehle zu identifizieren, die ausgeführt werden sollen, wenn der Container ausgeführt wird (CMD oder ENTRYPOINT), und den Container mit dem System zu verbinden, auf dem er ausgeführt werden soll (indem der Container, unter dem er ausgeführt werden soll, ein Lokal VOLUME zum Mounten oder die Ports identifiziert werden). EXPOSE

Während der `docker` Befehl und der Dienst traditionell zum Erstellen von Containern (`docker build`) verwendet wurden, gehören [podman](#) und [nerdctl](#) zu anderen Tools, die zum Erstellen von Container-Images verfügbar sind. Weitere Informationen zum [Erstellen von Containern finden Sie unter Bessere Container-Images](#) erstellen oder [Überblick über Docker Build](#).

Speichern von Containern

Sobald Sie Ihr Container-Image erstellt haben, können Sie es in einer [Container-Distributionsregistrierung](#) auf Ihrer Workstation oder in einer öffentlichen Container-Registry speichern. Wenn Sie eine private Container-Registry auf Ihrer Workstation betreiben, können Sie Container-Images lokal speichern, sodass sie Ihnen jederzeit zur Verfügung stehen.

Um Container-Images öffentlicher zu speichern, können Sie sie in eine öffentliche Container-Registry übertragen. Öffentliche Container-Register bieten einen zentralen Ort für die Speicherung und Verteilung von Container-Images. Beispiele für öffentliche Container-Registries sind die [Amazon Elastic Container Registry](#), [Red Hat Quay](#) Registry und [Docker Hub](#) Registry.

Wenn containerisierte Workloads auf Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden, empfehlen wir, Kopien der offiziellen Docker-Images abzurufen, die in Amazon Elastic

Container Registry gespeichert sind. Amazon ECR speichert diese Bilder seit 2021. Sie können in der [Amazon ECR Public Gallery](#) nach beliebigen Container-Images suchen, und speziell nach den Docker Hub-Images können Sie in der [Amazon ECR](#) Docker Gallery suchen.

Container ausführen

Da Container in einem Standardformat erstellt werden, kann ein Container auf jedem Computer ausgeführt werden, auf dem eine Container-Laufzeit ausgeführt werden kann (z. B. Docker) und dessen Inhalt der Architektur des lokalen Computers entspricht (z. B. x86_64 oder aarch64). Um einen Container zu testen oder ihn einfach auf Ihrem lokalen Desktop auszuführen, können Sie `podman run` Befehle `docker run` oder verwenden, um einen Container auf dem Localhost zu starten. Bei Kubernetes ist jedoch für jeden Worker-Knoten eine Container-Runtime bereitgestellt, und es liegt an Kubernetes, zu verlangen, dass ein Knoten einen Container ausführt.

Sobald einem Container die Ausführung auf einem Knoten zugewiesen wurde, prüft der Knoten, ob die angeforderte Version des Container-Images bereits auf dem Knoten vorhanden ist. Ist dies nicht der Fall, weist Kubernetes die Container-Laufzeit an, diesen Container aus der entsprechenden Container-Registry abzurufen und diesen Container dann lokal auszuführen. Denken Sie daran, dass sich ein Container-Image auf das Softwarepaket bezieht, das zwischen Ihrem Laptop, der Container-Registry und den Kubernetes-Knoten verschoben wird. Ein Container bezieht sich auf eine laufende Instanz dieses Images.

Pods

Sobald Ihre Container bereit sind, umfasst die Arbeit mit Pods das Konfigurieren, Bereitstellen und Zugänglichmachen der Pods.

Konfiguration von Pods

Wenn Sie einen Pod definieren, weisen Sie ihm eine Reihe von Attributen zu. Diese Attribute müssen mindestens den Pod-Namen und das Container-Image enthalten, damit sie ausgeführt werden können. Es gibt jedoch noch viele andere Dinge, die Sie mit Ihren Pod-Definitionen konfigurieren möchten (Einzelheiten darüber, was in einen Pod aufgenommen werden kann, finden Sie auf der [PodSpec](#)Seite). Dazu zählen:

- Speicher — Wenn ein laufender Container gestoppt und gelöscht wird, verschwindet der Datenspeicher in diesem Container, sofern Sie keinen permanenten Speicher einrichten. [Kubernetes unterstützt viele verschiedene Speichertypen und abstrahiert sie unter dem Dach von Volumes](#). Zu den Speichertypen gehören [CephFS](#), [NFS](#), [iSCSI](#) und andere. Sie können sogar ein [lokales Blockgerät vom lokalen Computer](#) aus verwenden. Wenn einer dieser Speichertypen

in Ihrem Cluster verfügbar ist, können Sie das Speichervolume an einem ausgewählten Bereitstellungspunkt im Dateisystem Ihres Containers mounten. Ein [persistentes Volume](#) ist ein Volume, das auch nach dem Löschen des Pods weiterhin existiert, während ein [flüchtiges Volume](#) gelöscht wird, wenn der Pod gelöscht wird. Wenn Ihr Clusteradministrator verschiedene [Speicherklassen](#) für Ihren Cluster erstellt hat, haben Sie möglicherweise die Möglichkeit, die Attribute des von Ihnen verwendeten Speichers auszuwählen, z. B. ob das Volume gelöscht oder nach der Verwendung zurückgewonnen wird, ob es erweitert wird, wenn mehr Speicherplatz benötigt wird, und sogar, ob es bestimmte Leistungsanforderungen erfüllt.

- **Secrets** — Indem Sie [Secrets](#) in Pod-Spezifikationen für Container verfügbar machen, können Sie die Berechtigungen bereitstellen, die diese Container für den Zugriff auf Dateisysteme, Datenbanken oder andere geschützte Ressourcen benötigen. Schlüssel, Passwörter und Token gehören zu den Elementen, die als Geheimnisse gespeichert werden können. Durch die Verwendung von Geheimnissen müssen Sie diese Informationen nicht in Container-Images speichern, sondern müssen die Geheimnisse nur laufenden Containern zur Verfügung stellen. Ähnlich wie Secrets sind [ConfigMaps](#). A enthält in der ConfigMap Regel weniger wichtige Informationen, wie z. B. Schlüssel-Wert-Paare für die Konfiguration eines Dienstes.
- **Container-Ressourcen** — Objekte für die weitere Konfiguration von Containern können die Form einer Ressourcenkonfiguration annehmen. Für jeden Container können Sie die Menge an Speicher und CPU anfordern, die er verwenden kann, sowie Beschränkungen für die Gesamtmenge dieser Ressourcen festlegen, die der Container verwenden kann. Beispiele finden Sie unter [Ressourcenverwaltung für Pods und Container](#).
- **Unterbrechungen** — Pods können unfreiwillig (ein Knoten fällt aus) oder freiwillig (ein Upgrade ist gewünscht) unterbrochen werden. Durch die Konfiguration eines [Budgets für Pod-Unterbrechungen](#) können Sie kontrollieren, wie verfügbar Ihre Anwendung bei Störungen bleibt. Beispiele finden [Sie unter Festlegung eines Unterbrechungsbudgets](#) für Ihre Anwendung.
- **Namespaces** — Kubernetes bietet verschiedene Möglichkeiten, Kubernetes-Komponenten und -Workloads voneinander zu isolieren. Das Ausführen aller Pods für eine bestimmte Anwendung im selben [Namespace](#) ist eine gängige Methode, um diese Pods gemeinsam zu sichern und zu verwalten. Sie können Ihre eigenen Namespaces zur Verwendung erstellen oder sich dafür entscheiden, keinen Namespace anzugeben (was dazu führt, dass Kubernetes den Namespace verwendet). default [Die Komponenten der Kubernetes-Steuerungsebene werden normalerweise im Kube-System-Namespace ausgeführt](#).

Die gerade beschriebene Konfiguration wird normalerweise in einer YAML-Datei zusammengefasst, die auf den Kubernetes-Cluster angewendet wird. Für persönliche Kubernetes-Cluster können Sie

diese YAML-Dateien einfach auf Ihrem lokalen System speichern. Bei kritischeren Clustern und Workloads [GitOps](#) ist dies jedoch eine beliebte Methode, um Speicher und Updates sowohl für Workloads als auch für Kubernetes-Infrastrukturressourcen zu automatisieren.

Die Objekte, die zum Sammeln und Bereitstellen von Pod-Informationen verwendet werden, werden durch eine der folgenden Bereitstellungsmethoden definiert.

Bereitstellen von Pods

Die Methode, die Sie für die Bereitstellung von Pods wählen würden, hängt von der Art der Anwendung ab, die Sie mit diesen Pods ausführen möchten. Hier sind einige Ihrer Optionen:

- **Zustandslose Anwendungen** — Eine statuslose Anwendung speichert die Sitzungsdaten eines Clients nicht, sodass in einer anderen Sitzung nicht auf das zurückgegriffen werden muss, was mit einer vorherigen Sitzung passiert ist. Dies macht es einfacher, Pods einfach durch neue zu ersetzen, wenn sie fehlerhaft werden, oder sie zu verschieben, ohne den Status zu speichern. Wenn Sie eine statuslose Anwendung (z. B. einen Webserver) ausführen, können Sie [Pods](#) und mithilfe eines [Deployments](#) bereitstellen. [ReplicaSets](#) A ReplicaSet definiert, wie viele Instanzen eines Pods gleichzeitig ausgeführt werden sollen. Obwohl Sie einen ReplicaSet direkt ausführen können, ist es üblich, Replikate direkt in einem Deployment auszuführen, um zu definieren, wie viele Replikate eines Pods gleichzeitig ausgeführt werden sollen.
- **Stateful-Anwendungen** — Bei einer statusbehafteten Anwendung sind die Identität des Pods und die Reihenfolge, in der Pods gestartet werden, wichtig. Diese Anwendungen benötigen dauerhaften Speicher, der stabil ist und konsistent bereitgestellt und skaliert werden muss. Um eine statusbehaftete Anwendung in Kubernetes bereitzustellen, können Sie verwenden. [StatefulSets](#) Ein Beispiel für eine Anwendung, die normalerweise als ausgeführt wird, StatefulSet ist eine Datenbank. In einer StatefulSet könnten Sie Replikate, den Pod und seine Container, zu mountende Speichervolumes und Speicherorte im Container, an denen Daten gespeichert werden, definieren. Ein Beispiel für [eine Datenbank, die als bereitgestellt wird, finden Sie unter Ausführen einer replizierten Stateful-Anwendung](#). ReplicaSet
- **Anwendungen pro Knoten** — Manchmal möchten Sie eine Anwendung auf jedem Knoten in Ihrem Kubernetes-Cluster ausführen. In Ihrem Rechenzentrum kann es beispielsweise erforderlich sein, dass auf jedem Computer eine Überwachungsanwendung oder ein bestimmter Fernzugriffsdienst ausgeführt wird. Für Kubernetes können Sie a verwenden, [DaemonSet](#)um sicherzustellen, dass die ausgewählte Anwendung auf jedem Knoten in Ihrem Cluster ausgeführt wird.
- **Anwendungen werden bis zum Abschluss ausgeführt** — Es gibt einige Anwendungen, die Sie ausführen möchten, um eine bestimmte Aufgabe abzuschließen. Dazu könnte eine Software gehören, die monatliche Statusberichte erstellt oder alte Daten bereinigt. Ein [Job-Objekt](#) kann

verwendet werden, um eine Anwendung so einzurichten, dass sie gestartet und ausgeführt wird und dann beendet wird, wenn die Aufgabe erledigt ist. Mit einem [CronJob](#)-Objekt können Sie eine Anwendung so einrichten, dass sie zu einer bestimmten Stunde, Minute, an einem bestimmten Tag des Monats, Monats oder Wochentags ausgeführt wird. Dabei wird eine Struktur verwendet, die durch das [Linux-Crontab-Format](#) definiert ist.

Anwendungen vom Netzwerk aus zugänglich machen

Da Anwendungen oft als eine Reihe von Microservices bereitgestellt wurden, die an verschiedene Orte verlagert wurden, benötigte Kubernetes eine Möglichkeit, damit diese Microservices einander finden konnten. Damit andere auf eine Anwendung außerhalb des Kubernetes-Clusters zugreifen konnten, benötigte Kubernetes außerdem eine Möglichkeit, diese Anwendung auf externen Adressen und Ports verfügbar zu machen. Diese netzwerkbezogenen Funktionen werden mit Service- bzw. Ingress-Objekten ausgeführt:

- Dienste — Da sich ein Pod zu verschiedenen Knoten und Adressen bewegen kann, kann es für einen anderen Pod, der mit dem ersten Pod kommunizieren muss, schwierig sein, seinen Standort zu finden. [Um dieses Problem zu lösen, können Sie mit Kubernetes eine Anwendung als Service darstellen.](#) Mit einem Dienst können Sie einen Pod oder eine Gruppe von Pods mit einem bestimmten Namen identifizieren und dann angeben, welcher Port den Dienst dieser Anwendung vom Pod aus verfügbar macht und welche Ports eine andere Anwendung verwenden könnte, um diesen Dienst zu kontaktieren. Ein anderer Pod innerhalb eines Clusters kann einen Service einfach anhand des Namens anfordern, und Kubernetes leitet diese Anfrage an den richtigen Port für eine Pod-Instanz weiter, auf der dieser Dienst ausgeführt wird.
- Ingress — Durch [Ingress](#) können Anwendungen, die durch Kubernetes Services repräsentiert werden, für Clients verfügbar gemacht werden, die sich außerhalb des Clusters befinden. Zu den grundlegenden Funktionen von Ingress gehören ein Load Balancer (verwaltet von Ingress), der Ingress-Controller und Regeln für die Weiterleitung von Anfragen vom Controller an den Service. Es gibt mehrere [Ingress-Controller, aus denen Sie bei Kubernetes](#) wählen können.

Nächste Schritte

Wenn Sie die grundlegenden Kubernetes-Konzepte und ihren Zusammenhang mit Amazon EKS verstehen, können Sie sich sowohl in der Amazon EKS-Dokumentation als auch in der [Kubernetes-Dokumentation](#) zurechtfinden, um die Informationen zu finden, die Sie für die Verwaltung von Amazon EKS-Clustern und die Bereitstellung von Workloads in diesen Clustern benötigen. Um mit der Nutzung von Amazon EKS zu beginnen, wählen Sie aus den folgenden Optionen:

- [the section called “Cluster erstellen \(eksctl\)”](#)
- [the section called “Erstellen eines -Clusters”](#)
- [the section called “Beispielbereitstellung \(Linux\)”](#)
- [Clusterverwaltung](#)

Stellen Sie Amazon EKS-Cluster in Cloud- und lokalen Umgebungen bereit

Verstehen Sie die Bereitstellungsoptionen von Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) ist ein vollständig verwalteter Kubernetes-Service, mit dem Sie Kubernetes nahtlos in der Cloud und in Ihren lokalen Umgebungen ausführen können.

In der Cloud automatisiert Amazon EKS die Verwaltung der Kubernetes-Cluster-Infrastruktur für die Kubernetes-Steuerebene und die Knoten. Dies ist wichtig für die Planung von Containern, die Verwaltung der Anwendungsverfügbarkeit, die dynamische Skalierung von Ressourcen, die Optimierung der Datenverarbeitung, das Speichern von Clusterdaten und die Ausführung anderer kritischer Funktionen. Mit Amazon EKS erhalten Sie die robuste Leistung, Skalierbarkeit, Zuverlässigkeit und Verfügbarkeit der AWS Infrastruktur sowie native Integrationen mit AWS Netzwerk-, Sicherheits-, Speicher- und Observability-Diensten.

Um die Ausführung von Kubernetes in Ihren lokalen Umgebungen zu vereinfachen, können Sie dieselben Amazon EKS-Cluster, Funktionen und Tools für [Amazon EKS-Hybridknoten](#) in Ihrer eigenen Infrastruktur verwenden, oder Sie können [Amazon EKS Anywhere](#) für eigenständige Air-Gap-Umgebungen verwenden. [the section called “Knoten”](#)

Amazon EKS in der Cloud

Sie können Amazon EKS mit Berechnungen in AWS Regionen, AWS Local Zones und AWS Wellenlängenzonen verwenden. Mit Amazon EKS in der Cloud werden die Sicherheit, Skalierbarkeit und Verfügbarkeit der Kubernetes-Steuerebene vollständig von AWS in der AWS Region verwaltet. Wenn Sie Anwendungen mit Compute in AWS Regions ausführen, erhalten Sie die gesamte Bandbreite der AWS Amazon EKS-Funktionen, einschließlich Amazon EKS Auto Mode, der das Kubernetes-Cluster-Infrastrukturmanagement für Datenverarbeitung, Speicher und Netzwerke AWS mit einem einzigen Klick vollständig automatisiert. Wenn Sie Anwendungen mit Rechenleistung in

AWS lokalen Zonen und AWS Wellenlängenzonen ausführen, können Sie selbstverwaltete Amazon EKS-Knoten verwenden, um EC2 Amazon-Instances für Ihre Cluster-Datenverarbeitung zu verbinden und die anderen verfügbaren AWS Dienste in AWS Local Zones und AWS Wavelength Zones nutzen. Weitere Informationen finden Sie unter Funktionen für [AWS Local Zones und Funktionen für AWS Wellenlängenzonen](#).

	Amazon EKS in AWS Regionen	Amazon EKS in lokalen/Wellenlängenzonen
Verwaltung der Kubernetes-Steuerebene	AWS-verwaltet	AWS-verwaltet
Ort der Kubernetes-Steuerebene	AWS Regionen	AWS Regionen
Kubernetes-Datenebene	• Automatischer Amazon EKS-Modus • Von Amazon EKS verwaltete Knotengruppen • EC2 Selbstverwaltete Amazon-Knoten • AWS Fargate	• Von Amazon EKS verwaltete Knotengruppen (nur Local Zones) • EC2 Selbstverwaltete Amazon-Knoten
Ort der Kubernetes-Datenebene	AWS Regionen	AWS Lokale Zonen oder Wellenlängenzonen

Amazon EKS in Ihren Rechenzentren oder Edge-Umgebungen

Wenn Sie Anwendungen in Ihren eigenen Rechenzentren oder Edge-Umgebungen ausführen müssen, können Sie unsere [Amazon EKS Hybrid Nodes](#) verwenden [Amazon EKS auf AWS Outposts](#). Sie können selbstverwaltete Knoten mit EC2 Amazon-Instances auf AWS Outposts für Ihre Cluster-Datenverarbeitung verwenden, oder Sie können Amazon EKS-Hybridknoten mit Ihrer eigenen lokalen oder Edge-Infrastruktur für Ihre Cluster-Datenverarbeitung verwenden. AWS Outposts ist eine AWS verwaltete Infrastruktur, die Sie in Ihren Rechenzentren oder Colocation-Einrichtungen betreiben, wohingegen Amazon EKS Hybrid Nodes auf Ihren physischen oder virtuellen Maschinen ausgeführt wird, die Sie in Ihren lokalen oder Edge-Umgebungen verwalten. Amazon EKS on AWS

Outposts und Amazon EKS Hybrid Nodes erfordern eine zuverlässige Verbindung von Ihren lokalen Umgebungen zu einer AWS Region, und Sie können dieselben Amazon EKS-Cluster, Funktionen und Tools verwenden, die Sie für die Ausführung von Anwendungen in der Cloud verwenden. Bei der Ausführung auf AWS Outposts können Sie alternativ den gesamten Kubernetes-Cluster auf AWS Outposts mit lokalen Amazon EKS-Clustern auf Outposts bereitstellen. AWS

	Amazon EKS-Hybridknoten	Amazon EKS auf AWS Outposts
Verwaltung der Kubernetes-Steuerebene	AWS-verwaltet	AWS-verwaltet
Ort der Kubernetes-Steuerebene	AWS Regionen	AWS Regionen oder AWS Outposts
Kubernetes-Datenebene	Vom Kunden verwaltete physische oder virtuelle Maschinen	EC2 Selbstverwaltete Amazon-Knoten
Ort der Kubernetes-Datenebene	Rechenzentrum oder Edge-Umgebung des Kunden	Rechenzentrum oder Edge-Umgebung des Kunden

Amazon EKS Anywhere für Air-Gap-Umgebungen

[Amazon EKS Anywhere](#) vereinfacht das Kubernetes-Cluster-Management durch die Automatisierung undifferenzierter Aufgaben wie die Einrichtung der Infrastruktur und den Lebenszyklus von Kubernetes-Clustern in lokalen und Edge-Umgebungen. Im Gegensatz zu Amazon EKS ist Amazon EKS Anywhere ein vom Kunden verwaltetes Produkt, und Kunden sind für den Cluster-Lebenszyklusbetrieb und die Wartung von Amazon EKS Anywhere Anywhere-Clustern verantwortlich. Amazon EKS Anywhere basiert auf der Cluster-API (CAPI) des Kubernetes-Unterprojekts und unterstützt eine Reihe von Infrastrukturen, darunter VMware vSphere, Bare Metal, Nutanix, Apache und Snow. CloudStack AWS Amazon EKS Anywhere kann in Air-Gap-Umgebungen ausgeführt werden und bietet optionale Integrationen mit regionalen AWS Diensten für Observability und Identitätsmanagement. Um Support für Amazon EKS Anywhere und Zugriff auf AWS angebotene Kubernetes-Add-Ons zu erhalten, können Sie [Amazon EKS Anywhere Enterprise-Abonnements](#) erwerben.

	Amazon EKS Anywhere
Verwaltung der Kubernetes-Steuerebene	Vom Kunden verwaltet
Ort der Kubernetes-Steuerebene	Rechenzentrum oder Edge-Umgebung des Kunden
Kubernetes-Datenebene	Vom Kunden verwaltete physische oder virtuelle Maschinen
Ort der Kubernetes-Datenebene	Rechenzentrum oder Edge-Umgebung des Kunden

Amazon EKS-Tools

Sie können den [Amazon EKS-Connector](#) verwenden, um jeden konformen Kubernetes-Cluster zu registrieren und zu verbinden AWS und ihn in der Amazon EKS-Konsole anzuzeigen. Nachdem ein Cluster verbunden wurde, können Sie den Status, die Konfiguration und die Workloads für diesen Cluster in der Amazon-EKS-Konsole anzeigen. Sie können diese Funktion verwenden, um verbundene Cluster in der Amazon EKS-Konsole anzuzeigen, aber der Amazon EKS-Connector ermöglicht keine Verwaltungs- oder Mutationsvorgänge für Ihre verbundenen Cluster über die Amazon EKS-Konsole.

[Amazon EKS Distro](#) ist die AWS Distribution der zugrunde liegenden Kubernetes-Komponenten, die alle Amazon EKS-Angebote unterstützen. Es umfasst die Kernkomponenten, die für einen funktionierenden Kubernetes-Cluster erforderlich sind, wie z. B. Komponenten der Kubernetes-Steuerungsebene (etcd, kube-apiserver, kube-scheduler) und Netzwerkkomponenten (CoreDNS, kube-proxy, CNI-Plugins kube-controller-manager). Amazon EKS Distro kann verwendet werden, um Kubernetes-Cluster mit Tools Ihrer Wahl selbst zu verwalten. Bereitstellungen von Amazon EKS Distro sind nicht durch AWS Supportpläne abgedeckt.

Für die Verwendung von Amazon EKS einrichten

Um sich auf die Befehlszeilenverwaltung Ihrer Amazon EKS-Cluster vorzubereiten, müssen Sie mehrere Tools installieren. Verwenden Sie Folgendes, um Anmeldeinformationen einzurichten, Cluster zu erstellen und zu ändern und mit Clustern zu arbeiten, sobald sie ausgeführt werden:

- [AWS CLI einrichten](#) — Holen Sie sich die AWS CLI, um die Services einzurichten und zu verwalten, die Sie für die Arbeit mit Amazon EKS-Clustern benötigen. Insbesondere benötigen Sie AWS CLI, um Anmeldeinformationen zu konfigurieren, aber Sie benötigen es auch für andere AWS Dienste.
- [Kubect1 und eksctl einrichten](#) — Die eksctl CLI interagiert mit, um Amazon EKS-Cluster AWS zu erstellen, zu ändern und zu löschen. Sobald ein Cluster aktiv ist, verwenden Sie den kubect1 Open-Source-Befehl, um Kubernetes-Objekte in Ihren Amazon EKS-Clustern zu verwalten.
- Richten Sie eine Entwicklungsumgebung ein (optional) — Erwägen Sie, die folgenden Tools hinzuzufügen:
 - Lokales Bereitstellungstool — [Wenn Sie noch nicht mit Kubernetes vertraut sind, sollten Sie erwägen, ein lokales Bereitstellungstool wie Minikube oder ähnliches zu installieren](#). Mit diesen Tools können Sie auf Ihrem lokalen Computer einen Amazon EKS-Cluster zum Testen von Anwendungen einrichten.
 - Paketmanager — [helm](#) ist ein beliebter Paketmanager für Kubernetes, der die Installation und Verwaltung komplexer Pakete vereinfacht. Mit [Helm](#) ist es einfacher, Pakete wie den Load AWS Balancer Controller auf Ihrem Amazon EKS-Cluster zu installieren und zu verwalten.

Nächste Schritte

- [AWS CLI einrichten](#)
- [Richten Sie kubect1 und eksctl ein](#)
- [Schnellstart: Stellen Sie eine Web-App bereit und speichern Sie Daten](#)

AWS CLI einrichten

Die [AWS CLI](#) ist ein Befehlszeilentool für die Arbeit mit AWS Services, einschließlich Amazon EKS. Es wird auch verwendet, um IAM-Benutzer oder -Rollen für den Zugriff auf den Amazon EKS-Cluster und andere AWS Ressourcen von Ihrem lokalen Computer aus zu authentifizieren. Um Ressourcen

über die AWS Befehlszeile bereitzustellen, benötigen Sie eine AWS Zugriffsschlüssel-ID und einen geheimen Schlüssel, die Sie in der Befehlszeile verwenden können. Anschließend müssen Sie diese Anmeldeinformationen in der AWS CLI konfigurieren. Wenn Sie die AWS CLI noch nicht installiert haben, finden [Sie weitere Informationen unter Installieren oder Aktualisieren der neuesten Version der AWS CLI](#) im AWS Command Line Interface User Guide.

So erstellen Sie einen Zugriffsschlüssel

1. Melden Sie sich beim [AWS Management Console](#) an.
2. Für Einzelbenutzer- oder Mehrbenutzerkonten:
 - Einzelbenutzerkonto —:: Wählen Sie oben rechts Ihren AWS Benutzernamen, um das Navigationsmenü zu öffnen. Wählen Sie **webadmin** zum Beispiel.
 - Konto für mehrere Benutzer —:: Wählen Sie IAM aus der Liste der Dienste aus. Wählen Sie im IAM-Dashboard Benutzer und dann den Namen des Benutzers aus.
3. Wählen Sie Sicherheitsanmeldeinformationen aus.
4. Wählen Sie unter Zugriffsschlüssel die Option Zugriffsschlüssel erstellen aus.
5. Wählen Sie Befehlszeilenschnittstelle (CLI) und anschließend Weiter aus.
6. Wählen Sie Zugriffsschlüssel erstellen aus.
7. Wählen Sie CSV-Datei herunterladen aus.

Um die AWS CLI zu konfigurieren

Führen Sie nach der Installation der AWS CLI die folgenden Schritte aus, um sie zu konfigurieren. Weitere Informationen finden [Sie unter Configure the AWS CLI](#) im AWS Command Line Interface User Guide.

1. Geben Sie in einem Terminal-Fenster den folgenden Befehl ein:

```
aws configure
```

Optional können Sie ein benanntes Profil konfigurieren, z. B. `--profile cluster-admin`. Wenn Sie ein benanntes Profil in der AWS CLI konfigurieren, müssen Sie dieses Flag in nachfolgenden Befehlen immer übergeben.

2. Geben Sie Ihre AWS Anmeldeinformationen ein. Zum Beispiel:

```
Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: region-code
Default output format [None]: json
```

So rufen Sie ein Sicherheitstoken ab

Führen Sie bei Bedarf den folgenden Befehl aus, um ein neues Sicherheitstoken für die AWS CLI abzurufen. Weitere Informationen finden Sie [get-session-token](#) in der AWS CLI-Befehlsreferenz.

Das Token ist standardmäßig 15 Minuten lang gültig. Das standardmäßige Sitzungs-Timeout kann durch Übergeben des Flags `--duration-seconds` geändert werden. Zum Beispiel:

```
aws sts get-session-token --duration-seconds 3600
```

Dieser Befehl gibt die temporären Sicherheitsanmeldeinformationen für eine AWS CLI-Sitzung zurück. Die ausgegebene Antwort sollte wie folgt aussehen:

```
{
  "Credentials": {
    "AccessKeyId": "ASIA5FTRU3LOEXAMPLE",
    "SecretAccessKey": "JnKgwfqUD9mNsPoi9IbxAYEXAMPLE",
    "SessionToken": "VERYLONGSESSIONTOKENSTRING",
    "Expiration": "2023-02-17T03:14:24+00:00"
  }
}
```

So überprüfen Sie die Benutzeridentität

Führen Sie bei Bedarf den folgenden Befehl aus, um die AWS Anmeldeinformationen für Ihre IAM-Benutzeridentität (z. B. *ClusterAdmin*) für die Terminalsitzung zu überprüfen.

```
aws sts get-caller-identity
```

Dieser Befehl gibt den Amazon-Ressourcennamen (ARN) der IAM-Entität zurück, die für die AWS CLI konfiguriert ist. Die ausgegebene Antwort sollte beispielsweise wie folgt aussehen:

```
{
```

```
"UserId": "AKIAIOSFODNN7EXAMPLE",  
"Account": "01234567890",  
"Arn": "arn:aws:iam::01234567890:user/ClusterAdmin"  
}
```

Nächste Schritte

- [Richten Sie kubectl und eksctl ein](#)
- [Schnellstart: Stellen Sie eine Web-App bereit und speichern Sie Daten](#)

Einrichten **kubectl** und **eksctl**

Sobald die AWS CLI installiert ist, sollten Sie zwei weitere Tools installieren, um Ihre Kubernetes-Cluster zu erstellen und zu verwalten:

- **kubectl**: Das **kubectl** Befehlszeilentool ist das Haupttool, mit dem Sie Ressourcen in Ihrem Kubernetes-Cluster verwalten werden. Auf dieser Seite wird beschrieben, wie Sie die **kubectl** Binärdatei herunterladen und einrichten, die der Version Ihres Kubernetes-Clusters entspricht. Siehe [Kubectl installieren oder aktualisieren](#).
- **eksctl**: Das **eksctl** Befehlszeilentool dient zum Erstellen von EKS-Clustern in der AWS Cloud oder vor Ort (mit EKS Anywhere) sowie zum Ändern und Löschen dieser Cluster. Siehe [Installation von eksctl](#).

Installieren oder aktualisieren **kubectl**

In diesem Thema finden Sie Hinweise zum Herunterladen und Installieren der **kubectl**-Binärdatei auf Ihrem Gerät. Die Binärdatei ist identisch mit den [Upstream-Gemeinschaftsversionen](#). Die Binärdatei gilt nicht nur für Amazon EKS oder AWS. Gehen Sie wie folgt vor, um die spezifische Version zu erhalten **kubectl**, die Sie benötigen, obwohl viele Builder sie einfach ausführen, `brew install kubectl` um sie zu installieren.

Note

Sie müssen eine **kubectl**-Version verwenden, die nur in der Minor-Version von Ihrer Amazon-EKS-Cluster-Steuerebene abweicht. Beispielsweise sollte ein 1.32-**kubectl**-Client mit Kubernetes 1.31-, 1.32- und 1.33-Clustern funktionieren.

Schritt 1: Überprüfen Sie, ob **kubectl** es installiert ist

Stellen Sie fest, ob Sie `kubectl` bereits auf Ihrem Gerät installiert haben.

```
kubectl version --client
```

Wenn `kubectl` im Pfad Ihres Geräts installiert ist, enthält die Beispielausgabe ähnliche Informationen wie die folgende. Wenn Sie die Version, die Sie derzeit installiert haben, mit einer neueren Version aktualisieren möchten, führen Sie den nächsten Schritt aus und stellen Sie sicher, dass Sie die neue Version an demselben Speicherort installieren, an dem sich Ihre aktuelle Version befindet.

```
Client Version: v1.31.X-eks-1234567
```

Wenn Sie keine Ausgabe erhalten, haben Sie es entweder nicht `kubectl` installiert, oder es ist nicht an einem Ort installiert, der sich im Pfad Ihres Geräts befindet.

Schritt 2: Installation oder Aktualisierung **kubectl**

Installieren oder aktualisieren Sie `kubectl` auf einem der folgenden Betriebssysteme:

- [the section called “macOS”](#)
- [the section called “Linux \(amd64\)”](#)
- [the section called “Linux \(arm64\)”](#)
- [the section called “Windows”](#)

Note

Wenn die Downloads in Ihrer AWS Region aus den in diesem Abschnitt verwendeten AWS Regionen langsam sind, sollten Sie erwägen, den Inhalt so einzurichten, CloudFront dass der Inhalt zuerst angezeigt wird. Weitere Informationen finden Sie unter [Erste Schritte mit einer CloudFront Basisdistribution](#).

macOS

Gehen Sie wie folgt vor, um die Installation `kubectl` auf macOS durchzuführen. Zu diesen Schritten gehören:

- Wählen Sie die Binärdatei für die gewünschte Kubernetes-Version aus und laden Sie sie herunter.
- Optionales Überprüfen der Prüfsumme der Binärdatei.
- Execute wird den Berechtigungen der Binärdatei hinzugefügt.
- Die Binärdatei in einen Ordner in Ihrem PATH kopieren.
- Optionales Hinzufügen des Verzeichnisses der Binärdatei zu Ihrem PATH.

Verfahren:

1. Laden Sie die Binärdatei für die Kubernetes-Version Ihres Clusters von Amazon S3 herunter.

- Kubernetes 1.33

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/darwin/amd64/kubectl
```

- Kubernetes 1.32

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/darwin/amd64/kubectl
```

- Kubernetes 1.31

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/darwin/amd64/kubectl
```

- Kubernetes 1.30

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/darwin/amd64/kubectl
```

- Kubernetes 1.29

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/darwin/amd64/kubectl
```

- Kubernetes 1.28

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/darwin/amd64/kubectl
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2025-01-10/bin/darwin/amd64/kubectl
```

- Kubernetes 1.26

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/darwin/amd64/kubectl
```

2. (Optional) Überprüfen Sie die heruntergeladene Binärdatei mit der SHA-256-Prüfsumme für Ihre Binärdatei.

a. Laden Sie die SHA-256 Prüfsumme für die Kubernetes-Version Ihres Clusters herunter.

- Kubernetes 1.33

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.32

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.31

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.30

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.29

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.28


```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2025-01-10/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.26

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/darwin/amd64/kubectl.sha256
```

b. Überprüfen Sie die SHA-256-Prüfsumme für Ihre heruntergeladene Binärdatei.

```
openssl sha1 -sha256 kubectl
```

c. Stellen Sie sicher, dass die generierte Prüfsumme in der Ausgabe mit der Prüfsumme in der heruntergeladenen `kubectl.sha256`-Datei übereinstimmt.

3. Wenden Sie Ausführungsberechtigungen auf die Binärdatei an.

```
chmod +x ./kubectl
```

4. Kopieren Sie die Binärdatei in ein Verzeichnis in Ihrer `PATH`-Variable. Wenn Sie bereits eine Version von `kubectl` installiert haben, empfehlen wir, eine `$HOME/bin/kubectl`-Datei zu erstellen und sicherzustellen, dass `$HOME/bin` in der `$PATH`-Variablen zuerst vorkommt.

```
mkdir -p $HOME/bin && cp ./kubectl $HOME/bin/kubectl && export PATH=$HOME/bin:$PATH
```

5. (Optional) Fügen Sie den Pfad `$HOME/bin` zu Ihrer Shell-Initialisierungsdatei hinzu, um den Pfad bereits beim Öffnen einer Shell zu konfigurieren.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bash_profile
```

Linux (amd64)

Gehen Sie wie folgt vor, um die Installation `kubectl` unter Linux (amd64) durchzuführen. Zu diesen Schritten gehören:

- Wählen Sie die Binärdatei für die gewünschte Kubernetes-Version aus und laden Sie sie herunter.
- Optionales Überprüfen der Prüfsumme der Binärdatei.
- Execute wird den Berechtigungen der Binärdatei hinzugefügt.
- Die Binärdatei in einen Ordner in Ihrem PATH kopieren.
- Optionales Hinzufügen des Verzeichnisses der Binärdatei zu Ihrem PATH.

Verfahren:

1. Laden Sie die `kubectl` Binärdatei für die Kubernetes-Version Ihres Clusters von Amazon S3 herunter.

- Kubernetes 1.33

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/linux/amd64/kubectl
```

- Kubernetes 1.32

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/linux/amd64/kubectl
```

- Kubernetes 1.31

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/linux/amd64/kubectl
```

- Kubernetes 1.30

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/linux/amd64/kubectl
```

- Kubernetes 1.29

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/linux/amd64/kubectl
```

- Kubernetes 1.28

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/linux/amd64/kubectl
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2024-12-12/bin/linux/amd64/kubectl
```

- Kubernetes 1.26

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/linux/amd64/kubectl
```

2. (Optional) Überprüfen Sie die heruntergeladene Binärdatei mit der SHA-256-Prüfsumme für Ihre Binärdatei.

- a. Laden Sie die SHA-256 Prüfsumme für die Kubernetes-Version Ihres Clusters von Amazon S3 herunter, indem Sie den Befehl für die Hardwareplattform Ihres Geräts verwenden.

- Kubernetes 1.33

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/linux/amd64/kubectl.sha256
```

- Kubernetes 1.32

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/linux/amd64/kubectl.sha256
```

- Kubernetes 1.31

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/linux/amd64/kubectl.sha256
```

- Kubernetes 1.30

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/linux/amd64/kubectl.sha256
```

- Kubernetes 1.29

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/linux/amd64/kubectl.sha256
```

- Kubernetes 1.28

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/
linux/amd64/kubectl.sha256
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2024-12-12/bin/
linux/amd64/kubectl.sha256
```

- Kubernetes 1.26

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/
linux/amd64/kubectl.sha256
```

- b. Überprüfen Sie die SHA-256-Prüfsumme für die heruntergeladene Binärdatei mit einem der folgenden Befehle.

```
sha256sum -c kubectl.sha256
```

or

```
openssl sha1 -sha256 kubectl
```

- c. Zum einen sollten Sie sehen `kubectl: OK`, zum anderen können Sie überprüfen, ob die generierte Prüfsumme in der Ausgabe mit der Prüfsumme in der heruntergeladenen Datei übereinstimmt. `kubectl.sha256`

3. Wenden Sie Ausführungsberechtigungen auf die Binärdatei an.

```
chmod +x ./kubectl
```

4. Kopieren Sie die Binärdatei in ein Verzeichnis in Ihrer PATH-Variable. Wenn Sie bereits eine Version von `kubectl` installiert haben, empfehlen wir, eine `$HOME/bin/kubectl`-Datei zu erstellen und sicherzustellen, dass `$HOME/bin` in der `$PATH`-Variablen zuerst vorkommt.

```
mkdir -p $HOME/bin && cp ./kubectl $HOME/bin/kubectl && export PATH=$HOME/bin:$PATH
```

5. (Optional) Fügen Sie den Pfad `$HOME/bin` zu Ihrer Shell-Initialisierungsdatei hinzu, um den Pfad bereits beim Öffnen einer Shell zu konfigurieren.

 Note

Bei diesem Schritt wird davon ausgegangen, dass Sie das Bash-Shell verwenden. Wenn Sie eine andere Shell nutzen, ändern Sie den Befehl zur Angabe der spezifischen Shell-Initialisierungsdatei.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc
```

Linux (arm64)

Gehen Sie zur Installation `kubectl` unter Linux (arm64) wie folgt vor. Zu diesen Schritten gehören:

- Wählen Sie die Binärdatei für die gewünschte Kubernetes-Version aus und laden Sie sie herunter.
- Optionales Überprüfen der Prüfsumme der Binärdatei.
- Execute wird den Berechtigungen der Binärdatei hinzugefügt.
- Die Binärdatei in einen Ordner in Ihrem PATH kopieren.
- Optionales Hinzufügen des Verzeichnisses der Binärdatei zu Ihrem PATH.

Verfahren:

1. Laden Sie die `kubectl` Binärdatei für die Kubernetes-Version Ihres Clusters von Amazon S3 herunter.

- Kubernetes 1.33

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/linux/arm64/kubectl
```

- Kubernetes 1.32

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/linux/arm64/kubectl
```

- Kubernetes 1.31

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/linux/arm64/kubectl
```

- Kubernetes 1.30

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/linux/arm64/kubectl
```

- Kubernetes 1.29

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/linux/arm64/kubectl
```

- Kubernetes 1.28

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/linux/arm64/kubectl
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2024-12-12/bin/linux/arm64/kubectl
```

- Kubernetes 1.26

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/linux/arm64/kubectl
```

2. (Optional) Überprüfen Sie die heruntergeladene Binärdatei mit der SHA-256-Prüfsumme für Ihre Binärdatei.

- a. Laden Sie die SHA-256 Prüfsumme für die Kubernetes-Version Ihres Clusters von Amazon S3 herunter, indem Sie den Befehl für die Hardwareplattform Ihres Geräts verwenden.

- Kubernetes 1.33

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/linux/arm64/kubectl.sha256
```

- Kubernetes 1.32

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/  
linux/arm64/kubectl.sha256
```

- **Kubernetes 1.31**

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/  
linux/arm64/kubectl.sha256
```

- **Kubernetes 1.30**

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/  
linux/arm64/kubectl.sha256
```

- **Kubernetes 1.29**

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/  
linux/arm64/kubectl.sha256
```

- **Kubernetes 1.28**

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/  
linux/arm64/kubectl.sha256
```

- **Kubernetes 1.27**

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2024-12-12/bin/  
linux/arm64/kubectl.sha256
```

- **Kubernetes 1.26**

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/  
linux/arm64/kubectl.sha256
```

- b. Überprüfen Sie die SHA-256-Prüfsumme für die heruntergeladene Binärdatei mit einem der folgenden Befehle.

```
sha256sum -c kubectl.sha256
```

or

```
openssl sha1 -sha256 kubect1
```

- c. Zum einen sollten Sie sehen `kubect1`: OK, zum anderen können Sie überprüfen, ob die generierte Prüfsumme in der Ausgabe mit der Prüfsumme in der heruntergeladenen Datei übereinstimmt. `kubect1.sha256`

3. Wenden Sie Ausführungsberechtigungen auf die Binärdatei an.

```
chmod +x ./kubect1
```

4. Kopieren Sie die Binärdatei in ein Verzeichnis in Ihrer PATH-Variable. Wenn Sie bereits eine Version von `kubect1` installiert haben, empfehlen wir, eine `$HOME/bin/kubect1`-Datei zu erstellen und sicherzustellen, dass `$HOME/bin` in der `$PATH`-Variablen zuerst vorkommt.

```
mkdir -p $HOME/bin && cp ./kubect1 $HOME/bin/kubect1 && export PATH=$HOME/bin:$PATH
```

5. (Optional) Fügen Sie den Pfad `$HOME/bin` zu Ihrer Shell-Initialisierungsdatei hinzu, um den Pfad bereits beim Öffnen einer Shell zu konfigurieren.

Note

Bei diesem Schritt wird davon ausgegangen, dass Sie das Bash-Shell verwenden. Wenn Sie eine andere Shell nutzen, ändern Sie den Befehl zur Angabe der spezifischen Shell-Initialisierungsdatei.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc
```

Windows

Gehen Sie zur Installation unter Windows wie folgt `kubect1` vor. Zu diesen Schritten gehören:

- Wählen Sie die Binärdatei für die gewünschte Kubernetes-Version aus und laden Sie sie herunter.
- Optionales Überprüfen der Prüfsumme der Binärdatei.
- Die Binärdatei in einen Ordner in Ihrem PATH kopieren.
- Optionales Hinzufügen des Verzeichnisses der Binärdatei zu Ihrem PATH.

Verfahren:

1. Öffnen Sie ein PowerShell Terminal.
2. Laden Sie die `kubectl` Binärdatei für die Kubernetes-Version Ihres Clusters von Amazon S3 herunter.

- Kubernetes 1.33

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.32

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.31

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.30

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.29

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.28

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.27

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2024-12-12/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.26

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/windows/amd64/kubectl.exe
```

3. (Optional) Überprüfen Sie die heruntergeladene Binärdatei mit der SHA-256-Prüfsumme für Ihre Binärdatei.

a. Laden Sie die SHA-256 Prüfsumme für die Kubernetes-Version Ihres Clusters für Windows herunter.

- Kubernetes 1.33

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.33.0/2025-05-01/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.32

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.32.3/2025-04-17/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.31

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.31.7/2025-04-17/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.30

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.30.11/2025-04-17/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.29

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.29.15/2025-04-17/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.28

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.15/2025-04-17/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.27

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.16/2024-12-12/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.26

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.15/2024-12-12/bin/windows/amd64/kubectl.exe.sha256
```

- b. Überprüfen Sie die SHA-256-Prüfsumme für Ihre heruntergeladene Binärdatei.

```
Get-FileHash kubectl.exe
```

- c. Stellen Sie sicher, dass die generierte Prüfsumme in der Ausgabe mit der Prüfsumme in der heruntergeladenen `kubectl.sha256`-Datei übereinstimmt. Die PowerShell Ausgabe sollte eine entsprechende Zeichenfolge in Großbuchstaben sein.
4. Kopieren Sie die Binärdatei in ein Verzeichnis in Ihrer PATH-Variable. Wenn Sie in Ihrem PATH ein Verzeichnis vorhanden ist, das Sie für Befehlszeilen-Dienstprogramme verwenden, kopieren Sie die Binärdatei in dieses Verzeichnis. Führen Sie andernfalls die folgenden Schritte aus.
- a. Erstellen Sie ein neues Verzeichnis für Ihre Befehlszeilen-Binärdateien, z. B. `C:\bin`.
 - b. Kopieren Sie die `kubectl.exe`-Binärdatei in Ihr neues Verzeichnis.
 - c. Bearbeiten Sie Ihre Benutzer- oder System-PATH-Umgebungsvariable, um das neue Verzeichnis zu Ihrem PATH hinzuzufügen.
 - d. Schließen Sie Ihr PowerShell Terminal und öffnen Sie ein neues, um die neue PATH Variable aufzurufen.
5. Nach der Installation von `kubectl` können Sie die Version prüfen:

```
kubectl version --client
```

6. Bei der ersten Installation `kubectl` ist es noch nicht für die Kommunikation mit einem Server konfiguriert. Wir werden diese Konfiguration bei Bedarf in anderen Verfahren behandeln. Wenn Sie jemals die Konfiguration aktualisieren müssen, um mit einem bestimmten Cluster zu kommunizieren, können Sie den folgenden Befehl ausführen. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

7. Erwägen Sie die Konfiguration der auto Vervollständigung, sodass Sie mit der Tabulatortaste `kubectl` Unterbefehle ausführen können, nachdem Sie die ersten Buchstaben eingegeben haben. Einzelheiten finden Sie unter [Kubectl autocomplete](#) in der Kubernetes-Dokumentation.

Installieren `eksctl`

Die `eksctl` CLI wird für die Arbeit mit EKS-Clustern verwendet. Sie automatisiert viele einzelne Aufgaben. Anweisungen [zur Installation](#) finden Sie in der `eksctl` Dokumentation unter `Installationeksctl`. Verwenden Sie für Linux die UNIX-Anweisungen.

Wenn Sie `eksctl` den von Ihnen verwendeten IAM-Sicherheitsprinzipal verwenden, müssen Sie über Berechtigungen für die Arbeit mit Amazon EKS IAM-Rollen, serviceverknüpften Rollen AWS CloudFormation, einer VPC und verwandten Ressourcen verfügen. Weitere Informationen finden Sie unter [Aktionen](#) und [Verwenden von serviceverknüpften Rollen im IAM-Benutzerhandbuch](#). Sie müssen alle Schritte in diesem Handbuch als derselbe Benutzer ausführen. Führen Sie den folgenden Befehl aus, um den aktuellen Benutzer zu überprüfen:

```
aws sts get-caller-identity
```

Nächste Schritte

- [Schnellstart: Stellen Sie eine Web-App bereit und speichern Sie Daten](#)

Schnellstart: Eine Web-App bereitstellen und Daten speichern

Stellen Sie eine Spielanwendung bereit und speichern Sie ihre Daten auf Amazon EKS

[Dieses Schnellstart-Tutorial zeigt die Schritte zur Bereitstellung der 2048-Spielbeispielanwendung und zur Persistenz ihrer Daten auf einem Amazon EKS Auto Mode-Cluster mithilfe von eksctl.](#)

Amazon EKS Auto Mode automatisiert Routineaufgaben für Cluster-Blockspeicher, Netzwerke, Lastenausgleich und automatische Rechenskalierung.

Im weiteren Verlauf führen wir Sie durch den Cluster-Setup-Prozess. Amazon EKS Auto Mode automatisiert Aufgaben zum Erstellen eines Knotens mithilfe einer EC2 verwalteten Instance, zum Erstellen eines Application Load Balancers und zum Erstellen eines EBS-Volumes.

Insgesamt stellen Sie einen Beispiel-Workload mit den benutzerdefinierten Anmerkungen bereit, die für eine vollständige Integration mit Services erforderlich sind. AWS

In diesem Tutorial

Mithilfe der folgenden eksctl Clustervorlage erstellen Sie einen Cluster mit EKS Auto Mode für die automatisierte Knotenbereitstellung.

VPC-Konfiguration Wenn Sie die folgende eksctl-Clustervorlage verwenden, erstellt eksctl automatisch eine IPv4 Virtual Private Cloud (VPC) für den Cluster. Standardmäßig konfiguriert eksctl eine VPC, die alle Netzwerkanforderungen erfüllt und sowohl öffentliche als auch private Endpunkte erstellt.

Instance Management EKS Auto Mode fügt dynamisch Knoten in Ihrem EKS-Cluster hinzu oder entfernt sie, je nach den Anforderungen Ihrer Kubernetes-Anwendungen.

Datenpersistenz Verwenden Sie die Blockspeicherfunktion des EKS Auto Mode, um die Persistenz von Anwendungsdaten sicherzustellen, auch in Szenarien mit Pod-Neustarts oder -Ausfällen.

Externer App-Zugriff Verwenden Sie die Lastausgleichsfunktion von EKS Auto Mode, um einen Application Load Balancer (ALB) dynamisch bereitzustellen.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen für die Verwendung von Amazon EKS erfüllt haben:

- AWS CLI einrichten und Anmeldeinformationen konfigurieren
- Installieren Sie eksctl
- Installieren Sie kubectl

Weitere Informationen finden Sie unter [Einrichten](#).

Konfigurieren Sie den Cluster

In diesem Abschnitt erstellen Sie einen Cluster mit dem automatischen EKS-Modus für die dynamische Knotenbereitstellung.

Erstellen Sie eine `cluster-config.yaml` Datei und fügen Sie den folgenden Inhalt ein. `region-code` Ersetzen Sie durch eine gültige Region, z. B. `us-east-1`:

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: web-quickstart
  region: <region-code>

autoModeConfig:
  enabled: true
```

Jetzt sind wir bereit, den Cluster zu erstellen.

Erstellen Sie den Amazon EKS-Cluster:

```
eksctl create cluster -f cluster-config.yaml
```

 Important

Wenn Sie `eksctl` nicht verwenden, um den Cluster zu erstellen, müssen Sie die VPC-Subnetze manuell taggen.

Erstellen IngressClass

Erstellen Sie einen Kubernetes IngressClass für EKS Auto Mode. Das IngressClass definiert, wie der automatische EKS-Modus mit Ingress-Ressourcen umgeht. In diesem Schritt wird die Lastenausgleichsfunktion von EKS Auto Mode konfiguriert. Wenn Sie Ingress-Ressourcen für Ihre Anwendungen erstellen, verwendet EKS Auto Mode diese, IngressClass um automatisch Load Balancer bereitzustellen und zu verwalten und Ihre Kubernetes-Anwendungen mit Lastausgleichsdiensten zu integrieren. AWS

Speichern Sie die folgende Yaml-Datei als: `ingressclass.yaml`

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: alb
  annotations:
    ingressclass.kubernetes.io/is-default-class: "true"
spec:
  controller: eks.amazonaws.com/alb
```

Wenden Sie das IngressClass auf Ihren Cluster an:

```
kubectl apply -f ingressclass.yaml
```

Stellen Sie die Beispielanwendung für das Spiel 2048 bereit

In diesem Abschnitt führen wir Sie durch die Schritte zur Bereitstellung des beliebten Spiels „2048“ als Beispielanwendung innerhalb des Clusters. Das bereitgestellte Manifest enthält benutzerdefinierte Anmerkungen für den Application Load Balancer (ALB). Diese Anmerkungen sind in EKS integriert und weisen den EKS an, eingehenden HTTP-Verkehr als „mit dem Internet verbunden“ zu behandeln und ihn unter Verwendung des Zieltyps „ip“ an den entsprechenden Dienst im `game-2048` Namespace weiterzuleiten.

 Note

Das `docker-2048` Image im Beispiel ist ein `x86_64` Container-Image und kann nicht auf anderen Architekturen ausgeführt werden.

1. Erstellen Sie einen Kubernetes-Namespace, der mit dem Flag aufgerufen wird `game-2048`. --
`save-config`

```
kubectl create namespace game-2048 --save-config
```

Die ausgegebene Antwort sollte wie folgt aussehen:

```
namespace/game-2048 created
```

2. Stellen Sie die [2048](#) Game Sample-Anwendung bereit.

```
kubectl apply -n game-2048 -f https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.8.0/docs/examples/2048/2048_full.yaml
```

Dieses Manifest richtet ein Kubernetes-Deployment, einen Dienst und einen Ingress für den `game-2048` Namespace ein und schafft so die notwendigen Ressourcen, um die Anwendung innerhalb des Clusters bereitzustellen und verfügbar zu machen. `game-2048` Es umfasst die Erstellung eines Dienstes mit dem Namensservice-2048, der die Bereitstellung auf dem Port verfügbar macht 80, und einer Ingress-Ressource mit dem Namen, `ingress-2048` die Routing-Regeln für eingehenden HTTP-Verkehr und Anmerkungen für einen mit dem Internet verbundenen Application Load Balancer (ALB) definiert. Die ausgegebene Antwort sollte wie folgt aussehen:

```
namespace/game-2048 configured
deployment.apps/deployment-2048 created
service/service-2048 created
ingress.networking.k8s.io/ingress-2048 created
```

3. Führen Sie den folgenden Befehl aus, um die Ingress-Ressource für den Namespace abzurufen.
`game-2048`

```
kubectl get ingress -n game-2048
```


Die ausgegebene Antwort sollte wie folgt aussehen:

NAME	CLASS	HOSTS	ADDRESS
		PORTS	AGE
ingress-2048	alb	*	k8s-game2048-ingress2-eb379a0f83-378466616.region-code.elb.amazonaws.com
		80	31s

Sie müssen einige Minuten warten, bis der Application Load Balancer (ALB) bereitgestellt ist, bevor Sie mit den folgenden Schritten beginnen.

4. Öffnen Sie einen Webbrowser und geben Sie den Code ADDRESS aus dem vorherigen Schritt ein, um auf die Webanwendung zuzugreifen. Zum Beispiel:

```
k8s-game2048-ingress2-eb379a0f83-378466616.region-code.elb.amazonaws.com
```

Sie sollten das Spiel 2048 in Ihrem Browser sehen. Spiel!

2048

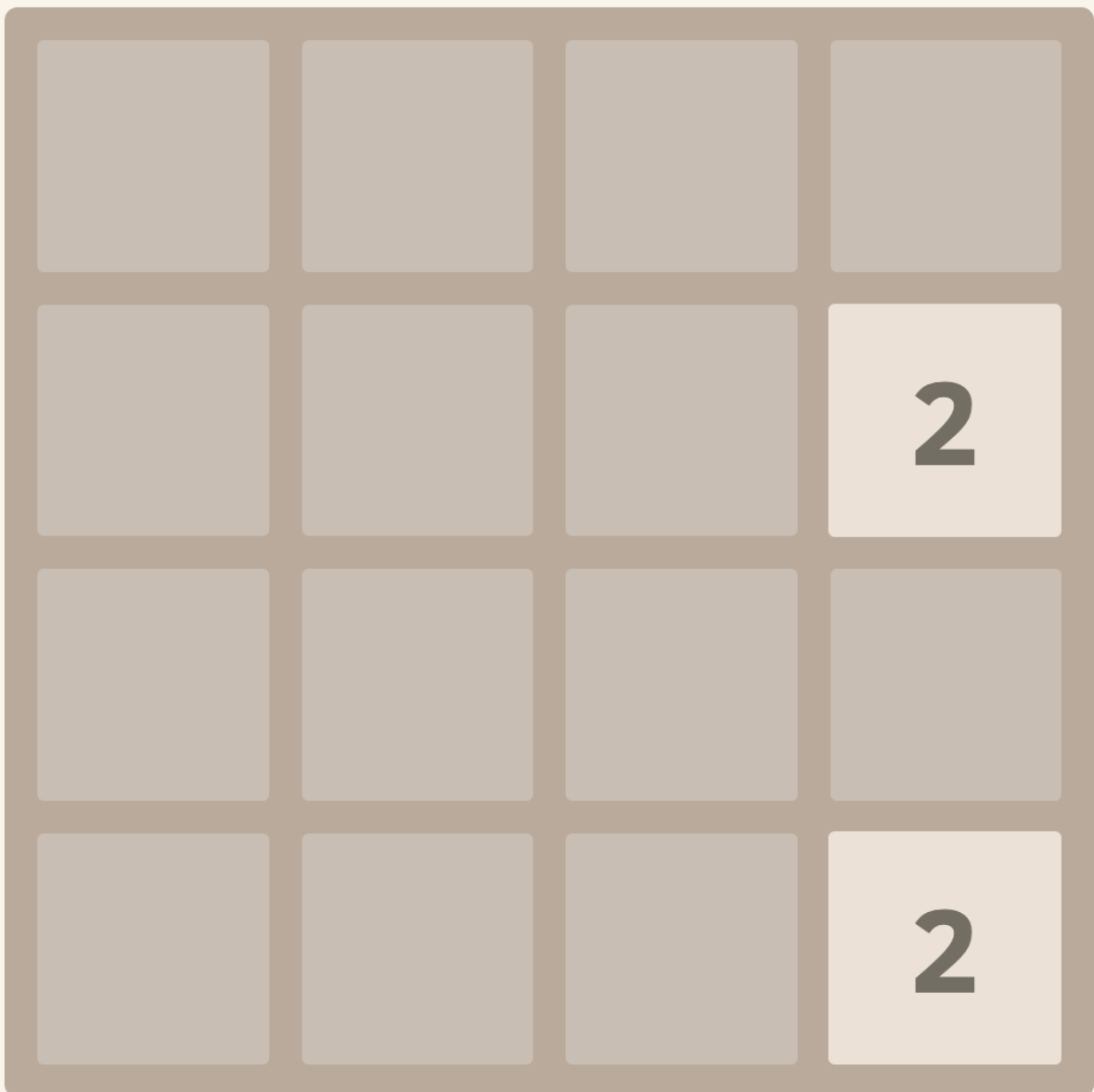
SCORE

0

BEST

48

Join the numbers and get to the **2048** tile!

[New Game](#)

Daten im automatischen Modus von Amazon EKS dauerhaft speichern

Jetzt, da das Spiel 2048 auf Ihrem Amazon EKS-Cluster läuft, ist es an der Zeit, sicherzustellen, dass Ihre Spieldaten mithilfe der Blockspeicherfunktion von Amazon EKS Auto Mode sicher gespeichert werden.

1. Erstellen Sie eine Datei namens `storage-class.yaml`:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: auto-ebs-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: ebs.csi.eks.amazonaws.com
volumeBindingMode: WaitForFirstConsumer
parameters:
  type: gp3
  encrypted: "true"
```

2. Wenden Sie Folgendes an: StorageClass

```
kubectl apply -f storage-class.yaml
```

3. Erstellen Sie einen Persistent Volume Claim (PVC), um Speicherplatz für Ihre Spieldaten anzufordern. Erstelle eine Datei mit dem Namen `ebs-pvc.yaml` und füge ihr den folgenden Inhalt hinzu:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: game-data-pvc
  namespace: game-2048
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 10Gi
```

```
storageClassName: auto-ebs-sc
```

4. Tragen Sie das PVC auf Ihren Cluster auf:

```
kubectl apply -f ebs-pvc.yaml
```

Die ausgegebene Antwort sollte wie folgt aussehen:

```
persistentvolumeclaim/game-data-pvc created
```

5. Jetzt müssen Sie Ihre 2048-Spielbereitstellung aktualisieren, um dieses PVC zum Speichern von Daten zu verwenden. Die folgende Bereitstellung ist so konfiguriert, dass das PVC zum Speichern von Spieldaten verwendet wird. Erstellen Sie eine Datei mit dem Namen `ebs-deployment.yaml` und fügen Sie ihr den folgenden Inhalt hinzu:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  namespace: game-2048
  name: deployment-2048
spec:
  replicas: 3 # Adjust the number of replicas as needed
  selector:
    matchLabels:
      app.kubernetes.io/name: app-2048
  template:
    metadata:
      labels:
        app.kubernetes.io/name: app-2048
    spec:
      containers:
        - name: app-2048
          image: public.ecr.aws/l6m2t8p7/docker-2048:latest
          imagePullPolicy: Always
          ports:
            - containerPort: 80
          volumeMounts:
            - name: game-data
              mountPath: /var/lib/2048
      volumes:
        - name: game-data
          persistentVolumeClaim:
```

```
claimName: game-data-pvc
```

6. Wenden Sie die aktualisierte Bereitstellung an:

```
kubectl apply -f ebs-deployment.yaml
```

Die ausgegebene Antwort sollte wie folgt aussehen:

```
deployment.apps/deployment-2048 configured
```

Mit diesen Schritten ist Ihr 2048-Spiel auf dem Cluster jetzt so eingerichtet, dass es Daten mithilfe der Blockspeicherfunktion von Amazon EKS Auto Mode persistiert. Dadurch wird sichergestellt, dass Ihr Spielfortschritt und Ihre Daten auch bei Pod- oder Node-Ausfällen sicher sind.

Wenn dir dieses Tutorial gefallen hat, lass es uns wissen, indem du uns Feedback gibst, damit wir dir weitere anwendungsfallspezifische Schnellstart-Tutorials wie dieses zur Verfügung stellen können.

Löschen Sie Ihren Cluster und Ihre Knoten

Wenn Sie mit dem Cluster fertig sind, den Sie für dieses Tutorial erstellt haben, sollten Sie ihn bereinigen, indem Sie den Cluster mit dem folgenden Befehl löschen. Wenn Sie vor dem Aufräumen mehr aus diesem Cluster machen möchten, finden Sie weitere Informationen unter [Nächste Schritte](#).

```
eksctl delete cluster -f ./cluster-config.yaml
```

EKS bereinigt automatisch alle Knoten, die es bereitgestellt hat, wenn der Cluster gelöscht wird.

Lernen Sie Amazon EKS anhand eines Beispiels kennen

Übersicht

Dieses Amazon EKS-Benutzerhandbuch enthält allgemeine Verfahren zur Erstellung Ihres ersten EKS-Clusters über die [Befehlszeile](#) oder [AWS Management Console](#) eine solide Referenz für alle wichtigen Amazon EKS-Komponenten. Als Amazon EKS-Clusteradministrator oder -Entwickler können Sie jedoch ein tieferes Verständnis von Amazon EKS erlangen, indem Sie den Lernpfaden folgen, die es auf Websites außerhalb dieses Handbuchs gibt. Diese Websites können Ihnen helfen:

- Richten Sie bestimmte Clustertypen ein. Spezifische Clustertypen können auf Ihren Workload-Typen oder Sicherheitsanforderungen basieren. Möglicherweise möchten Sie einen Cluster für die Ausführung von Batch-, Machine Learning- oder rechenintensiven Workloads optimieren.
- Verbessern Sie Ihre Cluster. Sie können Ihrem Cluster erweiterte Funktionen hinzufügen, um beispielsweise Observability, flexiblen Speicher, automatische Skalierung oder spezielle Cluster-Netzwerke bereitzustellen.
- Automatisieren Sie Updates. Mithilfe von Funktionen wie GitOps können Sie die automatische Bereitstellung von Cluster-Infrastruktur und Workloads einrichten, basierend auf Änderungen, die an diesen Komponenten in Ihren Git-Repositorys vorgenommen werden.
- Verwenden Sie erweiterte Cluster-Setup-Tools. `eksctl` bietet zwar eine schnelle Möglichkeit, einen Cluster zu erstellen, aber es gibt auch andere Tools, die die Konfiguration und Aktualisierung komplexerer Cluster erleichtern können. Dazu gehören Tools wie [Terraform](#) und [CloudFormation](#).

Um mit Ihrem Amazon EKS-Lernpfad zu beginnen, empfehle ich Ihnen, einige der auf dieser Seite beschriebenen Websites zu besuchen. Falls Sie unterwegs auf Probleme stoßen, gibt es auch Ressourcen, die Ihnen helfen, diese zu lösen. Mit dem [re:POST Knowledge Center](#) können Sie beispielsweise die Support-Datenbank nach Support-Problemen im Zusammenhang mit Amazon EKS durchsuchen. Außerdem bietet der [Amazon EKS Best Practices Guide](#) Tipps zu den besten Methoden zur Einrichtung Ihrer produktionsstauglichen Cluster.

Workshop zu Amazon EKS

Der Amazon [EKS-Workshop beginnt mit einem grundlegenden Verständnis von Kubernetes und Containern und ist eine Lernplattform, auf der ein Clusteradministrator durch wichtige Funktionen von Amazon EKS](#) geführt wird. So können Sie am Amazon EKS-Workshop teilnehmen:

- Grundlagen von Amazon EKS: Sehen Sie sich das Video auf der [Einführungsseite](#) an, um zu erfahren, wie Amazon EKS Kubernetes-Funktionen in der AWS Cloud implementiert. Wenn Sie ein noch grundlegendes Verständnis von Kubernetes benötigen, schauen Sie sich das Video [Was ist Kubernetes](#) an.
- Amazon EKS Setup: Wenn Sie ein AWS Konto haben, hilft Ihnen der Abschnitt [Setup](#) dabei, eine CloudShell Umgebung für die Erstellung eines Clusters für Sie einzurichten. Es bietet eine Auswahl zwischen [eksctl](#) (eine einfache Befehlszeile zur Clustererstellung) und [Terraform](#) (ein umfassenderer infrastructure-as-code Ansatz zum Erstellen eines Clusters) für die Erstellung Ihres Amazon EKS-Clusters.
- Amazon EKS Erste Schritte: Probieren Sie einen einfachen Webshop aus dem Abschnitt [Beispielanwendung](#) aus. Sie können dies in den anderen Übungen verwenden. In diesem Abschnitt erfahren Sie auch, wie [Container-Images gepackt](#) werden und wie Microservices mithilfe von Kubernetes-Pods, Deployments, Services und Namespaces verwaltet werden. StatefulSets Verwenden Sie dann Kustomize, um Änderungen an Kubernetes-Manifesten bereitzustellen.
- Grundlagen von Amazon EKS: Mithilfe von AWS Funktionen wie dem [Load AWS Balancer Controller](#) zeigt Ihnen der Workshop, wie Sie Ihre Anwendungen der Außenwelt zugänglich machen können. In Bezug auf Speicher zeigt der Workshop, wie [Amazon EBS für Blockspeicher](#), [Amazon EFS für Dateisystemspeicher](#) und [Amazon FSx für NetApp ONTAP](#) zur Verwaltung von ONTAP-Dateisystemen verwendet werden. AWS [Für die Knotenverwaltung hilft Ihnen der Workshop bei der Einrichtung verwalteter Knotengruppen](#).
- Erweiterte Funktionen von Amazon EKS: Zu den erweiterten Funktionen, die im Amazon EKS-Workshop angeboten werden, gehören Übungen zur Einrichtung von:
 - [Autoscaling](#): Dazu gehören die automatische Skalierung von Knoten (mit Cluster Autoscaler oder Karpenter) und die automatische Skalierung von Workloads (mit Horizontal Pod Autoscaler und Cluster Proportional Autoscaler).
 - [Observability](#): Erfahren Sie in einer Reihe von Observability-Labs mehr über [Logging](#), [OpenSearch](#), [Container Insights on Amazon EKS](#) und [Cost Visibility with Kubecost](#).
 - [Sicherheit](#): In diesen [Sicherheitslaboren](#) können Sie sich mit [Secrets Management](#), [Amazon GuardDuty](#), [Pod Security Standards](#) und [Kyverno Policy](#) Management vertraut machen.
 - [Netzwerk](#): Lernen Sie die Netzwerkfunktionen für Amazon EKS in [Networking](#) Labs kennen, zu denen [Amazon VPC CNI](#) (unterstützende Netzwerk-Plugins) und [Amazon VPC Lattice](#) (für die Konfiguration von Clustern für VC und Benutzerkonten) gehören.
 - [Automatisierung](#): Labs on [Automation](#) führt Sie durch [GitOps](#) Methoden zur Verwaltung Ihrer Cluster und Projekte wie [AWS Controllers for Kubernetes](#) und [Crossplane](#) zur Verwaltung von Amazon EKS-Kontrollebenen.

Praktische Anleitungen zur Einrichtung von Amazon EKS-Clustern

Eine Reihe von [Tutorials zur Einrichtung von Amazon EKS-Clustern](#) auf der AWS Community-Website kann Ihnen helfen, spezielle Amazon EKS-Cluster zu erstellen und diese Cluster auf verschiedene Weise zu erweitern. Die Tutorials sind in drei verschiedene Typen unterteilt:

Cluster aufbauen

Diese Tutorials helfen Ihnen beim Erstellen von Clustern, die für spezielle Zwecke verwendet werden können. Zu diesen speziellen Zwecken gehört die Fähigkeit, Folgendes auszuführen:

- [Weltweit skalierbare Anwendungen auf der Grundlage von IPv6](#)
- [Asynchrone Batch-Aufgaben](#)
- [Mikroservices mit hohem Datenaufkommen](#)
- [Autoscaling mit Karpenter auf Fargate](#)
- [Finanzielle Arbeitsbelastung](#)
- [Von Windows verwaltete Knotengruppen](#)

Verbesserung von Clustern

Sobald Sie über einen vorhandenen Cluster verfügen, können Sie diesen Cluster so erweitern und verbessern, dass er spezielle Workloads ausführen und die Cluster anderweitig verbessern kann. Diese Tutorials bieten Möglichkeiten für:

- [Bereitstellung von Speicherlösungen mit EFS CSI](#)
- [Stellen Sie dynamischen Datenbankspeicher mit EBS CSI bereit](#)
- [Bereitstellen von Anwendungen auf IPv4 Clustern mithilfe des AWS Load Balancer Controllers](#)
- [Bereitstellen von Anwendungen auf IPv6 Clustern mithilfe des AWS Load Balancer Controllers](#)

Optimierung von Diensten AWS

Mithilfe dieser Tutorials können Sie Ihre Cluster besser in AWS Dienste integrieren. Diese Tutorials enthalten solche, die Ihnen helfen:

- [DNS-Einträge für Microservices mit ExternalDNS verwalten](#)
- [Überwachen Sie Anwendungen mit CloudWatch](#)

- [Verwaltung asynchroner Aufgaben mit SQS- und EFS-Speicher](#)
- [AWS Secrets Manager Secrets aus Workloads nutzen](#)
- [Richten Sie mTLS mit Fargate, NGINX und ACM PCA ein](#)

Amazon EKS-Beispiele

Das [Amazon EKS Samples](#) Repository speichert Manifeste zur Verwendung mit Amazon EKS. Diese Manifeste bieten Ihnen die Möglichkeit, verschiedene Arten von Anwendungen in Amazon EKS auszuprobieren oder bestimmte Typen von Amazon EKS-Clustern zu erstellen. Zu den Beispielen gehören Manifeste für:

- [Erstellen Sie einen AWS Amazon EKS Fargate-Cluster](#)
- [Erstellen Sie einen Cluster mit einer vorhandenen IAM-Rolle](#)
- [Fügen Sie einem Cluster eine von Ubuntu verwaltete Knotengruppe hinzu](#)
- [Pod-Speicher mit Volume-Snapshots Backup und wiederherstellen](#)
- [Stellen Sie EBS-Volumes wieder her, die wie PVCs bei mehreren Konten bereitgestellt wurden](#)
- [Aktivieren Sie das Proxyprotokoll für den NGINX Ingress Controller mit Classic Load Balancers](#)
- [Logging on Fargate konfigurieren für AWS OpenSearch](#)
- [Führen Sie das Python-SDK mit einem Web Federated Identity Provider aus](#)
- [Stellen Sie eine Beispiel-App auf einem NFS-CSI-Controller bereit](#)
- [Verwenden Sie Volume-Snapshots für StatefulSets](#)
- [Stellen Sie Pods knotenübergreifend in verschiedenen Verfügbarkeitszonen bereit](#)

Beachten Sie, dass diese Beispiele nur zu Lern- und Testzwecken dienen und nicht für den Einsatz in der Produktion vorgesehen sind.

AWS Tutorials

Die [AWS Tutorials-Website](#) veröffentlicht einige Amazon EKS-Tutorials, bietet aber auch eine Suchfunktion, um andere Tutorials zu finden, die auf AWS Websites (wie der AWS Community-Website) veröffentlicht wurden. Zu den direkt auf dieser Website veröffentlichten Amazon EKS-Tutorials gehören:

- [Stellen Sie eine Container-Web-App auf Amazon EKS bereit](#)

- [Kubernetes-Cluster für weniger Geld ausführen \(Amazon EKS- und Spot-Instances\)](#)
- [Wie lassen sich Jenkins-Jobs auf Kubernetes kostenoptimieren](#)

Workshop für Entwickler

Wenn Sie ein Softwareentwickler sind und Anwendungen für die Ausführung auf Amazon EKS erstellen oder umgestalten möchten, ist der [Amazon EKS Developers Workshop](#) ein guter Ausgangspunkt. Der Workshop hilft Ihnen nicht nur bei der Erstellung containerisierter Anwendungen, sondern hilft Ihnen auch dabei, diese Container in einer Container Registry ([ECR](#)) und von dort in einem Amazon EKS-Cluster bereitzustellen.

Beginnen Sie mit dem [Amazon EKS Python Workshop](#), um den Prozess des Refactorings einer Python-Anwendung zu durchlaufen, und richten Sie dann Ihre Entwicklungsumgebung ein, um die Bereitstellung der Anwendung vorzubereiten. Gehen Sie die Abschnitte zu Containern, Kubernetes und Amazon EKS durch, um sich darauf vorzubereiten, Ihre containerisierten Anwendungen in diesen Umgebungen auszuführen.

Terraform-Workshop

Terraform `eksctl` ist zwar ein einfaches Tool zum Erstellen eines Clusters, aber für komplexere infrastructure-as-code Arten von Amazon EKS-Bereitstellungen ist [Terraform](#) ein beliebtes Tool zur Erstellung und Verwaltung von Amazon EKS-Clustern. Der [Terraform Amazon EKS-Workshop](#) zeigt, wie Sie Terraform verwenden, um eine AWS VPC zu erstellen, Amazon EKS-Cluster zu erstellen und Ihrem Cluster optionale Erweiterungen hinzuzufügen. Insbesondere gibt es einen Abschnitt zum Erstellen eines [privaten Amazon EKS-Clusters](#)

AWS Amazon EKS-Schulung

AWS bietet formelle Schulungen zum Kennenlernen von Amazon EKS an. Ein dreitägiger Schulungskurs mit dem Titel [Running Containers on Amazon Elastic Kubernetes Service vermittelt](#):

- Grundlagen von Kubernetes und Amazon EKS
- So erstellen Sie Amazon EKS-Cluster
- Sicherung von Amazon EKS mit AWS IAM- und Kubernetes-RBAC-Autorisierung
- GitOps Automatisierungstools
- Überwachungstools

- Techniken zur Verbesserung von Kosten, Effizienz und Ausfallsicherheit

Erste Schritte mit Amazon EKS

Vergewissern Sie sich, dass Sie für die Verwendung von Amazon EKS bereit sind, bevor Sie sich mit den Anleitungen für die ersten Schritte beschäftigen. Weitere Informationen finden Sie unter [Einrichten](#).

Es gibt zwei Handbücher „Erste Schritte“ für das Erstellen eines neuen Kubernetes-Clusters mit Knoten in Amazon EKS:

- [Erste Schritte mit Amazon EKS — eksctl](#) — Dieser Leitfaden für die ersten Schritte hilft Ihnen bei der Installation aller Ressourcen, die für die ersten Schritte mit Amazon EKS erforderlich sind. Dabei handelt es sich um ein einfaches Befehlszeilenprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS. `eksctl` Am Ende des Tutorials haben Sie einen laufenden Amazon-EKS-Cluster, auf dem Sie Anwendungen bereitstellen können. Dies ist die schnellste und einfachste Möglichkeit zum Einstieg in Amazon EKS.
- [Erste Schritte mit Amazon EKS — AWS Management Console und AWS CLI](#) — Dieser Leitfaden für die ersten Schritte hilft Ihnen dabei, alle erforderlichen Ressourcen für die ersten Schritte mit Amazon EKS mithilfe der AWS Management Console und AWS CLI zu erstellen. Am Ende des Tutorials haben Sie einen laufenden Amazon-EKS-Cluster, auf dem Sie Anwendungen bereitstellen können. In diesem Handbuch erstellen Sie manuell jede Ressource, die für einen Amazon-EKS-Cluster erforderlich ist. Die Verfahren geben Ihnen einen Überblick darüber, wie jede Ressource erstellt wird und wie die Ressourcen miteinander interagieren.

Wir bieten auch die folgenden Referenzen an:

- Eine Sammlung praktischer Tutorials finden Sie unter [EKS-Cluster-Setup](#) in der AWS Community.
- Codebeispiele finden Sie unter [Codebeispiele für die Verwendung von Amazon EKS AWS SDKs](#).

Erste Schritte mit Amazon EKS — EKS Auto Mode

Wie bei anderen EKS-Einstiegserlebnissen wird auch beim Erstellen Ihres ersten Clusters mit dem EKS-Automatikmodus die Verwaltung des Clusters selbst an diesen delegiert AWS. Der automatische Modus von EKS erweitert jedoch die EKS-Automatisierung, indem er die Verantwortung für viele wichtige Dienste überträgt, die für die Einrichtung der Workload-Infrastruktur (Knoten, Netzwerke und verschiedene Dienste) erforderlich sind. Dies erleichtert die Verwaltung von Knoten und die Skalierung, um den Workload-Anforderungen gerecht zu werden.

Wählen Sie eine der folgenden Möglichkeiten, um einen Cluster mit EKS Auto Mode zu erstellen:

- [the section called “ AWS CLI”](#): Verwenden Sie die aws Befehlszeilenschnittstelle, um einen Cluster zu erstellen.
- [the section called “Verwaltungskonsole”](#): Verwenden Sie den AWS Management Console , um einen Cluster zu erstellen.
- [the section called “eksctl CLI”](#): Verwenden Sie die eksctl Befehlszeilenschnittstelle, um einen Cluster zu erstellen.

Wenn Sie verschiedene Ansätze zur Erstellung Ihres ersten EKS-Clusters vergleichen, sollten Sie wissen, dass EKS Auto Mode zusätzliche Clusterverwaltungsaufgaben AWS übernommen hat, einschließlich der Einrichtung von Komponenten für:

- Starten und skalieren Sie Knoten, wenn der Workload-Bedarf steigt und sinkt.
- Aktualisieren Sie regelmäßig den Cluster selbst (Steuerungsebene), die Knotenbetriebssysteme und die Dienste, die auf den Knoten ausgeführt werden.
- Wählen Sie Standardeinstellungen, die Dinge wie Größe und Geschwindigkeit des Knotenspeichers und die Pod-Netzwerkconfiguration bestimmen.

Einzelheiten zu den Vorteilen von EKS-Automodus-Clustern finden Sie unter [Automatischer EKS-Modus](#).

Erste Schritte mit Amazon EKS — **eksctl**

Note

In diesem Thema werden die ersten Schritte ohne den automatischen EKS-Modus behandelt. Der automatische EKS-Modus automatisiert Routineaufgaben für Cluster-Computing, Speicher und Netzwerke. [Erfahren Sie, wie Sie mit Amazon EKS Auto Mode beginnen können.](#)

Dieses Handbuch hilft Ihnen beim Erstellen aller erforderlichen Ressourcen für die ersten Schritte mit Amazon Elastic Kubernetes Service (Amazon EKS) mithilfe von eksctl, einem einfachen Befehlszeilendienstprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon

EKS. Am Ende dieses Tutorials haben Sie einen laufenden Amazon-EKS-Cluster, auf dem Sie Anwendungen bereitstellen können.

Die Verfahren in diesem Handbuch erstellen automatisch mehrere Ressourcen für Sie, die Sie manuell erstellen müssen, wenn Sie Ihren Cluster mit der AWS Management Console. Wenn Sie die meisten Ressourcen lieber manuell erstellen möchten, um besser zu verstehen, wie sie miteinander interagieren, verwenden Sie die AWS Management Console, um Ihren Cluster und Ihre Berechnungen zu erstellen. Weitere Informationen finden Sie unter [the section called “Cluster erstellen \(Konsole und CLI\)”](#).

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, müssen Sie die Tools AWS CLI, kubectl und eksctl installieren und konfigurieren, wie unter [Einrichtung zur Verwendung von Amazon EKS](#) beschrieben.

Schritt 1: Erstellen Sie Ihren Amazon-EKS-Cluster und -Knoten

Important

Für einen möglichst einfachen und schnellen Einstieg enthält dieses Thema Schritte zum Erstellen eines Clusters und von Knoten mit Standardeinstellungen. Bevor Sie einen Cluster und Knoten für den Produktionseinsatz erstellen, empfehlen wir Ihnen, sich mit allen Einstellungen vertraut zu machen und einen Cluster und Knoten mit den Einstellungen bereitzustellen, die Ihren Anforderungen entsprechen. Weitere Informationen erhalten Sie unter [the section called “Erstellen eines -Clusters”](#) und [Rechenleistung verwalten](#). Einige Einstellungen können nur aktiviert werden, wenn Sie Ihren Cluster und Ihre Knoten erstellen.

Sie können einen Cluster mit einem der folgenden Knotentypen erstellen. Weitere Informationen zu den einzelnen Typen finden Sie unter [Rechenleistung verwalten](#). Nachdem Ihr Cluster bereitgestellt wurde, können Sie andere Knotentypen hinzufügen.

- **Fargate — Linux** — Wählen Sie diesen Knotentyp, wenn Sie Linux-Anwendungen ausführen [the section called “AWS Fargate”](#) möchten. Fargate ist eine serverlose Compute-Engine, mit der Sie Kubernetes-Pods bereitstellen können, ohne Amazon-Instances verwalten zu müssen. EC2
- **Verwaltete Knoten — Linux** — Wählen Sie diesen Knotentyp, wenn Sie Amazon Linux-Anwendungen auf EC2 Amazon-Instances ausführen möchten. Obwohl in diesem Handbuch nicht

behandelt, können Sie Ihrem Cluster auch [selbstverwaltete Windows](#)- und [Bottlerocket](#)-Knoten hinzufügen.

Erstellen Sie Ihren Amazon-EKS-Cluster mit dem folgenden Befehl. Sie können *my-cluster* durch Ihren eigenen Wert ersetzen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. *region-code* Ersetzen Sie durch eine beliebige AWS Region, die von Amazon EKS unterstützt wird. Eine Liste der AWS Regionen finden Sie unter [Amazon EKS-Endpunkte und Kontingente](#) im AWS Allgemeinen Referenzhandbuch.

Example

Fargate - Linux

```
eksctl create cluster --name my-cluster --region region-code --fargate
```

Managed nodes - Linux

```
eksctl create cluster --name my-cluster --region region-code
```

Die Clustererstellung dauert mehrere Minuten. Während der Erstellung werden Sie mehrere Ausgabezeilen sehen. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[...]
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

eksctl hat eine kubectl Konfigurationsdatei in Ihrem Computer erstellt ~/.kube/config oder die Konfiguration des neuen Clusters zu einer vorhandenen Konfigurationsdatei hinzugefügt. ~/.kube/config

Nachdem die Clustererstellung abgeschlossen ist, sehen Sie sich den eksctl-*my-cluster*-cluster in der AWS CloudFormation [Konsole](#) genannten AWS CloudFormation Stack an, um alle Ressourcen zu sehen, die erstellt wurden.

Schritt 2: Anzeigen von Kubernetes-Ressourcen

1. Zeigen Sie Ihre Cluster-Knoten an.

```
kubectl get nodes -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

Example

Fargate - Linux

NAME	STATUS	ROLES	AGE
VERSION	OS-IMAGE		KERNEL-VERSION
CONTAINER-RUNTIME			
fargate-ip-192-0-2-0.region-code.compute.internal	Ready	<none>	
8m3s v1.2.3-eks-1234567 192.0.2.0 <none>		Amazon Linux 2	
1.23.456-789.012.amzn2.x86_64 containerd://1.2.3			
fargate-ip-192-0-2-1.region-code.compute.internal	Ready	<none>	
7m30s v1.2.3-eks-1234567 192-0-2-1 <none>		Amazon Linux 2	
1.23.456-789.012.amzn2.x86_64 containerd://1.2.3			

Managed nodes - Linux

NAME	STATUS	ROLES	AGE	VERSION
INTERNAL-IP EXTERNAL-IP OS-IMAGE		KERNEL-VERSION		
CONTAINER-RUNTIME				
ip-192-0-2-0.region-code.compute.internal	Ready	<none>	6m7s	
v1.2.3-eks-1234567 192.0.2.0 192.0.2.2		Amazon Linux 2		
1.23.456-789.012.amzn2.x86_64 containerd://1.2.3				
ip-192-0-2-1.region-code.compute.internal	Ready	<none>	6m4s	
v1.2.3-eks-1234567 192.0.2.1 192.0.2.3		Amazon Linux 2		
1.23.456-789.012.amzn2.x86_64 containerd://1.2.3				

Weitere Informationen dazu, was in der Ausgabe angezeigt wird, finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

2. Zeigen Sie die Workloads an, die auf Ihrem Cluster ausgeführt werden.

```
kubectl get pods -A -o wide
```


Eine Beispielausgabe sieht wie folgt aus.

Example

Fargate - Linux

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP
	NODE					
	READINESS GATES					
kube-system	coredns-1234567890-abcde	1/1	Running	0	18m	
192.0.2.0	fargate-ip-192-0-2-0.region-code.compute.internal				<none>	
<none>						
kube-system	coredns-1234567890-12345	1/1	Running	0	18m	
192.0.2.1	fargate-ip-192-0-2-1.region-code.compute.internal				<none>	
<none>						

Managed nodes - Linux

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP
	NODE					
	GATES					
kube-system	aws-node-12345	1/1	Running	0	7m43s	
192.0.2.1	ip-192-0-2-1.region-code.compute.internal			<none>		<none>
kube-system	aws-node-67890	1/1	Running	0	7m46s	
192.0.2.0	ip-192-0-2-0.region-code.compute.internal			<none>		<none>
kube-system	coredns-1234567890-abcde	1/1	Running	0	14m	
192.0.2.3	ip-192-0-2-3.region-code.compute.internal			<none>		<none>
kube-system	coredns-1234567890-12345	1/1	Running	0	14m	
192.0.2.4	ip-192-0-2-4.region-code.compute.internal			<none>		<none>
kube-system	kube-proxy-12345	1/1	Running	0	7m46s	
192.0.2.0	ip-192-0-2-0.region-code.compute.internal			<none>		<none>
kube-system	kube-proxy-67890	1/1	Running	0	7m43s	
192.0.2.1	ip-192-0-2-1.region-code.compute.internal			<none>		<none>

Weitere Informationen dazu, was in der Ausgabe angezeigt wird, finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

Schritt 3: Löschen Ihrer Cluster und Knoten

Wenn Sie mit dem Cluster und den Knoten fertig sind, die Sie für dieses Tutorial erstellt haben, sollten Sie den Cluster und die Knoten mit dem folgenden Befehl löschen. Wenn Sie vor dem Bereinigen mehr mit diesem Cluster tun möchten, lesen Sie [the section called “Nächste Schritte”](#).

```
eksctl delete cluster --name my-cluster --region region-code
```

Nächste Schritte

Die folgenden Dokumentationsthemen helfen Ihnen bei der Erweiterung der Funktionalität Ihres Clusters.

- Stellen Sie eine [Beispielanwendung](#) für Ihr Cluster bereit.
- Der [IAM-Prinzipal](#), der den Cluster erstellt hat, ist der einzige Prinzipal, der Aufrufe an den Kubernetes-API-Server mit `kubectl` oder dem tätigen kann. AWS Management Console Wenn Sie möchten, dass andere IAM-Prinzipale Zugriff auf Ihren Cluster haben, müssen Sie sie hinzufügen. Weitere Informationen erhalten Sie unter [the section called “Kubernetes-API-Zugriff”](#) und [the section called “Erforderliche Berechtigungen”](#).
- Bevor Sie einen Cluster für die Produktion bereitstellen, empfehlen wir Ihnen, sich mit allen Einstellungen für [Cluster](#) und [Knoten](#) vertraut zu machen. Einige Einstellungen (z. B. die Aktivierung des SSH-Zugriffs auf EC2 Amazon-Knoten) müssen bei der Erstellung des Clusters vorgenommen werden.
- Um die Sicherheit für Ihren Cluster zu erhöhen, [konfigurieren Sie das Amazon VPC Container Networking Interface-Plugin für die Verwendung von IAM-Rollen für Servicekonten](#).

Erste Schritte mit Amazon EKS — AWS Management Console und AWS CLI

Note

In diesem Thema werden die ersten Schritte ohne EKS Auto Mode behandelt. Es verwendet verwaltete Knotengruppen, um Knoten bereitzustellen.

Der automatische Modus von EKS automatisiert Routineaufgaben für Cluster-Computing, Speicher und Netzwerke. [Erfahren Sie, wie Sie mit Amazon EKS Auto Mode beginnen](#)

[können](#). Der automatische EKS-Modus ist die bevorzugte Methode zur Bereitstellung von Knoten.

Dieses Handbuch hilft Ihnen dabei, alle erforderlichen Ressourcen für die ersten Schritte mit Amazon Elastic Kubernetes Service (Amazon EKS) mithilfe der AWS Management Console und der AWS CLI zu erstellen. In diesem Leitfaden erstellen Sie jede Ressource manuell. Am Ende dieses Tutorials haben Sie einen laufenden Amazon-EKS-Cluster, auf dem Sie Anwendungen bereitstellen können.

Die Verfahren in diesem Handbuch geben Ihnen vollständige Einsichten in die Erstellung der einzelnen Ressourcen und in die Interaktionen der Ressourcen. Wenn Sie die meisten Ressourcen lieber automatisch für Sie erstellen lassen möchten, verwenden Sie die `eksctl` CLI, um Ihren Cluster und Ihre Knoten zu erstellen. Weitere Informationen finden Sie unter [the section called “Cluster erstellen \(eksctl\)”](#).

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, müssen Sie die folgenden Werkzeuge und Ressourcen installieren und konfigurieren, die Sie zum Erstellen und Verwalten eines Amazon-EKS-Clusters benötigen.

- **AWS CLI** — Ein Befehlszeilentool für die Arbeit mit AWS Services, einschließlich Amazon EKS. Weitere Informationen finden Sie unter [Installation](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Wir empfehlen, dass Sie die AWS CLI nach der Installation ebenfalls konfigurieren. Weitere Informationen finden Sie unter [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Beachten Sie, dass AWS CLI v2 erforderlich ist, um die auf dieser Seite gezeigte Option `update-kubeconfig` zu verwenden.
- **kubectl** — Ein Befehlszeilentool für die Arbeit mit Kubernetes-Clustern. Weitere Informationen finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- **Erforderliche IAM-Berechtigungen** — Der von Ihnen verwendete IAM-Sicherheitsprinzpal muss über Berechtigungen verfügen, um mit Amazon EKS-IAM-Rollen, serviceverknüpften Rollen AWS CloudFormation, einer VPC und verwandten Ressourcen zu arbeiten. Weitere Informationen finden Sie unter [Aktionen](#) und [Verwenden von serviceverknüpften Rollen](#) im IAM-Benutzerhandbuch. Sie müssen alle Schritte in diesem Handbuch als derselbe Benutzer ausführen. Führen Sie den folgenden Befehl aus, um den aktuellen Benutzer zu überprüfen:

```
aws sts get-caller-identity
```

Wir empfehlen, dass Sie die Schritte in diesem Thema in einer Bash-Shell ausführen. Wenn Sie keine Bash-Shell verwenden, müssen einige Skriptbefehle wie Zeilenfortsetzungszeichen und die Art und Weise, wie Variablen gesetzt und verwendet werden, an Ihrer Shell angepasst werden. Darüber hinaus können die Zitier- und Escape-Regeln für Ihre Shell unterschiedlich sein. Weitere Informationen finden Sie unter [Verwenden von Anführungszeichen mit Zeichenfolgen in der AWS CLI](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

Schritt 1: Erstellen Sie Ihre Amazon-EKS-Cluster

Important

Für einen möglichst einfachen und schnellen Einstieg enthält dieses Thema Schritte zum Erstellen eines Clusters mit Standardeinstellungen. Bevor Sie einen Cluster für den Produktionseinsatz erstellen, empfehlen wir Ihnen, sich mit allen Einstellungen vertraut zu machen und einen Cluster mit den Einstellungen bereitzustellen, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie unter [the section called “Erstellen eines - Clusters”](#). Einige Einstellungen können nur aktiviert werden, wenn Sie Ihren Cluster erstellen.

1. Erstellen Sie eine Amazon VPC mit öffentlichen und privaten Subnetzen, die die Amazon-EKS-Anforderungen erfüllt. *region-code* Ersetzen Sie durch eine beliebige AWS Region, die von Amazon EKS unterstützt wird. Eine Liste der AWS Regionen finden Sie unter [Amazon EKS-Endpunkte und Kontingente](#) im AWS Allgemeinen Referenzhandbuch. Sie können *my-eks-vpc-stack* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
aws cloudformation create-stack \  
  --region region-code \  
  --stack-name my-eks-vpc-stack \  
  --template-url https://s3.us-west-2.amazonaws.com/amazon-eks/  
cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml
```

Tip

Eine Liste aller Ressourcen, die der vorherige Befehl erstellt hat, finden Sie in der AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation/>. Wählen Sie das *my-eks-vpc-stack*-Stack, und wählen Sie dann die Registerkarte Ressourcen.

2. Erstellen Sie eine Cluster-IAM-Rolle und fügen Sie ihr die erforderliche von Amazon EKS IAM verwaltete Richtlinie hinzu. Von Amazon EKS verwaltete Kubernetes-Cluster rufen in Ihrem Namen andere AWS Services auf, um die Ressourcen zu verwalten, die Sie mit dem Service verwenden.
 - a. Kopieren Sie den folgenden Inhalt in eine Datei namens *eks-cluster-role-trust-policy.json*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- b. Erstellen Sie die -Rolle.

```
aws iam create-role \
  --role-name myAmazonEKSClusterRole \
  --assume-role-policy-document file://"eks-cluster-role-trust-policy.json"
```

- c. Hängen Sie die erforderliche von Amazon EKS verwaltete IAM-Richtlinie an die Rolle an.

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy \
  --role-name myAmazonEKSClusterRole
```

3. Öffnen Sie die Amazon EKS-Konsole unter <https://console.aws.amazon.com/eks/home#/clusters>.

Stellen Sie sicher, dass die AWS Region, die oben rechts auf Ihrer Konsole angezeigt wird, die AWS Region ist, in der Sie Ihren Cluster erstellen möchten. Ist dies nicht der Fall, wählen Sie das Drop-down-Menü neben dem Namen der AWS Region aus und wählen Sie die AWS Region aus, die Sie verwenden möchten.

4. Wählen Sie Cluster erstellen. Wenn Sie diese Option nicht sehen, wählen Sie zunächst im linken Navigationsbereich Clusters aus.
 5. Führen Sie auf der Seite Configure cluster (Cluster konfigurieren) die folgenden Schritte aus:

- a. Wählen Sie Benutzerdefinierte Konfiguration und deaktivieren Sie „EKS-Automatikmodus verwenden“. (Wenn Sie einen EKS-Auto-Modus-Cluster bevorzugen, finden Sie stattdessen Informationen unter [the section called “Verwaltungskonsole”](#).)
 - b. Geben Sie einen Namen für Ihren Cluster ein, z. B. *my-cluster*. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
 - c. Wählen Sie für Cluster Service Role die Option *myAmazonEKSClusterRole*.
 - d. Belassen Sie die restlichen Einstellungen auf ihren Standardwerten und wählen Sie Weiter aus.
6. Gehen Sie auf der Seite Netzwerk angeben wie folgt vor:
- a. Wählen Sie in der Dropdown-Liste VPC (VPC) die ID der VPC aus, die Sie in einem vorherigen Schritt erstellt haben. Es ist so etwas wie ** / my-eks-vpc-stack-VPC*.
 - b. Wählen Sie die in einem vorherigen Schritt erstellten Subnetze aus der Dropdownliste Subnetze aus. Die Subnetze werden ungefähr so aussehen. ** / my-eks-vpc-stack-**
 - c. Wählen Sie die in einem vorherigen Schritt erstellte Sicherheitsgruppe aus der Dropdownliste Zusätzliche Sicherheitsgruppen aus. Es ist so etwas wie ** / my-eks-vpc-stack-ControlPlaneSecurityGroup-**.
 - d. Belassen Sie die restlichen Einstellungen auf ihren Standardwerten und wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Beobachtbarkeit konfigurieren die Option Weiter aus.
8. Wählen Sie auf der Seite Add-Ons auswählen die Option Weiter aus.

Weitere Informationen zu Add-Ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

9. Wählen Sie auf der Seite Konfigurieren ausgewählter Add-Ons-Einstellungen die Option Weiter aus.
10. Wählen Sie auf der Seite Überprüfen und erstellen die Option Erstellen aus.

Rechts neben dem Namen des Clusters wird für einige Minuten der Clusterstatus Creating angezeigt, bis der Cluster-Bereitstellungsprozess abgeschlossen ist. Fahren Sie erst mit dem nächsten Schritt fort, wenn der Status Aktiv lautet.

 Note

Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu

erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called “Unzureichende Kapazität”](#).

Schritt 2: Konfigurieren Sie Ihren Computer für die Kommunikation mit Ihrem Cluster

In diesem Abschnitt erstellen Sie eine kubeconfig-Datei für Ihren Cluster. Die Einstellungen in dieser Datei ermöglichen der kubectl-CLI die Kommunikation mit Ihrem Cluster.

Bevor Sie fortfahren, stellen Sie sicher, dass Ihre Clustererstellung in Schritt 1 erfolgreich abgeschlossen wurde.

1. Erstellen oder aktualisieren Sie eine kubeconfig-Datei für Ihren Cluster. *region-code* Ersetzen Sie es durch die AWS Region, in der Sie Ihren Cluster erstellt haben. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

Standardmäßig wird die config Datei in erstellt ~/.kube oder die Konfiguration des neuen Clusters wird zu einer vorhandenen config Datei in hinzugefügt ~/.kube.

2. Testen Sie Ihre Konfiguration.

```
kubectl get svc
```

Note

Wenn Sie Autorisierungs- oder Ressourcenfehler erhalten, finden Sie weitere Informationen unter [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#) im Thema zur Fehlerbehebung.

Eine Beispielausgabe sieht wie folgt aus.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
svc/kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	1m

Schritt 3: Erstellen von Knoten

Important

Um den Einstieg so einfach und schnell wie möglich zu gestalten, enthält dieses Thema Schritte zum Erstellen von Knoten mit überwiegend Standardeinstellungen. Bevor Sie Knoten für den Produktionseinsatz erstellen, empfehlen wir Ihnen, sich mit allen Einstellungen vertraut zu machen und Knoten mit den Einstellungen bereitzustellen, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie unter [Rechenleistung verwalten](#). Einige Einstellungen können nur aktiviert werden, wenn Sie Ihre Knoten erstellen.

Mit diesem Verfahren wird Ihr Cluster so konfiguriert, dass verwaltete Knotengruppen zum Erstellen von Knoten verwendet werden. Dabei werden die Subnetze und die Knoten-IAM-Rolle angegeben, die Sie in den vorherigen Schritten erstellt haben. Damit können Sie Amazon Linux-Anwendungen auf EC2 Amazon-Instances ausführen.

Weitere Informationen über die verschiedenen Möglichkeiten zur Konfiguration von Knoten in EKS finden Sie unter [Rechenleistung verwalten](#). Nachdem Ihr Cluster bereitgestellt wurde, können Sie andere Knotentypen hinzufügen. Obwohl in diesem Handbuch nicht behandelt, können Sie Ihrem Cluster auch [selbstverwaltete Windows](#)- und [Bottlerocket](#)-Knoten hinzufügen.

So erstellen Sie Ihre verwaltete EC2 Linux-Knotengruppe

1. Erstellen Sie eine Knoten-IAM-Rolle und fügen Sie ihr die erforderliche von Amazon EKS IAM verwaltete Richtlinie hinzu. Der Amazon EKS Node kubelet Daemon ruft in Ihrem Namen AWS APIs an. Knoten erhalten über ein IAM-Instance-Profil und zugehörige Richtlinien Berechtigungen für diese API-Aufrufe.
 - a. Kopieren Sie den folgenden Inhalt in eine Datei namens `node-role-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```



```
"Effect": "Allow",
"Principal": {
  "Service": "ec2.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
```

b. Erstellen Sie die Knoten-IAM-Rolle.

```
aws iam create-role \
  --role-name myAmazonEKSNodeRole \
  --assume-role-policy-document file://\"node-role-trust-policy.json\"
```

c. Hängen Sie die erforderlichen verwalteten IAM-Richtlinien an die Rolle an.

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy \
  --role-name myAmazonEKSNodeRole
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly \
  --role-name myAmazonEKSNodeRole
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
  --role-name myAmazonEKSNodeRole
```

d. Öffnen Sie die Amazon EKS-Konsole unter <https://console.aws.amazon.com/eks/home#/clusters>.

e. Wählen Sie den Namen des Clusters aus, den Sie in [Schritt 1: Amazon EKS-Cluster erstellen](#) erstellt haben, z. **my-cluster** B.

f. Gehen Sie auf der **my-cluster** Seite wie folgt vor:

g. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.

h. Wählen Sie Add Node Group (Knotengruppe hinzufügen) aus.

2. Führen Sie auf der Seite Configure Node Group (Knotengruppe konfigurieren) die folgenden Schritte aus:

a. Für Name geben Sie einen eindeutigen Namen für die verwaltete Knotengruppe ein, wie z. B. **my-nodegroup**. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.

- b. Wählen Sie als Node IAM-Rollenname die *myAmazonEKSTaskRole* Rolle aus, die Sie in einem vorherigen Schritt erstellt haben. Wir empfehlen, dass jede Knotengruppe ihre eigene eindeutige IAM-Rolle verwendet.
- c. Wählen Sie Weiter aus.
3. Akzeptieren Sie auf der Seite Computing- und Skalierungskonfiguration festlegen die Standardwerte und wählen Sie Weiter aus.
4. Akzeptieren Sie auf der Seite Netzwerk angeben die Standardwerte und wählen Sie Weiter aus.
5. Überprüfen Sie auf der Seite Review and create (Überprüfen und Erstellen) die Konfiguration der verwalteten Knoten, und wählen Sie Create (Erstellen).
6. Nach einigen Minuten ändert sich der Status im Abschnitt Konfiguration der Knotengruppe von Wird erstellt auf Aktiv. Fahren Sie erst mit dem nächsten Schritt fort, wenn der Status Aktiv lautet.

Schritt 4: Ressourcen anzeigen

Sie können Ihre Knoten und Kubernetes-Workloads anzeigen.

1. Wählen Sie im linken Navigationsbereich Cluster aus. Wählen Sie in der Clusterliste den Namen des Clusters aus, den Sie erstellt haben, z. *my-cluster* B.
2. Wählen Sie auf der *my-cluster* Seite Folgendes aus:
 - a. Registerkarte Compute (Datenverarbeitung) – Es wird eine Liste der Knoten angezeigt, die für den Cluster bereitgestellt wurden. Sie können den Namen eines Knotens auswählen, um weitere Informationen darüber anzuzeigen.
 - b. Registerkarte „Ressourcen“ — Sie sehen alle Kubernetes-Ressourcen, die standardmäßig in einem Amazon EKS-Cluster bereitgestellt werden. Wählen Sie einen Ressourcentyp in der Konsole aus, um mehr über ihn zu erfahren.

Schritt 5: Löschen von Ressourcen

Nachdem Sie mit dem Cluster und den Knoten fertig sind, die Sie für dieses Tutorial erstellt haben, sollten Sie die von Ihnen erstellten Ressourcen löschen. Wenn Sie vor dem Löschen der Ressourcen mehr mit diesem Cluster tun möchten, lesen Sie [the section called “Nächste Schritte”](#).

1. Löschen Sie alle Knotengruppenprofile, die Sie erstellt haben.
 - a. Öffnen Sie die Amazon EKS-Konsole unter <https://console.aws.amazon.com/eks/home#/clusters>.

- b. Wählen Sie im linken Navigationsbereich Cluster aus. Wählen Sie in der Liste der Cluster *my-cluster*.
 - c. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
 - d. Wenn Sie eine Knotengruppe erstellt haben, wählen Sie die *my-nodegroup* Knotengruppe und dann Löschen aus. Geben Sie *my-nodegroup* ein und klicken Sie auf Delete (Löschen).
 - e. Fahren Sie erst fort, wenn die Knotengruppenprofile gelöscht sind.
2. Löschen Sie den -Cluster.
- a. Wählen Sie im linken Navigationsbereich die Option Cluster aus. Wählen Sie in der Liste der Cluster *my-cluster*.
 - b. Wählen Sie Delete cluster (Cluster löschen) aus.
 - c. Geben Sie *my-cluster* ein und wählen Sie Delete (Löschen). Fahren Sie nicht fort, bis der Cluster gelöscht ist.
3. Löschen Sie den AWS CloudFormation VPC-Stack, den Sie erstellt haben.
- a. Öffnen Sie die CloudFormation Konsole unter. <https://console.aws.amazon.com/cloudformation/>
 - b. Wählen Sie den *my-eks-vpc-stack*-Stack und anschließend Delete Löschen aus.
 - c. Wählen Sie im *my-eks-vpc-stack* Bestätigungsdiaologfeld für das Löschen die Option Stapel löschen aus.
4. Löschen Sie die IAM-Rollen, die Sie erstellt haben.
- a. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
 - b. Wählen Sie im linken Navigationsbereich Roles aus.
 - c. Wählen Sie jede Rolle, die Sie erstellt haben *myAmazonEKSClusterRole*, aus der Liste aus (sowie *myAmazonEKSNodeRole*) aus. Klicken Sie auf Delete (Löschen), geben Sie den angeforderten Bestätigungstext ein und wählen Sie Delete (Löschen) aus.

Nächste Schritte

Die folgenden Dokumentationsthemen helfen Ihnen bei der Erweiterung der Funktionalität Ihres Clusters.

- Der [IAM-Prinzipal](#), der den Cluster erstellt hat, ist der einzige Prinzipal, der Aufrufe an den Kubernetes-API-Server mit `kubectl` oder dem tätigen kann. AWS Management Console Wenn Sie möchten, dass andere IAM-Prinzipale Zugriff auf Ihren Cluster haben, müssen Sie sie

hinzufügen. Weitere Informationen erhalten Sie unter [the section called “Kubernetes-API-Zugriff”](#) und [the section called “Erforderliche Berechtigungen”](#).

- Stellen Sie eine [Beispielanwendung](#) für Ihr Cluster bereit.
- Bevor Sie einen Cluster für die Produktion bereitstellen, empfehlen wir Ihnen, sich mit allen Einstellungen für [Cluster](#) und [Knoten](#) vertraut zu machen. Einige Einstellungen (z. B. die Aktivierung des SSH-Zugriffs auf EC2 Amazon-Knoten) müssen bei der Erstellung des Clusters vorgenommen werden.
- Um die Sicherheit für Ihren Cluster zu erhöhen, [konfigurieren Sie das Amazon VPC Container Networking Interface-Plugin für die Verwendung von IAM-Rollen für Servicekonten](#).

Automatisieren Sie die Cluster-Infrastruktur mit dem EKS Auto Mode

EKS Auto Mode erweitert die AWS Verwaltung von Kubernetes-Clustern über den Cluster selbst hinaus, sodass AWS Sie auch die Infrastruktur einrichten und verwalten können, die den reibungslosen Betrieb Ihrer Workloads ermöglicht. Sie können wichtige Infrastrukturentscheidungen delegieren und das Fachwissen von for Operations nutzen. AWS day-to-day Die Cluster-Infrastruktur, die von verwaltet wird, AWS umfasst viele Kubernetes-Funktionen als Kernkomponenten, im Gegensatz zu Add-Ons wie Compute-Autoscaling, Pod- und Service-Networking, Anwendungslastausgleich, Cluster-DNS, Blockspeicher und GPU-Unterstützung.

Zu Beginn können Sie einen neuen EKS-Auto-Modus-Cluster bereitstellen oder den EKS Auto Mode auf einem vorhandenen Cluster aktivieren. Sie können Ihre EKS-Auto-Mode-Cluster mithilfe von eksctl, der AWS CLI, dem, EKS oder Ihren bevorzugten AWS Management Console infrastructure-as-code Tools bereitstellen APIs, aktualisieren oder ändern.

Mit dem automatischen Modus von EKS können Sie Ihre bevorzugten Kubernetes-kompatiblen Tools weiterhin verwenden. Der EKS Auto Mode lässt sich in AWS Dienste wie Amazon EC2, Amazon EBS und ELB integrieren und nutzt AWS Cloud-Ressourcen, die bewährten Methoden folgen. Diese Ressourcen werden automatisch skaliert, kostenoptimiert und regelmäßig aktualisiert, um die Betriebskosten und den Overhead zu minimieren.

Features

Der EKS-Automatikmodus bietet die folgenden Funktionen auf hohem Niveau:

Optimieren Sie das Kubernetes-Clustermanagement: Der EKS Auto Mode optimiert das EKS-Management, indem er produktionsbereite Cluster mit minimalem Betriebsaufwand bereitstellt. Mit dem automatischen Modus von EKS können Sie anspruchsvolle, dynamische Workloads souverän ausführen, ohne dass tiefes EKS-Fachwissen erforderlich ist.

Anwendungsverfügbarkeit: Der automatische Modus von EKS fügt je nach den Anforderungen Ihrer Kubernetes-Anwendungen dynamisch Knoten in Ihrem EKS-Cluster hinzu oder entfernt sie. Dadurch wird der Bedarf an manueller Kapazitätsplanung minimiert und die Anwendungsverfügbarkeit sichergestellt.

Effizienz: Der automatische Modus von EKS wurde entwickelt, um die Rechenkosten zu optimieren und gleichzeitig die Flexibilität zu wahren, die sich aus Ihren Anforderungen NodePool und den

Workload-Anforderungen ergibt. Außerdem beendet er ungenutzte Instanzen und konsolidiert Workloads auf anderen Knoten, um die Kosteneffizienz zu verbessern.

Sicherheit: EKS Auto Mode verwendet AMIs, die für Ihre Knoten als unveränderlich behandelt werden. Diese AMIs setzen gesperrte Software durch, ermöglichen SELinux obligatorische Zugriffskontrollen und bieten schreibgeschützte Root-Dateisysteme. Darüber hinaus haben Knoten, die im automatischen Modus von EKS gestartet werden, eine maximale Lebensdauer von 21 Tagen (die Sie reduzieren können). Danach werden sie automatisch durch neue Knoten ersetzt. Dieser Ansatz verbessert Ihre Sicherheitslage, indem er die Knoten regelmäßig wechselt und sich dabei an bewährten Verfahren orientiert, die bereits von vielen Kunden übernommen wurden.

Automatisierte Upgrades: Der automatische Modus von EKS hält Ihren Kubernetes-Cluster, Ihre Knoten und die zugehörigen Komponenten auf dem neuesten Stand und berücksichtigt gleichzeitig Ihre konfigurierten Pod-Disruption-Budgets (PDBs) und NodePool Disruption-Budgets (). NDBs Bis zur maximalen Lebensdauer von 21 Tagen kann ein Eingreifen erforderlich sein, wenn Blockierungen PDBs oder andere Konfigurationen Updates verhindern.

Verwaltete Komponenten: Der automatische Modus von EKS umfasst Kubernetes- und AWS Cloud-Funktionen als Kernkomponenten, die andernfalls als Add-Ons verwaltet werden müssten. Dazu gehört die integrierte Unterstützung für Pod-IP-Adresszuweisungen, Pod-Netzwerkrichtlinien, lokale DNS-Dienste, GPU-Plug-ins, Health Checker und EBS CSI-Speicher.

Anpassbar NodePools und NodeClasses: Wenn Ihre Arbeitslast Änderungen an den Speicher-, Rechen- oder Netzwerkkonfigurationen erfordert, können Sie benutzerdefinierte Konfigurationen erstellen NodePools und den EKS-Automatikmodus NodeClasses verwenden. Sie sollten die NodePools Standardkonfigurationen zwar nicht bearbeiten NodeClasses, aber Sie können neue benutzerdefinierte Konfigurationen NodePools oder NodeClasses zusätzlich zu den Standardkonfigurationen hinzufügen, um Ihren spezifischen Anforderungen gerecht zu werden.

Automatisierte Komponenten

Der EKS-Automatikmodus optimiert den Betrieb Ihrer Amazon EKS-Cluster durch die Automatisierung wichtiger Infrastrukturkomponenten. Durch die Aktivierung des EKS Auto Mode wird der Aufwand für die Verwaltung Ihrer EKS-Cluster weiter reduziert.

Im Folgenden finden Sie eine Liste der Komponenten der Datenebene, die automatisiert sind:

- **Datenverarbeitung:** Bei vielen Workloads können Sie mit dem automatischen Modus von EKS viele Aspekte der Datenverarbeitung für Ihre EKS-Cluster vergessen. Dazu zählen:

- **Knoten:** Die Knoten im automatischen Modus von EKS sind so konzipiert, dass sie wie Appliances behandelt werden können. Der EKS-Automatikmodus macht Folgendes:
 - Wählt ein geeignetes AMI aus, das mit vielen Diensten konfiguriert ist, die für die Ausführung Ihrer Workloads ohne Eingreifen erforderlich sind.
 - Sperrt den Zugriff auf Dateien im AMI mithilfe des SELinux Erzwingungsmodus und eines schreibgeschützten Root-Dateisystems.
 - Verhindert den direkten Zugriff auf die Knoten, indem der SSH- oder SSM-Zugriff verboten wird.
 - Beinhaltet GPU-Unterstützung mit separaten Kernel-Treibern und Plug-ins für NVIDIA und Neuron GPUs, was Hochleistungs-Workloads ermöglicht.
 - Verarbeitet automatisch Benachrichtigungen über [Unterbrechungen der EC2 EC2 Spot-Instance](#) und Instance-Integritätsereignisse
- **Automatische Skalierung:** Der EKS Auto Mode stützt sich auf die automatische Skalierung von [Karpenter](#) und überwacht Pods, die nicht geplant werden können, und ermöglicht die Bereitstellung neuer Knoten, um diese Pods auszuführen. Wenn Workloads beendet werden, unterbricht und beendet der EKS Auto Mode dynamisch Knoten, wenn sie nicht mehr benötigt werden, wodurch die Ressourcennutzung optimiert wird.
- **Upgrades:** Die Übernahme der Kontrolle über Ihre Knoten optimiert die Fähigkeit von EKS Auto Mode, Sicherheitspatches sowie Betriebssystem- und Komponenten-Upgrades nach Bedarf bereitzustellen. Diese Upgrades sind so konzipiert, dass Ihre Workloads nur minimal unterbrochen werden. Der automatische EKS-Modus erzwingt eine maximale Knotenlebensdauer von 21 Tagen, um sicherzustellen, dass up-to-date Software und APIs
- **Lastenausgleich:** Der EKS Auto Mode optimiert den Lastenausgleich durch die Integration mit dem Elastic Load Balancing Service von Amazon und automatisiert die Bereitstellung und Konfiguration von Load Balancern für Kubernetes Services und Ingress-Ressourcen. Er unterstützt erweiterte Funktionen sowohl für Application als auch für Network Load Balancer, verwaltet deren Lebenszyklus und skaliert sie entsprechend den Cluster-Anforderungen. Diese Integration bietet eine einsatzbereite Load-Balancing-Lösung, die den AWS Best Practices entspricht, sodass Sie sich auf Anwendungen statt auf das Infrastrukturmanagement konzentrieren können.
- **Speicher:** Der automatische Modus von EKS konfiguriert temporären Speicher für Sie, indem er Volumetypen, Volume-Größen, Verschlüsselungsrichtlinien und Löschrichtlinien bei Kündigung des Knotens einrichtet.

- **Netzwerk:** Der EKS-Automatikmodus automatisiert wichtige Netzwerkaufgaben für die Pod- und Service-Konnektivität. Dazu gehören IPv4 IPv6 /-Unterstützung und die Verwendung sekundärer CIDR-Blöcke zur Erweiterung von IP-Adressräumen.
- **Identity and Access Management:** Sie müssen den EKS Pod Identity Agent nicht auf EKS-Auto-Mode-Clustern installieren.

Weitere Informationen zu diesen Komponenten finden Sie unter [the section called “Funktionsweise”](#).

Konfiguration

Der automatische EKS-Modus verwaltet zwar die meisten Ihrer Datenebenendienste effektiv, ohne dass Sie eingreifen müssen, aber es kann vorkommen, dass Sie das Verhalten einiger dieser Dienste ändern möchten. Sie können die Konfiguration Ihrer EKS-Auto-Mode-Cluster auf folgende Weise ändern:

- **Kubernetes DaemonSets:** Anstatt die auf Ihren Knoten installierten Dienste zu ändern, können Sie stattdessen Kubernetes-Daemonsets verwenden. Daemonsets sind so konzipiert, dass sie von Kubernetes verwaltet werden können, aber auf jedem Knoten im Cluster ausgeführt werden. Auf diese Weise können Sie spezielle Dienste zur Überwachung oder sonstigen Überwachung Ihrer Knoten hinzufügen.
- **Benutzerdefiniert NodePools und NodeClasses:** Standard NodePools und NodeClasses werden vom EKS Auto Mode konfiguriert und sollten nicht bearbeitet werden. Um das Verhalten von Knoten anzupassen, können Sie zusätzliche NodePools oder NodeClasses für folgende Anwendungsfälle erstellen:
 - Auswahl bestimmter Instance-Typen (z. B. beschleunigte Prozessoren oder EC2 Spot-Instances).
 - Isolieren von Workloads zu Sicherheits- oder Kostenverfolgungszwecken.
 - Konfiguration kurzlebiger Speichereinstellungen wie IOPS, Größe und Durchsatz.
- **Lastenausgleich:** Einige Dienste, wie z. B. Load Balancing, die EKS Auto Mode als Kubernetes-Objekte ausführt, können direkt auf Ihren EKS-Auto-Mode-Clustern konfiguriert werden.

Weitere Informationen zu Optionen für die Konfiguration des EKS Auto Mode finden Sie unter [the section called “Konfiguration”](#)

Erstellen Sie einen Cluster mit Amazon EKS Auto Mode

In diesem Kapitel wird erklärt, wie Sie mithilfe verschiedener Tools und Schnittstellen einen Amazon EKS-Cluster mit aktiviertem Auto-Modus erstellen. Der automatische Modus vereinfacht die Cluster-Erstellung, indem er die Rechen-, Netzwerk- und Speicherinfrastruktur des Clusters automatisch konfiguriert und verwaltet. Sie erfahren, wie Sie mit der AWS CLI oder dem Befehlszeilentool `eksctl` einen Auto-Mode-Cluster erstellen. AWS Management Console

Note

Der EKS Auto Mode erfordert Kubernetes Version 1.29 oder höher. Der automatische EKS-Modus ist in den `ap-southeast-7` Regionen oder nicht verfügbar. `mx-central-1` AWS

Wählen Sie Ihr bevorzugtes Tool je nach Ihren Bedürfnissen: Es AWS Management Console bietet eine visuelle Oberfläche, die sich ideal eignet, um mehr über die Funktionen des automatischen Modus von EKS zu erfahren und individuelle Cluster zu erstellen. Die AWS CLI eignet sich am besten für Skript- und Automatisierungsaufgaben, insbesondere bei der Integration der Clustererstellung in bestehende Workflows oder CI/CD-Pipelines. Die `eksctl`-CLI bietet ein Kubernetes-natives Erlebnis und wird Benutzern empfohlen, die mit Kubernetes-Tools vertraut sind und vereinfachte Befehlszeilenoperationen mit sinnvollen Standardeinstellungen wünschen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die erforderlichen Voraussetzungen installiert und konfiguriert haben, einschließlich der entsprechenden IAM-Berechtigungen zum Erstellen von EKS-Clustern. Informationen zur Installation von CLI-Tools wie `kubectl` `aws eksctl`, und finden Sie unter [Einrichten](#).

Sie können die AWS CLI AWS Management Console, oder `eksctl` CLI verwenden, um einen Cluster mit Amazon EKS Auto Mode zu erstellen.

Themen

- [Erstellen Sie einen EKS-Auto-Mode-Cluster mit der `eksctl`-CLI](#)
- [Erstellen Sie einen EKS-Auto-Mode-Cluster mit der AWS CLI](#)
- [Erstellen Sie einen EKS-Auto-Mode-Cluster mit dem AWS Management Console](#)

Erstellen Sie einen EKS-Auto-Mode-Cluster mit der eksctl-CLI

In diesem Thema erfahren Sie, wie Sie mithilfe der eksctl-Befehlszeilenschnittstelle (CLI) einen Amazon EKS Auto Mode-Cluster erstellen. Sie können einen Auto-Mode-Cluster erstellen, indem Sie entweder einen einzigen CLI-Befehl ausführen oder eine YAML-Konfigurationsdatei anwenden. Beide Methoden bieten dieselbe Funktionalität, wobei der YAML-Ansatz eine detailliertere Steuerung der Clustereinstellungen ermöglicht.

Die eksctl-CLI vereinfacht den Prozess der Erstellung und Verwaltung von EKS-Auto-Mode-Clustern, indem sie die Erstellung und Konfiguration der zugrunde liegenden AWS Ressourcen übernimmt. Bevor Sie fortfahren, stellen Sie sicher, dass Sie die erforderlichen AWS Anmeldeinformationen und Berechtigungen auf Ihrem lokalen Computer konfiguriert haben. In diesem Handbuch wird davon ausgegangen, dass Sie mit den grundlegenden Konzepten von Amazon EKS vertraut sind und die erforderlichen CLI-Tools bereits installiert haben.

Note

Sie müssen Version 0.195.0 oder höher von eksctl installieren. Weitere Informationen finden Sie unter [eksctl releases](#) on GitHub

Erstellen Sie einen EKS-Auto-Mode-Cluster mit einem CLI-Befehl

Sie müssen die eksctl Tools aws und D installiert haben. Sie müssen bei der AWS CLI angemeldet sein und über ausreichende Berechtigungen verfügen, um AWS Ressourcen wie EC2 Instanzen, EC2 Netzwerke, EKS-Cluster und IAM-Rollen zu verwalten. Weitere Informationen finden Sie unter [Einrichten](#).

Führen Sie den folgenden Befehl aus, um einen neuen EKS-Auto-Mode-Cluster mit zu erstellen

```
eksctl create cluster --name=<cluster-name> --enable-auto-mode
```

Erstellen Sie einen EKS-Auto-Mode-Cluster mit einer YAML-Datei

Sie müssen die aws und eksctl -Tools installiert haben. Sie müssen bei der AWS CLI angemeldet sein und über ausreichende Berechtigungen verfügen, um AWS Ressourcen wie EC2 Instanzen, EC2 Netzwerke, EKS-Cluster und IAM-Rollen zu verwalten. Weitere Informationen finden Sie unter [Einrichten](#).

Sehen Sie sich die Konfigurationsoptionen für den automatischen EKS-Modus in der folgenden ClusterConfig Beispielressource an. Die vollständige ClusterConfig Spezifikation finden Sie in der [eksctl-Dokumentation](#).

AWS schlägt vor, den EKS-Automatikmodus zu aktivieren. Wenn Sie zum ersten Mal einen EKS-Auto-Modus-Cluster erstellen, lassen Sie den Wert `nodeRoleARN` unspecified stehen, um eine Node-IAM-Rolle für den EKS-Auto-Modus zu erstellen. Wenn Sie bereits eine Node-IAM-Rolle in Ihrem AWS Konto haben, AWS schlägt vor, diese wiederzuverwenden.

AWS schlägt vor, keinen Wert für `nodePools` anzugeben. Der automatische Modus von EKS erstellt Standard-Knotenpools. Sie können die Kubernetes-API verwenden, um zusätzliche Knotenpools zu erstellen.

```
# cluster.yaml
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: <cluster-name>
  region: <aws-region>

iam:
  # ARN of the Cluster IAM Role
  # optional, eksctl creates a new role if not supplied
  # suggested to use one Cluster IAM Role per account
  serviceRoleARN: <arn-cluster-iam-role>

autoModeConfig:
  # defaults to false
  enabled: boolean
  # optional, defaults to [general-purpose, system].
  # suggested to leave unspecified
  # To disable creation of nodePools, set it to the empty array ([]).
  nodePools: []string
  # optional, eksctl creates a new role if this is not supplied
  # and nodePools are present.
  nodeRoleARN: string
```

Speichern Sie die ClusterConfig Datei unter und verwenden Sie den folgenden Befehl `cluster.yaml`, um den Cluster zu erstellen:

```
eksctl create cluster -f cluster.yaml
```

Erstellen Sie einen EKS-Auto-Mode-Cluster mit der AWS CLI

EKS-Auto-Mode-Cluster automatisieren routinemäßige Clusterverwaltungsaufgaben für Datenverarbeitung, Speicher und Netzwerke. EKS-Auto-Mode-Cluster erkennen beispielsweise automatisch, wenn zusätzliche Knoten erforderlich sind, und stellen neue EC2 Instanzen bereit, um den Workload-Anforderungen gerecht zu werden.

Dieses Thema führt Sie durch die Erstellung eines neuen EKS-Auto-Mode-Clusters mithilfe der AWS CLI und optional durch die Bereitstellung eines Beispiel-Workloads.

Voraussetzungen

- Die neueste Version der AWS Befehlszeilenschnittstelle (AWS CLI) ist auf Ihrem Gerät installiert und konfiguriert. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version`. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration](#) mit `aws configure` im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- Melden Sie sich mit ausreichenden IAM-Berechtigungen bei der CLI an, um AWS Ressourcen wie IAM-Richtlinien, IAM-Rollen und EKS-Cluster zu erstellen.
- Das kubectl-Befehlszeilentool, das auf Ihrem Gerät installiert ist. AWS schlägt vor, dass Sie dieselbe kubectl-Version wie die Kubernetes-Version Ihres EKS-Clusters verwenden. Informationen zur Installation oder zum Upgrade von kubectl finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#)

VPC-Subnetze angeben

Amazon EKS Auto Mode stellt Knoten in VPC-Subnetzen bereit. Beim Erstellen eines EKS-Clusters müssen Sie die VPC-Subnetze angeben, in denen die Knoten bereitgestellt werden. Sie können die Standard-VPC-Subnetze in Ihrem AWS Konto verwenden oder eine dedizierte VPC für kritische Workloads erstellen.

- AWS schlägt vor, eine dedizierte VPC für Ihren Cluster zu erstellen. Weitere Informationen erhalten Sie unter [the section called “Erstellen einer VPC”](#).
- Die EKS-Konsole hilft bei der Erstellung einer neuen VPC. Weitere Informationen erhalten Sie unter [the section called “Verwaltungskonsole”](#).

- Alternativ können Sie die Standard-VPC Ihres AWS Kontos verwenden. Verwenden Sie die folgenden Anweisungen, um das IDs Subnetz zu finden.

So finden Sie das Subnetz IDs Ihrer Standard-VPC

Verwenden der AWS CLI:

1. Führen Sie den folgenden Befehl aus, um die Standard-VPC und ihre Subnetze aufzulisten:

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=$(aws ec2 describe-vpcs --query 'Vpcs[?IsDefault==`true`].VpcId' --output text)" --query 'Subnets[*].{ID:SubnetId,AZ:AvailabilityZone}' --output table
```

2. Speichern Sie die Ausgabe und notieren Sie sich das Subnetz. IDs

Beispielausgabe:

```
-----
| DescribeSubnets |
|-----|
| SubnetId | AvailabilityZone |
|-----|-----|
| subnet-012345678 | us-west-2a |
| subnet-234567890 | us-west-2b |
| subnet-345678901 | us-west-2c |
|-----|-----|
```

IAM-Rollen für EKS-Cluster im automatischen Modus

Cluster-IAM-Rolle

Für den automatischen EKS-Modus ist eine Cluster-IAM-Rolle erforderlich, um Aktionen in Ihrem AWS Konto auszuführen, z. B. die Bereitstellung neuer Instanzen. EC2 Sie müssen diese Rolle erstellen, um EKS die erforderlichen Berechtigungen zu erteilen. AWS empfiehlt, die folgenden AWS verwalteten Richtlinien an die Cluster-IAM-Rolle anzuhängen:

- [EKSCoordinateAmazon-Richtlinie](#)
- [AmazonEKSBLOCKStoragePolicy](#)
- [AmazonEKSLoadBalancingPolicy](#)

- [EKSNetworkingAmazon-Richtlinie](#)
- [EKSClusterAmazon-Richtlinie](#)

IAM-Rolle des Knotens

Wenn Sie einen EKS-Auto-Mode-Cluster erstellen, geben Sie eine Node-IAM-Rolle an. Wenn der automatische Modus von EKS Knoten zur Verarbeitung ausstehender Workloads erstellt, wird jedem neuen EC2 Instanzknoten die Node-IAM-Rolle zugewiesen. Diese Rolle ermöglicht dem Knoten die Kommunikation mit EKS, wird aber im Allgemeinen nicht von Workloads aufgerufen, die auf dem Knoten ausgeführt werden.

Wenn Sie Berechtigungen für Workloads gewähren möchten, die auf einem Knoten ausgeführt werden, verwenden Sie EKS Pod Identity. Weitere Informationen finden Sie unter [the section called "Pod-Identität"](#).

Sie müssen diese Rolle erstellen und die folgende AWS verwaltete Richtlinie anhängen:

- [AmazonEKSWorkerNodeMinimalPolicy](#)
- [AmazonEC2ContainerRegistryPullOnly](#)

Serviceverknüpfte Rolle

Für den automatischen Modus von EKS ist außerdem eine serviceverknüpfte Rolle erforderlich, die automatisch von AWS erstellt und konfiguriert wird. Weitere Informationen finden Sie unter [AWSServiceRoleForAmazonEKS](#).

Erstellen Sie eine EKS-Cluster-IAM-Rolle im automatischen Modus

Schritt 1: Erstellen Sie die Vertrauensrichtlinie

Erstellen Sie eine Vertrauensrichtlinie, die es dem Amazon EKS-Service ermöglicht, die Rolle zu übernehmen. Speichern Sie die Richtlinie als `trust-policy.json`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      }
    }
  ]
}
```

```
    },  
    "Action": [  
        "sts:AssumeRole",  
        "sts:TagSession"  
    ]  
  }  
]  
}
```

Schritt 2: Erstellen Sie die IAM-Rolle

Verwenden Sie die Vertrauensrichtlinie, um die Cluster-IAM-Rolle zu erstellen:

```
aws iam create-role \  
  --role-name AmazonEKSAutoClusterRole \  
  --assume-role-policy-document file://trust-policy.json
```

Schritt 3: Notieren Sie sich den Rollen-ARN

Rufen Sie den ARN der neuen Rolle ab und speichern Sie ihn zur Verwendung in nachfolgenden Schritten:

```
aws iam get-role --role-name AmazonEKSAutoClusterRole --query "Role.Arn" --output text
```

Schritt 4: Erforderliche Richtlinien anhängen

Fügen Sie der Cluster-IAM-Rolle die folgenden AWS verwalteten Richtlinien hinzu, um die erforderlichen Berechtigungen zu gewähren:

EKSClusterAmazon-Richtlinie:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSClusterPolicy
```

EKSComputeAmazon-Richtlinie:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSClusterPolicy
```

Amazon EKSBLOCK StoragePolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSBlockStoragePolicy
```

Amazon EKSLoad BalancingPolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSLoadBalancingPolicy
```

EKSNetworkingAmazon-Richtlinie:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSNetworkingPolicy
```

Erstellen Sie eine IAM-Rolle für einen EKS-Knoten im automatischen Modus

Schritt 1: Erstellen Sie die Vertrauensrichtlinie

Erstellen Sie eine Vertrauensrichtlinie, die es dem Amazon EKS-Service ermöglicht, die Rolle zu übernehmen. Speichern Sie die Richtlinie als `alsnode-trust-policy.json`:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "ec2.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

Schritt 2: Erstellen Sie die Node-IAM-Rolle

Verwenden Sie die `node-trust-policyJSON`-Datei aus dem vorherigen Schritt, um zu definieren, welche Entitäten die Rolle übernehmen können. Führen Sie den folgenden Befehl aus, um die Node-IAM-Rolle zu erstellen:


```
aws iam create-role \  
  --role-name AmazonEKSAutoNodeRole \  
  --assume-role-policy-document file:///node-trust-policy.json
```

Schritt 3: Notieren Sie sich den Rollen-ARN

Rufen Sie nach dem Erstellen der Rolle den ARN der Node-IAM-Rolle ab und speichern Sie ihn. Sie benötigen diesen ARN in den nachfolgenden Schritten. Verwenden Sie den folgenden Befehl, um den ARN abzurufen:

```
aws iam get-role --role-name AmazonEKSAutoNodeRole --query "Role.Arn" --output text
```

Schritt 4: Erforderliche Richtlinien anhängen

Fügen Sie der Node-IAM-Rolle die folgenden AWS verwalteten Richtlinien hinzu, um die erforderlichen Berechtigungen bereitzustellen:

Amazon EKSWorker NodeMinimalPolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoNodeRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy
```

Amazon EC2 ContainerRegistryPullOnly:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoNodeRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEC2ContainerRegistryPullOnly
```

Erstellen Sie einen EKS-Auto-Modus-Cluster

Übersicht

Um einen EKS-Auto-Mode-Cluster mit der AWS CLI zu erstellen, benötigen Sie die folgenden Parameter:

- `cluster-name`: Der Name des Clusters.
- `k8s-version`: Die Kubernetes-Version (z. B. 1.31).
- `subnet-ids`: In den vorherigen Schritten IDs identifiziertes Subnetz.

- `cluster-role-arn`: ARN der Cluster-IAM-Rolle.
- `node-role-arn`: ARN der Node-IAM-Rolle.

Standard-Cluster-Konfigurationen

Überprüfen Sie diese Standardwerte und Funktionen, bevor Sie den Cluster erstellen:

- `nodePools`: Der automatische Modus von EKS umfasst allgemeine und systemeigene Standard-Knotenpools. Erfahren Sie mehr über [Node Pools](#).

Hinweis: Knotenpools im EKS Auto Mode unterscheiden sich von Amazon EKS Managed Node Groups, können aber gleichzeitig im selben Cluster existieren.

- `computeConfig.enabled`: Automatisiert routinemäßige Rechenaufgaben wie das Erstellen und Löschen EC2 von Instances.
- `kubernetesNetworkConfig.elasticLoadBalancing.enabled`: Automatisiert Load-Balancing-Aufgaben, einschließlich des Erstellens und Löschens von Elastic Load Balancers.
- `storageConfig.blockStorage.enabled`: Automatisiert Speicheraufgaben wie das Erstellen und Löschen von Amazon EBS-Volumes.
- `accessConfig.authenticationMode`: Erfordert EKS-Zugriffseinträge. Erfahren Sie mehr über die [EKS-Authentifizierungsmodi](#).

Führen Sie den Befehl aus

Verwenden Sie den folgenden Befehl, um den Cluster zu erstellen:

```
aws eks create-cluster \
  --region ${AWS_REGION} \
  --cli-input-json \
  "{
    \"name\": \"${CLUSTER_NAME}\",
    \"version\": \"${K8S_VERSION}\",
    \"roleArn\": \"${CLUSTER_ROLE_ARN}\",
    \"resourcesVpcConfig\": {
      \"subnetIds\": ${SUBNETS_JSON},
      \"endpointPublicAccess\": true,
      \"endpointPrivateAccess\": true
    },
  },
```

```
\ "computeConfig\": {
  \ "enabled\": true,
  \ "nodeRoleArn\": \"${NODE_ROLE_ARN}\",
  \ "nodePools\": [\"general-purpose\", \"system\"]
},
\ "kubernetesNetworkConfig\": {
  \ "elasticLoadBalancing\": {
    \ "enabled\": true
  }
},
\ "storageConfig\": {
  \ "blockStorage\": {
    \ "enabled\": true
  }
},
\ "accessConfig\": {
  \ "authenticationMode\": \"API\"
}
}
```

Überprüfen Sie den Clusterstatus

Schritt 1: Überprüfen Sie die Clustererstellung

Führen Sie den folgenden Befehl aus, um den Status Ihres Clusters zu überprüfen. Die Clustererstellung dauert in der Regel etwa 15 Minuten:

```
aws eks describe-cluster --name "${CLUSTER_NAME}" --output json
```

Schritt 2: Kubeconfig aktualisieren

Sobald der Cluster bereit ist, aktualisieren Sie Ihre lokale kubeconfig-Datei, um die Kommunikation mit dem Cluster `kubectl` zu ermöglichen. Diese Konfiguration verwendet die AWS CLI für die Authentifizierung.

```
aws eks update-kubeconfig --name "${CLUSTER_NAME}"
```

Schritt 3: Überprüfen Sie die Knotenpools

Führen Sie die Knotenpools in Ihrem Cluster mit dem folgenden Befehl auf:

```
kubectl get nodepools
```

Nächste Schritte

- Erfahren Sie, wie Sie [einen Beispiel-Workload auf Ihrem neuen EKS-Auto-Mode-Cluster bereitstellen](#).

Erstellen Sie einen EKS-Auto-Mode-Cluster mit dem AWS Management Console

Das Erstellen eines EKS-Auto-Modus-Clusters in der AWS Management Console erfordert weniger Konfiguration als andere Optionen. EKS lässt sich in AWS IAM- und VPC-Netzwerke integrieren, um Sie bei der Erstellung der Ressourcen zu unterstützen, die einem EKS-Cluster zugeordnet sind.

Sie haben zwei Möglichkeiten, einen Cluster in der Konsole zu erstellen:

- Schnelle Konfiguration (mit EKS Auto Mode)
- Benutzerdefinierte Konfiguration

In diesem Thema erfahren Sie, wie Sie mithilfe der Schnellkonfigurationsoption einen EKS-Auto-Modus-Cluster erstellen.

Erstellen Sie mithilfe der Schnellkonfigurationsoption einen EKS-Automatikmodus

Sie müssen AWS Management Console mit ausreichenden Berechtigungen angemeldet sein, um AWS Ressourcen wie EC2 Instanzen, EC2 Netzwerke, EKS-Cluster und IAM-Rollen zu verwalten.

1. Navigieren Sie zur EKS-Konsole
2. Klicken Sie auf Cluster erstellen
3. Vergewissern Sie sich, dass die Option Schnellkonfiguration ausgewählt ist
4. Ermitteln Sie die folgenden Werte, oder verwenden Sie die Standardwerte für einen Testcluster.
 - Clustername
 - Kubernetes-Version
5. Wählen Sie die Cluster-IAM-Rolle aus. Wenn Sie zum ersten Mal einen EKS-Auto-Mode-Cluster erstellen, verwenden Sie die Option Empfohlene Rolle erstellen.
 - Optional können Sie eine einzelne Cluster-IAM-Rolle in Ihrem AWS Konto für alle EKS-Auto-Mode-Cluster wiederverwenden.

- Die Cluster-IAM-Rolle umfasst die erforderlichen Berechtigungen für den automatischen EKS-Modus zur Verwaltung von Ressourcen wie EC2 Instances, EBS-Volumes und EC2 Load Balancers.
 - Die Option „Empfohlene Rolle erstellen“ füllt alle Felder vorab mit empfohlenen Werten aus. Wählen Sie Weiter und dann Erstellen aus. Die Rolle verwendet den vorgeschlagenen `AmazonEKSAutoClusterRole` Namen.
 - Wenn Sie kürzlich eine neue Rolle erstellt haben, verwenden Sie das Aktualisierungssymbol, um das Drop-down-Menü für die Rollenauswahl erneut zu laden.
6. Wählen Sie die Node-IAM-Rolle aus. Wenn Sie zum ersten Mal einen EKS-Auto-Mode-Cluster erstellen, verwenden Sie die Option Empfohlene Rolle erstellen.
- Optional können Sie eine einzelne Node-IAM-Rolle in Ihrem AWS Konto für alle EKS-Auto-Mode-Cluster wiederverwenden.
 - Die Node-IAM-Rolle enthält die erforderlichen Berechtigungen für Knoten im automatischen Modus, um eine Verbindung zum Cluster herzustellen. Die Node-IAM-Rolle muss Berechtigungen zum Abrufen von ECR-Images für Ihre Container enthalten.
 - Die Option Empfohlene Rolle erstellen füllt alle Felder vorab mit empfohlenen Werten aus. Wählen Sie Weiter und dann Erstellen aus. Die Rolle verwendet den vorgeschlagenen `AmazonEKSAutoNodeRole` Namen.
 - Wenn Sie kürzlich eine neue Rolle erstellt haben, verwenden Sie das Aktualisierungssymbol, um das Drop-down-Menü für die Rollenauswahl erneut zu laden.
7. Wählen Sie die VPC für Ihren EKS-Auto-Mode-Cluster aus. Wählen Sie Create VPC, um eine neue VPC für EKS zu erstellen, oder wählen Sie eine VPC, die Sie zuvor für EKS erstellt haben.
- Wenn Sie die VPC-Konsole verwenden, um eine neue VPC zu erstellen, AWS schlägt vor, mindestens ein NAT-Gateway pro Availability Zone zu erstellen. Andernfalls können Sie alle anderen Standardeinstellungen verwenden.
 - Weitere Informationen und Einzelheiten zu den IPv6 Clusteranforderungen finden Sie unter [the section called “Erstellen einer VPC”](#).
8. (optional) Der automatische EKS-Modus füllt die privaten Subnetze für Ihre ausgewählte VPC automatisch auf. Sie können unerwünschte Subnetze entfernen.
- EKS wählt automatisch private Subnetze aus der VPC aus und folgt dabei bewährten Methoden. Sie können optional zusätzliche Subnetze aus der VPC auswählen, z. B. öffentliche Subnetze.
9. (optional) Wählen Sie Standardwerte für die Schnellkonfiguration anzeigen aus, um alle Konfigurationswerte für den neuen Cluster zu überprüfen. Aus der Tabelle geht hervor, dass einige Werte nach der Erstellung des Clusters nicht bearbeitet werden können.

10. Wählen Sie Cluster erstellen aus. Beachten Sie, dass es fünfzehn Minuten dauern kann, bis die Clustererstellung abgeschlossen ist.

Nächste Schritte

- Erfahren Sie, wie Sie [einen Beispiel-Workload auf Ihrem EKS-Auto-Mode-Cluster bereitstellen](#)

Aktivieren Sie den EKS-Automatikmodus auf vorhandenen EKS-Clustern

Sie können den automatischen EKS-Modus auf vorhandenen EKS-Clustern aktivieren.

Note

Der automatische EKS-Modus erfordert Kubernetes Version 1.29 oder höher. Der automatische EKS-Modus ist in den `ap-southeast-7` Regionen oder nicht verfügbar. `mx-central-1` AWS

AWS unterstützt die folgenden Migrationen:

- Migration von Karpenter zu EKS Auto Mode-Knoten. Weitere Informationen finden Sie unter [the section called “Migrieren Sie von Karpenter”](#).
- Migration von EKS Managed Node Groups zu EKS Auto Mode-Knoten. Weitere Informationen finden Sie unter [the section called “Migrieren Sie von MNGs”](#).
- Migration von EKS Fargate zum EKS Auto Mode. Weitere Informationen finden Sie unter [the section called “Von Fargate migrieren”](#).

AWS unterstützt die folgenden Migrationen nicht:

- Migration von Volumes vom EBS CSI-Controller (mithilfe des Amazon EKS-Add-ons) zum EKS Auto Mode EBS CSI-Controller (verwaltet von EKS Auto Mode). PVCs Die Daten, die mit einem erstellt wurden, können nicht vom anderen bereitgestellt werden, da sie zwei verschiedene Kubernetes-Volume Provisioner verwenden.
 - Das [eks-auto-mode-ebs-migration-tool](#) (AWS Labs-Projekt) ermöglicht die Migration zwischen Standard-EBS CSI StorageClass (`ebs.csi.aws.com`) und EKS Auto EBS CSI

(). StorageClass `ebs.csi.eks.amazonaws.com` Beachten Sie, dass für die Migration das Löschen und Neuerstellen vorhandener PersistentVolumeClaim/PersistentVolume Ressourcen erforderlich ist. Daher ist vor der Implementierung eine Validierung in einer Umgebung außerhalb der Produktion unerlässlich.

- Migration von Load Balancern vom Load AWS Balancer Controller in den EKS-Automatikmodus

Sie können den Load AWS Balancer Controller auf einem Amazon EKS Auto Mode-Cluster installieren. Verwenden Sie die `loadBalancerClass` Optionen `IngressClass` oder, um Service- und Ingress-Ressourcen entweder dem Load Balancer Controller oder dem EKS-Automatikmodus zuzuordnen.

- Migration von EKS-Clustern mit alternativen CNIs oder anderen nicht unterstützten Netzwerkkonfigurationen

Referenz zur Migration

Verwenden Sie die folgende Migrationsreferenz, um Kubernetes-Ressourcen so zu konfigurieren, dass sie entweder selbstverwalteten Controllern oder EKS Auto Mode gehören.

Funktion	Ressource	Feld	Selbstverwaltet	Automatischer EKS-Modus
Blockspeicher	StorageClass	<code>provisioner</code>	<code>ebs.csi.aws.com</code>	<code>ebs.csi.eks.amazonaws.com</code>
Load Balancing	Service	<code>loadBalancerClass</code>	<code>service.k8s.aws/nlb</code>	<code>eks.amazonaws.com/nlb</code>
Load Balancing	IngressClass	<code>controller</code>	<code>ingress.k8s.aws/alb</code>	<code>eks.amazonaws.com/alb</code>
Load Balancing	IngressClassParams	<code>apiversion</code>	<code>elbv2.k8s.aws/v1beta1</code>	<code>eks.amazonaws.com/v1</code>

Funktion	Ressource	Feld	Selbstverwaltet	Automatischer EKS-Modus
Load Balancing	TargetGroupBinding	apiversion	elbv2.k8s.aws/v1beta1	eks.amazonaws.com/v1
Datenverarbeitung	NodeClass	apiVersion	karpenter.sh/v1	eks.amazonaws.com/v1

Migration von EBS-Volumes

Bei der Migration von Workloads in den automatischen EKS-Modus müssen Sie sich aufgrund verschiedener CSI-Treiberanbieter um die Migration von EBS-Volumes kümmern:

- Provisioner für den automatischen Modus von EKS: `ebs.csi.eks.amazonaws.com`
- Open-Source-EBS-CSI-Provisioner: `ebs.csi.aws.com`

Gehen Sie wie folgt vor, um Ihre persistenten Volumes zu migrieren:

1. Richtlinie zur Aufbewahrung von Volumes ändern: Ändern Sie die vorhandenen Plattformversionen (PVs) `persistentVolumeReclaimPolicy`, `Retain` um sicherzustellen, dass das zugrunde liegende EBS-Volume nicht gelöscht wird.
2. PV aus Kubernetes entfernen: Löschen Sie die alte PV-Ressource, während das tatsächliche EBS-Volume intakt bleibt.
3. Erstellen Sie eine neue PV mit statischer Bereitstellung: Erstellen Sie eine neue PV, die auf dasselbe EBS-Volume verweist, aber mit dem Ziel-CSI-Treiber funktioniert.
4. An ein neues PVC binden: Erstellen Sie mithilfe des Felds ein neues PVC, das speziell auf Ihr PV verweist. `volumeName`

Überlegungen

- Stellen Sie sicher, dass Ihre Anwendungen gestoppt sind, bevor Sie mit dieser Migration beginnen.
- Erstellen Sie eine Sicherungskopie Ihrer Daten, bevor Sie mit dem Migrationsprozess beginnen.

- Dieser Vorgang muss für jedes persistente Volume durchgeführt werden.
- Der Workload muss aktualisiert werden, um das neue PVC verwenden zu können.

Load Balancer migrieren

Sie können vorhandene Load Balancer nicht direkt vom selbstverwalteten AWS Load Balancer-Controller in den EKS-Automatikmodus übertragen. Stattdessen müssen Sie eine blaugüne Bereitstellungsstrategie implementieren. Dazu müssen Sie Ihre bestehende Load Balancer-Konfiguration beibehalten und gleichzeitig neue Load Balancer unter dem verwalteten Controller erstellen.

Um Serviceunterbrechungen so gering wie möglich zu halten, empfehlen wir einen DNS-basierten Ansatz zur Verkehrsverlagerung. Erstellen Sie zunächst mithilfe des automatischen EKS-Modus neue Load Balancer, während Ihre bestehende Konfiguration betriebsbereit bleibt. Verwenden Sie dann DNS-Routing (z. B. Route 53), um den Verkehr schrittweise von den alten Load Balancern auf die neuen zu verlagern. Sobald der Verkehr erfolgreich migriert wurde und Sie die neue Konfiguration verifiziert haben, können Sie die alten Load Balancer und den selbstverwalteten Controller außer Betrieb nehmen.

Aktivieren Sie den EKS-Automatikmodus auf einem vorhandenen Cluster

In diesem Thema wird beschrieben, wie Sie den Amazon EKS-Automodus auf Ihren vorhandenen Amazon EKS-Clustern aktivieren. Um den automatischen Modus auf einem vorhandenen Cluster zu aktivieren, müssen die IAM-Berechtigungen aktualisiert und die wichtigsten EKS-Einstellungen für den automatischen Modus konfiguriert werden. Nach der Aktivierung können Sie mit der Migration Ihrer vorhandenen Rechen-Workloads beginnen, um die Vorteile der vereinfachten Abläufe und der automatisierten Infrastrukturverwaltung im Auto-Modus zu nutzen.

Important

Vergewissern Sie sich, dass Sie die mindestens erforderliche Version bestimmter Amazon EKS-Add-ons installiert haben, bevor Sie den EKS Auto Mode aktivieren. Weitere Informationen finden Sie unter [the section called “Erforderliche Zusatzversionen”](#).

Bevor Sie beginnen, stellen Sie sicher, dass Sie Administratorzugriff auf Ihren Amazon EKS-Cluster und Berechtigungen zum Ändern von IAM-Rollen haben. Die Schritte in diesem Thema führen Sie durch die Aktivierung des automatischen Modus mit der AWS Management Console oder AWS CLI.

AWS Management Console

Sie müssen mit der Berechtigung zur Verwaltung von IAM, EKS und EC2 Ressourcen an der AWS Konsole angemeldet sein.

Note

Die Cluster-IAM-Rolle eines EKS-Clusters kann nach der Erstellung des Clusters nicht geändert werden. Der automatische EKS-Modus erfordert zusätzliche Berechtigungen für diese Rolle. Sie müssen der aktuellen Rolle zusätzliche Richtlinien hinzufügen.

Cluster-IAM-Rolle aktualisieren

1. Öffnen Sie Ihre Cluster-Übersichtsseite in der AWS Management Console.
2. Wählen Sie unter Cluster-IAM-Rolle ARN die Option In IAM anzeigen aus.
3. Wählen Sie in der Dropdownliste „Berechtigungen hinzufügen“ die Option Richtlinien anhängen aus.
4. Verwenden Sie das Suchfeld, um die folgenden Richtlinien zu suchen und auszuwählen:
 - AmazonEKSComputePolicy
 - AmazonEKSBLOCKStoragePolicy
 - AmazonEKSLoadBalancingPolicy
 - AmazonEKSNetworkingPolicy
 - AmazonEKSClusterPolicy
5. Wählen Sie Berechtigungen hinzufügen
6. Wählen Sie auf der Registerkarte Vertrauensbeziehungen die Option Vertrauensrichtlinie bearbeiten
7. Fügen Sie die folgende Vertrauensrichtlinie für die Cluster-IAM-Rolle ein und wählen Sie Richtlinie aktualisieren

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
    "Principal": {
      "Service": "eks.amazonaws.com"
    },
    "Action": [
      "sts:AssumeRole",
      "sts:TagSession"
    ]
  }
]
```

Aktivieren Sie den automatischen EKS-Modus

1. Öffnen Sie Ihre Cluster-Übersichtsseite im AWS Management Console.
2. Wählen Sie unter EKS Auto Mode die Option Verwalten
3. Schalten Sie den EKS-Automatikmodus ein.
4. Wählen Sie in der Dropdownliste EKS Node Pool die Standard-Knotenpools aus, die Sie erstellen möchten.
 - Erfahren Sie mehr über Node Pools im EKS Auto Mode. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).
5. Wenn Sie für dieses AWS Konto bereits eine Knoten-IAM-Rolle im automatischen Modus von EKS erstellt haben, wählen Sie sie in der Dropdownliste Node-IAM-Rolle aus. Wenn Sie diese Rolle noch nicht erstellt haben, wählen Sie Empfohlene Rolle erstellen aus und folgen Sie den Schritten.

AWS CLI

Voraussetzungen

- Die Cluster-IAM-Rolle des vorhandenen EKS-Clusters muss ausreichende Berechtigungen für den automatischen EKS-Modus enthalten, z. B. die folgenden Richtlinien:
 - AmazonEKSClusterPolicy
 - AmazonEKSBLOCKStoragePolicy
 - AmazonEKSLoadBalancingPolicy
 - AmazonEKSNetworkPolicy
 - AmazonEKSClusterPolicy

- Die Cluster-IAM-Rolle muss über eine aktualisierte Vertrauensrichtlinie verfügen, die die Aktion `sts:TagSession` enthält. Weitere Informationen zum Erstellen einer Cluster-IAM-Rolle finden Sie unter [the section called “ AWS CLI”](#)
- `awscli` installiert, angemeldet und eine ausreichende Version. Sie benötigen die Berechtigung, IAM, EKS und Ressourcen zu verwalten. EC2 Weitere Informationen finden Sie unter [Einrichten](#).

Verfahren

Verwenden Sie die folgenden Befehle, um den automatischen EKS-Modus auf einem vorhandenen Cluster zu aktivieren.

Note

Die Rechen-, Blockspeicher- und Lastausgleichsfunktionen müssen alle in derselben Anfrage aktiviert oder deaktiviert werden.

```
aws eks update-cluster-config \
  --name $CLUSTER_NAME \
  --compute-config enabled=true \
  --kubernetes-network-config '{"elasticLoadBalancing":{"enabled": true}}' \
  --storage-config '{"blockStorage":{"enabled": true}}'
```

Erforderliche Zusatzversionen

Wenn Sie planen, den automatischen EKS-Modus auf einem vorhandenen Cluster zu aktivieren, müssen Sie möglicherweise bestimmte Add-Ons aktualisieren. Bitte beachten Sie Folgendes:

- Dies gilt nur für bestehende Cluster, die in den EKS-Automatikmodus übergehen.
- Für neue Cluster, die mit aktiviertem EKS-Automatikmodus erstellt wurden, sind diese Updates nicht erforderlich.

Wenn Sie eines der folgenden Add-Ons installiert haben, stellen Sie sicher, dass es mindestens die angegebene Mindestversion hat:

Name des Add-ons	Erforderliche Mindestversion
Amazon-VPC-CNI-Plug-In für Kubernetes	v1.19.0-eksbuild.1
Kube-Proxy	• v1.26.15-eksbuild.19 • v1.27.16-eksbuild.14 • v1.28.15-eksbuild.4 • v1.29.10-eksbuild.3 • v1.30.6-eksbuild.3 • v1.31.2-eksbuild.3
Amazon-EBS-CSI-Treiber	v1.37.0-eksbuild.1
CSI-Snapshot-Controller	v8.1.0-eksbuild.2
EKS Pod Identity Agent	v1.3.4-eksbuild.1

Weitere Informationen finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#).

Nächste Schritte

- Informationen zur Migration von Manage Node Group-Workloads finden Sie unter. [the section called “Migrieren Sie von MNGs”](#)
- Informationen zur Migration von Self-Managed Karpenter finden Sie unter. [the section called “Migrieren Sie von Karpenter”](#)

Migrieren Sie mit kubectl von Karpenter zum EKS Auto Mode

Dieses Thema führt Sie durch den Prozess der Migration von Workloads von Karpenter zum Amazon EKS Auto Mode mithilfe von kubectl. Die Migration kann schrittweise durchgeführt werden, sodass Sie Workloads in Ihrem eigenen Tempo verschieben und gleichzeitig die Cluster-Stabilität und Anwendungsverfügbarkeit während des gesamten Übergangs aufrechterhalten können.

Der unten beschriebene step-by-step Ansatz ermöglicht es Ihnen, Karpenter und EKS Auto Mode während des Migrationszeitraums parallel auszuführen. Diese duale Betriebsstrategie trägt zu einem reibungslosen Übergang bei, indem Sie das Workload-Verhalten im automatischen EKS-

Modus überprüfen können, bevor Sie Karpenter vollständig außer Betrieb nehmen. Sie können Anwendungen einzeln oder in Gruppen migrieren, sodass Sie flexibel auf Ihre spezifischen betrieblichen Anforderungen und Ihre Risikobereitschaft eingehen können.

Voraussetzungen

Bevor Sie mit der Migration beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Karpenter v1.1 oder höher ist auf Ihrem Cluster installiert. Weitere Informationen finden Sie unter [Upgrade auf 1.1.0+ in den Karpenter Dokumenten](#).
- `kubect1` installiert und mit Ihrem Cluster verbunden. Weitere Informationen finden Sie unter [Einrichten](#).

Dieses Thema setzt voraus, dass Sie mit Karpenter und vertraut sind. NodePools Weitere Informationen finden Sie in der [Karpenter](#) Dokumentation.

Schritt 1: Aktivieren Sie den EKS-Automatikmodus auf dem Cluster

Aktivieren Sie den EKS-Automatikmodus auf Ihrem vorhandenen Cluster mithilfe der AWS CLI oder der Management Console. Weitere Informationen finden Sie unter [the section called “Auf dem Cluster aktivieren”](#).

Note

Während Sie den automatischen EKS-Modus aktivieren, sollten Sie den `general purpose` Nodepool zu diesem Zeitpunkt während des Übergangs nicht aktivieren. Dieser Knotenpool ist nicht selektiv.

Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).

Schritt 2: Erstellen Sie einen fehlerhaften EKS-Automatikmodus NodePool

Erstellen Sie einen neuen NodePool für EKS Auto Mode mit einem Makel. Dadurch wird sichergestellt, dass bestehende Pods nicht automatisch auf den neuen EKS-Automodus-Knoten eingeplant werden. Dieser Knotenpool verwendet den in EKS default NodeClass integrierten Automatikmodus. Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Knotenklasse”](#).

Beispiel für einen Knotenpool mit Taint:

```
apiVersion: karpenter.sh/v1
kind: NodePool
metadata:
  name: eks-auto-mode
spec:
  template:
    spec:
      requirements:
        - key: "eks.amazonaws.com/instance-category"
          operator: In
          values: ["c", "m", "r"]
      nodeClassRef:
        group: eks.amazonaws.com
        kind: NodeClass
        name: default
      taints:
        - key: "eks-auto-mode"
          effect: "NoSchedule"
```

Aktualisieren Sie die Anforderungen für den Knotenpool so, dass sie der Karpenter-Konfiguration entsprechen, von der Sie migrieren. Sie benötigen mindestens eine Anforderung.

Schritt 3: Workloads für die Migration aktualisieren

Identifizieren und aktualisieren Sie die Workloads, die Sie in den automatischen EKS-Modus migrieren möchten. Fügen Sie diesen Workloads sowohl Toleranzen als auch Knotenselektoren hinzu:

```
apiVersion: apps/v1
kind: Deployment
spec:
  template:
    spec:
      tolerations:
        - key: "eks-auto-mode"
          effect: "NoSchedule"
      nodeSelector:
        eks.amazonaws.com/compute-type: auto
```

Diese Änderung ermöglicht die Planung der Arbeitslast auf den neuen EKS-Automodus-Knoten.

EKS Auto Mode verwendet andere Labels als Karpenter. Beschriftungen, die sich auf EC2 verwaltete Instanzen beziehen, beginnen mit `eks.amazonaws.com`. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).

Schritt 4: Schrittweise Migration von Workloads

Wiederholen Sie Schritt 3 für jeden Workload, den Sie migrieren möchten. Auf diese Weise können Sie Workloads je nach Ihren Anforderungen und Ihrer Risikobereitschaft einzeln oder in Gruppen verschieben.

Schritt 5: Entfernen Sie den ursprünglichen Karpenter NodePool

Sobald alle Workloads migriert wurden, können Sie den ursprünglichen Karpenter entfernen: NodePool

```
kubectl delete nodepool <original-nodepool-name>
```

Schritt 6: Entfernen Sie den Makel aus dem EKS-Automatikmodus (optional) NodePool

Wenn Sie möchten, dass der EKS-Automodus zum Standard für neue Workloads wird, können Sie den Makel aus dem EKS-Automatikmodus entfernen: NodePool

```
apiVersion: karpenter.sh/v1
kind: NodePool
metadata:
  name: eks-auto-mode
spec:
  template:
    spec:
      nodeClassRef:
        group: eks.amazonaws.com
        kind: NodeClass
        name: default
      # Remove the taints section
```

Schritt 7: Knotenselektoren aus Workloads entfernen (optional)

Wenn Sie den Makel aus dem automatischen EKS-Modus entfernt haben NodePool, können Sie optional die Knotenselektoren aus Ihren Workloads entfernen, da der automatische EKS-Modus jetzt der Standard ist:


```
apiVersion: apps/v1
kind: Deployment
spec:
  template:
    spec:
      # Remove the nodeSelector section
      tolerations:
        - key: "eks-auto-mode"
          effect: "NoSchedule"
```

Schritt 8: Deinstallieren Sie Karpenter von Ihrem Cluster

Die Schritte zum Entfernen von Karpenter hängen davon ab, wie Sie es installiert haben. Weitere Informationen finden Sie in der Installationsanleitung von [Karpenter](#).

Migrieren Sie von EKS Managed Node Groups zum EKS Auto Mode

Wenn Sie Ihren Amazon EKS-Cluster auf den auto EKS-Modus umstellen, können Sie Ihre vorhandenen Workloads mithilfe des eksctl-CLI-Tools problemlos aus verwalteten Knotengruppen (MNGs) migrieren. Dieser Prozess gewährleistet eine kontinuierliche Anwendungsverfügbarkeit, während der auto EKS-Modus Ihre Rechenressourcen optimiert. Die Migration kann mit minimaler Unterbrechung Ihrer laufenden Anwendungen durchgeführt werden.

Dieses Thema führt Sie durch die Schritte, mit denen Sie Pods sicher aus Ihren vorhandenen verwalteten Knotengruppen löschen und es dem auto EKS-Modus ermöglichen können, sie auf neu bereitgestellten Instanzen neu zu planen. Wenn Sie dieses Verfahren befolgen, können Sie die Vorteile der intelligenten Workload-Konsolidierung im auto EKS-Modus nutzen und gleichzeitig die Verfügbarkeit Ihrer Anwendung während der Migration aufrechterhalten.

Voraussetzungen

- Cluster mit aktiviertem EKS-Automatikmodus
- eksctl CLI ist installiert und mit Ihrem Cluster verbunden. Weitere Informationen finden Sie unter [Einrichten](#).
- Karpenter ist nicht auf dem Cluster installiert.

Verfahren

Verwenden Sie den folgenden `eksctl` CLI-Befehl, um das Entleeren von Pods aus den vorhandenen verwalteten Knotengruppeninstanzen zu initiieren. Der automatische EKS-Modus erstellt neue Knoten zur Unterstützung der verdrängten Pods.

```
eksctl delete nodegroup --cluster=<clusterName> --name=<nodegroupName>
```

Sie müssen diesen Befehl für jede verwaltete Knotengruppe in Ihrem Cluster ausführen.

Weitere Informationen zu diesem Befehl finden Sie unter [Löschen und Entleeren von Knotengruppen in den eksctl-Dokumenten](#).

Migrieren Sie von EKS Fargate zum EKS Auto Mode

Dieses Thema führt Sie durch den Prozess der Migration von Workloads von EKS Fargate zum Amazon EKS Auto Mode mithilfe von `kubectl`. Die Migration kann schrittweise durchgeführt werden, sodass Sie Workloads in Ihrem eigenen Tempo verschieben und gleichzeitig die Cluster-Stabilität und Anwendungsverfügbarkeit während des gesamten Übergangs aufrechterhalten können.

Der unten beschriebene step-by-step Ansatz ermöglicht es Ihnen, EKS Fargate und EKS Auto Mode während des Migrationszeitraums parallel auszuführen. Diese duale Betriebsstrategie trägt zu einem reibungslosen Übergang bei, indem Sie das Workload-Verhalten im EKS-Automatikmodus überprüfen können, bevor Sie EKS Fargate vollständig außer Betrieb nehmen. Sie können Anwendungen einzeln oder in Gruppen migrieren, sodass Sie flexibel auf Ihre spezifischen betrieblichen Anforderungen und Ihre Risikobereitschaft eingehen können.

Vergleich von Amazon EKS Auto Mode und EKS mit AWS Fargate

Amazon EKS mit AWS Fargate bleibt eine Option für Kunden, die EKS ausführen möchten, aber Amazon EKS Auto Mode ist in Zukunft der empfohlene Ansatz. EKS Auto Mode ist vollständig Kubernetes-konform und unterstützt alle Upstream-Kubernetes-Primitiven und Plattformtools wie Istio, die Fargate nicht unterstützen kann. Der automatische Modus von EKS unterstützt außerdem vollständig alle EC2 Runtime-Kaufoptionen, einschließlich GPU- und Spot-Instances, sodass Kunden ausgehandelte EC2 Rabatte und andere Sparmechanismen nutzen können. Diese Funktionen sind bei der Verwendung von EKS mit Fargate nicht verfügbar.

Darüber hinaus ermöglicht EKS Auto Mode Kunden, dasselbe Isolationsmodell wie Fargate zu erreichen und dabei die standardmäßigen Kubernetes-Planungsfunktionen zu verwenden, um sicherzustellen, dass auf jeder EC2 Instanz ein einziger Anwendungscontainer ausgeführt wird.

Durch die Einführung von Amazon EKS Auto Mode können Kunden alle Vorteile der Ausführung von Kubernetes nutzen AWS — eine vollständig Kubernetes-konforme Plattform, die die Flexibilität bietet, die gesamte Bandbreite an Kaufoptionen zu nutzen und gleichzeitig die Benutzerfreundlichkeit EC2 und Abstraktion von der Infrastrukturverwaltung beizubehalten, die Fargate bietet.

Voraussetzungen

Bevor Sie mit der Migration beginnen, stellen Sie sicher, dass Sie

- Richten Sie einen Cluster mit Fargate ein. Weitere Informationen finden Sie unter [the section called “Erste Schritte”](#).
- Installiert und mit `kubectl` Ihrem Cluster verbunden. Weitere Informationen finden Sie unter [Einrichten](#).

Schritt 1: Überprüfen Sie den Fargate-Cluster

1. Prüfen Sie, ob der EKS-Cluster mit Fargate läuft:

```
kubectl get node
```

```
NAME STATUS ROLES AGE VERSION
fargate-ip-192-168-92-52.ec2.internal Ready <none> 25m v1.30.8-eks-2d5f260
fargate-ip-192-168-98-196.ec2.internal Ready <none> 24m v1.30.8-eks-2d5f260
```

2. Überprüfen Sie die laufenden Pods:

```
kubectl get pod -A
```

```
NAMESPACE NAME READY STATUS RESTARTS AGE
kube-system coredns-6659cb98f6-gxpjz 1/1 Running 0 26m
kube-system coredns-6659cb98f6-gzzsx 1/1 Running 0 26m
```

3. Erstellen Sie ein Deployment in einer Datei mit dem Namen `deployment_fargate.yaml`:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
```

```

    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
      annotations:
        eks.amazonaws.com/compute-type: fargate
    spec:
      containers:
      - name: nginx
        image: nginx
        ports:
        - containerPort: 80

```

4. Wenden Sie die Bereitstellung an:

```
kubectl apply -f deployment_fargate.yaml
```

```
deployment.apps/nginx-deployment created
```

5. Überprüfen Sie die Pods und Bereitstellungen:

```
kubectl get pod,deploy
```

NAME	READY	STATUS	RESTARTS	AGE
pod/nginx-deployment-5c7479459b-6trtm	1/1	Running	0	61s
pod/nginx-deployment-5c7479459b-g8ssb	1/1	Running	0	61s
pod/nginx-deployment-5c7479459b-mq4mf	1/1	Running	0	61s

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/nginx-deployment	3/3	3	3	61s

6. Überprüfen Sie den Knoten:

```
kubectl get node -owide
```

NAME	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE	STATUS	ROLES	AGE	VERSION
							KERNEL-VERSION
							CONTAINER-RUNTIME
fargate-ip-192-168-111-43	192.168.111.43	<none>	ec2.internal	Ready	<none>	31s	v1.30.8-eks-2d5f260
			Amazon Linux 2				5.10.234-225.910.amzn2.x86_64
							containerd://1.7.25
fargate-ip-192-168-117-130	192.168.117.130	<none>	ec2.internal	Ready	<none>	36s	v1.30.8-eks-2d5f260
			Amazon Linux 2				5.10.234-225.910.amzn2.x86_64
							containerd://1.7.25
fargate-ip-192-168-74-140	192.168.74.140	<none>	ec2.internal	Ready	<none>	36s	v1.30.8-eks-2d5f260
			Amazon Linux 2				5.10.234-225.910.amzn2.x86_64
							containerd://1.7.25

Schritt 2: Aktivieren Sie den EKS-Automatikmodus auf dem Cluster

1. Aktivieren Sie den EKS-Automatikmodus auf Ihrem vorhandenen Cluster mithilfe der AWS CLI oder der Managementkonsole. Weitere Informationen finden Sie unter [the section called “Auf dem Cluster aktivieren”](#).
2. Überprüfen Sie den Nodepool:

```
kubectl get nodepool
```

NAME	NODECLASS	NODES	READY	AGE
general-purpose	default	1	True	6m58s
system	default	0	True	3d14h

Schritt 3: Workloads für die Migration aktualisieren

Identifizieren und aktualisieren Sie die Workloads, die Sie in den automatischen EKS-Modus migrieren möchten.

Um einen Workload von Fargate in den EKS Auto Mode zu migrieren, wenden Sie die Anmerkung `eks.amazonaws.com/compute-type: ec2` an. Dadurch wird sichergestellt, dass die Arbeitslast trotz des Fargate-Profiles nicht von Fargate geplant wird, sondern vom EKS-Automatikmodus übernommen wird. NodePool Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).

1. Ändern Sie Ihre Bereitstellungen (z. B. die `deployment_fargate.yaml` Datei), um den Berechnungstyp wie folgt zu ändern: `ec2`

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    annotations:
      eks.amazonaws.com/compute-type: ec2
    spec:
      containers:
      - name: nginx
        image: nginx
        ports:
        - containerPort: 80
```

2. Wenden Sie die Bereitstellung an. Diese Änderung ermöglicht die Planung der Arbeitslast auf den neuen EKS-Automodus-Knoten:

```
kubectl apply -f deployment_fargate.yaml
```

3. Überprüfen Sie, ob die Bereitstellung im EKS-Auto-Mode-Cluster ausgeführt wird:

```
kubectl get pod -o wide
```

NAME	READY	STATUS	RESTARTS	AGE	IP
NODE	NOMINATED NODE	READINESS	GATES		
nginx-deployment-97967b68d-ffxxh	1/1	Running	0	3m31s	
192.168.43.240	i-0845aafcb51630ffb	<none>	<none>		
nginx-deployment-97967b68d-mbcgj	1/1	Running	0	2m37s	
192.168.43.241	i-0845aafcb51630ffb	<none>	<none>		

```
nginx-deployment-97967b68d-qpd8x    1/1    Running    0    2m35s
192.168.43.242    i-0845aafcb51630ffb    <none>    <none>
```

4. Stellen Sie sicher, dass in den verwalteten EKS-Automodus-Knoten kein Fargate-Knoten läuft und keine Bereitstellung ausgeführt wird:

```
kubectl get node -owide
```

```
NAME                                STATUS ROLES  AGE    VERSION                                INTERNAL-IP    EXTERNAL-IP
IP OS-IMAGE                                KERNEL-VERSION CONTAINER-RUNTIME
i-0845aafcb51630ffb Ready   <none>  3m30s  v1.30.8-eks-3c20087 192.168.41.125
3.81.118.95 Bottlerocket (EKS Auto) 2025.3.14 (aws-k8s-1.30) 6.1.129
containerd://1.7.25+bottlerocket
```

Schritt 4: Schrittweise Migration von Workloads

Wiederholen Sie Schritt 3 für jeden Workload, den Sie migrieren möchten. Auf diese Weise können Sie Workloads je nach Ihren Anforderungen und Ihrer Risikobereitschaft einzeln oder in Gruppen verschieben.

Schritt 5: Entfernen Sie das ursprüngliche Fargate-Profil

Sobald alle Workloads migriert wurden, können Sie das ursprüngliche Profil entfernen. `fargate` Ersetze es *<fargate profile name>* durch den Namen deines Fargate-Profiles:

```
aws eks delete-fargate-profile --cluster-name eks-fargate-demo-cluster --fargate-
profile-name <fargate profile name>
```

Schritt 6: CoreDNS herunterskalieren

Da der EKS Auto-Modus CoreDNS verarbeitet, skalieren Sie die `coredns` Bereitstellung auf 0 herunter:

```
kubectl scale deployment coredns -n kube-system --replicas=0
```

Führen Sie Beispiel-Workloads in EKS-Clustern im automatischen Modus aus

Dieses Kapitel enthält Beispiele für die Bereitstellung verschiedener Arten von Workloads auf Amazon EKS-Clustern, die im Auto-Modus ausgeführt werden. Die Beispiele zeigen wichtige Workload-Muster, darunter Beispielanwendungen, Webanwendungen mit Lastenausgleich, statusbehaftete Workloads mit persistentem Speicher und Workloads mit spezifischen Anforderungen an die Knotenplatzierung. Jedes Beispiel enthält vollständige Manifeste und step-by-step Bereitstellungsanweisungen, die Sie als Vorlagen für Ihre eigenen Anwendungen verwenden können.

Bevor Sie mit den Beispielen fortfahren, stellen Sie sicher, dass ein EKS-Cluster im Auto-Modus läuft und dass Sie AWS CLI und `kubectl` installiert haben. Weitere Informationen finden Sie unter [Einrichten](#). Die Beispiele setzen grundlegende Vertrautheit mit Kubernetes-Konzepten und `kubectl`-Befehlen voraus.

Sie können diese auf Anwendungsfällen basierenden Beispiele verwenden, um Workloads in EKS-Auto-Mode-Clustern auszuführen.

[the section called “Stellen Sie einen aufgeblasenen Workload bereit”](#)

Zeigt, wie ein Beispiel-Workload mithilfe `kubectl` von Befehlen auf einem EKS-Auto-Modus-Cluster bereitgestellt wird.

[the section called “Stellen Sie den Load Balancer bereit”](#)

Zeigt, wie eine containerisierte Version des Spiels 2048 auf Amazon EKS bereitgestellt wird.

[the section called “Stellen Sie einen statusbehafteten Work”](#)

Zeigt, wie eine statusbehaftete Beispielanwendung in einem EKS-Auto-Mode-Cluster bereitgestellt wird.

[the section called “Steuern Sie die Bereitstellung”](#)

Zeigt, wie mithilfe einer Anmerkung gesteuert wird, ob eine Arbeitslast auf Knoten bereitgestellt wird, die vom EKS Auto Mode verwaltet werden.

Einen Beispiel-Workload zum Aufblasen in einem Amazon EKS Auto Mode-Cluster bereitstellen

In diesem Tutorial erfahren Sie, wie Sie einen Beispiel-Workload in einem EKS-Auto-Mode-Cluster bereitstellen und beobachten, wie dieser automatisch die erforderlichen Rechenressourcen bereitstellt. Sie werden `kubectl` Befehle verwenden, um das Verhalten des Clusters zu beobachten und aus erster Hand zu erfahren, wie der Auto Mode den Kubernetes-Betrieb vereinfacht. AWS Am Ende dieses Tutorials werden Sie verstehen, wie der automatische Modus von EKS auf Workload-Bereitstellungen reagiert, indem er die zugrunde liegenden Rechenressourcen automatisch verwaltet, ohne dass eine manuelle Konfiguration der Knotengruppen erforderlich ist.

Voraussetzungen

- Ein Amazon EKS Auto Mode-Cluster. Notieren Sie sich den Namen und die AWS Region des Clusters.
- Ein IAM-Prinzipal, z. B. ein Benutzer oder eine Rolle, mit ausreichenden Berechtigungen zur Verwaltung von Netzwerk-, Rechen- und EKS-Ressourcen.
 - Weitere Informationen finden Sie unter [Rollen erstellen und Richtlinien anhängen im IAM-Benutzerhandbuch im IAM-Benutzerhandbuch](#).
- `awsCLI` wurde mit einer IAM-Identität installiert und konfiguriert.
- `kubectl` CLI ist installiert und mit dem Cluster verbunden.
 - Weitere Informationen finden Sie unter [Einrichten](#).

Schritt 1: Überprüfen Sie die vorhandenen Rechenressourcen (optional)

Verwenden Sie dies zunächst, `kubectl` um die Knotenpools in Ihrem Cluster aufzulisten.

```
kubectl get nodepools
```

Beispielausgabe:

```
general-purpose
```

In diesem Tutorial werden wir einen Workload bereitstellen, der für die Verwendung des `general-purpose` Knotenpools konfiguriert ist. Dieser Knotenpool ist in den automatischen Modus von EKS integriert und enthält angemessene Standardeinstellungen für allgemeine Workloads wie

Microservices und Web-Apps. Sie können Ihren eigenen Knotenpool erstellen. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).

Zweitens, `kubectl` um die Knoten aufzulisten, die mit Ihrem Cluster verbunden sind.

```
kubectl get nodes
```

Wenn Sie gerade einen EKS-Auto-Mode-Cluster erstellt haben, haben Sie keine Knoten.

In diesem Tutorial stellen Sie einen Beispiel-Workload bereit. Wenn Sie keine Knoten haben oder der Workload nicht auf vorhandene Knoten passt, stellt EKS Auto Mode einen neuen Knoten bereit.

Schritt 2: Stellen Sie eine Beispielanwendung auf dem Cluster bereit

Sehen Sie sich die folgende Kubernetes-Bereitstellung an und speichern Sie sie unter `inflate.yaml`

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: inflate
spec:
  replicas: 1
  selector:
    matchLabels:
      app: inflate
  template:
    metadata:
      labels:
        app: inflate
    spec:
      terminationGracePeriodSeconds: 0
      nodeSelector:
        eks.amazonaws.com/compute-type: auto
      securityContext:
        runAsUser: 1000
        runAsGroup: 3000
        fsGroup: 2000
      containers:
        - name: inflate
          image: public.ecr.aws/eks-distro/kubernetes/pause:3.7
          resources:
```

```
requests:
  cpu: 1
securityContext:
  allowPrivilegeEscalation: false
```

Beachten Sie, dass der `eks.amazonaws.com/compute-type: auto` Selektor erfordert, dass der Workload auf einem Amazon EKS Auto Mode-Knoten bereitgestellt wird.

Wenden Sie das Deployment auf Ihren Cluster an.

```
kubectl apply -f inflate.yaml
```

Schritt 3: Kubernetes-Ereignisse ansehen

Verwenden Sie den folgenden Befehl, um Kubernetes-Ereignisse zu beobachten, einschließlich der Erstellung eines neuen Knotens. Wird verwendet `ctrl+c`, um das Ansehen von Ereignissen zu beenden.

```
kubectl get events -w --sort-by '.lastTimestamp'
```

Wird verwendet `kubectl`, um die Knoten, die mit Ihrem Cluster verbunden sind, erneut aufzulisten. Notieren Sie sich den neu erstellten Knoten.

```
kubectl get nodes
```

Schritt 4: Knoten und Instanzen in der AWS Konsole anzeigen

Sie können die EKS-Automodus-Knoten in der EKS-Konsole und die zugehörigen EC2 Instanzen in der EC2 Konsole anzeigen.

EC2 Instances, die im automatischen Modus von EKS bereitgestellt werden, sind eingeschränkt. Sie können keine beliebigen Befehle auf EKS Auto Mode-Knoten ausführen.

Schritt 5: Löschen Sie die Bereitstellung

Wird verwendet `kubectl`, um die Beispielpreparierung zu löschen

```
kubectl delete -f inflate.yaml
```

Wenn Sie keine anderen Workloads in Ihrem Cluster bereitgestellt haben, ist der vom EKS Auto Mode erstellte Knoten leer.

In der Standardkonfiguration erkennt der automatische EKS-Modus Knoten, die dreißig Sekunden lang leer waren, und beendet sie.

Verwenden Sie `kubectl` oder die EC2 Konsole, um zu bestätigen, dass die zugehörige Instanz gelöscht wurde.

Einen Beispiel-Load Balancer-Workload im automatischen EKS-Modus bereitstellen

Dieser Leitfaden führt Sie durch die Bereitstellung einer containerisierten Version des Spiels 2048 auf Amazon EKS, komplett mit Lastenausgleich und Internetzugriff.

Voraussetzungen

- Ein EKS-Auto-Modus-Cluster
- `kubectl` konfiguriert für die Interaktion mit Ihrem Cluster
- Entsprechende IAM-Berechtigungen für die Erstellung von ALB-Ressourcen

Schritt 1: Erstellen Sie den Namespace

Erstellen Sie zunächst einen dedizierten Namespace für die 2048-Spieleanwendung.

Erstellen Sie eine Datei namens `01-namespace.yaml`:

```
apiVersion: v1
kind: Namespace
metadata:
  name: game-2048
```

Wenden Sie die Namespace-Konfiguration an:

```
kubectl apply -f 01-namespace.yaml
```

Schritt 2: Stellen Sie die Anwendung bereit

Die Anwendung führt mehrere Repliken des 2048-Spielcontainers aus.

Erstellen Sie eine Datei namens `02-deployment.yaml`:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  namespace: game-2048
  name: deployment-2048
spec:
  selector:
    matchLabels:
      app.kubernetes.io/name: app-2048
  replicas: 5
  template:
    metadata:
      labels:
        app.kubernetes.io/name: app-2048
    spec:
      containers:
        - image: public.ecr.aws/l6m2t8p7/docker-2048:latest
          imagePullPolicy: Always
          name: app-2048
          ports:
            - containerPort: 80
          resources:
            requests:
              cpu: "0.5"
```

Note

Wenn Sie beim Laden des Images einen Fehler erhalten, vergewissern Sie sich `public.ecr.aws/l6m2t8p7/docker-2048:latest`, dass Ihre Node-IAM-Rolle über ausreichende Berechtigungen verfügt, um Bilder aus ECR abzurufen. Weitere Informationen finden Sie unter [the section called "Knoten-IAM-Rolle"](#). Außerdem ist das `docker-2048` Image im Beispiel ein `x86_64` Image und kann nicht auf anderen Architekturen ausgeführt werden.

Die wichtigsten Komponenten:

- Stellt 5 Replikate der Anwendung bereit
- Verwendet ein öffentliches ECR-Image

- Fordert 0,5 CPU-Kerne pro Pod an
- Macht Port 80 für HTTP-Verkehr verfügbar

Wenden Sie die Bereitstellung an:

```
kubectl apply -f 02-deployment.yaml
```

Schritt 3: Erstellen Sie den Dienst

Der Dienst macht die Bereitstellung dem Cluster-Netzwerk zugänglich.

Erstellen Sie eine Datei namens `03-service.yaml`:

```
apiVersion: v1
kind: Service
metadata:
  namespace: game-2048
  name: service-2048
spec:
  ports:
    - port: 80
      targetPort: 80
      protocol: TCP
  selector:
    app.kubernetes.io/name: app-2048
```

Die wichtigsten Komponenten:

- Erzeugt einen NodePort Dienst
- Ordnet Port 80 dem Port 80 des Containers zu
- Verwendet den Label-Selector, um Pods zu finden

Wenden Sie den Dienst an:

```
kubectl apply -f 03-service.yaml
```

Schritt 4: Load Balancing konfigurieren

Sie richten einen Ingress ein, um die Anwendung dem Internet zugänglich zu machen.

Erstellen Sie zunächst die `IngressClass`. Erstellen Sie eine Datei namens `04-ingressclass.yaml`:

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  labels:
    app.kubernetes.io/name: LoadBalancerController
  name: alb
spec:
  controller: eks.amazonaws.com/alb
```

Note

Der automatische Modus von EKS erfordert Subnetz-Tags, um öffentliche und private Subnetze zu identifizieren.

Wenn Sie Ihren Cluster mit `eksctl` erstellt haben, verfügen Sie bereits über diese Tags.

Weitere Informationen erhalten Sie unter [the section called “Taggen Sie Subnetze”](#).

Erstellen Sie dann die Ingress-Ressource. Erstellen Sie eine Datei namens `05-ingress.yaml`:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  namespace: game-2048
  name: ingress-2048
  annotations:
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
spec:
  ingressClassName: alb
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: service-2048
                port:
```

```
number: 80
```

Die wichtigsten Komponenten:

- Erzeugt ein ALB mit Internetzugriff
- Verwendet den IP-Zieltyp für direktes Pod-Routing
- Leitet den gesamten Datenverkehr (/) an den Spieldienst weiter

Wenden Sie die Eingangskonfigurationen an:

```
kubectl apply -f 04-ingressclass.yaml  
kubectl apply -f 05-ingress.yaml
```

Schritt 5: Überprüfen Sie die Bereitstellung

1. Stellen Sie sicher, dass alle Pods laufen:

```
kubectl get pods -n game-2048
```

2. Stellen Sie sicher, dass der Dienst erstellt wurde:

```
kubectl get svc -n game-2048
```

3. Holen Sie sich den ALB-Endpunkt:

```
kubectl get ingress -n game-2048
```

Das ADDRESS-Feld in der Eingangsausgabe zeigt Ihren ALB-Endpunkt an. Warten Sie 2-3 Minuten, bis der ALB alle Ziele bereitgestellt und registriert hat.

Schritt 6: Greifen Sie auf das Spiel zu

Öffne deinen Webbrowser und rufe die URL des ALB-Endpunkts aus dem vorherigen Schritt auf. Du solltest die Spieloberfläche von 2048 sehen.

Schritt 7: Bereinigen

Um alle in diesem Tutorial erstellten Ressourcen zu entfernen:


```
kubectl delete namespace game-2048
```

Dadurch werden alle Ressourcen im Namespace gelöscht, einschließlich der Bereitstellungs-, Dienst- und Eingangsressourcen.

Was passiert hinter den Kulissen

1. Durch die Bereitstellung werden 5 Pods erstellt, auf denen das Spiel 2048 ausgeführt wird
2. Der Dienst bietet einen stabilen Netzwerkzugriff auf diese Pods
3. EKS-Automatikmodus:
 - Erstellt einen Application Load Balancer in AWS
 - Konfiguriert Zielgruppen für die Pods
 - Richtet Routing-Regeln ein, um den Verkehr an den Dienst weiterzuleiten

Fehlerbehebung

Wenn das Spiel nicht geladen wird:

- Stellen Sie sicher, dass alle Pods laufen: `kubectl get pods -n game-2048`
- Überprüfen Sie den Eingangsstatus: `kubectl describe ingress -n game-2048`
- Überprüfen Sie die ALB-Zustandsprüfungen: Überprüfen Sie den Zustand der Zielgruppe in der Konsole AWS

Bereitstellen eines statusbehafteten Beispiel-Workloads im automatischen Modus von EKS

Dieses Tutorial führt Sie durch die Bereitstellung einer statusbehafteten Beispielanwendung in Ihrem EKS-Auto-Mode-Cluster. Die Anwendung schreibt Zeitstempel auf ein persistentes Volume und demonstriert so die automatischen EBS-Volume-Bereitstellungs- und Persistenzfunktionen von EKS Auto Mode.

Voraussetzungen

- Ein EKS-Auto-Mode-Cluster
- Die AWS CLI ist mit den entsprechenden Berechtigungen konfiguriert

- `kubectl` installiert und konfiguriert
 - Weitere Informationen finden Sie unter [Einrichten](#).

Schritt 1: Konfigurieren Sie Ihre Umgebung

1. Stellen Sie Ihre Umgebungsvariablen ein:

```
export CLUSTER_NAME=my-auto-cluster
export AWS_REGION="us-west-2"
```

2. Aktualisiere deine kubeconfig:

```
aws eks update-kubeconfig --name "${CLUSTER_NAME}"
```

Schritt 2: Erstellen Sie die Speicherklasse

Das StorageClass definiert, wie EKS Auto Mode EBS-Volumes bereitstellt.

Der automatische EKS-Modus erstellt keine StorageClass für Sie. Sie müssen eine StorageClass Referenzierung erstellen `ebs.csi.eks.amazonaws.com`, um die Speicherfunktion von EKS Auto Mode nutzen zu können.

1. Erstellen Sie eine Datei namens `storage-class.yaml`:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: auto-ebs-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: ebs.csi.eks.amazonaws.com
volumeBindingMode: WaitForFirstConsumer
parameters:
  type: gp3
  encrypted: "true"
```

2. Wenden Sie Folgendes an StorageClass:

```
kubectl apply -f storage-class.yaml
```

Die wichtigsten Komponenten:

- `provisioner: ebs.csi.eks.amazonaws.com`- Verwendet den EKS-Automatikmodus
- `volumeBindingMode: WaitForFirstConsumer`- Verzögert die Volume-Erstellung, bis ein Pod sie benötigt
- `type: gp3`— Gibt den EBS-Volumetyp an
- `encrypted: "true"`- EBS verwendet den `aws/ebs` Standardschlüssel zur Verschlüsselung von Volumes, die mit dieser Klasse erstellt wurden. Dies ist zwar optional, wird aber empfohlen.
- `storageclass.kubernetes.io/is-default-class: "true"`- Kubernetes verwendet diese Speicherklasse standardmäßig, es sei denn, Sie geben für einen Anspruch auf ein persistentes Volume eine andere Volume-Klasse an. Seien Sie vorsichtig, wenn Sie diesen Wert festlegen, wenn Sie von einem anderen Speichercontroller migrieren. (optional)

Schritt 3: Erstellen Sie den Anspruch auf beständiges Volumen

Das PVC fordert Speicher von der `anStorageClass`.

1. Erstellen Sie eine Datei namens `pvc.yaml`:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: auto-ebs-claim
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: auto-ebs-sc
  resources:
    requests:
      storage: 8Gi
```

2. Tragen Sie das PVC auf:

```
kubectl apply -f pvc.yaml
```

Die wichtigsten Komponenten:

- `accessModes`: `ReadWriteOnce`- Das Volumen kann von einem Knoten nach dem anderen gemountet werden
- `storage`: `8Gi`- Fordert ein 8-GiB-Volumen an
- `storageClassName`: `auto-ebs-sc`- Referenzen, die StorageClass wir erstellt haben

Schritt 4: Stellen Sie die Anwendung bereit

Bei der Bereitstellung wird ein Container ausgeführt, der Zeitstempel auf das persistente Volume schreibt.

1. Erstellen Sie eine Datei namens `deployment.yaml`:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: inflate-stateful
spec:
  replicas: 1
  selector:
    matchLabels:
      app: inflate-stateful
  template:
    metadata:
      labels:
        app: inflate-stateful
    spec:
      terminationGracePeriodSeconds: 0
      nodeSelector:
        eks.amazonaws.com/compute-type: auto
      containers:
        - name: bash
          image: public.ecr.aws/docker/library/bash:4.4
          command: ["/usr/local/bin/bash"]
          args: ["-c", "while true; do echo $(date -u) >> /data/out.txt; sleep 60;
done"]
      resources:
        requests:
          cpu: "1"
      volumeMounts:
        - name: persistent-storage
          mountPath: /data
```

```
volumes:
  - name: persistent-storage
    persistentVolumeClaim:
      claimName: auto-ebs-claim
```

2. Wenden Sie das Deployment an:

```
kubectl apply -f deployment.yaml
```

Die wichtigsten Komponenten:

- Einfacher Bash-Container, der Zeitstempel in eine Datei schreibt
- Montiert das PVC an /data
- Fordert 1 CPU-Kern an
- Verwendet den Knotenselektor für von EKS verwaltete Knoten

Schritt 5: Überprüfen Sie das Setup

1. Vergewissern Sie sich, dass der Pod läuft:

```
kubectl get pods -l app=inflate-stateful
```

2. Stellen Sie sicher, dass das PVC gebunden ist:

```
kubectl get pvc auto-ebs-claim
```

3. Überprüfen Sie das EBS-Volumen:

```
# Get the PV name
PV_NAME=$(kubectl get pvc auto-ebs-claim -o jsonpath='{.spec.volumeName}')
# Describe the EBS volume
aws ec2 describe-volumes \
  --filters Name=tag:CSIVolumeName,Values=${PV_NAME}
```

4. Stellen Sie sicher, dass Daten geschrieben werden:

```
kubectl exec "$(kubectl get pods -l app=inflate-stateful \
-o=jsonpath='{.items[0].metadata.name}')" -- \
cat /data/out.txt
```

Schritt 6: Bereinigen

Führen Sie den folgenden Befehl aus, um alle in diesem Tutorial erstellten Ressourcen zu entfernen:

```
# Delete all resources in one command
kubectl delete deployment/inflate-stateful pvc/auto-ebs-claim storageclass/auto-ebs-sc
```

Was passiert hinter den Kulissen

1. Das PVC bittet um Speicherplatz bei StorageClass
2. Wenn der Pod geplant ist:
 - a. Der EKS-Automatikmodus stellt ein EBS-Volume bereit
 - b. Erzeugt ein PersistentVolume
 - c. Hängt das Volume an den Knoten an
3. Der Pod hängt das Volume ein und beginnt mit dem Schreiben von Zeitstempeln

Snapshot-Controller

Der EKS Auto Mode ist mit dem Kubernetes CSI Snapshotter kompatibel, der auch als Snapshot-Controller bezeichnet wird. Der EKS Auto Mode beinhaltet jedoch nicht den Snapshot-Controller. Sie sind für die Installation und Konfiguration des Snapshot-Controllers verantwortlich. Weitere Informationen finden Sie unter [the section called “CSI-Snapshot-Controller”](#).

Lesen Sie den folgenden Abschnitt `VolumeSnapshotClass`, der sich auf die Speicherfähigkeit von EKS Auto Mode bezieht.

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: auto-ebs-vsclass
driver: ebs.csi.eks.amazonaws.com
deletionPolicy: Delete
```

[Erfahren Sie mehr über den Kubernetes CSI Snapshotter.](#)

Einstellungen für den EKS-Automatikmodus konfigurieren

In diesem Kapitel wird beschrieben, wie Sie bestimmte Aspekte Ihrer Amazon Elastic Kubernetes Service (EKS) Auto Mode-Cluster konfigurieren. Während der EKS Auto Mode die meisten Infrastrukturkomponenten automatisch verwaltet, können Sie bestimmte Funktionen an Ihre Workload-Anforderungen anpassen.

Mithilfe der in diesem Thema beschriebenen Konfigurationsoptionen können Sie Netzwerkeinstellungen, Rechenressourcen und Lastausgleichsverhalten ändern und gleichzeitig die Vorteile der automatisierten Infrastrukturverwaltung beibehalten. Bevor Sie Änderungen an der Konfiguration vornehmen, überprüfen Sie die verfügbaren Optionen in den folgenden Abschnitten, um festzustellen, welcher Ansatz Ihren Anforderungen am besten entspricht.

Welche Funktionen möchten Sie konfigurieren?	Konfigurationsoption
Knotenvernetzung und Speicher • Konfigurieren Sie die Knotenplatzierung in öffentlichen und privaten Subnetzen • Definieren Sie benutzerdefinierte Sicherheitsgruppen für die Knotenzugriffskontrolle • Passen Sie die SNAT-Richtlinien (Network Address Translation) an • Aktivieren Sie Kubernetes-Netzwerkrichtlinien, detaillierte Protokollierung und Überwachung von Netzwerkrichtlinien • Legen Sie temporäre Speicherparameter (Größe, IOPS, Durchsatz) fest • Konfigurieren Sie verschlüsselten kurzlebigen Speicher mit benutzerdefinierten KMS-Schlüsseln • Isolieren Sie den Pod-Verkehr in separaten Subnetzen von den Knoten	the section called “Erstellen Sie eine Knotenklasse”
Rechenressourcen für Knoten	the section called “Erstellen Sie einen Knotenpool”

Welche Funktionen möchten Sie konfigurieren?	Konfigurationsoption
• Wählen Sie bestimmte EC2 Instanztypen und -familien aus • Definieren Sie CPU-Architekturen (x86_64, ARM64) • Konfigurieren Sie Kapazitätstypen (On-Demand, Spot) • Geben Sie Verfügbarkeitszonen an • Konfigurieren Sie Knoten-Taints und Labels • Legen Sie die minimale und maximale Knotenanzahl fest	
Einstellungen für den Application Load Balancer • Stellen Sie interne oder mit dem Internet verbundene Load Balancer bereit • Konfigurieren des zonenübergreifenden Load Balancing • Legen Sie Timeout-Zeiträume für Leerlauf fest • Aktivieren Sie HTTP/2 und unterstützen Sie WebSocket • Konfigurieren Sie die Parameter für die Integritätsprüfung • Geben Sie Einstellungen für das TLS-Zertifikat an • Definieren Sie Zielgruppenattribute • Stellen Sie den IP-Adresstyp ein (IPv4, Dual-Stack)	<u>the section called “Ingress-Klasse erstellen”</u>

Welche Funktionen möchten Sie konfigurieren?	Konfigurationsoption
Einstellungen für den Network Load Balancer • Konfigurieren Sie direktes Pod-IP-Routing • Aktivieren von zonenübergreifendem Load Balancing • Legen Sie das Timeout für Verbindungsinaktivität fest • Konfigurieren Sie die Parameter für die Integritätsprüfung • Geben Sie die Platzierung des Subnetzes an • Stellen Sie den IP-Adresstyp ein (IPv4, Dual-Stack) • Konfigurieren Sie „Client-Quell-IP beibehalten“ • Definieren Sie Zielgruppenattribute	<u>the section called “Service erstellen”</u>
Einstellungen für die Speicherklasse • Definieren Sie EBS-Volumetypen (gp3, io1, io2 usw.) • Konfigurieren Sie die Volumenverschlüsselung und die Verwendung von KMS-Schlüsseln • Legen Sie IOPS- und Durchsatzparameter fest • Als Standard-Speicherklasse festlegen • Definieren Sie benutzerdefinierte Tags für bereitgestellte Volumes	<u>the section called “Erstellen StorageClass”</u>

Welche Funktionen möchten Sie konfigurieren?	Konfigurationsoption
Steuern Sie die ODCR-Nutzung • Konfigurieren Sie die Workload-Bereitstellung für EC2 Kapazitätsreservierungen auf Abruf • Wählen Sie für die gezielte Kapazitätsnutzung explizit eine bestimmte ODCRs ID aus • Verwenden Sie die Tag-basierte Auswahl für folgende Zielgruppen ODCRs • ODCRs Filtern Sie für kontoübergreifende Szenarien nach dem eigenen AWS Konto • Steuern Sie, ob Workloads automatisch „Öffnen“ verwenden ODCRs	the section called “Steuern Sie den ODCR-Einsatz”

Erstellen Sie eine Knotenklasse für Amazon EKS

Amazon EKS Node Classes sind Vorlagen, die eine detaillierte Kontrolle über die Konfiguration Ihrer von EKS Auto Mode verwalteten Knoten bieten. Eine Node-Klasse definiert Einstellungen auf Infrastrukturebene, die für Knotengruppen in Ihrem EKS-Cluster gelten, einschließlich Netzwerkkonfiguration, Speichereinstellungen und Ressourcen-Tagging. In diesem Thema wird erklärt, wie Sie eine Knotenklasse erstellen und konfigurieren, die Ihren spezifischen Betriebsanforderungen entspricht.

Wenn Sie anpassen müssen, wie EKS Auto Mode EC2 Instances über die Standardeinstellungen hinaus bereitstellt und konfiguriert, können Sie durch die Erstellung einer Node-Klasse präzise Kontrolle über kritische Infrastrukturparameter haben. Sie können beispielsweise die Platzierung eines privaten Subnetzes für mehr Sicherheit angeben, kurzlebigen Instanzspeicher für leistungsabhängige Workloads konfigurieren oder benutzerdefinierte Markierungen für die Kostenzuweisung anwenden.

Erstellen Sie eine Knotenklasse

Gehen Sie folgendermaßen vor, um eine `NodeClass` zu erstellen:

1. Erstellen Sie eine YAML-Datei (z. B. `nodeclass.yaml`) mit Ihrer Node-Class-Konfiguration

2. Wenden Sie die Konfiguration auf Ihren Cluster an mit `kubectl`
3. Verweisen Sie in Ihrer Node Pool-Konfiguration auf die Node-Klasse. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).

Sie müssen `kubectl` installiert und konfiguriert sein. Weitere Informationen finden Sie unter [Einrichten](#).

Grundlegendes Beispiel für eine Knotenklasse

Hier ist ein Beispiel für eine Knotenklasse:

```
apiVersion: eks.amazonaws.com/v1
kind: NodeClass
metadata:
  name: private-compute
spec:
  subnetSelectorTerms:
    - tags:
        Name: "private-subnet"
        kubernetes.io/role/internal-elb: "1"
  securityGroupSelectorTerms:
    - tags:
        Name: "eks-cluster-sg"
  ephemeralStorage:
    size: "160Gi"
```

Dies NodeClass erhöht die Menge an flüchtigem Speicher auf dem Knoten.

Wenden Sie diese Konfiguration an, indem Sie:

```
kubectl apply -f nodeclass.yaml
```

Verweisen Sie als Nächstes auf die Node Class in Ihrer Node Pool-Konfiguration. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).

Erstellen Sie einen Eintrag zum Zugriff auf die Knotenklasse

Wenn Sie eine benutzerdefinierte Knotenklasse erstellen, müssen Sie einen EKS-Zugriffseintrag erstellen, damit die Knoten dem Cluster beitreten können. EKS erstellt automatisch Zugriffseinträge, wenn Sie die integrierte Knotenklasse und die Knotenpools verwenden.

Informationen zur Funktionsweise von Access Entries finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#).

Beim Erstellen von Zugriffseinträgen für EKS Auto Mode-Knotenklassen müssen Sie den EC2 Zugriffseintragstyp verwenden.

Zugriffseintrag mit CLI erstellen

Um einen Zugriffseintrag für EC2 Knoten zu erstellen und die EKS Auto Node Policy zuzuordnen:

Aktualisieren Sie die folgenden CLI-Befehle mit Ihrem Clusternamen und dem ARN für die Knotenrolle. Die Knotenrolle ARN ist in der Knotenklasse YAML spezifiziert.

```
# Create the access entry for EC2 nodes
aws eks create-access-entry \
  --cluster-name <cluster-name> \
  --principal-arn <node-role-arn> \
  --type EC2

# Associate the auto node policy
aws eks associate-access-policy \
  --cluster-name <cluster-name> \
  --principal-arn <node-role-arn> \
  --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSAutoNodePolicy \
  --access-scope type=cluster
```

Erstellen Sie einen Zugangseintrag mit CloudFormation

Um einen Zugriffseintrag für EC2 Knoten zu erstellen und die EKS Auto Node Policy zuzuordnen:

Aktualisieren Sie Folgendes CloudFormation mit Ihrem Clusternamen und dem ARN für die Knotenrolle. Die Knotenrolle ARN ist in der Knotenklasse YAML spezifiziert.

```
EKSAutoNodeRoleAccessEntry:
  Type: AWS::EKS::AccessEntry
  Properties:
    ClusterName: <cluster-name>
    PrincipalArn: <node-role-arn>
    Type: "EC2"
    AccessPolicies:
      - AccessScope:
          Type: cluster
        PolicyArn: arn:aws:eks::aws:cluster-access-policy/AmazonEKSAutoNodePolicy
```

```
DependsOn: [ <cluster-name> ] # previously defined in CloudFormation
```

Informationen zum Bereitstellen von CloudFormation Stacks finden Sie unter [Erste Schritte](#) mit CloudFormation

Spezifikation der Knotenklasse

```
apiVersion: eks.amazonaws.com/v1
kind: NodeClass
metadata:
  name: my-node-class
spec:
  # Required fields
  role: MyNodeRole # IAM role for EC2 instances

  subnetSelectorTerms:
    - tags:
        Name: "private-subnet"
        kubernetes.io/role/internal-elb: "1"
      # Alternative using direct subnet ID
      # - id: "subnet-0123456789abcdef0"

  securityGroupSelectorTerms:
    - tags:
        Name: "eks-cluster-sg"
      # Alternative approaches:
      # - id: "sg-0123456789abcdef0"
      # - name: "eks-cluster-security-group"

  # Optional: Pod subnet selector for advanced networking
  podSubnetSelectorTerms:
    - tags:
        Name: "pod-subnet"
        kubernetes.io/role/pod: "1"
      # Alternative using direct subnet ID
      # - id: "subnet-0987654321fedcba0"

  # Optional: Selects on-demand capacity reservations and capacity blocks
  # for EKS Auto Mode to prioritize.
  capacityReservationSelectorTerms:
    - id: cr-56fac701cc1951b03
      # Alternative Approaches
```

```

- tags:
  Name: "targeted-odcr"
  # Optional owning account ID filter
  owner: "012345678901"

# Optional fields
snatPolicy: Random # or Disabled

networkPolicy: DefaultAllow # or DefaultDeny
networkPolicyEventLogs: Disabled # or Enabled

ephemeralStorage:
  size: "80Gi" # Range: 1-59000Gi or 1-64000G or 1-58Ti or 1-64T
  iops: 3000 # Range: 3000-16000
  throughput: 125 # Range: 125-1000
  # Optional KMS key for encryption
  kmsKeyID: "arn:aws:kms:region:account:key/key-id"
  # Accepted formats:
  # KMS Key ID
  # KMS Key ARN
  # Key Alias Name
  # Key Alias ARN

# Optional: Forward proxy, commonly requires certificateBundles as well
#for EC2, see https://repost.aws/knowledge-center/eks-http-proxy-containerd-
automation
advancedNetworking:
  httpsProxy: http://192.0.2.4:3128 #commonly port 3128 (Squid) or 8080 (NGINX) #Max
255 characters
  #httpsProxy: http://[2001:db8::4]:3128 # IPv6 address with port, use []
  noProxy: #Max 50 entries
    - localhost #Max 255 characters each
    - 127.0.0.1
    #- ::1 # IPv6 localhost
    #- 0:0:0:0:0:0:0:1 # IPv6 localhost
    - 169.254.169.254 # EC2 Instance Metadata Service
    #- [fd00:ec2::254] # IPv6 EC2 Instance Metadata Service
    # Domains to exclude, put all VPC endpoints here
    - .internal
    - .eks.amazonaws.com

# Optional: Custom certificate bundles.
certificateBundles:
  - name: "custom-cert"

```

```

    data: "base64-encoded-cert-data"

# Optional: Additional EC2 tags (with restrictions)
tags:
  Environment: "production"
  Team: "platform"
# Note: Cannot use restricted tags like:
# - kubernetes.io/cluster/*
# - karpenter.sh/provisioner-name
# - karpenter.sh/nodepool
# - karpenter.sh/nodeclaim
# - karpenter.sh/managed-by
# - eks.amazonaws.com/nodeclass

```

Überlegungen

- **Volumenverschlüsselung** — EKS verwendet den konfigurierten benutzerdefinierten KMS-Schlüssel, um das schreibgeschützte Root-Volume der Instance und das Datenvolume zu verschlüsseln. read/write
- **Ersetzen Sie die Knoten-IAM-Rolle** — Wenn Sie die Knoten-IAM-Rolle ändern, die mit einem `nodeClass` verknüpft ist, müssen Sie einen neuen Zugriffseintrag erstellen. EKS erstellt bei der Clustererstellung automatisch einen Zugriffseintrag für die Knoten-IAM-Rolle. Für die Knoten-IAM-Rolle ist die `AmazonEKSAutoNodePolicy` EKS-Zugriffsrichtlinie erforderlich. Weitere Informationen finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#).
- **maximale Pod-Dichte** — EKS begrenzt die maximale Anzahl von Pods auf einem Knoten auf 110. Dieses Limit wird nach der Berechnung der vorhandenen maximalen Anzahl an Pods angewendet. Weitere Informationen finden Sie unter [the section called “EC2 Amazon-Instance-Typen”](#).
- **Tags** — Wenn Sie Tags von Kubernetes an weitergeben möchten EC2, müssen Sie zusätzliche IAM-Berechtigungen konfigurieren. Weitere Informationen finden Sie unter [the section called “Identität und Zugriff”](#).
- **Standard-Knotenklasse** — Benennen Sie Ihre benutzerdefinierte Knotenklasse nicht. `default` Dies liegt daran, `default` dass der automatische EKS-Modus einen `NodeClass` Anruf enthält, der automatisch bereitgestellt wird, wenn Sie mindestens einen integrierten `NodePool` Modus aktivieren. Informationen zur Aktivierung der integrierten Funktion finden Sie `NodePools` unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).
- **`subnetSelectorTerms`** Verhalten mit mehreren Subnetzen — Wenn es mehrere Subnetze gibt, die den `subnetSelectorTerms` Bedingungen entsprechen oder die Sie anhand der ID angeben, erstellt der automatische Modus von EKS Knoten, die über die Subnetze verteilt sind.

- Wenn sich die Subnetze in unterschiedlichen Availability Zones (AZ) befinden, können Sie Kubernetes-Funktionen wie [Spread-Beschränkungen für die Pod-Topologie und Topology Aware Routing](#) verwenden, um Pods bzw. Traffic über die Zonen zu verteilen.
- Wenn es in derselben AZ mehrere Subnetze gibt, die den entsprechen, erstellt der automatische Modus von EKS Pods auf jedem KnotensubnetSelectorTerms, die über die Subnetze in dieser AZ verteilt sind. Der EKS-Automatikmodus erstellt sekundäre Netzwerkschnittstellen auf jedem Knoten in den anderen Subnetzen in derselben AZ. Es wählt anhand der Anzahl der verfügbaren IP-Adressen in jedem Subnetz aus, um die Subnetze effizienter zu nutzen. Sie können jedoch nicht angeben, welches Subnetz EKS Auto Mode für jeden Pod verwendet. Wenn Pods in bestimmten Subnetzen ausgeführt werden sollen, verwenden Sie stattdessen. [the section called "Subnetauswahl für Pods"](#)

Subnetauswahl für Pods

Die podSecurityGroupSelectorTerms Felder podSubnetSelectorTerms und ermöglichen erweiterte Netzwerkkonfigurationen, da Pods in anderen Subnetzen als ihren Knoten ausgeführt werden können. Diese Trennung ermöglicht eine verbesserte Kontrolle über das Routing des Netzwerkverkehrs und die Sicherheitsrichtlinien. Beachten Sie, dass diese zusammen mit dem erforderlich podSecurityGroupSelectorTerms sind podSubnetSelectorTerms.

Anwendungsfälle

Verwenden Sie podSubnetSelectorTerms es, wenn Sie:

- Trennen Sie den Infrastrukturverkehr (node-to-node Kommunikation) vom Anwendungsverkehr (pod-to-pod Kommunikation)
- Wenden Sie auf Knoten-Subnetze andere Netzwerkkonfigurationen als auf Pod-Subnetze an.
- Implementieren Sie unterschiedliche Sicherheitsrichtlinien oder Routing-Regeln für Knoten und Pods.
- Konfigurieren Sie Reverse-Proxys oder Netzwerkfilterung speziell für den Knotenverkehr, ohne den Pod-Verkehr zu beeinträchtigen. Verwenden Sie advancedNetworking und certificateBundles, um Ihren Reverse-Proxy und alle selbstsignierten oder privaten Zertifikate für den Proxy zu definieren.

Beispielkonfiguration

```
apiVersion: eks.amazonaws.com/v1
```



```
kind: NodeClass
metadata:
  name: advanced-networking
spec:
  role: MyNodeRole

  # Subnets for EC2 instances (nodes)
  subnetSelectorTerms:
    - tags:
        Name: "node-subnet"
        kubernetes.io/role/internal-elb: "1"

  securityGroupSelectorTerms:
    - tags:
        Name: "eks-cluster-sg"

  # Separate subnets for pods
  podSubnetSelectorTerms:
    - tags:
        Name: "pod-subnet"
        kubernetes.io/role/pod: "1"

  podSecurityGroupSelectorTerms:
    - tags:
        Name: "eks-pod-sg"
```

Überlegungen zu Subnetz-Selektoren für Pods

- Reduzierte Pod-Dichte: Bei der Verwendung können weniger Pods auf jedem Knoten ausgeführt werden `podSubnetSelectorTerms`, da sich die primäre Netzwerkschnittstelle des Nodes im Knoten-Subnetz befindet und nicht für Pods im Pod-Subnetz verwendet werden kann.
- Einschränkungen bei der Subnetzauswahl: Der Standard `subnetSelectorTerms` und die `securityGroupSelectorTerms` Konfigurationen gelten nicht für die Auswahl des Pod-Subnetzes.
- Netzwerkplanung: Sorgen Sie für ausreichend IP-Adressraum sowohl in den Knoten- als auch in den Pod-Subnetzen, um Ihre Workload-Anforderungen zu erfüllen.
- Routing-Konfiguration: Stellen Sie sicher, dass die Routing-Tabelle und die Netzwerk-Zugriffskontrollliste (ACL) der Pod-Subnetze ordnungsgemäß für die Kommunikation zwischen Knoten- und Pod-Subnetzen konfiguriert sind.

Erstellen Sie einen Knotenpool für den automatischen Modus von EKS

Amazon EKS-Knotenpools bieten eine flexible Möglichkeit, Rechenressourcen in Ihrem Kubernetes-Cluster zu verwalten. In diesem Thema wird gezeigt, wie Sie Knotenpools mithilfe von Karpenter erstellen und konfigurieren, einem Knotenbereitstellungstool, das zur Optimierung der Clusterskalierung und Ressourcennutzung beiträgt. Mit den NodePool Ressourcen von Karpenter können Sie spezifische Anforderungen für Ihre Rechenressourcen definieren, einschließlich Instanztypen, Availability Zones, Architekturen und Kapazitätstypen.

Sie können die integrierten Pools `system` und `general-purpose` die Knotenpools nicht ändern. Sie können sie nur aktivieren oder deaktivieren. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).

Die NodePool Spezifikation ermöglicht eine detaillierte Steuerung der Rechenressourcen Ihres EKS-Clusters durch verschiedene unterstützte Labels und Anforderungen. Dazu gehören Optionen zur Angabe von EC2 Instanzkategorien, CPU-Konfigurationen, Availability Zones, Architekturen (ARM64/AMD64) und Kapazitätstypen (Spot oder On-Demand). Sie können auch Ressourcenlimits für die CPU- und Speicherauslastung festlegen, um sicherzustellen, dass Ihr Cluster innerhalb der erforderlichen Betriebsgrenzen bleibt.

EKS Auto Mode nutzt bekannte Kubernetes-Labels, um konsistente und standardisierte Methoden zur Identifizierung von Knotenmerkmalen bereitzustellen. Diese Labels, beispielsweise `topology.kubernetes.io/zone` für Availability Zones und `kubernetes.io/arch` für die CPU-Architektur, folgen etablierten Kubernetes-Konventionen. Darüber hinaus erweitern EKS-spezifische Labels (mit Präfix `eks.amazonaws.com/`) diese Funktionalität um AWS spezifische Attribute wie Instance-Typen, CPU-Hersteller, GPU-Fähigkeiten und Netzwerkspezifikationen. Dieses standardisierte Kennzeichnungssystem ermöglicht eine nahtlose Integration mit bestehenden Kubernetes-Tools und bietet gleichzeitig eine umfassende Infrastrukturintegration. AWS

Erstellen Sie ein NodePool

Gehen Sie wie folgt vor, um einen NodePool für Ihren Amazon EKS-Cluster zu erstellen:

1. Erstellen Sie eine YAML-Datei `nodepool1.yaml` mit dem Namen Ihrer erforderlichen NodePool Konfiguration. Sie können die folgende Beispielkonfiguration verwenden.
2. Wenden Sie das NodePool auf Ihren Cluster an:

```
kubectl apply -f nodepool1.yaml
```

3. Stellen Sie sicher, dass das erfolgreich erstellt NodePool wurde:

```
kubectl get nodepools
```

4. (Optional) Überwachen Sie den NodePool Status:

```
kubectl describe nodepool default
```

Stellen Sie sicher, dass Ihre NodePool Referenzen gültig sind NodeClass und in Ihrem Cluster vorhanden sind. Das NodeClass definiert AWS-spezifische Konfigurationen für Ihre Rechenressourcen. Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Knotenklasse”](#).

Beispiel NodePool

```
apiVersion: karpenter.sh/v1
kind: NodePool
metadata:
  name: my-node-pool
spec:
  template:
    metadata:
      labels:
        billing-team: my-team
    spec:
      nodeClassRef:
        group: eks.amazonaws.com
        kind: NodeClass
        name: default

      requirements:
        - key: "eks.amazonaws.com/instance-category"
          operator: In
          values: ["c", "m", "r"]
        - key: "eks.amazonaws.com/instance-cpu"
          operator: In
          values: ["4", "8", "16", "32"]
        - key: "topology.kubernetes.io/zone"
          operator: In
          values: ["us-west-2a", "us-west-2b"]
        - key: "kubernetes.io/arch"
```

```
operator: In
values: ["arm64", "amd64"]

limits:
  cpu: "1000"
  memory: 1000Gi
```

Von EKS Auto Mode unterstützte Labels

Der EKS-Automatikmodus unterstützt die folgenden bekannten Labels.

Note

Der EKS Auto Mode verwendet andere Labels als Karpenter. Beschriftungen, die sich auf EC2 verwaltete Instanzen beziehen, beginnen mit. `eks.amazonaws.com`

Label (Bezeichnung)	Beispiel	Beschreibung
<code>topology.kubernetes.io/zone</code>	<code>us-east-2a</code>	AWS Region
<code>node.kubernetes.io/instance-type</code>	<code>g4dn.8xlarge</code>	AWS Instanztyp
<code>kubernetes.io/arch</code>	<code>amd64</code>	Architekturen werden durch GOARCH-Werte auf der Instanz definiert
<code>karpenter.sh/capacity-type</code>	Stelle	Zu den Kapazitätstypen spot gehören on-demand
<code>eks.amazonaws.com/instance-hypervisor</code>	Nitro	Instanztypen, die einen bestimmten Hypervisor verwenden
<code>eks.amazonaws.com/compute-type</code>	auto	Identifiziert verwaltete EKS-Automodus-Knoten
<code>eks.amazonaws.com/instance-encryption-in-transit</code> -unterstützt	true	Instance-Typen, die Verschlüsselung bei der Übertragung unterstützen (oder nicht)

Label (Bezeichnung)	Beispiel	Beschreibung
eks.amazonaws.com/instance-category	g	Instance-Typen derselben Kategorie, normalerweise die Zeichenfolge vor der Generationsnummer
eks.amazonaws.com/instance-generation	4	Generationsnummer des Instance-Typs innerhalb einer Instance-Kategorie
eks.amazonaws.com/instance-family	g4dn	Instance-Typen mit ähnlichen Eigenschaften, aber unterschiedlichen Ressourcenmengen
eks.amazonaws.com/instance-size	8xlarge	Instance-Typen mit ähnlichen Ressourcennmengen, aber unterschiedlichen Eigenschaften
eks.amazonaws.com/instance-cpu	32	Nummer von auf der Instance CPUs
eks.amazonaws.com/instance-cpu-manufacturer	aws	Name des CPU-Herstellers
eks.amazonaws.com/instance-memory	131072	Anzahl der Mebibyte Speicher auf der Instanz
eks.amazonaws.com/instance-ebs-bandwidth	9500	Anzahl der maximal auf der Instance verfügbaren EBS-Megabit
eks.amazonaws.com/instance-network-bandwidth	131072	Anzahl der auf der Instance verfügbaren Basis-Megabit
eks.amazonaws.com/instance-gpu-name	t4	Name der GPU auf der Instance, falls verfügbar
eks.amazonaws.com/instance-gpu-manufacturer	nvidia	Name des GPU-Herstellers
eks.amazonaws.com/instance-gpu-count	1	Nummer von auf der Instance GPUs

Label (Bezeichnung)	Beispiel	Beschreibung
eks.amazonaws.com/ instance-gpu-memory	16384	Anzahl der Mebibyte Speicher auf der GPU
eks.amazonaws.com/ instance-local-nvme	900	Anzahl der Gibibytes des lokalen NVME-Speichers auf der Instance

Note

Der automatische Modus von EKS unterstützt nur bestimmte Instanzen und hat Mindestgrößenanforderungen. Weitere Informationen finden Sie unter [the section called “Referenz zu den von EKS Auto Mode unterstützten Instanzen”](#).

Der EKS-Automatikmodus wird nicht unterstützt. Labels

Der EKS-Automatikmodus unterstützt die folgenden Bezeichnungen nicht.

- Der EKS-Automatikmodus unterstützt nur Linux
 - `node.kubernetes.io/windows-build`
 - `kubernetes.io/os`

Deaktivieren Sie integrierte Knotenpools

Wenn Sie benutzerdefinierte Knotenpools erstellen, können Sie die integrierten Knotenpools deaktivieren. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).

Cluster ohne integrierte Knotenpools

Sie können einen Cluster ohne die integrierten Knotenpools erstellen. Dies ist hilfreich, wenn Ihre Organisation benutzerdefinierte Knotenpools erstellt hat.

Note

Wenn Sie einen Cluster ohne integrierte Knotenpools erstellen, default NodeClass wird dieser nicht automatisch bereitgestellt. Sie müssen einen benutzerdefinierten NodeClass

erstellen. Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Knotenklasse”](#).

Überblick:

1. Erstellen Sie einen EKS-Cluster mit leeren `nodeRoleArn` Werten `nodePools` sowohl als auch.

- Beispiel `eksctl autoModeConfig`:

```
autoModeConfig:
  enabled: true
  nodePools: []
  # Do not set a nodeRoleARN
```

Weitere Informationen finden Sie unter [the section called “eksctl CLI”](#).

2. Erstellen Sie eine benutzerdefinierte Knotenklasse mit einer Knotenrolle ARN

- Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Knotenklasse”](#).

3. Erstellen Sie einen Zugriffseintrag für die benutzerdefinierte Knotenklasse

- Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Eintrag zum Zugriff auf die Knotenklasse”](#).

4. Erstellen Sie einen benutzerdefinierten Knotenpool, wie oben beschrieben.

Störung

Sie können den EKS-Automodus so konfigurieren, dass er Nodes auf verschiedene NodePool Weise unterbricht. Sie können

`spec.disruption.consolidationPolicy` `spec.disruption.consolidateAfter`, oder `spec.template.spec.expireAfter` verwenden. Sie können auch die Unterbrechung des EKS Auto Mode durch die NodePool s begrenzen `spec.disruption.budgets`. Sie können auch die Zeitfenster und die Anzahl der gleichzeitig unterbrochenen Knoten steuern. Anweisungen zur Konfiguration dieses Verhaltens finden Sie unter [Disruption](#) in der Karpenter Documentation.

Sie können die Unterbrechung für Knotenpools so konfigurieren, dass:

- Identifizieren Sie, wann Instanzen nicht ausgelastet sind, und konsolidieren Sie Workloads.
- Richten Sie ein Budget für Störungen im Knotenpool ein, um die Anzahl der Knotenabbrüche aufgrund von Drift, Leerheit und Konsolidierung zu begrenzen.

Standardmäßig ist der automatische EKS-Modus:

- Konsolidiert nicht ausgelastete Instanzen.
- Beendet Instanzen nach 336 Stunden.
- Legt ein einzelnes Ausfallbudget von 10% der Knoten fest.
- Ermöglicht den Austausch von Knoten aufgrund von Drift, wenn ein neues Auto-Modus-AMI veröffentlicht wird, was ungefähr einmal pro Woche der Fall ist.

Kündigung, Nachfrist.

Wenn `a` in einem EKS Auto nicht explizit definiert `terminationGracePeriod` ist `NodePool`, wendet das System automatisch eine standardmäßige Kündigungsfrist von 24 Stunden auf die zugehörige Datei an `NodeClaim`. Kunden von EKS Auto werden in ihren benutzerdefinierten `NodePool` Konfigurationen zwar keinen `terminationGracePeriod` Standardwert sehen, aber sie werden diesen Standardwert auf der verwenden. `NodeClaim` Die Funktionalität bleibt konsistent, unabhängig davon, ob der Kulanzz Zeitraum explizit auf `NodePool` oder standardmäßig auf dem festgelegt ist `NodeClaim`, wodurch ein vorhersehbares Verhalten bei der Knotenbeendigung im gesamten Cluster gewährleistet wird.

Erstellen Sie einen IngressClass , um einen Application Load Balancer zu konfigurieren

Der automatische Modus von EKS automatisiert Routineaufgaben für den Lastenausgleich, einschließlich der Bereitstellung von Cluster-Apps im Internet.

AWS schlägt vor, Application Load Balancers (ALB) zur Bereitstellung von HTTP- und HTTPS-Verkehr zu verwenden. Application Load Balancers können Anfragen basierend auf dem Inhalt der Anfrage weiterleiten. Weitere Informationen zu Application Load Balancers finden Sie unter [Was ist Elastic Load Balancing?](#)

Der automatische EKS-Modus erstellt und konfiguriert Application Load Balancers (). ALBs Beispielsweise erstellt der automatische Modus von EKS einen Load Balancer, wenn Sie ein Ingress Kubernetes-Objekt erstellen, und konfiguriert ihn so, dass der Datenverkehr an Ihren Cluster-Workload weitergeleitet wird.

Übersicht

1. Erstellen Sie einen Workload, den Sie dem Internet zugänglich machen möchten.

2. Erstellen Sie eine `IngressClassParams` Ressource und geben Sie AWS bestimmte Konfigurationswerte an, z. B. das zu verwendende Zertifikat SSL/TLS und VPC-Subnetze.
3. Erstellen Sie eine `IngressClass` Ressource und geben Sie an, dass EKS Auto Mode der Controller für die Ressource sein soll.
4. Erstellen Sie eine `Ingress` Ressource, die einem Cluster-Workload einen HTTP-Pfad und -Port zuordnet.

Der automatische Modus von EKS erstellt einen Application Load Balancer, der auf die in der Ressource angegebene Arbeitslast verweist, wobei die in der `Ingress` Ressource angegebene Load Balancer-Konfiguration verwendet wird. `IngressClassParams`

Voraussetzungen

- Der automatische EKS-Modus ist auf einem Amazon EKS-Cluster aktiviert
- Kubectl ist für die Verbindung mit Ihrem Cluster konfiguriert
 - Sie können `kubectl apply -f <filename>` die folgenden YAML-Beispielkonfigurationsdateien auf Ihren Cluster anwenden.

Note

Der automatische EKS-Modus benötigt Subnetz-Tags, um öffentliche und private Subnetze zu identifizieren.

Wenn Sie Ihren Cluster mit `eksctl` erstellt haben, verfügen Sie bereits über diese Tags. Weitere Informationen erhalten Sie unter [the section called “Taggen Sie Subnetze”](#).

Schritt 1: Erstellen Sie einen Workload

Erstellen Sie einen Workload, den Sie dem Internet zugänglich machen möchten. Dabei kann es sich um eine beliebige Kubernetes-Ressource handeln, die HTTP-Verkehr bedient, z. B. ein Deployment oder ein Service. In diesem Beispiel verwenden wir einen einfachen HTTP-Dienst `namensservice-2048`, der HTTP-Verkehr auf Port 80 bedient.

Schritt 2: Erstellen `IngressClassParams`

Erstellen Sie ein `IngressClassParams` Objekt, um AWS spezifische Konfigurationsoptionen für den Application Load Balancer anzugeben. In diesem Beispiel erstellen wir eine

IngressClassParams Ressource mit dem Namen alb (die Sie im nächsten Schritt verwenden werden), die das Load Balancer-Schema wie internet-facing in einer Datei mit dem Namen alb-ingressclassparams.yaml

```
apiVersion: eks.amazonaws.com/v1
kind: IngressClassParams
metadata:
  name: alb
spec:
  scheme: internet-facing
```

Wenden Sie die Konfiguration auf Ihren Cluster an:

```
kubectl apply -f alb-ingressclassparams.yaml
```

Schritt 3: Erstellen IngressClass

Erstellen Sie eine IngressClass, die auf die AWS spezifischen Konfigurationswerte verweist, die in der IngressClassParams Ressource in einer Datei mit dem Namen alb-ingressclass.yaml. Notieren Sie sich den Namen der IngressClass. In diesem Beispiel IngressClassParams sind IngressClass sowohl die als auch benannt alb.

Verwenden Sie die is-default-class Anmerkung, um zu steuern, ob Ingress Ressourcen diese Klasse standardmäßig verwenden sollen.

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: alb
  annotations:
    # Use this annotation to set an IngressClass as Default
    # If an Ingress doesn't specify a class, it will use the Default
    ingressclass.kubernetes.io/is-default-class: "true"
spec:
  # Configures the IngressClass to use EKS Auto Mode
  controller: eks.amazonaws.com/alb
  parameters:
    apiGroup: eks.amazonaws.com
    kind: IngressClassParams
    # Use the name of the IngressClassParams set in the previous step
    name: alb
```

Weitere Informationen zu Konfigurationsoptionen finden Sie unter [the section called “IngressClassParams Referenz”](#).

Wenden Sie die Konfiguration auf Ihren Cluster an:

```
kubectl apply -f alb-ingressclass.yaml
```

Schritt 4: Ingress erstellen

Erstellen Sie eine Ingress Ressource in einer Datei mit dem Namen `alb-ingress.yaml`. Der Zweck dieser Ressource besteht darin, Pfade und Ports auf dem Application Load Balancer mit Workloads in Ihrem Cluster zu verknüpfen. In diesem Beispiel erstellen wir eine Ingress Ressource mit dem Namen, `2048-ingress` die den Datenverkehr an einen Dienst weiterleitet, der `service-2048` auf Port 80 benannt ist.

Weitere Informationen zur Konfiguration dieser Ressource finden Sie unter [Ingress](#) in der Kubernetes-Dokumentation.

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: 2048-ingress
spec:
  # this matches the name of IngressClass.
  # this can be omitted if you have a default ingressClass in cluster: the one with
  ingressclass.kubernetes.io/is-default-class: "true"  annotation
  ingressClassName: alb
  rules:
    - http:
        paths:
          - path: /*
            pathType: ImplementationSpecific
            backend:
              service:
                name: service-2048
                port:
                  number: 80
```

Wenden Sie die Konfiguration auf Ihren Cluster an:

```
kubectl apply -f alb-ingress.yaml
```

Schritt 5: Status überprüfen

Verwenden Sie `kubectl`, um den Status von `ingress` zu ermitteln. Es kann einige Minuten dauern, bis der Load Balancer verfügbar ist.

Verwenden Sie den Namen der Ingress Ressource, den Sie im vorherigen Schritt festgelegt haben. Zum Beispiel:

```
kubectl get ingress 2048-ingress
```

Sobald die Ressource bereit ist, rufen Sie den Domainnamen des Load Balancers ab.

```
kubectl get ingress 2048-ingress -o  
jsonpath='{.status.loadBalancer.ingress[0].hostname}'
```

Um den Dienst in einem Webbrowser anzuzeigen, überprüfen Sie den Port und den Pfad, die im Ingress Resource angegeben wurden.

Schritt 6: Bereinigen

Verwenden Sie den folgenden Befehl, um den Load Balancer zu bereinigen:

```
kubectl delete ingress 2048-ingress  
kubectl delete ingressclass alb  
kubectl delete ingressclassparams alb
```

Der automatische Modus von EKS löscht automatisch den zugehörigen Load Balancer in Ihrem AWS Konto.

IngressClassParams Referenz

Die folgende Tabelle ist eine Kurzreferenz für häufig verwendete Konfigurationsoptionen.

Feld	Beschreibung	Beispielwert
<code>scheme</code>	Definiert, ob das ALB intern oder mit dem Internet verbunden ist	<code>internet-facing</code>

Feld	Beschreibung	Beispielwert
<code>namespaceSelector</code>	Schränkt ein, welche Namespaces dies verwenden können IngressClass	<code>environment: prod</code>
<code>group.name</code>	Gruppiert mehrere Ingresses , sodass sie sich ein einziges ALB teilen	<code>retail-apps</code>
<code>ipAddressType</code>	Legt den IP-Adresstyp für den ALB fest	<code>dualstack</code>
<code>subnets.ids</code>	Liste der Subnetze IDs für die ALB-Bereitstellung	<code>subnet-xxxx, subnet-yyyy</code>
<code>subnets.tags</code>	Tag-Filter zur Auswahl von Subnetzen für ALB	<code>Environment: prod</code>
<code>certificateARNs</code>	ARNs der zu verwendenden SSL-Zertifikate	<code>arn:aws:acm:region:account:certificate/id</code>
<code>tags</code>	Benutzerdefinierte Tags für AWS Ressourcen	<code>Environment: prod, Team: platform</code>
<code>loadBalancerAttributes</code>	Load Balancer-spezifische Attribute	<code>idle_timeout.timeout_seconds: 60</code>

Überlegungen

- Sie können Anmerkungen nicht für eine verwenden, IngressClass um Load Balancer mit dem automatischen EKS-Modus zu konfigurieren.
- Sie müssen die Cluster-IAM-Rolle aktualisieren, um die Tag-Weitergabe von Kubernetes an AWS Load Balancer-Ressourcen zu ermöglichen. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte AWS Tags für EKS Auto-Ressourcen”](#).

- Informationen zum Zuordnen von Ressourcen zum automatischen Modus von EKS oder zum selbstverwalteten Load AWS Balancer Controller finden Sie unter. [the section called “Referenz zur Migration”](#)
- Informationen zur Behebung von Problemen mit Load Balancers finden Sie unter. [the section called “Fehlerbehebung”](#)
- Weitere Hinweise zur Verwendung der Lastenausgleichsfunktion von EKS Auto Mode finden Sie unter [the section called “Load Balancing”](#).

Die folgenden Tabellen bieten einen detaillierten Vergleich der Änderungen IngressClassParams, der Ingress-Anmerkungen und der TargetGroupBinding Konfigurationen für den automatischen EKS-Modus. In diesen Tabellen werden die wichtigsten Unterschiede zwischen der Lastenausgleichsfunktion von EKS Auto Mode und dem Open-Source-Load Balancer-Controller hervorgehoben, einschließlich API-Versionsänderungen, veralteter Funktionen und aktualisierter Parameternamen.

IngressClassParams

Zurück	Neu	Beschreibung
<code>elbv2.k8s.aws/v1beta1</code>	<code>eks.amazonaws.com/v1</code>	Änderung der API-Version
<code>spec.certificateArn</code>	<code>spec.certificateARNs</code>	Support für mehrere Zertifikate ARNs
<code>spec.subnets.tags</code>	<code>spec.subnets.matchTags</code>	Das Subnetz-Abgleichschema wurde geändert
<code>spec.listeners.listenerAttributes</code>	<code>spec.listeners.attributes</code>	Vereinfachte Attributenennung

Eingangs-Anmerkungen

Bisherige	Neu	Beschreibung
<code>kubernetes.io/ingress.class</code>	Nicht unterstützt	Für <code>spec.ingressClassName</code> Ingress-Objekte verwenden
<code>alb.ingress.kubernetes.io/group.name</code>	Nicht unterstützt	Geben Sie Gruppen nur in an IngressClass
<code>alb.ingress.kubernetes.io/waf-acl-id</code>	Nicht unterstützt	Verwenden Sie stattdessen WAF v2
<code>alb.ingress.kubernetes.io/web-acl-id</code>	Nicht unterstützt	Verwenden Sie stattdessen WAF v2
<code>alb.ingress.kubernetes.io/shield-advanced-protection</code>	Nicht unterstützt	Shield-Integration deaktiviert
<code>alb.ingress.kubernetes.io/auth-type: oidc</code>	Nicht unterstützt	Der OIDC-Authentifizierungstyp wird derzeit nicht unterstützt

TargetGroupBinding

Bisherige	Neu	Beschreibung
<code>elbv2.k8s.aws/v1beta1</code>	<code>eks.amazonaws.com/v1</code>	Änderung der API-Version
<code>spec.targetType</code> optional	<code>spec.targetType</code> erforderlich	Explizite Angabe des Zieltyps
<code>spec.networking.ingress.from</code>	Nicht unterstützt	Unterstützt NLB ohne Sicherheitsgruppen nicht mehr

Verwenden Sie Service Annotations, um Network Load Balancer zu konfigurieren

Erfahren Sie, wie Sie Network Load Balancers (NLB) in Amazon EKS mithilfe von Kubernetes-Serviceanmerkungen konfigurieren. In diesem Thema werden die Anmerkungen erläutert, die vom automatischen Modus von EKS zur Anpassung des NLB-Verhaltens unterstützt werden, einschließlich Internetzugriff, Integritätsprüfungen, Kündigung und IP-Targeting-Modi. SSL/TLS

Wenn Sie einen Kubernetes-Dienst vom Typ `LoadBalancer` im EKS-Automodus erstellen, stellt EKS automatisch einen AWS Network Load Balancer bereit und konfiguriert ihn auf der Grundlage der von Ihnen angegebenen Anmerkungen. Dieser deklarative Ansatz ermöglicht es Ihnen, Load Balancer-Konfigurationen direkt über Ihre Kubernetes-Manifeste zu verwalten und dabei die Infrastruktur als Code-Praktiken beizubehalten.

Der automatische Modus von EKS übernimmt standardmäßig die Bereitstellung von Network Load Balancer für alle Dienste dieses Typs `LoadBalancer` — es ist keine zusätzliche Controller-Installation oder -Konfiguration erforderlich. Die `loadBalancerClass: eks.amazonaws.com/nlb` Spezifikation wird automatisch als Cluster-Standard festgelegt, wodurch der Bereitstellungsprozess optimiert und gleichzeitig die Kompatibilität mit vorhandenen Kubernetes-Workloads gewahrt bleibt.

Note

Der automatische Modus von EKS benötigt Subnetz-Tags, um öffentliche und private Subnetze zu identifizieren.

Wenn Sie Ihren Cluster mit `eksctl` erstellt haben, verfügen Sie bereits über diese Tags. Weitere Informationen erhalten Sie unter [the section called “Taggen Sie Subnetze”](#).

Beispiel für einen Service

Weitere Informationen zur Service Kubernetes-Ressource finden Sie in [der Kubernetes-Dokumentation](#).

Sehen Sie sich die folgende Beispiellressource an: Service

```
apiVersion: v1
kind: Service
metadata:
  name: echoserver
```



```
annotations:
  # Specify the load balancer scheme as internet-facing to create a public-facing
  # Network Load Balancer (NLB)
  service.beta.kubernetes.io/aws-load-balancer-scheme: internet-facing
spec:
  selector:
    app: echoserver
  ports:
    - port: 80
      targetPort: 8080
      protocol: TCP
  type: LoadBalancer
  # Specify the new load balancer class for NLB as part of EKS Auto Mode feature
  # For clusters with Auto Mode enabled, this field can be omitted as it's the default
  loadBalancerClass: eks.amazonaws.com/nlb
```

Häufig verwendete Anmerkungen

In der folgenden Tabelle sind häufig verwendete Anmerkungen aufgeführt, die vom EKS Auto Mode unterstützt werden. Beachten Sie, dass der automatische EKS-Modus möglicherweise nicht alle Anmerkungen unterstützt.

Tip

Allen folgenden Anmerkungen muss ein Präfix vorangestellt werden
`service.beta.kubernetes.io/`

Feld	Beschreibung	Beispiel
<code>aws-load-balancer-type</code>	Gibt den Load Balancer-Typ an. Wird <code>external</code> für neue Bereitstellungen verwendet.	<code>external</code>
<code>aws-load-balancer-nlb-target-type</code>	Gibt an, ob der Datenverkehr an Knoteninstanzen oder direkt an den Pod IPs weitergeleitet werden soll. Wird <code>instance</code> für Standardbereitstellungen oder <code>ip</code>	<code>instance</code>

Feld	Beschreibung	Beispiel
	für direktes Pod-Routing verwendet.	
<code>aws-load-balancer-scheme</code>	Steuert, ob der Load Balancer intern oder mit dem Internet verbunden ist.	<code>internet-facing</code>
<code>aws-load-balancer-healthcheck-protocol</code>	Gesundheitscheck-Protokoll für die Zielgruppe. Übliche Optionen sind TCP (Standard) oder HTTP.	HTTP
<code>aws-load-balancer-healthcheck-path</code>	Der HTTP-Pfad für Integritätsprüfungen bei Verwendung HTTP/HTTPS des Protokolls.	<code>/healthz</code>
<code>aws-load-balancer-healthcheck-port</code>	Port, der für Integritätsprüfungen verwendet wird. Kann eine bestimmte Portnummer sein oder <code>traffic-port</code> .	<code>traffic-port</code>
<code>aws-load-balancer-subnets</code>	Gibt an, in welchen Subnetzen der Load Balancer erstellt werden soll. Kann Subnetz oder Namen IDs verwenden.	<code>subnet-xxxx</code> , <code>subnet-yyyy</code>
<code>aws-load-balancer-ssl-cert</code>	ARN des SSL-Zertifikats von AWS Certificate Manager für HTTPS/TLS.	<code>arn:aws:acm:region:account:certificate/cert-id</code>
<code>aws-load-balancer-ssl-ports</code>	Gibt an, welche Ports SSL/TLS verwenden sollen.	<code>443</code> , <code>8443</code>
<code>load-balancer-source-ranges</code>	CIDR-Bereiche, die auf den Load Balancer zugreifen dürfen.	<code>10.0.0.0/24</code> , <code>192.168.1.0/24</code>

Feld	Beschreibung	Beispiel
<code>aws-load-balancer-additional-resource-tags</code>	Zusätzliche AWS Tags, die auf den Load Balancer und verwandte Ressourcen angewendet werden sollen.	<code>Environment=prod,Team=platform</code>
<code>aws-load-balancer-ip-address-type</code>	Gibt an, ob der Load Balancer Dual-Stack (IPv4 +) verwendet IPv4 . IPv6	<code>ipv4</code> oder <code>dualstack</code>

Überlegungen

- Sie müssen die Cluster-IAM-Rolle aktualisieren, um die Tag-Weitergabe von Kubernetes an AWS Load Balancer-Ressourcen zu ermöglichen. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte AWS Tags für EKS Auto-Ressourcen”](#).
- Informationen zum Zuordnen von Ressourcen zum automatischen Modus von EKS oder zum selbstverwalteten Load AWS Balancer Controller finden Sie unter. [the section called “Referenz zur Migration”](#)
- Informationen zur Behebung von Problemen mit Load Balancern finden Sie unter. [the section called “Fehlerbehebung”](#)
- Weitere Hinweise zur Verwendung der Lastenausgleichsfunktion von EKS Auto Mode finden Sie unter [the section called “Load Balancing”](#).

Bei der Migration zum automatischen EKS-Modus für den Lastenausgleich sind mehrere Änderungen an den Dienstanmerkungen und Ressourcenkonfigurationen erforderlich. In den folgenden Tabellen werden die wichtigsten Unterschiede zwischen früheren und neuen Implementierungen aufgeführt, einschließlich nicht unterstützter Optionen und empfohlener Alternativen.

Anmerkungen zu den Diensten

Bisherige	Neu	Beschreibung
<code>service.beta.kubernetes.io/load-balancer-source-ranges</code>	Nicht unterstützt	Bei Service verwenden <code>spec.loadBalancerSourceRanges</code>

Bisherige	Neu	Beschreibung
<code>service.beta.kubernetes.io/aws-load-balancer-type</code>	Nicht unterstützt	Bei Service verwenden <code>spec.loadBalancerClass</code>
<code>service.beta.kubernetes.io/aws-load-balancer-internal</code>	Nicht unterstützt	Verwenden von <code>service.beta.kubernetes.io/aws-load-balancer-scheme</code>
Verschiedene Load Balancer-Attribute	Nicht unterstützt	Verwenden von <code>service.beta.kubernetes.io/aws-load-balancer-attributes</code>
<code>service.beta.kubernetes.io/aws-load-balancer-proxy-protocol</code>	Nicht unterstützt	Verwenden Sie stattdessen <code>service.beta.kubernetes.io/aws-load-balancer-attributes</code>
<code>service.beta.kubernetes.io/aws-load-balancer-access-log-enabled</code>	Nicht unterstützt	Verwenden Sie <code>service.beta.kubernetes.io/aws-load-balancer-attributes</code> stattdessen
<code>service.beta.kubernetes.io/aws-load-balancer-access-log-s3-bucket-name</code>	Nicht unterstützt	Verwenden Sie <code>service.beta.kubernetes.io/aws-load-balancer-attributes</code> stattdessen
<code>service.beta.kubernetes.io/aws-load-balancer-access-log-s3-bucket-prefix</code>	Nicht unterstützt	Verwenden Sie <code>service.beta.kubernetes.io/aws-load-balancer-attributes</code> stattdessen

Bisherige	Neu	Beschreibung
<code>service.beta.kubernetes.io/aws-load-balancer-cross-zone-load-balancing-enabled</code>	Nicht unterstützt	Verwenden Sie <code>service.beta.kubernetes.io/aws-load-balancer-attributes</code> stattdessen

Um von veralteten Load Balancer-Attributanmerkungen zu migrieren, konsolidieren Sie diese Einstellungen in der Anmerkung. `service.beta.kubernetes.io/aws-load-balancer-attributes` Diese Anmerkung akzeptiert eine durch Kommas getrennte Liste von Schlüssel-Wert-Paaren für verschiedene Load Balancer-Attribute. Verwenden Sie beispielsweise das folgende Format, um das Proxyprotokoll, die Zugriffsprotokollierung und den zonenübergreifenden Lastenausgleich anzugeben:

```
service.beta.kubernetes.io/aws-load-balancer-attributes: |
  access_logs.s3.enabled=true
  access_logs.s3.bucket=my-bucket
  access_logs.s3.prefix=my-prefix
  load_balancing.cross_zone.enabled=true
```

```
service.beta.kubernetes.io/aws-load-balancer-target-group-attributes: |
  proxy_protocol_v2.enabled=true
```

Dieses konsolidierte Format bietet eine konsistentere und flexiblere Möglichkeit, Load Balancer-Attribute zu konfigurieren und gleichzeitig die Anzahl der benötigten individuellen Anmerkungen zu reduzieren. Überprüfen Sie Ihre vorhandenen Servicekonfigurationen und aktualisieren Sie sie, um dieses konsolidierte Format zu verwenden.

TargetGroupBinding

Bisherige	Neu	Beschreibung
<code>elbv2.k8s.aws/v1beta1</code>	<code>eks.amazonaws.com/v1</code>	Änderung der API-Version

Bisherige	Neu	Beschreibung
<code>spec.targetType</code> optional	<code>spec.targetType</code> erforderlich	Explizite Angabe des Zieltyps
<code>spec.networking.ingress.from</code>	Nicht unterstützt	Unterstützt NLB ohne Sicherheitsgruppen nicht mehr

Erstellen Sie eine Speicherklasse

A definiert `StorageClass` im automatischen Modus von Amazon EKS, wie Amazon EBS-Volumes automatisch bereitgestellt werden, wenn Anwendungen persistenten Speicher anfordern. Auf dieser Seite wird erklärt, wie Sie eine erstellen und konfigurieren `StorageClass`, die mit dem Amazon EKS Auto Mode zur Bereitstellung von EBS-Volumes zusammenarbeitet.

Durch die Konfiguration von können Sie Standardeinstellungen für Ihre EBS-Volumes angeben, darunter Volumetyp, Verschlüsselung, IOPS und andere Speicherparameter. `StorageClass` Sie können die auch so konfigurieren `StorageClass`, dass AWS KMS-Schlüssel für das Verschlüsselungsmanagement verwendet werden.

Der automatische EKS-Modus erstellt keine `StorageClass` für Sie. Sie müssen eine `StorageClass` Referenzierung erstellen `ebs.csi.eks.amazonaws.com`, um die Speicherfunktion von EKS Auto Mode nutzen zu können.

Erstellen Sie zunächst eine Datei mit dem Namen `storage-class.yaml`:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: auto-ebs-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: ebs.csi.eks.amazonaws.com
volumeBindingMode: WaitForFirstConsumer
parameters:
  type: gp3
  encrypted: "true"
```

Zweitens wenden Sie die Speicherklasse auf Ihren Cluster an.

```
kubectl apply -f storage-class.yaml
```

Die wichtigsten Komponenten:

- `provisioner: ebs.csi.eks.amazonaws.com`- Verwendet den EKS-Automatikmodus
- `volumeBindingMode: WaitForFirstConsumer`- Verzögert die Volume-Erstellung, bis ein Pod sie benötigt
- `type: gp3`— Gibt den EBS-Volumetyp an
- `encrypted: "true"`- EBS verschlüsselt alle Volumes, die mit dem erstellt wurden. StorageClass EBS verwendet den `aws/ebs` Standard-Schlüsselalias. Weitere Informationen finden Sie unter [So funktioniert die Amazon EBS-Verschlüsselung](#) im Amazon EBS-Benutzerhandbuch. Dieser Wert ist optional, wird aber empfohlen.
- `storageclass.kubernetes.io/is-default-class: "true"`— Kubernetes verwendet diese Speicherklasse standardmäßig, es sei denn, Sie geben für einen Anspruch auf persistentes Volume eine andere Volume-Klasse an. Dieser Wert ist optional. Seien Sie vorsichtig, wenn Sie diesen Wert festlegen, wenn Sie von einem anderen Speichercontroller migrieren.

Verwenden Sie den selbstverwalteten KMS-Schlüssel, um EBS-Volumes zu verschlüsseln

Um einen selbstverwalteten KMS-Schlüssel zur Verschlüsselung von EBS-Volumes zu verwenden, die durch den automatischen Modus von EKS automatisiert werden, müssen Sie:

1. Erstellen Sie einen selbstverwalteten KMS-Schlüssel.
 - Weitere Informationen finden [Sie unter KMS-Schlüssel für symmetrische Verschlüsselung erstellen](#) oder [Wie Amazon Elastic Block Store \(Amazon EBS\) KMS verwendet im KMS-Benutzerhandbuch](#).
2. Erstellen Sie eine neue Richtlinie, die den Zugriff auf den KMS-Schlüssel ermöglicht.
 - Verwenden Sie die nachstehende Beispiel-IAM-Richtlinie, um die Richtlinie zu erstellen. Fügen Sie den ARN des neuen selbstverwalteten KMS-Schlüssels ein. Weitere Informationen finden Sie im AWS IAM-Benutzerhandbuch unter [Rollen erstellen und Richtlinien anhängen \(Konsole\)](#).
3. Hängen Sie die Richtlinie an die EKS-Clusterrolle an.
 - Verwenden Sie die AWS Konsole, um den ARN der EKS-Clusterrolle zu finden. Die Rolleninformationen sind im Abschnitt Übersicht sichtbar. Weitere Informationen finden Sie unter [the section called "Cluster-IAM-Rolle"](#).

4. Aktualisieren Sie das `StorageClass`, sodass es auf die KMS-Schlüssel-ID im `parameters.kmsKeyId` Feld verweist.

Beispiel für eine selbstverwaltete KMS-IAM-Richtlinie

Aktualisieren Sie die folgenden Werte in der Richtlinie unten:

- `<account-id>`— Ihre AWS Konto-ID, z. B. 111122223333
- `<aws-region>`— Die AWS Region Ihres Clusters, z. B. `us-west-2`

```
{
  "Version": "2012-10-17",
  "Id": "key-auto-policy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<account-id>:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access through EBS for all principals in the account that are authorized to use EBS",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```



```

        "kms:CallerAccount": "<account-id>",
        "kms:ViaService": "ec2.<aws-region>.amazonaws.com"
    }
}
]
}

```

Beispiel für ein selbstverwaltetes KMS **StorageClass**

```

parameters:
  type: gp3
  encrypted: "true"
  kmsKeyId: <custom-key-arn>

```

StorageClassReferenz zu den Parametern

Allgemeine Informationen zu den **StorageClass** Kubernetes-Ressourcen finden Sie in der Kubernetes-Dokumentation unter [Speicherklassen](#).

Der Abschnitt der **StorageClass** Ressource ist spezifisch für AWS. Verwenden Sie die folgende Tabelle, um die verfügbaren Optionen zu überprüfen.

Parameter	Werte	Standard	Beschreibung
„csi.storage.k8s.io/fstype“	xfs, ext2, ext3, ext4	ext4	Dateisystemtyp, der bei der Volumenerstellung formatiert wird. Bei diesem Parameter wird Groß- und Kleinschreibung beachtet!
„Typ“	io1, io2, gp2, gp3, sc1, st1, standard, sbp1, sbg1	gp3	EBS-Volumetyp.
„IOPSPer GB“			I/O-Operationen pro Sekunde pro GiB. Kann für IO1 IO2,

Parameter	Werte	Standard	Beschreibung
			und GP3 Volumes angegeben werden.
„Automatisch zulassen IOPSPerGB Increase“	true, false	false	Wenn "true" der CSI-Treiber die IOPS für ein Volume erhöht, wenn <code>iopsPerGB * <volume size></code> es zu niedrig ist, um in den von unterstützten IOPS-Bereich zu passen. AWS Auf diese Weise ist die dynamische Bereitstellung immer erfolgreich, auch wenn der Benutzer eine zu geringe PVC-Kapazität oder einen zu geringen Wert angibt. <code>iopsPerGB</code> Andererseits können dadurch zusätzliche Kosten entstehen, da solche Volumes höhere IOPS-Werte aufweisen als in angefordert. <code>iopsPerGB</code>
„IOPS“			I/O-Operationen pro Sekunde. Kann für IO1 IO2, und GP3 Volumes angegeben werden.

Parameter	Werte	Standard	Beschreibung
„Durchsatz“		125	Durchsatz in MiB/s. Nur wirksam, wenn der GP3-Volumetyp angegeben ist.
„verschlüsselt“	true, false	false	Ob das Volume verschlüsselt werden soll oder nicht. Gültige Werte sind „wahr“ oder „falsch“.
„BlockExpress“	true, false	false	Ermöglicht die Erstellung von io2 Block Express-Volumes.
"kmsKeyId"			Der vollständige ARN des Schlüssels, der beim Verschlüsseln des Volumes verwendet werden soll. Falls nicht angegeben, AWS wird der Standard-KMS-Schlüssel für die Region verwendet, in der sich das Volume befindet. Dies ist ein automatisch generierter Schlüssel, der aufgerufen wird, /aws/ebs wenn er nicht geändert wird.

Parameter	Werte	Standard	Beschreibung
„Blockgröße“			Die Blockgröße, die beim Formatieren des zugrunde liegenden Dateisystems verwendet werden soll. Wird nur auf Linux-Knoten und mit <code>fstype ext2, ext3, ext4</code> oder unterstützt. <code>xfs</code>
„Inode-Größe“			Die Inode-Größe, die beim Formatieren des zugrunde liegenden Dateisystems verwendet werden soll. Wird nur auf Linux-Knoten und mit <code>fstype ext2, ext3</code> oder unterstützt. <code>ext4 xfs</code>
"bytesPerInode"			Der bytes-per-inode, der beim Formatieren des zugrunde liegenden Dateisystems verwendet werden soll. Wird nur auf Linux-Knoten und mit <code>fstype ext2, unterstützt. ext3 ext4</code>

Parameter	Werte	Standard	Beschreibung
"numberOfInodes"			Die Anzahl der Inodes, die beim Formatieren des zugrundeliegenden Dateisystems verwendet werden soll. Wird nur auf Linux-Knoten und mit fstype ext2, ext3 oder ext4 unterstützt.
„ext4“ BigAlloc	true, false	false	Ändert das ext4 Dateisystem so, dass es die Blockzuweisung von Clustern verwendet, indem die bigalloc Formatierungsoption aktiviert wird. Warnung: Wird bigalloc möglicherweise nicht vollständig vom Linux-Kernel Ihres Nodes unterstützt.

Parameter	Werte	Standard	Beschreibung
„ext4ClusterSize“			Die Clustergröße, die beim Formatieren eines ext4 Dateisystems verwendet werden soll, wenn die bigalloc Funktion aktiviert ist. Hinweis: Der ext4BigAlloc Parameter muss auf true gesetzt sein.

Weitere Informationen finden Sie unter [AWS EBS CSI Driver](#) on GitHub.

Überlegungen

Die Blockspeicherfähigkeit des EKS-Automodus unterscheidet sich von der des EBS-CSI-Treibers.

- Statische Bereitstellung
 - Wenn Sie extern erstellte EBS-Volumes mit dem automatischen EKS-Modus verwenden möchten, müssen Sie manuell ein AWS Tag mit dem Schlüssel `eks:eks-cluster-name` und dem Wert des Clusternamens hinzufügen.
- Node Startup Taint
 - Sie können die Funktion „Node Startup Taint“ nicht verwenden, um das Pod-Scheduling zu verhindern, bevor die Speicherkapazität bereit ist
- Benutzerdefinierte Tags auf dynamisch bereitgestellten Volumes
 - Sie können das CLI-Flag für Extra-Tags nicht verwenden, um benutzerdefinierte Tags auf dynamisch bereitgestellten EBS-Volumes zu konfigurieren
 - Sie können StorageClass Tagging verwenden, um benutzerdefinierte Tags hinzuzufügen. Der automatische Modus von EKS fügt den zugehörigen AWS Ressourcen Tags hinzu. Sie müssen die Cluster-IAM-Rolle für benutzerdefinierte Tags aktualisieren. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte AWS Tags für EKS Auto-Ressourcen”](#).
- Detaillierte EBS-Leistungskennzahlen
 - Sie können nicht auf Prometheus-Metriken für die detaillierte EBS-Leistung zugreifen

Installieren Sie das CSI Snapshot Controller-Addon

Der EKS-Automatikmodus ist mit dem Amazon EKS-Add-on CSI Snapshot Controller kompatibel.

AWS schlägt vor, dass Sie dieses Add-on so konfigurieren, dass es im integrierten system Knotenpool ausgeführt wird.

Weitere Informationen finden Sie unter:

- [the section called “Führen Sie wichtige Add-Ons aus”](#)
- [the section called “Überprüfen Sie die integrierten Knotenpools”](#)
- [the section called “CSI-Snapshot-Controller”](#)

Um den Snapshot-Controller im Systemknotenpool zu installieren

1. Öffnen Sie Ihren EKS-Cluster in der AWS Konsole
2. Wählen Sie auf der Registerkarte „Add-ons“ die Option Weitere Add-Ons herunterladen
3. Wählen Sie den CSI Snapshot Controller und dann Weiter
4. Wählen Sie auf der Seite Ausgewählte Add-On-Einstellungen konfigurieren die Option Optionale Konfigurationseinstellungen aus, um das Add-on-Konfigurationsschema anzuzeigen
 - a. Fügen Sie das folgende Yaml ein, um den Snapshot-Controller dem system Knotenpool zuzuordnen. Der Snapshot-Controller beinhaltet eine Toleranz für den CriticalAddonsOnly Makel.

```
{
  "nodeSelector": {
    "karpenter.sh/nodepool": "system"
  }
}
```

- b. Wählen Sie Weiter

5. Überprüfen Sie die Konfiguration des Add-ons und wählen Sie dann Erstellen

Deaktivieren Sie den EKS-Automatikmodus

Sie können den EKS-Automatikmodus auf einem vorhandenen EKS-Cluster deaktivieren. Dies ist ein destruktiver Vorgang.

- EKS beendet alle vom EKS Auto Mode betriebenen EC2 Instanzen.
- EKS löscht alle Load Balancer, die vom EKS Auto Mode betrieben werden.
- EKS löscht keine EBS-Volumes, die vom EKS Auto Mode bereitgestellt wurden.

Der automatische Modus von EKS wurde für die vollständige Verwaltung der von ihm erstellten Ressourcen entwickelt. Manuelle Eingriffe können dazu führen, dass der EKS-Automatikmodus diese Ressourcen nicht vollständig bereinigt, wenn er deaktiviert ist. Wenn Sie beispielsweise in externen Sicherheitsgruppenregeln auf eine verwaltete Sicherheitsgruppe verwiesen haben und vergessen, diesen Verweis zu entfernen, bevor Sie den automatischen EKS-Modus für einen Cluster deaktivieren, wird die verwaltete Sicherheitsgruppe durchgesickern (nicht gelöscht). In den folgenden Schritten wird beschrieben, wie Sie eine durchgesickerte Sicherheitsgruppe entfernen können, falls dies der Fall sein sollte.

Deaktivieren Sie den EKS-Automatikmodus (AWS Konsole)

1. Öffnen Sie Ihre Cluster-Übersichtsseite im AWS Management Console.
2. Wählen Sie unter EKS Auto Mode die Option Verwalten
3. Schalten Sie den EKS-Automatikmodus auf off.

Wenn eine verwaltete Sicherheitsgruppe am Ende dieses Vorgangs nicht gelöscht wird, können Sie sie mithilfe der Beschreibungen unter [Sicherheitsgruppe löschen](#) manuell löschen.

Deaktivieren Sie den EKS-Automatikmodus (AWS CLI)

Verwenden Sie den folgenden Befehl, um den automatischen EKS-Modus auf einem vorhandenen Cluster zu deaktivieren.

Sie müssen die aws CLI installiert haben und mit ausreichenden Berechtigungen angemeldet sein, um EKS-Cluster zu verwalten. Weitere Informationen finden Sie unter [Einrichten](#).

Note

Die Rechen-, Blockspeicher- und Lastausgleichsfunktionen müssen alle in derselben Anfrage aktiviert oder deaktiviert werden.

```
aws eks update-cluster-config \
```



```
--name $CLUSTER_NAME \  
--compute-config enabled=false \  
--kubernetes-network-config '{"elasticLoadBalancing":{"enabled": false}}' \  
--storage-config '{"blockStorage":{"enabled": false}}'
```

Sie können wie folgt überprüfen, ob eine durchgesickerte Sicherheitsgruppe für den automatischen EKS-Modus nach der Deaktivierung des automatischen EKS-Modus nicht gelöscht werden konnte:

```
aws ec2 describe-security-groups \  
  --filters Name=tag:eks:eks-cluster-name,Values=<cluster-Name> Name=tag-  
key,Values=ingress.eks.amazonaws.com/resource,service.eks.amazonaws.com/resource --  
query "SecurityGroups[*].[GroupName]"
```

Um dann die Sicherheitsgruppe zu löschen:

```
aws ec2 delete-security-group --group-name=<sg-name>
```

Aktualisieren Sie die Kubernetes-Version eines EKS-Auto-Mode-Clusters

In diesem Thema wird erklärt, wie Sie die Kubernetes-Version Ihres Auto Mode-Clusters aktualisieren. Der automatische Modus vereinfacht den Versionsaktualisierungsprozess, indem er die Koordination von Updates auf der Steuerungsebene mit dem Austausch von Knoten übernimmt und gleichzeitig die Workload-Verfügbarkeit durch Budgets für Pod-Unterbrechungen gewährleistet.

Beim Upgrade eines Clusters im automatischen Modus werden viele Komponenten, für die bisher manuelle Updates erforderlich waren, jetzt im Rahmen des Service verwaltet. Wenn Sie die automatisierten Aspekte des Upgrade-Prozesses und Ihre Verantwortlichkeiten verstehen, können Sie einen reibungslosen Versionsübergang für Ihren Cluster sicherstellen.

Erfahren Sie mehr über Updates mit EKS Auto Mode

Nachdem Sie ein Upgrade der Steuerungsebene initiiert haben, aktualisiert EKS Auto Mode die Knoten in Ihrem Cluster. Wenn Knoten ablaufen, ersetzt sie der EKS-Automatikmodus durch neue Knoten. Die neuen Knoten haben die entsprechende neue Kubernetes-Version. Der automatische Modus von EKS berücksichtigt bei der Aktualisierung von Knoten die Budgets für Pod-Unterbrechungen.

Darüber hinaus müssen Sie Komponenten wie die folgenden nicht mehr aktualisieren:

- Amazon VPC CNI
- AWS Load Balancer Balancer-Controller
- CoreDNS
- kube-proxy
- Karpenter
- AWS EBS CSI-Treiber

Der EKS-Automatikmodus ersetzt diese Komponenten durch Servicefunktionen.

Sie sind weiterhin für die Aktualisierung von Folgendem verantwortlich:

- In Ihrem Cluster bereitgestellte Apps und Workloads
- Selbstverwaltete Add-Ons und Controller
- Amazon EKS-Add-Ons
 - Erfahren Sie, wie [the section called “Aktualisieren Sie ein Add-on”](#)

Erfahren Sie mehr über [bewährte Methoden für Cluster-Upgrades](#)

Starten Sie das Cluster-Update

Informationen zum Starten eines Cluster-Updates finden Sie unter [the section called “Kubernetes-Version aktualisieren”](#).

Integriert aktivieren oder deaktivieren NodePools

Der automatische Modus von EKS verfügt über zwei integrierte Funktionen NodePools. Sie können diese NodePools über die AWS Konsole, CLI oder API aktivieren oder deaktivieren.

Integrierte NodePool Referenz

- `system`
 - Das NodePool hat einen `CriticalAddonsOnly` Makel. Viele EKS-Add-Ons, wie CoreDNS, tolerieren diesen Makel. Verwenden Sie diesen Systemknotenpool, um clusterkritische Anwendungen zu trennen.
 - Unterstützt sowohl als auch amd64 Architekturen. arm64

- **general-purpose**
 - Dies NodePool bietet Unterstützung für das Starten von Knoten für allgemeine Workloads in Ihrem Cluster.
 - Verwendet nur amd64 Architektur.

Beide eingebaut NodePools:

- Verwenden Sie das Standard-EKS NodeClass
- Verwenden Sie nur EC2 On-Demand-Kapazität
- Verwenden Sie die EC2 Instanzfamilien C, M und R
- EC2 Instances der Generation 5 oder neuer erforderlich

Note

Die Aktivierung von mindestens einer integrierten NodePool Komponente ist erforderlich, damit EKS den „Standard“ bereitstellen kann NodeClass. Wenn Sie alle integrierten Funktionen deaktivieren NodePools, müssen Sie eine benutzerdefinierte Version erstellen NodeClass und eine konfigurieren NodePool , um sie zu verwenden. Weitere Informationen zu finden NodeClasses Sie unter [the section called “Erstellen Sie eine Knotenklasse”](#).

Verfahren

Voraussetzungen

- Die neueste Version der AWS Befehlszeilenschnittstelle (AWS CLI) ist auf Ihrem Gerät installiert und konfiguriert. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version`. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration](#) mit `aws configure` im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- Melden Sie sich mit ausreichenden IAM-Berechtigungen bei der CLI an, um AWS Ressourcen wie IAM-Richtlinien, IAM-Rollen und EKS-Cluster zu erstellen.

Mit AWS CLI aktivieren

Verwenden Sie den folgenden Befehl, um beide integrierten Funktionen zu aktivieren NodePools:

```
aws eks update-cluster-config \
  --name <cluster-name> \
  --compute-config '{
    "nodeRoleArn": "<node-role-arn>",
    "nodePools": ["general-purpose", "system"],
    "enabled": true
  }' \
  --kubernetes-network-config '{
    "elasticLoadBalancing":{"enabled": true}
  }' \
  --storage-config '{
    "blockStorage":{"enabled": true}
  }'
```

Sie können den Befehl ändern, um den selektiv zu aktivieren. NodePools

Mit AWS CLI deaktivieren

Verwenden Sie den folgenden Befehl, um beide integrierten Funktionen zu deaktivieren NodePools:

```
aws eks update-cluster-config \
  --name <cluster-name> \
  --compute-config '{
    "enabled": true,
    "nodePools": []
  }' \
  --kubernetes-network-config '{
    "elasticLoadBalancing":{"enabled": true}}' \
  --storage-config '{
    "blockStorage":{"enabled": true}
  }'
```

Steuern Sie, ob ein Workload auf EKS-Automodus-Knoten bereitgestellt wird

Wenn Sie Workloads in einem EKS-Cluster mit dem automatischen EKS-Modus ausführen, müssen Sie möglicherweise kontrollieren, ob bestimmte Workloads auf EKS-Automodus-Knoten oder anderen Compute-Typen ausgeführt werden. In diesem Thema wird beschrieben, wie Sie mithilfe von Knotenselektoren und Affinitätsregeln sicherstellen, dass Ihre Workloads auf der vorgesehenen Recheninfrastruktur geplant werden.

Die Beispiele in diesem Thema zeigen, wie Sie das `eks.amazonaws.com/compute-type` Label verwenden können, um die Workload-Bereitstellung auf EKS-Automodus-Knoten entweder vorzuschreiben oder zu verhindern. Dies ist besonders nützlich in Clustern im gemischten Modus, in denen Sie sowohl den automatischen EKS-Modus als auch andere Rechenarten ausführen, z. B. selbstverwaltete Karpenter Provisioner oder EKS Managed Node Groups.

EKS-Automodus-Knoten haben den Wert des Labels auf `gesetzt`. `eks.amazonaws.com/compute-type auto` Sie können dieses Label verwenden, um zu steuern, ob eine Arbeitslast auf Knoten bereitgestellt wird, die von EKS Auto Mode verwaltet werden.

Erfordert, dass ein Workload auf den Knoten im automatischen Modus von EKS bereitgestellt wird

 Note

Dieser `nodeSelector` Wert ist für den automatischen EKS-Modus nicht erforderlich. Dieser `nodeSelector` Wert ist nur relevant, wenn Sie einen Cluster in einem gemischten Modus ausführen, wobei die Knotentypen nicht vom EKS Auto Mode verwaltet werden. Beispielsweise können Sie statische Rechenkapazität mit EKS Managed Node Groups für Ihren Cluster bereitstellen und dynamische Rechenkapazität vom EKS Auto Mode verwalten lassen.

Sie können dies `nodeSelector` zu Bereitstellungen oder anderen Workloads hinzufügen, sodass Kubernetes sie auf EKS-Automodus-Knoten einplant.

```
apiVersion: apps/v1
kind: Deployment
spec:
  template:
    nodeSelector:
      eks.amazonaws.com/compute-type: auto
```

Erfordern Sie, dass kein Workload auf den EKS-Automodus-Knoten bereitgestellt wird

Sie können dies `nodeAffinity` zu Bereitstellungen oder anderen Workloads hinzufügen, sodass Kubernetes sie nicht auf EKS-Automodus-Knoten plant.

```
affinity:
```

```
nodeAffinity:
  requiredDuringSchedulingIgnoredDuringExecution:
    nodeSelectorTerms:
      - matchExpressions:
          - key: eks.amazonaws.com/compute-type
            operator: NotIn
            values:
              - auto
```

Führen Sie wichtige Add-Ons auf dedizierten Instanzen aus

In diesem Thema erfahren Sie, wie Sie einen Workload mit einer `CriticalAddonsOnly` Toleranz bereitstellen, sodass EKS Auto Mode ihn für den system Knotenpool einplant.

Der integrierte system Knotenpool von EKS Auto Mode ist für die Ausführung kritischer Add-Ons auf dedizierten Instanzen konzipiert. Diese Trennung stellt sicher, dass wichtige Komponenten über dedizierte Ressourcen verfügen und von allgemeinen Workloads isoliert sind, wodurch die allgemeine Stabilität und Leistung des Clusters verbessert wird.

In diesem Handbuch wird gezeigt, wie Sie mithilfe der `CriticalAddonsOnly` Toleranzwerte und der entsprechenden system Knotenauswahl Add-Ons für den Knotenpool bereitstellen. Wenn Sie diese Schritte befolgen, können Sie sicherstellen, dass Ihre kritischen Anwendungen auf den dedizierten system Knoten geplant werden. So können Sie die Vorteile der Isolierung und Ressourcenzuweisung nutzen, die die spezielle Knotenpoolstruktur von EKS Auto Mode bietet.

Der automatische Modus von EKS verfügt über zwei integrierte Knotenpools: `general-purpose` und `system`. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).

Der Zweck des system Knotenpools besteht darin, wichtige Add-Ons auf verschiedene Knoten zu verteilen. Knoten, die vom system Knotenpool bereitgestellt werden, haben einen `CriticalAddonsOnly` Kubernetes-Nachteil. Kubernetes plant Pods auf diesen Knoten nur dann ein, wenn für sie eine entsprechende Toleranz besteht. Weitere Informationen finden Sie unter [Taints and Tolerations](#) in der Kubernetes-Dokumentation.

Voraussetzungen

- EKS-Auto-Mode-Cluster mit aktiviertem integriertem Knotenpoolsystem. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#)

- `kubectl` installiert und konfiguriert. Weitere Informationen finden Sie unter [Einrichten](#).

Verfahren

Sehen Sie sich das folgende Beispiel für YAML an. Beachten Sie die folgenden Konfigurationen:

- `nodeSelector`— Dadurch wird die Arbeitslast dem integrierten `system` Knotenpool zugeordnet. Dieser Knotenpool muss mit der AWS API aktiviert werden. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).
- `tolerations`— Diese Toleranz überwindet den `CriticalAddonsOnly` Makel auf den Knoten im Knotenpool. `system`

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: sample-app
spec:
  replicas: 3
  selector:
    matchLabels:
      app: sample-app
  template:
    metadata:
      labels:
        app: sample-app
    spec:
      nodeSelector:
        karpenter.sh/nodepool: system
      tolerations:
        - key: "CriticalAddonsOnly"
          operator: "Exists"
      containers:
        - name: app
          image: nginx:latest
          resources:
            requests:
              cpu: "500m"
              memory: "512Mi"
```

Um einen Workload so zu aktualisieren, dass er im `system` Knotenpool ausgeführt wird, müssen Sie:

1. Aktualisieren Sie den vorhandenen Workload, um die folgenden oben beschriebenen Konfigurationen hinzuzufügen:
 - `nodeSelector`
 - `tolerations`
2. Stellen Sie den aktualisierten Workload in Ihrem Cluster bereit mit `kubectl apply`

Nach der Aktualisierung des Workloads wird er auf dedizierten Knoten ausgeführt.

Verwenden Sie Netzwerkrichtlinien mit dem automatischen Modus von EKS

Netzwerkrichtlinien ermöglichen es Ihnen, den Verkehrsfluss auf IP-Adresse- oder Portebene innerhalb Ihres Amazon EKS-Clusters zu steuern. In diesem Thema wird erklärt, wie Netzwerkrichtlinien mit dem automatischen Modus von EKS aktiviert und verwendet werden.

Voraussetzungen

- Ein Amazon EKS-Cluster mit aktiviertem EKS-Automatikmodus
- `kubectl` ist so konfiguriert, dass es eine Verbindung zu Ihrem Cluster herstellt

Schritt 1: Aktivieren Sie den Network Policy Controller

Um Netzwerkrichtlinien mit dem automatischen Modus von EKS zu verwenden, müssen Sie zunächst den Network Policy Controller aktivieren, indem Sie a ConfigMap auf Ihren Cluster anwenden.

1. Erstellen Sie eine Datei mit dem Namen `enable-network-policy.yaml` und dem folgenden Inhalt:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: amazon-vpc-cni
  namespace: kube-system
data:
  enable-network-policy-controller: "true"
```

2. Wenden Sie das ConfigMap auf Ihren Cluster an:

```
kubectl apply -f enable-network-policy.yaml
```


Schritt 2: Netzwerkrichtlinien in der Knotenklasse aktivieren

Bevor Sie Netzwerkrichtlinien verwenden können, müssen Sie sicherstellen, dass Ihre Node Class so konfiguriert ist, dass sie diese unterstützt. Dazu gehen Sie wie folgt vor:

1. Erstellen oder bearbeiten Sie eine Node Class-YAML-Datei (z. B. `nodeclass-network-policy.yaml`) mit dem folgenden Inhalt:

```
apiVersion: eks.amazonaws.com/v1
kind: NodeClass
metadata:
  name: network-policy-enabled
spec:
  # Enables network policy support
  networkPolicy: DefaultAllow
  # Optional: Enables logging for network policy events
  networkPolicyEventLogs: Enabled
  # Include other Node Class configurations as needed
```

2. Wenden Sie die Node Class-Konfiguration auf Ihren Cluster an:

```
kubectl apply -f nodeclass-network-policy.yaml
```

3. Stellen Sie sicher, dass die Node-Klasse erstellt wurde:

```
kubectl get nodeclass network-policy-enabled
```

4. Aktualisieren Sie Ihren Node-Pool, um diese Node-Klasse zu verwenden. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Knotenpool”](#).

Sobald Ihre Knoten diese Node-Klasse verwenden, können sie Netzwerkrichtlinien durchsetzen. Sie können nun mit der Erstellung und Anwendung von Netzwerkrichtlinien zur Steuerung des Datenverkehrs innerhalb Ihres Clusters fortfahren. Alle Konfigurationsoptionen für Knotenklassen finden Sie unter [the section called “Erstellen Sie eine Knotenklasse”](#).

Schritt 3: Netzwerkrichtlinien erstellen und testen

Ihr EKS-Auto-Mode-Cluster ist jetzt so konfiguriert, dass er Kubernetes-Netzwerkrichtlinien unterstützt. Sie können dies mit dem testen. [the section called “Stars Policy-Demo”](#)

Tag-Subnetze für EKS Auto Mode

Wenn Sie die Lastausgleichsfunktion von EKS Auto Mode verwenden, müssen Sie Ihren VPC-Subnetzen AWS Tags hinzufügen.

Hintergrund

Diese Tags identifizieren Subnetze als dem Cluster zugeordnet und, was noch wichtiger ist, ob es sich bei dem Subnetz um ein öffentliches oder privates Subnetz handelt.

Öffentliche Subnetze haben direkten Internetzugang über ein Internet-Gateway. Sie werden für Ressourcen verwendet, die öffentlich zugänglich sein müssen, z. B. für Load Balancer.

Private Subnetze haben keinen direkten Internetzugang und verwenden NAT-Gateways für ausgehenden Verkehr. Sie werden für interne Ressourcen wie EKS-Knoten verwendet, die keine öffentlichen Ressourcen benötigen. IPs

Weitere Informationen zu NAT-Gateways und Internet-Gateways finden Sie unter [Verbinden Ihrer VPC mit anderen Netzwerken](#) im Amazon Virtual Private Cloud (VPC) -Benutzerhandbuch.

Anforderung

Derzeit müssen Subnetze, die für den Lastenausgleich im automatischen Modus von EKS verwendet werden, über eines der folgenden Tags verfügen.

Öffentliche Subnetze

Öffentliche Subnetze werden für Load Balancer mit Internetzugriff verwendet. Diese Subnetze müssen die folgenden Tags haben:

Schlüssel	Value (Wert)
kubernetes.io/role/elb	1oder ``

Private Subnetze

Private Subnetze werden für interne Load Balancer verwendet. Diese Subnetze müssen die folgenden Tags haben:

Schlüssel	Value (Wert)
kubernetes.io/role/internal-elb	1oder ``

Verfahren

Stellen Sie zunächst fest, welche Subnetze öffentlich (mit Internet-Gateway-Zugriff) und welche privat (mit NAT-Gateway) sind. Sie benötigen Berechtigungen, um VPC-Ressourcen zu ändern.

AWS Management Console

1. Öffnen Sie die Amazon VPC-Konsole und navigieren Sie zu Subnetze
2. Wählen Sie das zu kennzeichnende Subnetz aus
3. Wählen Sie die Registerkarte „Tags“ und dann „Tag hinzufügen“
4. Fügen Sie das entsprechende Tag hinzu:
 - Für öffentliche Subnetze: Key= kubernetes.io/role/elb
 - Für private Subnetze: Key= kubernetes.io/role/internal-elb
5. Setzen Sie den Wert auf 1 oder lassen Sie das Feld leer
6. Speichern Sie und wiederholen Sie den Vorgang für die verbleibenden Subnetze

AWS CLI

Für öffentliche Subnetze:

```
aws ec2 create-tags \  
  --resources subnet-ID \  
  --tags Key=kubernetes.io/role/elb,Value=1
```

Für private Subnetze:

```
aws ec2 create-tags \  
  --resources subnet-ID \  
  --tags Key=kubernetes.io/role/internal-elb,Value=1
```

Ersetzen Sie es subnet - ID durch Ihre tatsächliche Subnetz-ID.

Stellen Sie einen beschleunigten Workload bereit

Dieses Tutorial zeigt, wie Amazon EKS Auto Mode das Starten beschleunigter Workloads vereinfacht. Amazon EKS Auto Mode optimiert Abläufe, die über den Cluster selbst hinausgehen, indem wichtige Infrastrukturkomponenten automatisiert werden und sofort einsatzbereite Rechen-, Netzwerk-, Lastausgleichs-, Speicher- und Identitätszugriffs- und Verwaltungsfunktionen bereitgestellt werden.

Amazon EKS Auto Mode umfasst die Treiber und Geräte-Plug-ins, die für bestimmte Instance-Typen wie NVIDIA- und AWS Neuron-Treiber erforderlich sind. Sie müssen diese Komponenten nicht installieren oder aktualisieren.

Der EKS Auto Mode verwaltet automatisch die Treiber für diese Beschleuniger:

- [AWS Trainium](#)
- [AWS Inferenz](#)
- [EC2 Beschleunigte Instances von NVIDIA GPUs auf Amazon](#)

Note

Der automatische Modus von EKS beinhaltet das NVIDIA-Geräte-Plugin für Kubernetes. Dieses Plugin wird automatisch ausgeführt und ist als Daemon-Set in Ihrem Cluster nicht sichtbar.

Zusätzliche Netzwerkunterstützung:

- [Elastic Fabric Adapter \(EFA\)](#)

Der automatische Modus von Amazon EKS macht die mühsame Verwaltung von Beschleunigertreibern und Geräte-Plug-ins überflüssig.

Sie können auch von Kosteneinsparungen profitieren, indem Sie den Cluster auf Null skalieren. Sie können den automatischen EKS-Modus so konfigurieren, dass Instanzen beendet werden, wenn keine Workloads ausgeführt werden. Dies ist nützlich für stapelbasierte Inferenz-Workloads.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie beschleunigte Workloads mit Amazon EKS Auto Mode starten können.

Voraussetzungen

- Ein Kubernetes-Cluster mit konfiguriertem Amazon EKS Auto Mode.
- Eine default EKS-Node-Klasse, die erstellt wurde, wenn die general-purpose oder system Managed Node Pools aktiviert sind.

Schritt 1: Stellen Sie einen GPU-Workload bereit

In diesem Beispiel erstellen Sie eine NodePool für NVIDIA-basierte Workloads, die 45 GB GPU-Speicher benötigen. Im automatischen Modus von EKS verwenden Sie Kubernetes-Scheduling-Einschränkungen, um Ihre Instanzanforderungen zu definieren.

Um den Amazon EKS Auto Mode NodePool und das Beispiel bereitzustellenworkload, überprüfen Sie Folgendes NodePool und die Pod-Definition und speichern Sie unter `nodepool-gpu.yaml` und `pod.yaml`:

`nodepool-gpu.yaml`

```
apiVersion: karpenter.sh/v1
kind: NodePool
metadata:
  name: gpu
spec:
  disruption:
    budgets:
      - nodes: 10%
    consolidateAfter: 1h
    consolidationPolicy: WhenEmpty
  template:
    metadata: {}
    spec:
      nodeClassRef:
        group: eks.amazonaws.com
        kind: NodeClass
        name: default
      requirements:
        - key: "karpenter.sh/capacity-type"
          operator: In
          values: ["on-demand"]
        - key: "kubernetes.io/arch"
          operator: In
```

```
    values: ["amd64"]
  - key: "eks.amazonaws.com/instance-family"
    operator: In
    values:
      - g6e
      - g6
  taints:
    - key: nvidia.com/gpu
      effect: NoSchedule
  terminationGracePeriod: 24h0m0s
```

pod.yaml

```
apiVersion: v1
kind: Pod
metadata:
  name: nvidia-smi
spec:
  nodeSelector:
    eks.amazonaws.com/instance-gpu-name: l40s
    eks.amazonaws.com/compute-type: auto
  restartPolicy: OnFailure
  containers:
    - name: nvidia-smi
      image: public.ecr.aws/amazonlinux/amazonlinux:2023-minimal
      args:
        - "nvidia-smi"
      resources:
        requests:
          memory: "30Gi"
          cpu: "3500m"
          nvidia.com/gpu: 1
        limits:
          memory: "30Gi"
          nvidia.com/gpu: 1
  tolerations:
    - key: nvidia.com/gpu
      effect: NoSchedule
      operator: Exists
```

Beachten Sie, dass der `eks.amazonaws.com/compute-type: auto` Selektor erfordert, dass der Workload auf einem Amazon EKS Auto Mode-Knoten bereitgestellt wird. Das ist NodePool auch ein Makel, dass nur Pods mit Toleranzen für Nvidia GPUs geplant werden können.

Wenden Sie die Arbeitslast NodePool und den Workload auf Ihren Cluster an.

```
kubectl apply -f nodepool-gpu.yaml
kubectl apply -f pod.yaml
```

Die Ausgabe sollte folgendermaßen aussehen:

```
nodepool.karpenter.sh/gpu configured created
pod/nvidia-smi created
```

Warten Sie ein paar Sekunden und überprüfen Sie die Knoten in Ihrem Cluster. Sie sollten jetzt einen neuen Knoten sehen, der in Ihrem Amazon EKS Auto Mode-Cluster bereitgestellt wurde:

```
> kubectl get nodes
```

NAME	TYPE	CAPACITY	ZONE	NODE	READY	AGE
gpu-dnknr	g6e.2xlarge	on-demand	us-west-2b	i-02315c7d7643cdee6	True	76s

Schritt 2: Validieren

Sie können sehen, dass Amazon EKS Auto Mode g6e.2xlarge statt eines gestartet hat, g6.2xlarge da für die Arbeitslast eine Instance mit I40s erforderlich warGPU, und zwar gemäß den folgenden Kubernetes-Scheduling-Einschränkungen:

```
...
nodeSelector:
  eks.amazonaws.com/instance-gpu-name: i40s
...
requests:
  memory: "30Gi"
  cpu: "3500m"
  nvidia.com/gpu: 1
limits:
  memory: "30Gi"
  nvidia.com/gpu: 1
```

Sehen Sie sich nun die Container-Logs an, indem Sie den folgenden Befehl ausführen:

```
kubectl logs nvidia-smi
```

Beispielausgabe:

```

+-----+
+
| NVIDIA-SMI 535.230.02                Driver Version: 535.230.02   CUDA Version: 12.2
|
|-----+-----+
+-----+
| GPU   Name                               Persistence-M | Bus-Id        Disp.A | Volatile Uncorr. ECC
|
| Fan   Temp   Perf           Pwr:Usage/Cap |      Memory-Usage | GPU-Util  Compute M.
|
|                               |                      |              MIG M.
|
|=====+=====+
+=====+
|    0   NVIDIA L40S                     On   | 00000000:30:00.0 Off |                  0
|
| N/A    27C    P8              23W / 350W |      0MiB / 46068MiB |      0%      Default
|
|                               |                      |              N/A
|
+-----+
+-----+

+-----+
+
| Processes:
|
| GPU   GI    CI          PID    Type    Process name                        GPU Memory
|
|       ID    ID
|
|=====+=====+
| No running processes found
|
+-----+
+

```

Sie können sehen, dass der Container erkannt hat, dass er auf einer Instance mit einer NVIDIA GPU läuft, und dass Sie keine Gerätetreiber installieren mussten, da dies vom Amazon EKS Auto Mode verwaltet wird.

Schritt 3: Aufräumen

Um alle erstellten Objekte zu entfernen, verwenden Sie, `kubectl` um die Beispielbereitstellung zu löschen, `NodePool` sodass der Knoten beendet wird:

```
kubectl delete -f nodepool-gpu.yaml
kubectl delete -f pod.yaml
```

NodePools Beispielreferenz

Erstellen Sie eine NVIDIA NodePool

Im Folgenden wird Folgendes NodePool definiert:

- Startet nur Instances von einer g6e g6 Familie
- Konsolidieren Sie Knoten, wenn sie 1 Stunde lang leer sind
 - Der Wert von 1 Stunde für `consolidateAfter` unterstützt hohe Arbeitslasten und reduziert die Abwanderung von Knoten. Sie können die Einstellungen an Ihre `consolidateAfter` Workload-Anforderungen anpassen.

Beispiel NodePool mit GPU-Instanzfamilie und Konsolidierung

```
apiVersion: karpenter.sh/v1
kind: NodePool
metadata:
  name: gpu
spec:
  disruption:
    budgets:
      - nodes: 10%
    consolidateAfter: 1h
    consolidationPolicy: WhenEmpty
  template:
    metadata: {}
    spec:
      nodeClassRef:
        group: eks.amazonaws.com
        kind: NodeClass
        name: default
      requirements:
```

```
- key: "karpenter.sh/capacity-type"
  operator: In
  values: ["on-demand"]
- key: "kubernetes.io/arch"
  operator: In
  values: ["amd64"]
- key: "eks.amazonaws.com/instance-family"
  operator: In
  values:
    - g6e
    - g6
terminationGracePeriod: 24h0m0s
```

Anstatt das festzulegen, `eks.amazonaws.com/instance-gpu-name` können Sie `eks.amazonaws.com/instance-family` die Instanzfamilie angeben. Weitere bekannte Bezeichnungen, die Einfluss auf die Überprüfung der Terminplanung haben, finden Sie unter [the section called "Von EKS Auto Mode unterstützte Labels"](#).

Wenn Sie spezielle Speicheranforderungen haben, können Sie den kurzlebigen Speicher der Knoten anpassen `size` und `throughput` Ihren eigenen Speicher erstellen `iops`, auf den Sie [NodeClass](#) zurückgreifen können. `NodePool` Erfahren Sie mehr über die [konfigurierbaren NodeClass](#) Optionen.

Beispiel für eine Speicherkonfiguration für `NodeClass`

```
apiVersion: eks.amazonaws.com/v1
kind: NodeClass
metadata:
  name: gpu
spec:
  ephemeralStorage:
    iops: 3000
    size: 80Gi
    throughput: 125
```

Definieren Sie ein AWS Trainium und Inferentia AWS `NodePool`

Im Folgenden `NodePool` ist `eks.amazonaws.com/instance-category` festgelegt, dass nur Instanzen der Inferentia- und Trainium-Familie gestartet werden sollen:

```
- key: "eks.amazonaws.com/instance-category"
  operator: In
```

```
values:
  - inf
  - trn
```

Generieren Sie CIS-Compliance-Berichte von Kubernetes-Knoten mit `kubectl debug`

In diesem Thema wird beschrieben, wie Sie mithilfe des `kubectl debug` Befehls CIS-Compliance-Berichte (Center for Internet Security) für Amazon EKS-Knoten generieren. Mit dem Befehl können Sie vorübergehend einen Debugging-Container auf einem Kubernetes-Knoten erstellen und CIS-Konformitätsprüfungen mithilfe des Tools ausführen. Das `apiclient` Tool ist Teil von Bottlerocket OS, dem Betriebssystem, das von EKS Auto Mode-Knoten verwendet wird.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Zugriff auf einen Amazon EKS-Cluster mit `kubectl` konfiguriertem (Version muss mindestens v1.32.0 sein; Typ `kubectl version` zur Überprüfung).
- Die entsprechenden IAM-Berechtigungen zum Debuggen von Knoten.
- Ein gültiges Profil, das Debug-Operationen ermöglicht (z. B.). `sysadmin`

Weitere Informationen zur Verwendung von Debugging-Profilen mit `kubectl` finden Sie unter [Debuggen eines Pods oder Nodes beim Anwenden eines Profils](#) in der Kubernetes-Dokumentation.

Verfahren

1. Ermitteln Sie die AWS Instanz-ID des Knotens, auf dem Sie den Bericht ausführen möchten. Verwenden Sie den folgenden Befehl, um die Knoten im Cluster aufzulisten. Die Instanz-ID befindet sich in der Namensspalte und beginnt mit `i-`:

```
kubectl get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
i-0ea0ba0f8ef9ad609	Ready	<none>	62s	v1.30.10-eks-1a9dacd

2. Führen Sie den folgenden Befehl aus und `<instance-id>` ersetzen Sie ihn durch die Instanz-ID des Knotens, den Sie abfragen möchten:

```
kubectl debug node/<instance-id> -it --profile=sysadmin --image=public.ecr.aws/amazonlinux/amazonlinux:2023 -- bash -c "yum install -q -y util-linux-core; nsenter -t 1 -m apiclient report cis --level 1 --format text"
```

Zu den Komponenten dieses Befehls gehören:

- `kubectl debug node/<instance-id>`— Erzeugt eine Debugging-Sitzung für die angegebene EC2 Instanz-ID.
- `-it`— Weist ein TTY (Befehlszeilen-Shell) zu und hält stdin für die interaktive Nutzung geöffnet.
- `--profile=sysadmin`— Verwendet das angegebene `kubectl` Profil mit den entsprechenden Berechtigungen.
- `--image=public.ecr.aws/amazonlinux/amazonlinux:2023`— Wird `amazonlinux:2023` als Container-Image für das Debuggen verwendet.
- `bash -c "..."` — Führt die folgenden Befehle in einer Bash-Shell aus:
 - `yum install -q -y util-linux-core`— Installiert im Hintergrund das erforderliche Dienstprogrammpaket.
 - `nsenter -t 1 -m`— Wird ausgeführt `nsenter`, um in den Namespace des Host-Prozesses zu gelangen (PID 1).
 - `apiclient report cis --level 1 --format text`— Führt den CIS-Konformitätsbericht auf Ebene 1 mit Textausgabe aus.

3. Überprüfen Sie die Textausgabe des Berichts.

Interpretieren der Ausgabe

Der Befehl generiert einen textbasierten Bericht, der den Konformitätsstatus verschiedener CIS-Kontrollen anzeigt. Die Ausgabe umfasst:

- Individuelle CIS-Steuerung IDs
- Beschreibung der einzelnen Kontrollen
- Status „Bestanden“, „Nicht bestanden“ oder „Übersprungen“ für jede Prüfung
- Einzelheiten, die etwaige Compliance-Probleme erläutern

Hier ist ein Beispiel für die Ausgabe des Berichts, der auf einer Bottlerocket-Instanz ausgeführt wurde:

```
Benchmark name:  CIS Bottlerocket Benchmark
Version:         v1.0.0
Reference:       https://www.cisecurity.org/benchmark/bottlerocket
Benchmark level: 1
Start time:      2025-04-11T01:40:39.055623436Z

[SKIP] 1.2.1      Ensure software update repositories are configured (Manual)
[PASS] 1.3.1      Ensure dm-verity is configured (Automatic)[PASS] 1.4.1      Ensure
setuid programs do not create core dumps (Automatic)
[PASS] 1.4.2      Ensure address space layout randomization (ASLR) is enabled
(Automatic)
[PASS] 1.4.3      Ensure unprivileged eBPF is disabled (Automatic)
[PASS] 1.5.1      Ensure SELinux is configured (Automatic)
[SKIP] 1.6        Ensure updates, patches, and additional security software are
installed (Manual)
[PASS] 2.1.1.1    Ensure chrony is configured (Automatic)
[PASS] 3.2.5      Ensure broadcast ICMP requests are ignored (Automatic)
[PASS] 3.2.6      Ensure bogus ICMP responses are ignored (Automatic)
[PASS] 3.2.7      Ensure TCP SYN Cookies is enabled (Automatic)
[SKIP] 3.4.1.3    Ensure IPv4 outbound and established connections are configured
(Manual)
[SKIP] 3.4.2.3    Ensure IPv6 outbound and established connections are configured
(Manual)
[PASS] 4.1.1.1    Ensure journald is configured to write logs to persistent disk
(Automatic)
[PASS] 4.1.2      Ensure permissions on journal files are configured (Automatic)

Passed:          11
Failed:           0
Skipped:          4
Total checks:    15
```

Informationen zum Benchmark finden Sie unter [Kubernetes Benchmark](#) vom Center for Internet Security (CIS).

Zugehörige Ressourcen

- [Bottlerocket CIS Benchmark in der Bottlerocket OS-Dokumentation](#).
- [Debuggen](#) Sie laufende Pods in der Kubernetes-Dokumentation.
- [Kubernetes-Benchmark](#) vom Center for Internet Security (CIS)

Aktivieren Sie die EBS-Volumenverschlüsselung mit vom Kunden verwalteten KMS-Schlüsseln für den automatischen EKS-Modus

Sie können das ephemere Root-Volume für EKS Auto Mode-Instances mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsseln.

Amazon EKS Auto Mode verwendet serviceverknüpfte Rollen, um Berechtigungen an andere AWS Services zu delegieren, wenn verschlüsselte EBS-Volumes für Ihre Kubernetes-Cluster verwaltet werden. In diesem Thema wird beschrieben, wie Sie die Schlüsselrichtlinie einrichten, die Sie benötigen, wenn Sie einen vom Kunden verwalteten Schlüssel für die Amazon EBS-Verschlüsselung mit EKS Auto Mode angeben.

Überlegungen:

- Der automatische EKS-Modus benötigt keine zusätzliche Autorisierung, um den standardmäßigen AWS verwalteten Schlüssel zum Schutz der verschlüsselten Volumes in Ihrem Konto zu verwenden.
- In diesem Thema wird das Verschlüsseln kurzlebiger Volumes, also der Root-Volumes für Instances, behandelt. EC2 Weitere Informationen zur Verschlüsselung von Datenvolumes, die für Workloads verwendet werden, finden Sie unter. [the section called “Erstellen StorageClass”](#)

Übersicht

Die folgenden AWS KMS-Schlüssel können für die Amazon EBS-Root-Volume-Verschlüsselung verwendet werden, wenn EKS Auto Mode Instances startet:

- AWS verwalteter Schlüssel — Ein Verschlüsselungsschlüssel in Ihrem Konto, den Amazon EBS erstellt, besitzt und verwaltet. Dies ist der Standardverschlüsselungsschlüssel für ein neues Konto.
- Vom Kunden verwalteter Schlüssel — Ein benutzerdefinierter Verschlüsselungsschlüssel, den Sie erstellen, besitzen und verwalten.

Note

Der Schlüssel muss symmetrisch sein. Amazon EBS unterstützt keine asymmetrischen vom Kunden verwalteten Schlüssel.

Schritt 1: Konfigurieren Sie die Schlüsselrichtlinie

Ihre KMS-Schlüssel müssen über eine Schlüsselrichtlinie verfügen, die es EKS Auto Mode ermöglicht, Instances mit Amazon EBS-Volumes zu starten, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind.

Konfigurieren Sie Ihre Schlüsselrichtlinie mit der folgenden Struktur:

Note

Diese Richtlinie umfasst nur Berechtigungen für den automatischen EKS-Modus. Für die Schlüsselrichtlinie sind möglicherweise zusätzliche Berechtigungen erforderlich, wenn andere Identitäten den Schlüssel verwenden oder Zuschüsse verwalten müssen.

```
{
  "Version": "2012-10-17",
  "Id": "MyKeyPolicy",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws: iam::<account-id>:role/ClusterServiceRole"
        ]
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow attachment of persistent resources",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws: iam::<account-id>:role/ClusterServiceRole"
        ]
      },
      "Action": [
        "kms:CreateAlias",
        "kms:UpdateAlias",
        "kms:DeleteAlias",
        "kms:ListAliases"
      ],
      "Resource": "*"
    }
  ]
}
```

```

        ]
      },
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    }
  ]
}

```

Stellen Sie sicher, dass Sie es <account-id> durch Ihre tatsächliche AWS Konto-ID ersetzen.

Gehen Sie bei der Konfiguration der Schlüsselrichtlinie wie folgt vor:

- Sie `ClusterServiceRole` müssen über die erforderlichen IAM-Berechtigungen verfügen, um den KMS-Schlüssel für Verschlüsselungsvorgänge verwenden zu können
- Die `kms:GrantIsForAWSResource` Bedingung stellt sicher, dass Zuschüsse nur für AWS Dienste gewährt werden können

Schritt 2: Konfigurieren Sie NodeClass mit Ihrem vom Kunden verwalteten Schlüssel

Nachdem Sie die Schlüsselrichtlinie konfiguriert haben, verweisen Sie in Ihrer NodeClass EKS-Konfiguration für den automatischen Modus auf den KMS-Schlüssel:

```

apiVersion: eks.amazonaws.com/v1
kind: NodeClass
metadata:
  name: my-node-class
spec:
  # Insert existing configuration

  ephemeralStorage:
    size: "80Gi" # Range: 1-59000Gi or 1-64000G or 1-58Ti or 1-64T
    iops: 3000 # Range: 3000-16000

```



```
throughput: 125 # Range: 125-1000

# KMS key for encryption
kmsKeyID: "arn:aws:kms:<region>:<account-id>:key/<key-id>"
```

Ersetzen Sie die Platzhalterwerte durch Ihre tatsächlichen Werte:

- `<region>` mit deiner Region AWS
- `<account-id>` mit deiner AWS Konto-ID
- `<key-id>` mit Ihrer KMS-Schlüssel-ID

Sie können den KMS-Schlüssel in einem der folgenden Formate angeben:

- KMS-Schlüssel-ID: `1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d`
- KMS-Schlüssel-ARN: `arn:aws:kms:us-west-2:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d`
- Aliasname des Schlüssels: `alias/eks-auto-mode-key`
- Schlüsselalias ARN: `arn:aws:kms:us-west-2:111122223333:alias/eks-auto-mode-key`

Wenden Sie die NodeClass Konfiguration mit `kubectl` an:

```
kubectl apply -f nodeclass.yaml
```

Verwandte Ressourcen

- [Erstellen Sie eine Knotenklasse für Amazon EKS](#)
- Weitere Informationen finden Sie im AWS Key Management Service Developer Guide
 - [Berechtigungen für AWS Dienste in wichtigen Richtlinien](#)
 - [Ändern Sie eine wichtige Richtlinie](#)
 - [Zuschüsse in AWS KMS](#)

Aktualisieren Sie die Organisationskontrollen für den EKS-Automatikmodus

Einige Organisationskontrollen können verhindern, dass der EKS-Automatikmodus ordnungsgemäß funktioniert. In diesem Fall müssen Sie diese Steuerelemente aktualisieren, damit EKS Auto Mode über die erforderlichen Berechtigungen verfügt, um EC2 Instanzen in Ihrem Namen zu verwalten.

Der automatische Modus von EKS verwendet eine Servicerolle für den Start der EC2 Instances, die die EKS Auto Mode Nodes unterstützen. Eine Servicerolle ist eine [IAM-Rolle](#), die in Ihrem Konto erstellt wird und von der ein Service übernimmt, Aktionen in Ihrem Namen auszuführen. Die [Richtlinien zur Servicesteuerung](#) (SCPs) gelten immer für Aktionen, die mit Servicerollen ausgeführt werden. Auf diese Weise kann ein SCP den Betrieb des Automatikmodus unterbinden. Am häufigsten kommt es vor, wenn ein SCP verwendet wird, um die Amazon Machine Images (AMIs) einzuschränken, die gestartet werden können. Damit der EKS-Automodus funktioniert, ändern Sie den SCP so, dass der Start AMIs von EKS-Automodus-Konten aus möglich ist.

Sie können auch die AMIs Funktion „[EC2 Zugelassen](#)“ verwenden, um die Sichtbarkeit von AMIs in anderen Konten einzuschränken. Wenn Sie diese Funktion verwenden, müssen Sie die Image-Kriterien so erweitern, dass sie auch die EKS-Automodus-AMI-Konten in den interessierenden Regionen einbeziehen.

Beispiel SCP, um alle AMIs außer dem EKS-Automatikmodus zu blockieren AMIs

Das unten stehende SCP verhindert Anrufe, `ec2:RunInstances` es sei denn, das AMI gehört zum EKS-Automodus-AMI-Konto für `us-west-2` oder `us-east-1`.

Note

Es ist wichtig, den Kontextschlüssel nicht zu verwenden. `ec2:Owner` Amazon besitzt die EKS Auto Mode AMI-Konten und der Wert für diesen Schlüssel wird immer sein `amazon`. Die Konstruktion eines SCP, das den Start ermöglicht, AMIs wenn der `ec2:Owner` IS `amazon` das Starten aller Amazon-eigenen AMI ermöglicht, nicht nur der AMIs für den EKS-Automatikmodus. *

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAMI",
```

```

    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:*:ec2:*::image/ami-*",
    "Condition": {
      "StringNotEquals": {
        "aws:ResourceAccount": [
          "767397842682",
          "992382739861"
        ]
      }
    }
  }
]
}

```

AMI-Konten im EKS-Automatikmodus

AWS Konten, die je nach Region variieren, hosten EKS Auto Mode public AMIs.

AWS Region	Account
af-south-1	471112993317
ap-east-1	590183728416
ap-northeast-1	851725346105
ap-northeast-2	992382805010
ap-northeast-3	891377407544
ap-south-1	975049899075
ap-south-2	590183737426
ap-southeast-1	339712723301
ap-southeast-2	58264376476
ap-southeast-3	471112941769
ap-southeast-4	590183863144

ap-southeast-5	654654202513
ap-southeast-7	533267217478
ca-central-1	992382439851
ca-west-1	767397959864
eu-central-1	891376953411
eu-central-2	381492036002
eu-north-1	339712696471
eu-south-1	975049955519
eu-south-2	471112620929
eu-west-1	381492008532
eu-west-2	590184142468
eu-west-3	891376969258
il-central-1	590183797093
me-central-1	637423494195
me-south-1	905418070398
mx-central-1	211125506622
sa-east-1	339712709251
us-east-1	992382739861
us-east-2	975050179949
us-west-1	975050035094
us-west-2	767397842682

Steuern Sie die Bereitstellung von Workloads für EC2 On-Demand-Kapazitätsreservierungen mit dem automatischen EKS-Modus

EC2 Kapazitätsreservierungen auf Abruf (ODCRs) ermöglichen es Ihnen, Rechenkapazität für Ihre EC2 Amazon-Instances in einer bestimmten Availability Zone für einen beliebigen Zeitraum zu reservieren. Wenn Sie den automatischen EKS-Modus verwenden, möchten Sie möglicherweise kontrollieren, ob Ihre Kubernetes-Workloads auf diesen Reserved Instances bereitgestellt werden, um die Nutzung der im Voraus erworbenen Kapazitäten zu maximieren oder um sicherzustellen, dass kritische Workloads Zugriff auf garantierte Ressourcen haben.

Standardmäßig wird der automatische EKS-Modus automatisch gestartet und geöffnet. ODCRs Durch die Konfiguration `capacityReservationSelectorTerms` auf `a` können Sie `NodeClass` jedoch explizit steuern, welche ODCRs Workloads verwendet werden. Knoten, die mithilfe von `configured ODCRs` bereitgestellt wurden, haben Vorrang vor On-Demand-Nodes `karpenter.sh/capacity-type: reserved` und Spot-Nodes und werden auch weiterhin priorisiert. Sobald diese Funktion aktiviert ist, verwendet der automatische EKS-Modus nicht mehr automatisch die Option „Öffnen“ ODCRs. Sie müssen explizit durch ein ausgewählt werden `NodeClass`, sodass Sie die Kapazitätsreservierungsnutzung in Ihrem gesamten Cluster genau steuern können.

Warning

Wenn Sie `NodeClass` in `capacityReservationSelectorTerms` einem Cluster eine Konfiguration vornehmen, verwendet EKS Auto Mode nicht mehr automatisch open ODCRs für alle `NodeClass` im Cluster.

Beispiel NodeClass

```
apiVersion: eks.amazonaws.com/v1
kind: NodeClass
spec:
  # Optional: Selects upon on-demand capacity reservations and capacity blocks
  # for EKS Auto Mode to prioritize.
  capacityReservationSelectorTerms:
    - id: cr-56fac701cc1951b03
    # Alternative Approaches
    - tags:
        app: "my-app"
    # Optional owning account ID filter
```

```
owner: "012345678901"
```

Dieses Beispiel NodeClass zeigt zwei Ansätze für die Auswahl ODCRs. Die erste Methode referenziert direkt über ihre ID (cr-56fac701cc1951b03) auf ein bestimmtes ODCR. Die zweite Methode verwendet eine Tag-basierte Auswahl, ODCRs wobei das Targeting anhand des Tags erfolgt. Name: "targeted-odcr" Sie können optional auch nach dem AWS Konto filtern, dem die Reservierung gehört. Dies ist besonders nützlich in kontoübergreifenden Szenarien oder bei der Arbeit mit Reservierungen für gemeinsame Kapazitäten.

Erfahren Sie, wie der EKS Auto Mode funktioniert

In diesem Kapitel erfahren Sie, wie die Komponenten von Amazon EKS Auto Mode-Clustern funktionieren.

Themen

- [Erfahren Sie mehr über Amazon EKS Auto Mode Managed Instances](#)
- [Erfahren Sie mehr über Identität und Zugriff im EKS Auto Mode](#)
- [Erfahren Sie mehr über VPC-Netzwerke und Load Balancing im EKS Auto Mode](#)

Erfahren Sie mehr über Amazon EKS Auto Mode Managed Instances

In diesem Thema wird erklärt, wie Amazon EKS Auto Mode EC2 Amazon-Instances in Ihrem EKS-Cluster verwaltet. Wenn Sie den automatischen EKS-Modus aktivieren, werden die Rechenressourcen Ihres Clusters automatisch von EKS bereitgestellt und verwaltet, wodurch sich die Art und Weise ändert, wie Sie mit den EC2 Instances interagieren, die als Knoten in Ihrem Cluster dienen.

Für die Planung Ihrer Workload-Bereitstellungsstrategie und Betriebsabläufe ist es wichtig zu verstehen, wie Amazon EKS Auto Mode Instances verwaltet. Im Gegensatz zu herkömmlichen EC2 Instances oder verwalteten Knotengruppen folgen diese Instances einem anderen Lebenszyklusmodell, bei dem EKS die Verantwortung für viele betriebliche Aspekte übernimmt und gleichzeitig bestimmte Zugriffs- und Anpassungsarten einschränkt.

Amazon EKS Auto Mode automatisiert Routineaufgaben zur Erstellung neuer EC2 Instances und fügt sie als Knoten an Ihren EKS-Cluster an. Der automatische Modus von EKS erkennt, wenn ein Workload nicht auf bestehende Knoten passt, und erstellt eine neue EC2 Instance.

Amazon EKS Auto Mode ist für das Erstellen, Löschen und Patchen von EC2 Instances verantwortlich. Sie sind für die Container und Pods verantwortlich, die auf der Instance bereitgestellt werden.

EC2 Mit EKS Auto Mode erstellte Instanzen unterscheiden sich von anderen EC2 Instances, es handelt sich um verwaltete Instanzen. Diese verwalteten Instanzen gehören EKS und sind stärker eingeschränkt. Sie können nicht direkt auf Software zugreifen oder sie auf Instanzen installieren, die von EKS Auto Mode verwaltet werden.

AWS schlägt vor, entweder den EKS-Automatikmodus oder den selbstverwalteten Karpenter auszuführen. Sie können beide während einer Migration oder in einer erweiterten Konfiguration installieren. Wenn Sie beide installiert haben, konfigurieren Sie Ihre Knotenpools so, dass Workloads entweder dem Karpenter- oder dem EKS Auto Mode zugeordnet sind.

Weitere Informationen finden Sie unter Von [Amazon EC2 verwaltete Instanzen](#) im EC2 Amazon-Benutzerhandbuch.

Vergleichstabelle

EC2 Standardinstanz	Verwaltete Instanz im automatischen Modus von EKS
Sie sind für das Patchen und Aktualisieren der Instanz verantwortlich.	AWS patcht und aktualisiert die Instanz automatisch.
EKS ist nicht verantwortlich für die Software auf der Instanz.	EKS ist für bestimmte Software auf der Instance verantwortlich <code>kubelet</code> , z. B. für die Container-Laufzeit und das Betriebssystem.
Sie können die EC2 Instance mithilfe der EC2 API löschen.	EKS bestimmt die Anzahl der in Ihrem Konto bereitgestellten Instanzen. Wenn Sie einen Workload löschen, reduziert EKS die Anzahl der Instanzen in Ihrem Konto.
Sie können SSH verwenden, um auf die EC2 Instance zuzugreifen.	Sie können Pods und Container auf der verwalteten Instanz bereitstellen.
Sie bestimmen das Betriebssystem und das Image (AMI).	AWS bestimmt das Betriebssystem und das Image.

EC2 Standardinstanz	Verwaltete Instanz im automatischen Modus von EKS
Sie können Workloads bereitstellen, die auf Windows- oder Ubuntu-Funktionen basieren.	Sie können Container bereitstellen, die auf Linux basieren, jedoch ohne spezifische Betriebssystemabhängigkeiten.
Sie bestimmen, welcher Instance-Typ und welche Familie gestartet werden sollen.	AWS bestimmt, welcher Instance-Typ und welche Instance-Familie gestartet werden sollen. Sie können einen Knotenpool verwenden, um die Instance-Typen einzuschränken, aus denen EKS Auto Mode auswählt.

Die folgende Funktionalität funktioniert sowohl für verwaltete Instances als auch für EC2 Standard-Instances:

- Sie können die Instanz in der AWS Konsole anzeigen.
- Sie können den Instanzspeicher als kurzlebigen Speicher für Workloads verwenden.

AMI-Unterstützung

AWS Bestimmt im EKS-Automatikmodus das Image (AMI), das für Ihre Rechenknoten verwendet wird. AWS überwacht den Rollout neuer EKS Auto Mode AMI-Versionen. Wenn Sie Probleme mit der Arbeitslast im Zusammenhang mit einer AMI-Version haben, erstellen Sie einen Support-Fall. Weitere Informationen finden Sie unter [Erstellen von Supportfällen und Fallmanagement](#) im AWS Support-Benutzerhandbuch.

Im Allgemeinen veröffentlicht EKS jede Woche ein neues AMI mit CVE- und Sicherheitsupdates.

Referenz zu den von EKS Auto Mode unterstützten Instanzen

Der automatische EKS-Modus erstellt nur Instanzen unterstützter Typen, die eine Mindestgrößenanforderung erfüllen.

Der automatische Modus von EKS unterstützt die folgenden Instance-Typen:

Familie	Instance-Typen
Für die Datenverarbeitung optimiert (C)	c8g, c7a, c7g, c7gn, c7gd, c7i, c7i-flex, c6a, c6g, c6i, c6gn, c6id, c6in, c6gd, c5, c5a, c5d, c5ad, c5n, c4
Allgemeiner Zweck (M)	m8g, m7i, m7a, m7g, m7gd, m7i-flex, m6a, m6i, m6in, m6in, m6g, m6idn, m6id, m6gd, m5, m5a, m5ad, m5n, m5dn, m5d, m5zn, m4
Speicheroptimiert (R)	r8g, r7a, r7iz, r7gd, r7i, r7g, r6a, r6i, r6id, r6in, r6idn, r6g, r6gd, r5, r5n, r5a, r5dn, r5b, r5ad, r5ad, r5d, r4
Burst-fähig (T)	t4g, t3, t3a, t2
Hoher Speicher (Z/X)	z1d, x8g, x2gd
Speicheroptimiert (I/D)	i4g, i4i, i3, i3en, is4gen, d3, d3en, im4gn
P/G/Inf/T nBeschleunigtes Rechnen ()	p5, p4d, p3, p3dn, gr6, g6e, g5g, g5, g4dn, inf2, inf1, trn1, trn1, trn1n
Hochleistungsrechnen (X2)	x2iezn, x2iedn, x2idn

Darüber hinaus erstellt der automatische Modus von EKS nur Instanzen, die die folgenden Anforderungen erfüllen: EC2

- Mehr als 1 CPU
- Die Instanzgröße ist nicht Nano, Micro oder Small

Weitere Informationen finden Sie unter [Benennungskonventionen für EC2 Amazon-Instance-Typen](#).

Instance-Metadatenservice

- Im automatischen Modus von EKS gilt standardmäßig ein IMDSv2 Hop-Limit von 1, was den bewährten AWS Sicherheitsmethoden entspricht.
- Diese Standardkonfiguration kann im Automatikmodus nicht geändert werden.
- Geben Sie bei Add-Ons, für die normalerweise IMDS-Zugriff erforderlich ist, während der Installation Parameter (z. B. AWS Region) an, um IMDS-Abfragen zu vermeiden. Weitere Informationen finden Sie unter [the section called “Felder, die Sie anpassen können”](#).
- Wenn ein Pod im Automatikmodus unbedingt IMDS-Zugriff benötigt, muss der Pod so konfiguriert werden, dass er mit ausgeführt werden kann. `hostNetwork: true` Dadurch kann der Pod direkt auf den Instanz-Metadatendienst zugreifen.
- Berücksichtigen Sie die Auswirkungen auf die Sicherheit, wenn Sie Pods Zugriff auf Instanz-Metadaten gewähren.

Weitere Informationen zum Amazon EC2 Instance Metadata Service (IMDS) finden [Sie unter Konfiguration der Optionen für den Instance-Metadaten-Service](#) im EC2 Amazon-Benutzerhandbuch.

Überlegungen

- Wenn der konfigurierte flüchtige Speicher in der kleiner NodeClass ist als der NVMe lokale Speicher für die Instance, macht der automatische EKS-Modus eine manuelle Konfiguration überflüssig, indem automatisch die folgenden Aktionen ausgeführt werden:
 - Verwendet ein kleineres (20 GiB) Amazon EBS-Datenvolumen, um die Kosten zu senken.
 - Formatiert und konfiguriert den NVMe lokalen Speicher für die Verwendung kurzlebiger Daten. Dies beinhaltet die Einrichtung eines RAID 0-Arrays, falls mehrere Laufwerke vorhanden sind.
- Amazon EKS Auto Mode unterstützt den AWS Fault Injection Service nicht. Weitere Informationen finden Sie unter [Managing Fault Injection Service-Experimente](#) im AWS Resilience Hub-Benutzerhandbuch.
- Sie müssen die Knoten im automatischen Modus nicht Neuron Device Plugin auf EKS installieren.

Wenn Sie andere Knotentypen in Ihrem Cluster haben, müssen Sie das Neuron Device-Plugin so konfigurieren, dass es nicht auf Knoten im automatischen Modus ausgeführt wird. Weitere Informationen finden Sie unter [the section called “Steuern Sie die Bereitstellung”](#).

Erfahren Sie mehr über Identität und Zugriff im EKS Auto Mode

In diesem Thema werden die Rollen und Berechtigungen für Identity and Access Management (IAM) beschrieben, die für die Verwendung des EKS Auto Mode erforderlich sind. Der automatische Modus von EKS verwendet zwei primäre IAM-Rollen: eine Cluster-IAM-Rolle und eine Node-IAM-Rolle. Diese Rollen arbeiten mit EKS Pod Identity und EKS-Zugriffseinträgen zusammen, um eine umfassende Zugriffsverwaltung für Ihre EKS-Cluster bereitzustellen.

Wenn Sie den automatischen EKS-Modus konfigurieren, müssen Sie diese IAM-Rollen mit spezifischen Berechtigungen einrichten, die es den AWS Diensten ermöglichen, mit Ihren Clusterressourcen zu interagieren. Dazu gehören Berechtigungen für die Verwaltung von Rechenressourcen, Speichervolumen, Load Balancern und Netzwerkkomponenten. Das Verständnis dieser Rollenkonfigurationen ist für den ordnungsgemäßen Betrieb und die Sicherheit des Clusters unerlässlich.

Im automatischen EKS-Modus werden AWS IAM-Rollen über EKS-Zugriffseinträge automatisch Kubernetes-Berechtigungen zugeordnet, sodass keine manuelle Konfiguration oder benutzerdefinierte Bindungen erforderlich sind. `aws-auth` ConfigMaps Wenn Sie einen neuen Auto-Mode-Cluster erstellen, erstellt EKS automatisch die entsprechenden Kubernetes-Berechtigungen mithilfe von Access-Einträgen und stellt so sicher, dass AWS Dienste und Clusterkomponenten sowohl innerhalb des Kubernetes-Autorisierungssystems als auch innerhalb des Kubernetes-Autorisierungssystems über die AWS entsprechenden Zugriffsebenen verfügen. Diese automatisierte Integration reduziert die Komplexität der Konfiguration und trägt dazu bei, berechtigungsbezogene Probleme zu vermeiden, die häufig bei der Verwaltung von EKS-Clustern auftreten.

Cluster-IAM-Rolle

Die Cluster-IAM-Rolle ist eine AWS Identity and Access Management (IAM) -Rolle, die von Amazon EKS zur Verwaltung von Berechtigungen für Kubernetes-Cluster verwendet wird. Diese Rolle gewährt Amazon EKS die erforderlichen Berechtigungen für die Interaktion mit anderen AWS Services im Namen Ihres Clusters und wird mithilfe von EKS-Zugriffseinträgen automatisch mit Kubernetes-Berechtigungen konfiguriert.

- Sie müssen dieser Rolle AWS IAM-Richtlinien zuordnen.
- Der automatische Modus von EKS fügt dieser Rolle mithilfe von EKS-Zugriffseinträgen automatisch Kubernetes-Berechtigungen zu.
- Schlägt mit dem automatischen Modus von EKS AWS vor, eine einzelne Cluster-IAM-Rolle pro Konto zu erstellen. AWS

- AWS schlägt vor, diese Rolle `AmazonEKSAutoClusterRole` zu benennen.
- Diese Rolle erfordert Berechtigungen für mehrere AWS Dienste zur Verwaltung von Ressourcen, einschließlich EBS-Volumes, Elastic Load Balancers und EC2 Instances.
- Die vorgeschlagene Konfiguration für diese Rolle umfasst mehrere AWS verwaltete IAM-Richtlinien, die sich auf die verschiedenen Funktionen von EKS Auto Mode beziehen.
 - `AmazonEKSCoordinatePolicy`
 - `AmazonEKSBlockStoragePolicy`
 - `AmazonEKSLoadBalancingPolicy`
 - `AmazonEKSNetworkPolicy`
 - `AmazonEKSClusterPolicy`

Weitere Informationen zur Cluster-IAM-Rolle und den AWS verwalteten IAM-Richtlinien finden Sie unter:

- [the section called “ AWS verwaltete Richtlinien”](#)
- [the section called “Cluster-IAM-Rolle”](#)

Weitere Informationen zum Kubernetes-Zugriff finden Sie unter:

- [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#)

Knoten-IAM-Rolle

Die Node-IAM-Rolle ist eine AWS Identity and Access Management (IAM) -Rolle, die von Amazon EKS verwendet wird, um Berechtigungen für Worker-Knoten in Kubernetes-Clustern zu verwalten. Diese Rolle gewährt EC2 Instances, die als Kubernetes-Knoten ausgeführt werden, die erforderlichen Berechtigungen für die Interaktion mit AWS Diensten und Ressourcen. Sie wird mithilfe von EKS-Zugriffseinträgen automatisch mit Kubernetes-RBAC-Berechtigungen konfiguriert.

- Sie müssen dieser Rolle IAM-Richtlinien zuordnen AWS .
- Der automatische Modus von EKS fügt dieser Rolle mithilfe von EKS-Zugriffseinträgen automatisch Kubernetes-RBAC-Berechtigungen zu.
- AWS schlägt vor, diese Rolle zu benennen. `AmazonEKSAutoNodeRole`
- Schlägt AWS vor, im automatischen Modus von EKS eine einzelne Node-IAM-Rolle pro AWS Konto zu erstellen.

- Diese Rolle hat eingeschränkte Berechtigungen. Zu den wichtigsten Berechtigungen gehören die Übernahme einer Pod-Identity-Rolle und das Abrufen von Bildern aus ECR.
- AWS schlägt die folgenden AWS verwalteten IAM-Richtlinien vor:
 - AmazonEKSTaskRoleMinimalPolicy
 - AmazonEC2ContainerRegistryPullOnly

Weitere Informationen zur Cluster-IAM-Rolle und zu AWS verwalteten IAM-Richtlinien finden Sie unter:

- [the section called “ AWS verwaltete Richtlinien”](#)
- [the section called “Knoten-IAM-Rolle”](#)

Weitere Informationen zum Kubernetes-Zugriff finden Sie unter:

- [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#)

Servicegebundene Rolle

Amazon EKS verwendet für bestimmte Vorgänge eine serviceverknüpfte Rolle (SLR). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

AWS erstellt und konfiguriert die Spiegelreflexkamera automatisch. Sie können eine Spiegelreflexkamera erst löschen, nachdem Sie zuerst die zugehörigen Ressourcen gelöscht haben. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Die SLR-Richtlinie gewährt Amazon EKS die Erlaubnis, zentrale Infrastrukturkomponenten zu beobachten und zu löschen: EC2 Ressourcen (Instances, Netzwerkschnittstellen, Sicherheitsgruppen), ELB-Ressourcen (Load Balancer, Zielgruppen), CloudWatch Funktionen (Protokollierung und Metriken) und IAM-Rollen mit dem Präfix „eks“. Sie ermöglicht auch private Endpunktnetze durch VPC/hosted Zonenzuweisung und beinhaltet Berechtigungen für die EventBridge Überwachung und Bereinigung von mit EKS markierten Ressourcen.

Weitere Informationen finden Sie unter:

- [the section called “AWS verwaltete Richtlinie: Amazon EKSService RolePolicy”](#)
- [the section called “Serviceverknüpfte Rollenberechtigungen für Amazon EKS”](#)

Benutzerdefinierte AWS Tags für EKS Auto-Ressourcen

Standardmäßig erlauben die verwalteten Richtlinien im Zusammenhang mit dem automatischen Modus von EKS nicht das Anwenden von benutzerdefinierten Tags auf im automatischen Modus bereitgestellte AWS Ressourcen. Wenn Sie benutzerdefinierte Tags auf AWS Ressourcen anwenden möchten, müssen Sie der Cluster-IAM-Rolle zusätzliche Berechtigungen zuweisen, die über ausreichende Berechtigungen verfügen, um Tags auf AWS Ressourcen zu erstellen und zu ändern. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die uneingeschränkten Tagging-Zugriff ermöglicht:

Beispiel für eine benutzerdefinierte Tag-Richtlinie anzeigen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Compute",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/eks:eks-cluster-name": "${aws:PrincipalTag/eks:eks-cluster-name}"
        },
        "StringLike": {
          "aws:RequestTag/eks:kubernetes-node-class-name": "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name": "*"
        }
      }
    },
    {
      "Sid": "Storage",
      "Effect": "Allow",

```

```

        "Action": [
            "ec2:CreateVolume",
            "ec2:CreateSnapshot"
        ],
        "Resource": [
            "arn:aws: ec2:*:*:volume/*",
            "arn:aws: ec2:*:*:snapshot/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/eks:eks-cluster-name": "${aws:PrincipalTag/eks:eks-
cluster-name}"
            }
        }
    },
    {
        "Sid": "Networking",
        "Effect": "Allow",
        "Action": "ec2:CreateNetworkInterface",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/eks:eks-cluster-name": "${aws:PrincipalTag/eks:eks-
cluster-name}"
            },
            "StringLike": {
                "aws:RequestTag/eks:kubernetes-cni-node-name": "*"
            }
        }
    },
    {
        "Sid": "LoadBalancer",
        "Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:CreateTargetGroup",
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:CreateRule",
            "ec2:CreateSecurityGroup"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {

```

```

        "aws:RequestTag/eks:eks-cluster-name": "${aws:PrincipalTag/eks:eks-
cluster-name}"
    }
}
},
{
    "Sid": "ShieldProtection",
    "Effect": "Allow",
    "Action": [
        "shield:CreateProtection"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/eks:eks-cluster-name": "${aws:PrincipalTag/eks:eks-
cluster-name}"
        }
    }
},
{
    "Sid": "ShieldTagResource",
    "Effect": "Allow",
    "Action": [
        "shield:TagResource"
    ],
    "Resource": "arn:aws:shield::*:protection/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/eks:eks-cluster-name": "${aws:PrincipalTag/eks:eks-
cluster-name}"
        }
    }
}
]
}

```

Referenz zur Zugriffsrichtlinie

Weitere Informationen zu den von EKS Auto Mode verwendeten Kubernetes-Berechtigungen finden Sie unter. [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#)

Erfahren Sie mehr über VPC-Netzwerke und Load Balancing im EKS Auto Mode

In diesem Thema wird erklärt, wie die Netzwerk- und Lastausgleichsfunktionen der Virtual Private Cloud (VPC) im automatischen Modus von EKS konfiguriert werden. Während der automatische EKS-Modus die meisten Netzwerkkomponenten automatisch verwaltet, können Sie dennoch bestimmte Aspekte der Netzwerkkonfiguration Ihres Clusters mithilfe von `NodeClass` Ressourcen und Load Balancer-Anmerkungen anpassen.

Wenn Sie EKS Auto Mode verwenden, AWS verwaltet es die VPC Container Network Interface (CNI) -Konfiguration und die Load Balancer-Bereitstellung für Ihren Cluster. Sie können das Netzwerkverhalten beeinflussen, indem Sie `NodeClass` Objekte definieren und spezifische Anmerkungen auf Ihre Service- und Ingress-Ressourcen anwenden, während Sie gleichzeitig das automatisierte Betriebsmodell beibehalten, das EKS Auto Mode bietet.

Netzwerkfähigkeit

Der automatische Modus von EKS verfügt über eine neue Netzwerkfunktion, die Knoten- und Pod-Netzwerke verwaltet. Sie können es konfigurieren, indem Sie ein `NodeClass` Kubernetes-Objekt erstellen.

Die Konfigurationsoptionen für das vorherige AWS VPC-CNI gelten nicht für den EKS-Automatikmodus.

Konfigurieren Sie das Netzwerk mit einem **NodeClass**

Mit der `NodeClass` Ressource im automatischen EKS-Modus können Sie bestimmte Aspekte der Netzwerkfähigkeit anpassen. Über `NodeClass` können Sie Sicherheitsgruppenauswahlen angeben, die Knotenplatzierung in VPC-Subnetzen steuern, SNAT-Richtlinien festlegen, Netzwerkrichtlinien konfigurieren und die Protokollierung von Netzwerkereignissen aktivieren. Dieser Ansatz behält das automatisierte Betriebsmodell von EKS Auto Mode bei und bietet gleichzeitig Flexibilität bei der Netzwerkanpassung.

Sie können `NodeClass` verwenden, um:

- Wählen Sie eine Sicherheitsgruppe für Knoten
- Steuern Sie, wie Knoten in VPC-Subnetzen platziert werden
- Stellen Sie die Node-SNAT-Richtlinie auf `random disabled` ein

- Aktivieren Sie Kubernetes-Netzwerkrichtlinien, einschließlich:
 - Stellen Sie die Netzwerkrichtlinie auf Standard Verweigern oder Standard Zulassen
 - Aktivieren Sie die Protokollierung von Netzwerkereignissen in einer Datei.
- Isolieren Sie den Pod-Verkehr vom Knotenverkehr, indem Sie Pods an verschiedene Subnetze anhängen.

Erfahren Sie, wie Sie [ein Amazon EKS erstellen NodeClass](#).

Überlegungen

Der automatische Modus von EKS unterstützt:

- EKS-Netzwerkrichtlinien.
- Die `HostPort` und `HostNetwork` Optionen für Kubernetes-Pods.
- Knoten und Pods in öffentlichen oder privaten Subnetzen.
- Zwischenspeichern von DNS-Abfragen auf dem Knoten.

Der EKS-Automatikmodus unterstützt nicht:

- Sicherheitsgruppen pro Pod (SGPP).
- Benutzerdefiniertes Netzwerk in der `ENIConfig`. Sie können Pods in mehreren Subnetzen platzieren oder sie ausschließlich vom Knotenverkehr isolieren. [the section called "Subnetauswahl für Pods"](#)
- Warme IP-, warme Präfix- und warme ENI-Konfigurationen.
- Minimale Konfiguration der IP-Ziele.
- Aktivierung oder Deaktivierung der Präfix-Delegierung.
- Andere Konfigurationen, die von der AWS Open-Source-VPC CNI unterstützt werden.
- Netzwerkrichtlinien-Konfigurationen wie die Conntrack-Timer-Anpassung (Standard ist 300s).
- Netzwerkereignisprotokolle exportieren nach CloudWatch

Verwaltung von Netzwerkressourcen

Der automatische Modus von EKS kümmert sich um die Verwaltung von Präfixen, IP-Adressen und Netzwerkschnittstellen, indem er die NodeClass Ressourcen für Netzwerkkonfigurationen überwacht. Der Dienst führt mehrere wichtige Operationen automatisch aus:

Präfix-Delegierung

Der automatische Modus von EKS stellt /28 IPv4 Präfixe für die primäre Netzwerkschnittstelle für Knoten bereit und verwaltet einen vordefinierten warmen Ressourcenpool, der auf der Grundlage der Anzahl der geplanten Pods skaliert wird. Bei Bedarf stellt er sekundäre Netzwerkschnittstellen mit identischen Sicherheitsgruppen wie die primäre Schnittstelle im Subnetz des Knotens bereit. Wenn Präfixe im Subnetz nicht mehr verfügbar sind, greift der Dienst auf sekundäre Adressen zurück. IPv4

Verwaltung der Abklingzeit

Der Dienst implementiert einen Cooldown-Pool für Präfixe oder sekundäre IPv4 Adressen, die nicht mehr verwendet werden. Nach Ablauf der Abklingzeit werden diese Ressourcen wieder an die VPC freigegeben. Wenn Pods diese Ressourcen jedoch während der Abklingzeit wiederverwenden, werden sie aus dem Abklingpool wiederhergestellt.

IPv6 Support

Für IPv6 Cluster stellt der automatische Modus von EKS ein /80 IPv6 Präfix pro Knoten auf der primären Netzwerkschnittstelle bereit.

Der Dienst gewährleistet außerdem die ordnungsgemäße Verwaltung und automatische Erfassung aller Netzwerkschnittstellen.

Load Balancing

Sie konfigurieren AWS Elastic Load Balancer, die vom EKS Auto Mode bereitgestellt werden, mithilfe von Anmerkungen zu Service- und Ingress-Ressourcen.

Weitere Informationen finden Sie unter [the section called “Ingress-Klasse erstellen”](#) oder [the section called “Service erstellen”](#).

Überlegungen zum Lastenausgleich mit dem EKS Auto Mode

- Der Standard-Targeting-Modus ist der IP-Modus, nicht der Instanzmodus.
- Der automatische EKS-Modus unterstützt nur den Sicherheitsgruppenmodus für Network Load Balancer.
- AWS unterstützt nicht die Migration von Load Balancern vom selbstverwalteten AWS Load Balancer-Controller zur Verwaltung durch den automatischen Modus von EKS.
- Das `networking.ingress.ipBlock` Feld in der TargetGroupBinding Spezifikation wird nicht unterstützt.

- Wenn Ihre Worker-Knoten benutzerdefinierte Sicherheitsgruppen (kein `eks-cluster-sg-` Benennungsmuster) verwenden, benötigt Ihre Clusterrolle zusätzliche IAM-Berechtigungen. Die von EKS verwaltete Standardrichtlinie erlaubt es EKS nur, benannte Sicherheitsgruppen zu ändern. `eks-cluster-sg-` Ohne die Erlaubnis, Ihre benutzerdefinierten Sicherheitsgruppen zu ändern, kann EKS die erforderlichen Eingangsregeln nicht hinzufügen, die es ALB/NLB-Verkehr ermöglichen, Ihre Pods zu erreichen.

Problembehandlung im EKS-Automatikmodus

AWS übernimmt mit dem automatischen Modus von EKS mehr Verantwortung für EC2 Instances in Ihrem AWS Konto. EKS übernimmt die Verantwortung für die Container-Laufzeit auf den Knoten, das Betriebssystem auf den Knoten und bestimmte Controller. Dazu gehören ein Blockspeicher-Controller, ein Load-Balancing-Controller und ein Compute-Controller.

Sie müssen Kubernetes verwenden AWS , um Fehler bei Knoten APIs zu beheben. Sie haben folgende Möglichkeiten:

- Verwenden Sie eine `NodeDiagnostic` Kubernetes-Ressource, um Knotenprotokolle mithilfe von abzurufen. [the section called “Agent zur Knotenüberwachung”](#) Weitere Schritte finden Sie unter. [the section called “Holen Sie sich Knotenprotokolle”](#)
- Verwenden Sie den AWS EC2 CLI-Befehl `get-console-output`, um die Konsolenausgabe von Knoten abzurufen. Weitere Schritte finden Sie unter [the section called “Rufen Sie mithilfe der AWS EC2 CLI die Konsolenausgabe von einer EC2 verwalteten Instanz ab”](#).
- Verwenden Sie Kubernetes-Debugging-Container, um Knotenprotokolle abzurufen. Weitere Schritte finden Sie unter. [the section called “Rufen Sie Knotenprotokolle mithilfe von Debug-Containern und der CLI ab kubectl”](#)

Note

Der automatische Modus von EKS verwendet EC2 verwaltete Instanzen. Sie können nicht direkt auf EC2 verwaltete Instanzen zugreifen, auch nicht über SSH.

Möglicherweise haben Sie die folgenden Probleme, für die es spezifische Lösungen für die Komponenten von EKS Auto Mode gibt:

- Pods bleiben im Pending Status hängen und werden nicht für Knoten im automatischen Modus geplant. Lösungen finden Sie unter [the section called “Beheben Sie die Fehlerbehebung, wenn der Pod nicht auf den Automodus-Knoten zugreifen kann”](#).
- EC2 verwaltete Instanzen, die dem Cluster nicht als Kubernetes-Knoten beitreten. Lösungen finden Sie unter [the section called “Problembehandlung für den Knoten, der dem Cluster nicht beitrifft”](#)
- Fehler und Probleme mit den NodePools, und PersistentVolumes, Services die die Controller verwenden, die im EKS-Automatikmodus enthalten sind. Lösungen finden Sie unter [the section called “Beheben Sie Fehler bei mitgelieferten Controllern im Automatikmodus”](#).
- Die verbesserte Pod-Sicherheit verhindert die gemeinsame Nutzung von Volumes zwischen Pods. Lösungen finden Sie unter [the section called “Volumes auf mehreren Pods teilen”](#).

Sie können die folgenden Methoden verwenden, um Fehler bei Komponenten im automatischen Modus von EKS zu beheben:

- [the section called “Rufen Sie mithilfe der AWS EC2 CLI die Konsolenausgabe von einer EC2 verwalteten Instanz ab”](#)
- [the section called “Rufen Sie Knotenprotokolle mithilfe von Debug-Containern und der CLI ab kubectl”](#)
- [the section called “Zeigen Sie die mit dem automatischen Modus von EKS verknüpften Ressourcen in der AWS Konsole an”](#)
- [the section called “IAM-Fehler in Ihrem AWS Konto anzeigen”](#)
- [the section called “Erkennen Sie Probleme mit der Knotenkonnektivität VPC Reachability Analyzer”](#)

Agent zur Knotenüberwachung

Der automatische EKS-Modus umfasst den Amazon EKS-Knotenüberwachungsagenten. Sie können diesen Agenten verwenden, um Informationen zur Fehlerbehebung und zum Debuggen von Knoten anzuzeigen. Der Node Monitoring Agent veröffentlicht Kubernetes events und Node. conditions. Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).

Rufen Sie mithilfe der AWS EC2 CLI die Konsolenausgabe von einer EC2 verwalteten Instanz ab

Dieses Verfahren hilft bei der Behebung von Problemen beim Booten oder auf Kernebene.

Zunächst müssen Sie die EC2 Instanz-ID der Instanz ermitteln, die Ihrem Workload zugeordnet ist. Verwenden Sie zweitens die AWS CLI, um die Konsolenausgabe abzurufen.

1. Vergewissern Sie sich, dass Sie Ihren Cluster `kubectl` installiert und eine Verbindung zu ihm hergestellt haben
2. (Optional) Verwenden Sie den Namen einer Kubernetes-Bereitstellung, um die zugehörigen Pods aufzulisten.

```
kubectl get pods -l app=<deployment-name>
```

3. Verwenden Sie den Namen des Kubernetes-Pods, um die EC2 Instanz-ID des zugehörigen Knotens zu ermitteln.

```
kubectl get pod <pod-name> -o wide
```

4. Verwenden Sie die EC2 Instanz-ID, um die Konsolenausgabe abzurufen.

```
aws ec2 get-console-output --instance-id <instance id> --latest --output text
```

Rufen Sie Knotenprotokolle mithilfe von Debug-Containern und der CLI ab **kubectl**

Die empfohlene Methode zum Abrufen von Protokollen von einem EKS-Automodus-Knoten ist die Verwendung `NodeDiagnostic` von Ressourcen. Informationen zu diesen Schritten finden Sie unter [the section called “Holen Sie sich Knotenprotokolle”](#).

Mit dem `kubectl debug node` Befehl können Sie jedoch Logs live von einer Instance streamen. Mit diesem Befehl wird auf dem Knoten, den Sie debuggen möchten, ein neuer Pod gestartet, den Sie dann interaktiv verwenden können.

1. Starten Sie einen Debug-Container. Der folgende Befehl verwendet `i-01234567890123456` die Instanz-ID des Knotens, `-it` weist `A tty` und `Attach stdin` für die interaktive Verwendung zu und verwendet das `sysadmin` Profil aus der Datei `kubeconfig`.

```
kubectl debug node/i-01234567890123456 -it --profile=sysadmin --image=public.ecr.aws/amazonlinux/amazonlinux:2023
```

Eine Beispielausgabe sieht wie folgt aus.

```
Creating debugging pod node-debugger-i-01234567890123456-nxb9c with container
debugger on node i-01234567890123456.
```

```
If you don't see a command prompt, try pressing enter.
bash-5.2#
```

2. Von der Shell aus können Sie nun installieren, `util-linux-core` welche den Befehl bereitstellt. `nsenter` Verwenden Sie `nsenter`, um den Mount-Namespace von PID 1 (`init`) auf dem Host aufzurufen und den `journalctl` Befehl auszuführen, um Logs aus dem `kubelet` folgenden Verzeichnis zu streamen:

```
yum install -y util-linux-core
nsenter -t 1 -m journalctl -f -u kubelet
```

Aus Sicherheitsgründen installiert das Amazon Linux-Container-Image standardmäßig nicht viele Binärdateien. Sie können den `yum whatprovides` Befehl verwenden, um das Paket zu identifizieren, das installiert werden muss, um eine bestimmte Binärdatei bereitzustellen.

```
yum whatprovides ps
```

```
Last metadata expiration check: 0:03:36 ago on Thu Jan 16 14:49:17 2025.
procps-ng-3.3.17-1.amzn2023.0.2.x86_64 : System and process monitoring utilities
Repo          : @System
Matched from:
Filename      : /usr/bin/ps
Provide       : /bin/ps

procps-ng-3.3.17-1.amzn2023.0.2.x86_64 : System and process monitoring utilities
Repo          : amazonlinux
Matched from:
Filename      : /usr/bin/ps
Provide       : /bin/ps
```

Zeigen Sie die mit dem automatischen Modus von EKS verknüpften Ressourcen in der AWS Konsole an

Sie können die AWS Konsole verwenden, um den Status der Ressourcen anzuzeigen, die Ihrem EKS-Auto-Mode-Cluster zugeordnet sind.

- [EBS-Volumes](#)

- Suchen Sie nach dem Tag-Schlüssel, um Volumes im EKS-Automatikmodus anzuzeigen
`eks:eks-cluster-name`

- [Load Balancer](#)

- Suchen Sie nach dem Tag-Schlüssel, um die Lastenausgleichsmodule im automatischen Modus von EKS anzuzeigen `eks:eks-cluster-name`

- [EC2 Instances](#)

- Suchen Sie nach dem Tag-Schlüssel, um die Instanzen im automatischen Modus von EKS anzuzeigen `eks:eks-cluster-name`

IAM-Fehler in Ihrem AWS Konto anzeigen

1. Navigieren Sie zur Konsole CloudTrail
2. Wählen Sie im linken Navigationsbereich „Event History“ aus
3. Wenden Sie Fehlercode-Filter an:
 - AccessDenied
 - UnauthorizedOperation
 - InvalidClientTokenId

Suchen Sie nach Fehlern im Zusammenhang mit Ihrem EKS-Cluster. Verwenden Sie die Fehlermeldungen, um Ihre EKS-Zugriffseinträge, Ihre Cluster-IAM-Rolle oder Ihre Knoten-IAM-Rolle zu aktualisieren. Möglicherweise müssen Sie diesen Rollen eine neue Richtlinie mit Berechtigungen für den automatischen EKS-Modus hinzufügen.

Beheben Sie die Fehlerbehebung, wenn der Pod nicht auf den Automodus-Knoten zugreifen kann

Wenn Pods im Pending Status verbleiben und nicht auf einem Knoten im auto Modus eingeplant werden, überprüfen Sie, ob Ihr Pod oder Ihr Bereitstellungsmanifest über eine verfügnodeSelector. Wenn ein vorhanden nodeSelector ist, stellen Sie sicher, dass es für `eks.amazonaws.com/compute-type: auto` die Planung auf Knoten verwendet wird, die im automatischen EKS-Modus erstellt wurden. Weitere Informationen zu den Knotenbezeichnungen, die von EKS Auto Mode verwendet werden, finden Sie unter [the section called “Steuern Sie die Bereitstellung”](#).

Problembehandlung für den Knoten, der dem Cluster nicht beiträgt

Der automatische EKS-Modus konfiguriert automatisch neue EC2 Instanzen mit den richtigen Informationen für den Beitritt zum Cluster, einschließlich des Cluster-Endpunkts und der Cluster-Zertifizierungsstelle (CA). Diese Instanzen können dem EKS-Cluster jedoch immer noch nicht als Knoten beitreten. Führen Sie die folgenden Befehle aus, um Instanzen zu identifizieren, die dem Cluster nicht beigetreten sind:

1. Führen Sie `kubectl get nodeclaim` aus, um zu überprüfen, ob NodeClaims dies der Fall `istReady = False`.

```
kubectl get nodeclaim
```

2. Führen Sie das Programm aus `kubectl describe nodeclaim <node_claim>` und suchen Sie unter Status nach Problemen, die den Knoten daran hindern, dem Cluster beizutreten.

```
kubectl describe nodeclaim <node_claim>
```

Häufige Fehlermeldungen:

Error getting launch template configs

Dieser Fehler wird möglicherweise angezeigt, wenn Sie benutzerdefinierte Tags NodeClass mit den standardmäßigen Cluster-IAM-Rollenberechtigungen einrichten. Siehe [the section called "Identität und Zugriff"](#).

Error creating fleet

Möglicherweise liegt ein Autorisierungsproblem beim RunInstances Aufrufen des Aufrufs über die EC2 API vor. AWS CloudTrail Suchen Sie nach Fehlern und [the section called "Cluster-IAM-Rolle im automatischen Modus"](#) nach den erforderlichen IAM-Berechtigungen.

Erkennen Sie Probleme mit der Knotenkonnektivität **VPC Reachability Analyzer**

Note

Ihnen wird jede Analyse in Rechnung gestellt, für die der VPC Reachability Analyzer ausgeführt wird. Preisdetails finden Sie unter [Amazon VPC-Preise](#).

Ein Grund dafür, dass eine Instance dem Cluster nicht beigetreten ist, ist ein Problem mit der Netzwerkkonnektivität, das sie daran hindert, den API-Server zu erreichen. Um dieses Problem zu diagnostizieren, können Sie den [VPC Reachability Analyzer](#) verwenden, um eine Analyse der Konnektivität zwischen einem Knoten, der dem Cluster nicht beitreten kann, und dem API-Server durchzuführen. Sie benötigen zwei Informationen:

- Instanz-ID eines Knotens, der dem Cluster nicht beitreten kann
- IP-Adresse des Kubernetes-API-Serverendpunkts

Um die Instanz-ID zu erhalten, müssen Sie einen Workload auf dem Cluster erstellen, damit EKS Auto Mode eine EC2 Instanz startet. Dadurch wird auch ein NodeClaim Objekt in Ihrem Cluster erstellt, das die Instanz-ID haben wird. Führen Sie `kubectl get nodeclaim -o yaml` den Befehl aus, um alle NodeClaims in Ihrem Cluster zu drucken. Jedes NodeClaim enthält die Instanz-ID als Feld und erneut in der ProviderID:

```
kubectl get nodeclaim -o yaml
```

Eine Beispielausgabe sieht wie folgt aus.

```
nodeName: i-01234567890123456
providerID: aws:///us-west-2a/i-01234567890123456
```

Sie können Ihren Kubernetes-API-Serverendpunkt ermitteln, indem Sie Folgendes ausführen. `kubectl get endpoint kubernetes -o yaml` Die Adressen befinden sich im Adressfeld:

```
kubectl get endpoints kubernetes -o yaml
```

Eine Beispielausgabe sieht wie folgt aus.

```
apiVersion: v1
kind: Endpoints
metadata:
  name: kubernetes
  namespace: default
subsets:
- addresses:
  - ip: 10.0.143.233
  - ip: 10.0.152.17
ports:
```

```
- name: https
  port: 443
  protocol: TCP
```

Mit diesen beiden Informationen können Sie die s-Analyse durchführen. Navigieren Sie zunächst zum VPC Reachability Analyzer in der AWS Management Console

1. Klicken Sie auf „Pfad erstellen und analysieren“
2. Geben Sie einen Namen für die Analyse ein (z. B. „Node Join Failure“)
3. Wählen Sie für den „Quellentyp“ die Option „Instances“
4. Geben Sie die Instanz-ID des ausfallenden Knotens als „Quelle“ ein
5. Wählen Sie für das „Pfadziel“ die Option „IP-Adresse“
6. Geben Sie eine der IP-Adressen für den API-Server als „Zieladresse“ ein
7. Erweitern Sie den Abschnitt „Konfiguration des zusätzlichen Paket-Headers“
8. Geben Sie als „Zielport“ 443 ein
9. Wählen Sie „Protocol“ als TCP aus, falls es noch nicht ausgewählt ist
10. Klicken Sie auf „Pfad erstellen und analysieren“
11. Es kann einige Minuten dauern, bis die Analyse abgeschlossen ist. Wenn die Analyseergebnisse darauf hindeuten, dass die Erreichbarkeit nicht gewährleistet ist, wird angezeigt, wo der Fehler im Netzwerkpfad aufgetreten ist, sodass Sie das Problem beheben können.

Volumes auf mehreren Pods teilen

EKS-Automodus-Knoten werden SELinux im Modus „Erzwingung“ konfiguriert, was für mehr Isolation zwischen Pods sorgt, die auf demselben Knoten ausgeführt werden. Wenn diese Option aktiviert ist, erhalten die meisten nicht privilegierten Pods automatisch ein eigenes Sicherheitslabel (Multi-Category Security, MCS). Dieses MCS-Label ist für jeden Pod einzigartig und soll sicherstellen, dass ein Prozess in einem Pod keinen Prozess in einem anderen Pod oder auf dem Host manipulieren kann. Selbst wenn ein Pod mit der Bezeichnung root ausgeführt wird und Zugriff auf das Host-Dateisystem hat, ist er nicht in der Lage, Dateien zu manipulieren, sensible Systemaufrufe auf dem Host durchzuführen, auf die Container-Laufzeit zuzugreifen oder das geheime Schlüsselmaterial von Kubelet abzurufen.

Aus diesem Grund können Probleme auftreten, wenn Sie versuchen, Daten zwischen Pods auszutauschen. `PersistentVolumeClaim` Bei einem Zugriffsmodus von `ReadWriteOnce` können beispielsweise immer noch nicht mehrere Pods gleichzeitig auf das Volume zugreifen.

Um diese gemeinsame Nutzung zwischen Pods zu ermöglichen, können Sie mithilfe der Pods `seLinuxOptions` dasselbe MCS-Label für diese Pods konfigurieren. In diesem Beispiel weisen wir dem Pod die drei Kategorien `c123`, `c456`, `c789` zu. Dies wird nicht mit Kategorien kollidieren, die Pods auf dem Knoten automatisch zugewiesen wurden, da ihnen nur zwei Kategorien zugewiesen werden.

```
securityContext:
  seLinuxOptions:
    level: "s0:c123,c456,c789"
```

Beheben Sie Fehler bei mitgelieferten Controllern im Automatikmodus

Wenn Sie ein Problem mit einem Controller haben, sollten Sie Folgendes untersuchen:

- Ob die mit diesem Controller verknüpften Ressourcen richtig formatiert und gültig sind.
- Wenn die AWS IAM- und Kubernetes-RBAC-Ressourcen für Ihren Cluster ordnungsgemäß konfiguriert sind. Weitere Informationen finden Sie unter [the section called “Identität und Zugriff”](#).

Lesen Sie die Versionshinweise zu EKS Auto Mode

Diese Seite dokumentiert Updates für Amazon EKS Auto Mode. Sie können auf dieser Seite regelmäßig nach Ankündigungen zu Funktionen, Bugfixes, bekannten Problemen und veralteten Funktionen suchen.

Um Benachrichtigungen über alle Änderungen an der Quelldatei auf dieser speziellen Dokumentationsseite zu erhalten, können Sie die folgende URL mit einem RSS-Reader abonnieren:

```
https://github.com/awsdocs/amazon-eks-user-guide/commits/mainline/latest/ug/automode/
auto-change.adoc.atom
```

30. Juni 2025

Feature: Der automatische Modus verwendet NodeClass jetzt den konfigurierten benutzerdefinierten KMS-Schlüssel, um zusätzlich zum Datenvolumen auch das schreibgeschützte Root-Volume der Instanz zu verschlüsseln. Bisher wurde der benutzerdefinierte KMS-Schlüssel nur zur Verschlüsselung des Datenvolumens verwendet.

20. Juni 2025

Funktion: Support für die Steuerung der Bereitstellung von Workloads in EC2 On-Demand-Kapazitätsreservierungen (ODCRs). Dadurch wird der optionale Schlüssel `capacityReservationSelectorTerms` hinzugefügt `NodeClass`, sodass Sie explizit steuern können, welche ODCRs Workloads verwenden. Weitere Informationen finden Sie unter [the section called “Steuern Sie den ODCR-Einsatz”](#).

13. Juni 2025

Feature: Support für separate Pod-Subnetze in der `NodeClass`. Dadurch werden die optionalen Schlüssel hinzugefügt `podSubnetSelectorTerms` und `podSecurityGroupSelectorTerms` die Subnetze und Sicherheitsgruppen für die Pods festgelegt. Weitere Informationen finden Sie unter [the section called “Subnetzauswahl für Pods”](#).

30. April 2025

Feature: Support für Forward-Netzwerk-Proxys in der `NodeClass`. Dadurch wird der optionale Schlüssel `advancedNetworking` zum Einstellen Ihres HTTPS-Proxys hinzugefügt. Weitere Informationen finden Sie unter [the section called “Spezifikation der Knotenklasse”](#).

18. April 2025

Feature: Support für die Auflösung von `.local`-Domains (normalerweise für Multicast-DNS reserviert) über Unicast-DNS.

11. April 2025

Feature: Hinzugefügt `certificateBundles` und `ephemeralStorage.kmsKeyID` zu `NodeClass`. Weitere Informationen finden Sie unter [the section called “Spezifikation der Knotenklasse”](#).

Feature: Verbesserte Geschwindigkeit beim Abrufen von Bildern, insbesondere für Instance-Typen mit lokalem Instanzspeicher, die von der schnelleren Bilddekomprimierung profitieren können.

Fehlerbehebung: Es wurde ein Race-Problem behoben `FailedCreatePodSandBox`, das zu einem Fehler beim Wählen führte: `dial tcp 127.0.0.1:50051: connect: Die Verbindung konnte manchmal nicht hergestellt werden`, wenn Pods direkt beim Start zu einem Node planten.

4. April 2025

Funktion: Erhöhen Sie den `registryPullQPS` Wert von 5 auf 25 und `registryBurst` von 10 auf 50, um die vom Client erzwungene Drosselung beim Abrufen von Bildern zu reduzieren () `Failed to pull image xyz: pull QPS exceeded`

31. März 2025

Fehlerbehebung: Behebt ein Problem, bei dem, wenn ein Core-DNS-Pod auf einem Knoten im automatischen Modus ausgeführt wird, DNS-Abfragen von Pods auf dem Knoten diesen Core-DNS-Pod statt den lokalen DNS-Server des Knotens treffen. DNS-Abfragen von Pods auf einem Automodus-Knoten werden immer an den lokalen DNS des Knotens weitergeleitet.

21. März 2025

Fehlerbehebung: Knoten im automatischen Modus werden jetzt `kube-dns.kube-system.svc.cluster.local` korrekt aufgelöst, wenn kein `kube-dns` Dienst im Cluster installiert ist. Behebt GitHub das Problem [#2546](#).

14. März 2025

Funktion: IPv4 Egress ist in IPv6 Clustern aktiviert. IPv4Der aus Clustern im IPv6 automatischen Modus ausgehende Datenverkehr wird jetzt automatisch in die v4 Adresse der primären ENI des Knotens übersetzt.

Organisieren Sie Workloads mit Amazon EKS-Clustern

Ein Amazon-EKS-Cluster besteht aus zwei primären Komponenten:

- Die Amazon-EKS-Steuerebene
- Amazon-EKS-Knoten, die in der Steuerebene registriert sind

Die Amazon-EKS-Steuerebene besteht aus Steuerebenenknoten, auf denen Kubernetes-Software wie etcd und der Kubernetes-API-Server ausgeführt werden. Die Kontrollebene wird in einem Konto ausgeführt, das von verwaltet wird AWS, und die Kubernetes-API wird über den Amazon EKS-Endpunkt verfügbar gemacht, der Ihrem Cluster zugeordnet ist. Jede Amazon EKS-Cluster-Steuerebene ist einmandantenfähig und einzigartig und wird auf ihren eigenen EC2 Amazon-Instances ausgeführt.

Alle von den etcd Knoten und den zugehörigen Amazon EBS-Volumes gespeicherten Daten werden mit AWS KMS verschlüsselt. Die Cluster-Steuerungsebene ist über mehrere Availability Zones verteilt und wird von einem Elastic Load Balancing Network Load Balancer unterstützt. Amazon EKS stellt in Ihren VPC-Subnetzen außerdem Elastic Network-Schnittstellen für die Verbindung zwischen Steuerebenen-Instances und -Knoten bereit (z. B. zur Unterstützung von `kubectl exec-logs-proxy`-Datenströmen).

Important

In der Amazon-EKS-Umgebung ist der etcd-Speicher gemäß [Upstream-Empfehlungen](#) auf 8 GiB beschränkt. Sie können eine Metrik für die aktuelle Datenbankgröße überwachen, indem Sie den folgenden Befehl ausführen. Wenn Ihr Cluster über eine der unten aufgeführten Kubernetes-Versionen verfügt¹, ersetzen Sie diese durch. `apiserver_storage_size_bytes` `apiserver_storage_db_total_size_in_bytes`

```
kubectl get --raw=/metrics | grep "apiserver_storage_size_bytes"
```

Amazon EKS-Knoten werden in Ihrem AWS Konto ausgeführt und stellen über den API-Serverendpunkt und eine Zertifikatsdatei, die für Ihren Cluster erstellt wurde, eine Verbindung zur Kontrollebene Ihres Clusters her.

 Note

- Wie die verschiedenen Komponenten von Amazon EKS funktionieren, erfahren [Sie unter Netzwerk für Amazon EKS-Cluster konfigurieren](#).
- Informationen zu verbundenen Clustern finden Sie unter [Amazon-EKS-Anschluss](#).

Themen

- [Erstellen Sie einen Amazon EKS Auto Mode-Cluster](#)
- [Erstellen Sie einen Amazon EKS-Cluster](#)
- [Bereiten Sie sich mit Cluster-Erkenntnissen auf Kubernetes-Versionsupgrades vor und beheben Sie Fehlkonfigurationen](#)
- [Aktualisieren Sie den vorhandenen Cluster auf die neue Kubernetes-Version](#)
- [Einen Cluster löschen](#)
- [Cluster-API-Serverendpunkt](#)
- [Stellen Sie Windows-Knoten auf EKS-Clustern bereit](#)
- [Windows-Unterstützung deaktivieren](#)
- [Stellen Sie private Cluster mit eingeschränktem Internetzugang bereit](#)
- [Verstehen Sie den Lebenszyklus der Kubernetes-Version auf EKS](#)
- [Amazon EKS-Plattformversionen für jede Kubernetes-Version anzeigen](#)
- [Skalieren Sie Cluster-Computing mit Karpenter und Cluster Autoscaler](#)
- [Erfahren Sie mehr über Zonal Shift von Amazon Application Recovery Controller \(ARC\) in Amazon EKS](#)
- [Aktivieren Sie EKS Zonal Shift, um beeinträchtigte Availability Zones zu vermeiden](#)

Erstellen Sie einen Amazon EKS Auto Mode-Cluster

Dieses Thema enthält detaillierte Anweisungen zum Erstellen eines Amazon EKS Auto Mode-Clusters mithilfe erweiterter Konfigurationsoptionen. Es behandelt Voraussetzungen, Netzwerkoptionen und Zusatzkonfigurationen. Der Prozess umfasst die Einrichtung von IAM-Rollen, die Konfiguration der Clustereinstellungen, die Angabe von Netzwerkparametern und die Auswahl von Add-Ons. Benutzer können Cluster entweder mit der AWS Management Console oder der AWS CLI erstellen, wobei step-by-step Anleitungen für beide Methoden bereitgestellt werden.

Für Benutzer, die einen weniger komplexen Einrichtungsprozess suchen, finden Sie im Folgenden vereinfachte Schritte zur Clustererstellung:

- [the section called “eksctl CLI”](#)
- [the section called “ AWS CLI”](#)
- [the section called “Verwaltungskonsole”](#)

Dieser Leitfaden zur erweiterten Konfiguration richtet sich an Benutzer, die eine genauere Kontrolle über die Einrichtung ihres EKS-Auto-Mode-Clusters benötigen und mit den Konzepten und Anforderungen von Amazon EKS vertraut sind. Bevor Sie mit der erweiterten Konfiguration fortfahren, stellen Sie sicher, dass Sie alle Voraussetzungen erfüllt haben und über umfassende Kenntnisse der Netzwerk- und IAM-Anforderungen für EKS-Auto-Mode-Cluster verfügen.

Für den EKS-Automatikmodus sind zusätzliche IAM-Berechtigungen erforderlich. Weitere Informationen finden Sie unter:

- [the section called “IAM-Rollen für EKS-Cluster im automatischen Modus”](#)
- [the section called “Identität und Zugriff”](#)

Note

Wenn Sie einen Cluster ohne den automatischen EKS-Modus erstellen möchten, finden Sie weitere Informationen unter [the section called “Erstellen eines -Clusters”](#). Dieses Thema behandelt die erweiterte Konfiguration. Informationen zu den ersten Schritten mit dem automatischen Modus von EKS finden Sie unter [the section called “Cluster erstellen”](#).

Voraussetzungen

- Eine vorhandene VPC und Subnetze, die die [Amazon-EKS-Anforderungen](#) erfüllen. Bevor Sie einen Cluster für den Produktionseinsatz bereitstellen, empfehlen wir, dass Sie sich ein umfassendes Verständnis der VPC- und Subnetzanforderungen aneignen. Wenn Sie keine VPC und keine Subnetze haben, können Sie diese mithilfe einer von [Amazon EKS bereitgestellten AWS CloudFormation](#) Vorlage erstellen.
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann dieselbe sein oder bis zu einer Nebenversion vor oder nach der Kubernetes-Version

Ihres Clusters. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie kubectl-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von kubectl finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).

- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version`. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- Ein [IAM-Prinzipal](#) mit Berechtigungen zum Erstellen und Ändern von EKS- und IAM-Ressourcen.

Cluster erstellen — Konsole AWS

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie Cluster hinzufügen und dann Erstellen aus.
3. Wählen Sie unter Konfigurationsoptionen die Option Benutzerdefinierte Konfiguration aus.
 - Dieses Thema behandelt die benutzerdefinierte Konfiguration. Informationen zur Schnellkonfiguration finden Sie unter [the section called “Verwaltungskonsole”](#).
4. Vergewissern Sie sich, dass „EKS-Automatikmodus verwenden“ aktiviert ist.
 - In diesem Thema wird das Erstellen von Clustern mit dem EKS-Automatikmodus behandelt. Weitere Informationen zum Erstellen von Clustern ohne den automatischen EKS-Modus finden Sie unter [the section called “Erstellen eines -Clusters”](#).
5. Füllen Sie auf der Seite Configure cluster (Cluster konfigurieren) die folgenden Felder aus:
 - Name – Ein Name für Ihren Cluster. Der Name darf nur alphanumerische Zeichen (Groß- und Kleinschreibung beachten), Bindestriche und Unterstriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
 - Cluster-IAM-Rolle — Wählen Sie die Amazon EKS-Cluster-IAM-Rolle aus, die Sie erstellt haben, damit die Kubernetes-Steuerebene AWS Ressourcen in Ihrem Namen verwalten kann. Wenn Sie noch keine Cluster-IAM-Rolle für den automatischen EKS-Modus erstellt haben, klicken Sie auf die Schaltfläche Empfohlene Rolle erstellen, um die Rolle mit den erforderlichen Berechtigungen in der IAM-Konsole zu erstellen.
 - Kubernetes-Version – Die Kubernetes-Version, die für den Cluster verwendet wird. Wir empfehlen, die frühere Version auszuwählen, es sei denn, Sie benötigen eine ältere Version.

- Upgrade-Richtlinie — Die Kubernetes-Versionsrichtlinie, die Sie für Ihren Cluster festlegen möchten. Wenn Sie möchten, dass Ihr Cluster nur auf einer Standard-Supportversion ausgeführt wird, können Sie Standard wählen. Wenn Sie möchten, dass Ihr Cluster am Ende der Standardunterstützung für eine Version in den erweiterten Support aufgenommen wird, können Sie Extended wählen. Wenn Sie eine Kubernetes-Version auswählen, für die derzeit der erweiterte Support gilt, können Sie den Standardsupport nicht als Option auswählen.
6. Geben Sie im Abschnitt Auto Mode Compute auf der Seite „Cluster konfigurieren“ die folgenden Felder ein:
- Knotenpools — Legen Sie fest, ob Sie die integrierten Knotenpools verwenden möchten. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die integrierten Knotenpools”](#).
 - Node-IAM-Rolle — Wenn Sie einen der integrierten Knotenpools aktivieren, müssen Sie eine Node-IAM-Rolle auswählen. Der automatische Modus von EKS weist diese Rolle neuen Knoten zu. Sie können diesen Wert nicht ändern, nachdem der Cluster erstellt wurde. Wenn Sie noch keine Node-IAM-Rolle für den automatischen EKS-Modus erstellt haben, klicken Sie auf die Schaltfläche Empfohlene Rolle erstellen, um die Rolle mit den erforderlichen Berechtigungen zu erstellen. Weitere Informationen über diese Rolle finden Sie unter [the section called “Identität und Zugriff”](#).
7. Geben Sie auf der Seite „Cluster konfigurieren“ im Abschnitt Clusterzugriff die folgenden Felder ein:
- Bootstrap-Cluster-Administratorzugriff — Der Cluster-Ersteller ist automatisch ein Kubernetes-Administrator. Wenn Sie dies deaktivieren möchten, wählen Sie Clusteradministratorzugriff verbieten aus.
 - Cluster-Authentifizierungsmodus — Der automatische EKS-Modus erfordert EKS-Zugriffseinträge, den EKS-API-Authentifizierungsmodus. Sie können den ConfigMap Authentifizierungsmodus optional aktivieren, indem Sie EKS API und auswählen ConfigMap.
8. Geben Sie die verbleibenden Felder auf der Seite „Cluster konfigurieren“ ein:
- Secrets-Verschlüsselung – (Optional) Aktivieren Sie die Secrets-Verschlüsselung von Kubernetes-Secrets mithilfe eines KMS-Schlüssels. Sie können diese auch aktivieren, nachdem Sie Ihren Cluster erstellt haben. Bevor Sie diese Funktion aktivieren, stellen Sie sicher, dass Sie mit den Informationen in vertraut sind [the section called “Aktivieren Sie die geheime Verschlüsselung”](#).
 - ARC Zonal Shift — Der EKS-Automatikmodus unterstützt Arc Zonal Shift nicht.

- Tags – (Optional) Fügen Sie Ihrem Cluster beliebige Tags hinzu. Weitere Informationen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#).

Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

9. Wählen Sie auf der Seite Specify networking (Netzwerk angeben) die Werte für die folgenden Felder aus:

- VPC – Wählen Sie eine vorhandene VPC aus, die die [Anforderungen für Amazon EKS VPC](#) erfüllt, um Ihren Cluster zu erstellen. Bevor Sie sich für eine VPC entscheiden, empfehlen wir Ihnen, sich mit allen Anforderungen und Überlegungen in [the section called “VPC- und Subnetz-Anforderungen”](#) vertraut zu machen. Sie können nach der Clustererstellung nicht ändern, welche VPC Sie verwenden möchten. Wenn keine aufgeführten VPCs sind, müssen Sie zuerst eine erstellen. Weitere Informationen finden Sie unter [the section called “Erstellen einer VPC”](#).
- Subnetze – Standardmäßig sind alle im vorherigen Feld angegebenen Subnetze in der VPC vorausgewählt. Sie müssen mindestens zwei auswählen.

Die von Ihnen gewählten Subnetze müssen die [Anforderungen für Amazon-EKS-Subnetze](#) erfüllen. Bevor Sie Subnetze auswählen, empfehlen wir, dass Sie mit allen [Anforderungen und Überlegungen zu Amazon EKS VPC und Subnetzen](#) vertraut sind.

Security groups (Sicherheitsgruppen) – (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die Amazon EKS den erstellten Netzwerkschnittstellen zuordnen soll.

Unabhängig davon, ob Sie Sicherheitsgruppen wählen oder nicht, erstellt Amazon EKS eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der Cluster-Sicherheitsgruppe, die Amazon EKS erstellt, finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Sie können die Regeln in der von Amazon EKS erstellten Cluster-Sicherheitsgruppe ändern.

- Cluster-IP-Adressfamilie wählen — Sie können entweder IPv4 oder IPv6 wählen.

Kubernetes weist Pods und Diensten standardmäßig IPv4 Adressen zu. Bevor Sie sich für die Verwendung der IPv6 Produktfamilie entscheiden, sollten Sie sicherstellen, dass Sie mit allen Überlegungen und Anforderungen in den [VPC-Anforderungen und Überlegungen](#), [the section called “Subnetz-Anforderungen und -Überlegungen”](#), [the section called “Anforderungen an Sicherheitsgruppen”](#), und [the section called “IPv6”](#) Themen vertraut sind. Wenn Sie sich für die IPv6 Familie entscheiden, können Sie keinen Adressbereich angeben, aus dem Kubernetes

IPv6 Dienstadressen zuweisen soll, wie Sie es für die Familie tun können. IPv4 Kubernetes weist Dienstadressen aus dem eindeutigen lokalen Adressbereich zu (). fc00::/7

- (Optional) Wählen Sie Configure Kubernetes Service IP address range (IP-Adressbereich des Kubernetes-Diensts konfigurieren) und geben Sie einen **IPv4**-Bereich für den Service an.

Wenn Sie Ihren eigenen Bereich angeben, können Sie Konflikte zwischen Kubernetes-Diensten und anderen Netzwerken vermeiden, die über Peering oder Verbindungen mit Ihrer VPC verbunden sind. Geben Sie einen Bereich in CIDR-Notation ein. Beispiel: 10.2.0.0/16.

Der CIDR-Block muss die folgenden Anforderungen erfüllen:

- Verwendet einen der folgenden Bereiche: 10.0.0.0/8, 172.16.0.0/12, oder 192.168.0.0/16.
- Hat eine Mindestgröße von /24 und eine maximale Größe von /12.
- Überschneidet sich nicht mit dem Bereich der VPC für Ihre Amazon-EKS-Ressourcen.

Sie können diese Option nur angeben, wenn Sie die IPv4-Adressfamilie verwenden, und nur bei Erstellen des Clusters. Wenn Sie dies nicht angeben, weist Kubernetes Dienst-IP-Adressen entweder aus den oder den CIDR-Blöcken zu. 10.100.0.0/16 172.20.0.0/16

- Wählen Sie eine Option für den Cluster-Endpunktzugriff aus. Nachdem Ihr Cluster erstellt wurde, können Sie diese Option ändern. Bevor Sie eine nicht standardmäßige Option auswählen, sollten Sie sich mit den Optionen und deren Auswirkungen vertraut machen. Weitere Informationen finden Sie unter [the section called “Cluster-Endpunktzugriff”](#).

Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

10.(Optional) Auf der Seite Beobachtbarkeit konfigurieren können Sie Metriken und Optionen zur Steuerebenen-Protokollierung aktivieren. Standardmäßig sind alle Protokollierungstypen deaktiviert.

- Weitere Informationen zur Option Prometheus-Metriken finden Sie unter. [the section called “Schritt 1: Prometheus-Metriken aktivieren”](#)
- Weitere Informationen zu den Optionen für die Steuerebenen-Protokollierung finden Sie unter [the section called “Protokolle der Kontrollebene”](#).
- Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

11.Wählen Sie auf der Seite Select add-ons (Add-Ons auswählen) die Add-Ons aus, die Sie Ihrem Cluster hinzufügen möchten. Sie können so viele Amazon EKS-Add-Ons und AWS Marketplace-Add-Ons auswählen, wie Sie benötigen. Wenn die AWS Marketplace-Add-Ons, die Sie installieren möchten, nicht aufgeführt sind, können Sie auf die Seitennummerierung klicken, um zusätzliche

Seitenergebnisse anzuzeigen, oder nach verfügbaren AWS Marketplace-Add-Ons suchen, indem Sie Text in das Suchfeld eingeben. Sie können auch nach Kategorie, Anbieter oder Preismodell filtern und dann die Add-Ons aus den Suchergebnissen auswählen. Beim Erstellen eines Clusters können Sie jedes Add-on, das EKS Pod Identities unterstützt, anzeigen, auswählen und installieren, wie unter beschrieben [the section called “Pod-Identität”](#).

- Der EKS-Automatikmodus automatisiert die Funktionalität bestimmter Add-Ons. Wenn Sie planen, EKS Managed Node Groups in Ihrem EKS Auto Mode Cluster bereitzustellen, wählen Sie Zusätzliche Amazon EKS Add-ons und überprüfen Sie die Optionen. Möglicherweise müssen Sie Add-Ons wie CoreDNS und Kube-Proxy installieren. EKS installiert die Add-Ons in diesem Abschnitt nur auf selbstverwalteten Knoten und Knotengruppen.
- Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

12. Wählen Sie auf der Seite Einstellungen für ausgewählte Add-ons konfigurieren die Version aus, die Sie installieren möchten. Sie können nach der Clustererstellung jederzeit auf eine neuere Version aktualisieren.

Bei Add-Ons, die EKS Pod Identities unterstützen, können Sie die Konsole verwenden, um die Rolle automatisch zu generieren, wobei der Name, die AWS verwaltete Richtlinie und die Vertrauensrichtlinie speziell für das Add-on vorab ausgefüllt sind. Sie können vorhandene Rollen wiederverwenden oder neue Rollen für unterstützte Add-Ons erstellen. Die Schritte zur Verwendung der Konsole zum Erstellen von Rollen für Add-Ons, die EKS Pod Identities unterstützen, finden Sie unter [the section called “Add-on erstellen \(AWS Konsole\)”](#). Wenn ein Add-On EKS Pod Identity nicht unterstützt, wird eine Meldung mit Anweisungen zur Verwendung des Assistenten zum Erstellen der IAM-Rollen für Dienstkonten (IRSA) angezeigt, nachdem der Cluster erstellt wurde.

Sie können die Konfiguration jedes Add-Ons nach der Cluster-Erstellung aktualisieren. Weitere Informationen zum Konfigurieren eines Add-Ons finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#). Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

13. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die Informationen, die Sie auf den vorherigen Seiten eingegeben oder ausgewählt haben. Wenn Sie Änderungen vornehmen müssen, wählen Sie Edit (Bearbeiten). Wenn Sie zufrieden sind, wählen Sie Create. Das Feld Status zeigt CREATING (WIRD ERSTELLT) an, während der Cluster bereitgestellt wird.

Note

Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu

erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called “Unzureichende Kapazität”](#).

Die Clusterbereitstellung dauert mehrere Minuten.

Cluster erstellen — AWS CLI

Die folgenden CLI-Anweisungen behandeln das Erstellen von IAM-Ressourcen und das Erstellen des Clusters.

Erstellen Sie eine EKS-Cluster-IAM-Rolle im automatischen Modus

Schritt 1: Erstellen Sie die Vertrauensrichtlinie

Erstellen Sie eine Vertrauensrichtlinie, die es dem Amazon EKS-Service ermöglicht, die Rolle zu übernehmen. Speichern Sie die Richtlinie als `trust-policy.json`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

Schritt 2: Erstellen Sie die IAM-Rolle

Verwenden Sie die Vertrauensrichtlinie, um die Cluster-IAM-Rolle zu erstellen:

```
aws iam create-role \  
  --role-name AmazonEKSAutoClusterRole \  
  --assume-role-policy-document file://trust-policy.json
```

Schritt 3: Notieren Sie sich den Rollen-ARN

Rufen Sie den ARN der neuen Rolle ab und speichern Sie ihn zur Verwendung in nachfolgenden Schritten:

```
aws iam get-role --role-name AmazonEKSAutoClusterRole --query "Role.Arn" --output text
```

Schritt 4: Erforderliche Richtlinien anhängen

Fügen Sie der Cluster-IAM-Rolle die folgenden AWS verwalteten Richtlinien hinzu, um die erforderlichen Berechtigungen zu gewähren:

EKSClusterAmazon-Richtlinie:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSClusterPolicy
```

EKSComputeAmazon-Richtlinie:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSClusterPolicy
```

Amazon EKSBLOCK StoragePolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSBLOCKStoragePolicy
```

Amazon EKSLoad BalancingPolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSLoadBalancingPolicy
```

EKSNetworkingAmazon-Richtlinie:


```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy
```

Erstellen Sie eine IAM-Rolle für einen EKS-Knoten im automatischen Modus

Schritt 1: Erstellen Sie die Vertrauensrichtlinie

Erstellen Sie eine Vertrauensrichtlinie, die es dem Amazon EKS-Service ermöglicht, die Rolle zu übernehmen. Speichern Sie die Richtlinie als `node-trust-policy.json`:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "ec2.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

Schritt 2: Erstellen Sie die Node-IAM-Rolle

Verwenden Sie die `node-trust-policyJSON`-Datei aus dem vorherigen Schritt, um zu definieren, welche Entitäten die Rolle übernehmen können. Führen Sie den folgenden Befehl aus, um die Node-IAM-Rolle zu erstellen:

```
aws iam create-role \  
  --role-name AmazonEKSAutoNodeRole \  
  --assume-role-policy-document file://node-trust-policy.json
```

Schritt 3: Notieren Sie sich den Rollen-ARN

Rufen Sie nach dem Erstellen der Rolle den ARN der Node-IAM-Rolle ab und speichern Sie ihn. Sie benötigen diesen ARN in den nachfolgenden Schritten. Verwenden Sie den folgenden Befehl, um den ARN abzurufen:

```
aws iam get-role --role-name AmazonEKSAutoNodeRole --query "Role.Arn" --output text
```

Schritt 4: Erforderliche Richtlinien anhängen

Fügen Sie der Node-IAM-Rolle die folgenden AWS verwalteten Richtlinien hinzu, um die erforderlichen Berechtigungen bereitzustellen:

Amazon EKSWorker NodeMinimalPolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoNodeRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy
```

Amazon EC2 ContainerRegistryPullOnly:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoNodeRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEC2ContainerRegistryPullOnly
```

Cluster erstellen

1. Erstellen Sie den Cluster mit dem folgenden Befehl. Nehmen Sie vor der Ausführung des Befehls die folgenden Ersetzungen vor:

- *region-code* Ersetzen Sie es durch die AWS Region, in der Sie Ihren Cluster erstellen möchten.
- Ersetzen Sie *my-cluster* durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (Groß- und Kleinschreibung beachten), Bindestriche und Unterstriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
- Ersetzen Sie *1.30* durch eine von [Amazon EKS unterstützte Version](#).
- Ersetzen Sie ihn *111122223333* durch Ihre Konto-ID
- Wenn Sie unterschiedlich benannte IAM-Rollen für die Cluster- und Node-Rollen erstellt haben, ersetzen Sie die ARNs.
- Ersetzen Sie *subnetIds* durch Ihre eigenen Werte. Sie können auch weitere IDs hinzufügen. Sie müssen mindestens zwei Subnetze IDs angeben.

Die von Ihnen gewählten Subnetze müssen die [Anforderungen für Amazon-EKS-Subnetze](#) erfüllen. Bevor Sie Subnetze auswählen, empfehlen wir, dass Sie mit allen [Anforderungen und Überlegungen zu Amazon EKS VPC und Subnetzen](#) vertraut sind.

- Wenn Sie keine Sicherheitsgruppen-ID angeben möchten, entfernen Sie sie ,securityGroupIds=sg-<ExampleID1> aus dem Befehl. Wenn Sie eine oder mehrere Sicherheitsgruppen angeben möchten IDs, ersetzen Sie die Werte für securityGroupIds durch Ihre eigenen. Sie können auch weitere hinzufügen IDs.

Unabhängig davon, ob Sie Sicherheitsgruppen wählen oder nicht, erstellt Amazon EKS eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der Cluster-Sicherheitsgruppe, die Amazon EKS erstellt, finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Sie können die Regeln in der von Amazon EKS erstellten Cluster-Sicherheitsgruppe ändern.

```
aws eks create-cluster \
  --region region-code \
  --name my-cluster \
  --kubernetes-version 1.30 \
  --role-arn arn:aws:iam::11112223333:role/AmazonEKSAutoClusterRole \
  --resources-vpc-config '{"subnetIds": ["subnet-ExampleID1", "subnet-ExampleID2"],
"securityGroupIds": ["sg-ExampleID1"], "endpointPublicAccess": true,
"endpointPrivateAccess": true}' \
  --compute-config '{"enabled": true, "nodeRoleArn": "arn:aws:
iam::11112223333:role/AmazonEKSAutoNodeRole", "nodePools": ["general-purpose",
"system"]}' \
  --kubernetes-network-config '{"elasticLoadBalancing": {"enabled": true}}' \
  --storage-config '{"blockStorage": {"enabled": true}}' \
  --access-config '{"authenticationMode": "API"}'
```

Note

Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called “Unzureichende Kapazität”](#).

Im Folgenden finden Sie optionale Einstellungen, die bei Bedarf dem vorherigen Befehl hinzugefügt werden müssen. Sie können diese Optionen nur aktivieren, wenn Sie den Cluster erstellen, nicht danach.

- Wenn Sie angeben möchten welchem IPv4 CIDR-Block (Classless Inter-Domain Routing) Kubernetes Service-IP-Adressen zuweist, geben Sie die Option `--kubernetes-network-config serviceIpv4Cidr=<cidr-block>` für den folgenden Befehl an.

Wenn Sie Ihren eigenen Bereich angeben, können Sie Konflikte zwischen Kubernetes-Diensten und anderen Netzwerken vermeiden, die über Peering oder Verbindungen mit Ihrer VPC verbunden sind. Geben Sie einen Bereich in CIDR-Notation ein. Beispiel: `10.2.0.0/16`.

Der CIDR-Block muss die folgenden Anforderungen erfüllen:

- Verwendet einen der folgenden Bereiche: `10.0.0.0/8`, `172.16.0.0/12`, oder `192.168.0.0/16`.
- Hat eine Mindestgröße von `/24` und eine maximale Größe von `/12`.
- Überschneidet sich nicht mit dem Bereich der VPC für Ihre Amazon-EKS-Ressourcen.

Sie können diese Option nur angeben, wenn Sie die IPv4-Adressfamilie verwenden, und nur bei Erstellen des Clusters. Wenn Sie dies nicht angeben, weist Kubernetes Dienst-IP-Adressen entweder aus den oder den CIDR-Blöcken zu. `10.100.0.0/16` `172.20.0.0/16`

- Wenn Sie einen Cluster erstellen und möchten, dass der Cluster Pods und Diensten IPv6 Adressen anstelle von IPv4 Adressen zuweist, fügen Sie den folgenden Befehl `--kubernetes-network-config ipFamily=ipv6` hinzu.

Kubernetes weist Pods und Diensten standardmäßig IPv4 Adressen zu. Bevor Sie sich für die Verwendung der IPv6 Produktfamilie entscheiden, sollten Sie sicherstellen, dass Sie mit allen Überlegungen und Anforderungen in den [VPC-Anforderungen und Überlegungen](#), [the section called “Subnetz-Anforderungen und -Überlegungen”](#), [the section called “Anforderungen an Sicherheitsgruppen”](#), und [the section called “IPv6”](#) Themen vertraut sind. Wenn Sie sich für die IPv6 Familie entscheiden, können Sie keinen Adressbereich angeben, aus dem Kubernetes IPv6 Dienstadressen zuweisen soll, wie Sie es für die Familie tun können. IPv4 Kubernetes weist Dienstadressen aus dem eindeutigen lokalen Adressbereich zu (`fc00::/7`).

2. Die Bereitstellung des Clusters dauert mehrere Minuten. Sie können den Status Ihres Clusters mit dem folgenden Befehl überprüfen.

```
aws eks describe-cluster --region region-code --name my-cluster --query  
"cluster.status"
```

Nächste Schritte

- [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#)
- [the section called “Erteilen Sie Berechtigungen”](#)
- [Aktivieren Sie die Secrets-Verschlüsselung für Ihren Cluster.](#)
- [Konfigurieren Sie die Protokollierung für Ihren Cluster.](#)
- [Fügen Sie Ihrem Cluster Knoten hinzu.](#)

Erstellen Sie einen Amazon EKS-Cluster

Note

Dieses Thema behandelt die Erstellung von EKS-Clustern ohne EKS Auto Mode.

Ausführliche Anweisungen zum Erstellen eines EKS-Auto-Mode-Clusters finden Sie unter [the section called “Autocluster erstellen”](#).

Informationen zu den ersten Schritten mit dem EKS-Automatikmodus finden Sie unter [the section called “Cluster erstellen \(EKS-Automatikmodus\)”](#).

Dieses Thema bietet einen Überblick über die verfügbaren Optionen und beschreibt, was zu beachten ist, wenn Sie einen Amazon-EKS-Cluster erstellen. Wenn Sie einen Cluster mit Ihrer lokalen Infrastruktur als Rechenleistung für Knoten erstellen müssen, finden Sie weitere Informationen unter [the section called “Cluster erstellen”](#). Wenn Sie zum ersten Mal einen Amazon EKS-Cluster erstellen, empfehlen wir Ihnen, einer unserer Anleitungen unter zu folgen [Erste Schritte](#). Diese Leitfäden helfen, einen einfachen Standard-Cluster zu erstellen, ohne auf alle verfügbaren Optionen einzugehen.

Voraussetzungen

- Eine vorhandene VPC und Subnetze, die die [Amazon-EKS-Anforderungen](#) erfüllen. Bevor Sie einen Cluster für den Produktionseinsatz bereitstellen, empfehlen wir, dass Sie sich ein

umfassendes Verständnis der VPC- und Subnetzanforderungen aneignen. Wenn Sie keine VPC und keine Subnetze haben, können Sie diese mithilfe einer von [Amazon EKS bereitgestellten AWS CloudFormation](#) Vorlage erstellen.

- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Ein [IAM-Prinzipal](#) mit Berechtigungen für das `create` und `describe` eines Amazon-EKS-Clusters. Weitere Informationen erhalten Sie unter [the section called “Erstellen Sie einen lokalen Kubernetes-Cluster auf einem Outpost”](#) und [the section called “Auflisten oder Beschreiben aller Cluster”](#).

Schritt 1: Cluster-IAM-Rolle erstellen

1. Wenn Sie bereits über eine Cluster-IAM-Rolle verfügen oder mit der Sie Ihren Cluster erstellen möchten `eksctl`, können Sie diesen Schritt überspringen. Standardmäßig erstellt `eksctl` eine Rolle für Sie.
2. Führen Sie den folgenden Befehl aus, um eine JSON-Datei für eine IAM-Vertrauensrichtlinie zu erstellen.

```
cat >eks-cluster-role-trust-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
"Principal": {
  "Service": "eks.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
}
EOF
```

3. Erstellen Sie die Amazon-EKS-Cluster-IAM-Rolle. Falls erforderlich, stellen Sie *eks-cluster-role-trust-policy.json* den Pfad auf Ihrem Computer voran, in den Sie im vorherigen Schritt die Datei geschrieben haben. Der Befehl verknüpft die im vorherigen Schritt erstellte Vertrauensrichtlinie mit der Rolle. Um eine IAM-Rolle zu erstellen, muss dem [IAM-Prinzipal](#), der die Rolle erstellt, die iam:CreateRole-Aktion (Berechtigung) zugewiesen werden.

```
aws iam create-role --role-name myAmazonEKSClusterRole --assume-role-policy-document
file://"eks-cluster-role-trust-policy.json"
```

4. Sie können entweder die von Amazon EKS verwaltete Richtlinie zuweisen oder Ihre eigene benutzerdefinierte Richtlinie erstellen. Informationen zu den Mindestberechtigungen, die Sie in Ihrer benutzerdefinierten Richtlinie verwenden müssen, finden Sie unter [the section called "Cluster-IAM-Rolle"](#).

Fügen Sie der Rolle die von Amazon EKS verwaltete Richtlinie mit dem Namen [Amazon EKSCluster Policy](#) hinzu. Um eine IAM-Richtlinie an einen [IAM-Prinzipal](#) anzuhängen, muss der Prinzipal, der die Richtlinie anhängt, eine der folgenden IAM-Aktionen (Berechtigungen) zugewiesen werden: iam:AttachUserPolicy oder iam:AttachRolePolicy.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/
AmazonEKSClusterPolicy --role-name myAmazonEKSClusterRole
```

Serviceverknüpfte Rolle

Amazon EKS erstellt automatisch eine serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonEKS`.

Dies ist eine Ergänzung zur Cluster-IAM-Rolle. Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Die Rolle ermöglicht Amazon EKS, Cluster in Ihrem Konto zu verwalten. Weitere Informationen finden Sie unter [the section called "Cluster--Rolle"](#).

Die IAM-Identität, die Sie zum Erstellen des EKS-Clusters verwenden, muss über die Berechtigung zum Erstellen der serviceverknüpften Rolle verfügen. Dies beinhaltet die `iam:CreateServiceLinkedRole` Erlaubnis.

Wenn die dienstverknüpfte Rolle noch nicht existiert und Ihre aktuelle IAM-Rolle nicht über ausreichende Berechtigungen verfügt, um sie zu erstellen, schlägt der Vorgang zur Clustererstellung fehl.

Schritt 2: Cluster erstellen

Sie können einen Cluster erstellen, indem Sie Folgendes verwenden:

- [eksctl](#)
- [der AWS Management Console](#)
- [die AWS CLI](#)

Cluster erstellen - eksctl

1. Sie benötigen eine Version `0.210.0` oder eine neuere Version des `eksctl` Befehlszeilentools, das auf Ihrem Gerät installiert ist oder. AWS CloudShell Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).
2. Erstellen Sie einen Amazon IPv4 EKS-Cluster mit der Amazon EKS-Standardversion von Kubernetes in Ihrer AWS Standardregion. Nehmen Sie vor der Ausführung des Befehls die folgenden Ersetzungen vor:
3. `region-code` Ersetzen Sie es durch die AWS Region, in der Sie Ihren Cluster erstellen möchten.
4. Ersetzen Sie `my-cluster` durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
5. Ersetzen Sie `1.33` durch eine von [Amazon EKS unterstützte Version](#).
6. Ändern Sie die Werte für `vpc-private-subnets`, um Ihre Anforderungen zu erfüllen. Sie können auch weitere hinzufügen IDs. Sie müssen mindestens zwei Subnetze IDs angeben. Wenn Sie lieber öffentliche Subnetze angeben möchten, können Sie zu wechseln `--vpc-private-subnets`. `--vpc-public-subnets` Öffentlichen Subnetzen ist eine Routing-Tabelle mit einer

Route zu einem Internet-Gateway zugeordnet, privaten Subnetzen ist jedoch keine Routing-Tabelle zugeordnet. Wir empfehlen, nach Möglichkeit private Subnetze zu verwenden.

Die von Ihnen gewählten Subnetze müssen die [Anforderungen für Amazon-EKS-Subnetze](#) erfüllen. Bevor Sie Subnetze auswählen, empfehlen wir, dass Sie mit allen [Anforderungen und Überlegungen zu Amazon EKS VPC und Subnetzen](#) vertraut sind.

7. Führen Sie den folgenden Befehl aus:

```
eksctl create cluster --name my-cluster --region region-code --version 1.33 --vpc-private-subnets subnet-ExampleID1,subnet-ExampleID2 --without-nodesgroup
```

Die Clusterbereitstellung dauert mehrere Minuten. Während der Cluster erstellt wird, werden mehrere Ausgabezeilen angezeigt. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

8. Fahren Sie fort mit [the section called "Schritt 3: Kubeconfig aktualisieren"](#)

Optionale Einstellungen

Sie können die meisten Optionen, die beim Erstellen eines Clusters mit `eksctl` angegeben werden können, über den Befehl `eksctl create cluster --help` anzeigen. Verwenden Sie eine config-Datei, um alle verfügbaren Optionen anzuzeigen. Weitere Informationen finden Sie unter [Verwenden von Config-Dateien](#) und im [Config-Datei-Schema](#) in der `eksctl`-Dokumentation. Auf GitHub finden Sie [Beispiele für Config-Dateien](#).

Im Folgenden finden Sie optionale Einstellungen, die bei Bedarf dem vorherigen Befehl hinzugefügt werden müssen. Sie können diese Optionen nur aktivieren, wenn Sie den Cluster erstellen, nicht danach. Wenn Sie diese Optionen angeben müssen, müssen Sie den Cluster mit einer [eksctl-Konfigurationsdatei](#) erstellen und die Einstellungen angeben, anstatt den vorherigen Befehl zu verwenden.

- Wenn Sie eine oder mehrere Sicherheitsgruppen angeben möchten, die Amazon EKS den von Amazon EKS erstellten Netzwerkschnittstellen zuweist, geben Sie die Option [SecurityGroup](#) an.

Unabhängig davon, ob Sie Sicherheitsgruppen wählen oder nicht, erstellt Amazon EKS eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der Cluster-Sicherheitsgruppe, die Amazon EKS

erstellt, finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Sie können die Regeln in der von Amazon EKS erstellten Cluster-Sicherheitsgruppe ändern.

- [Wenn Sie angeben möchten, welchem CIDR-Block \(IPv4Classless Inter-Domain Routing\) Kubernetes Service-IP-Adressen zuweist, geben Sie die Service-CIDR-Option an. IPv4](#)

Wenn Sie Ihren eigenen Bereich angeben, können Sie Konflikte zwischen Kubernetes-Diensten und anderen Netzwerken vermeiden, die über Peering oder Verbindungen mit Ihrer VPC verbunden sind. Geben Sie einen Bereich in CIDR-Notation ein. Beispiel: 10.2.0.0/16.

Der CIDR-Block muss die folgenden Anforderungen erfüllen:

- Verwendet einen der folgenden Bereiche: 10.0.0.0/8, 172.16.0.0/12, oder 192.168.0.0/16.
- Hat eine Mindestgröße von /24 und eine maximale Größe von /12.
- Überschneidet sich nicht mit dem Bereich der VPC für Ihre Amazon-EKS-Ressourcen.

Sie können diese Option nur angeben, wenn Sie die IPv4-Adressfamilie verwenden, und nur bei Erstellen des Clusters. Wenn Sie dies nicht angeben, weist Kubernetes Dienst-IP-Adressen entweder aus den oder den CIDR-Blöcken zu. 10.100.0.0/16 172.20.0.0/16

- [Wenn Sie einen Cluster erstellen und möchten, dass der Cluster Pods und Diensten IPv6 Adressen anstelle von IPv4 Adressen zuweist, geben Sie die Option IPFamily an.](#)

Kubernetes weist Pods und Diensten standardmäßig IPv4 Adressen zu. Bevor Sie sich für die Verwendung der IPv6 Produktreihe entscheiden, sollten Sie sicherstellen, dass Sie mit allen Überlegungen und Anforderungen in den Themen [the section called “VPC-Anforderungen und -Überlegungen”](#), [the section called “Subnetz-Anforderungen und -Überlegungen”](#) [the section called “Anforderungen an Sicherheitsgruppen”](#), und vertraut sind. [the section called “IPv6”](#) Wenn Sie sich für die IPv6 Familie entscheiden, können Sie keinen Adressbereich angeben, aus dem Kubernetes IPv6 Dienstadressen zuweisen soll, wie Sie es für die IPv4 Familie tun können. Kubernetes weist Dienstadressen aus dem eindeutigen lokalen Adressbereich zu (). fc00::/7

Cluster erstellen — Konsole AWS

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie Cluster hinzufügen und dann Erstellen aus.
3. Wählen Sie unter Konfigurationsoptionen die Option Benutzerdefinierte Konfiguration

- Informationen zum schnellen Erstellen eines Clusters mit dem automatischen EKS-Modus finden Sie unter [the section called “Verwaltungskonsole”](#).
4. Schalten Sie unter EKS-Automatikmodus die Option EKS-Automatikmodus verwenden aus.
- Informationen zum Erstellen eines EKS-Auto-Modus-Clusters mit benutzerdefinierter Konfiguration finden Sie unter [the section called “Autocluster erstellen”](#).
5. Füllen Sie auf der Seite Configure cluster (Cluster konfigurieren) die folgenden Felder aus:
- Name – Ein Name für Ihren Cluster. Der Name darf nur alphanumerische Zeichen (Groß- und Kleinschreibung beachten), Bindestriche und Unterstriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
 - Cluster-IAM-Rolle — Wählen Sie die Amazon EKS-Cluster-IAM-Rolle aus, die Sie erstellt haben, damit die Kubernetes-Steuerebene AWS Ressourcen in Ihrem Namen verwalten kann.
 - Kubernetes-Version – Die Kubernetes-Version, die für den Cluster verwendet wird. Wir empfehlen, die frühere Version auszuwählen, es sei denn, Sie benötigen eine ältere Version.
 - Unterstützungstyp — Die Kubernetes-Versionsrichtlinie, die Sie für Ihren Cluster festlegen möchten. Wenn Sie möchten, dass Ihr Cluster nur auf einer Standard-Supportversion ausgeführt wird, können Sie Standard-Support wählen. Wenn Sie möchten, dass Ihr Cluster am Ende des Standardsupports für eine Version in den erweiterten Support aufgenommen wird, können Sie den erweiterten Support wählen. Wenn Sie eine Kubernetes-Version auswählen, für die derzeit der erweiterte Support gilt, können Sie den Standardsupport nicht als Option auswählen.
 - Secrets-Verschlüsselung – (Optional) Aktivieren Sie die Secrets-Verschlüsselung von Kubernetes-Secrets mithilfe eines KMS-Schlüssels. Sie können diese auch aktivieren, nachdem Sie Ihren Cluster erstellt haben. Bevor Sie diese Funktion aktivieren, stellen Sie sicher, dass Sie mit den Informationen vertraut sind. [the section called “Aktivieren Sie die geheime Verschlüsselung”](#)
 - Tags – (Optional) Fügen Sie Ihrem Cluster beliebige Tags hinzu. Weitere Informationen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#).
 - ARC Zonal Shift — (Optional) Sie können den Route53 Application Recovery Controller verwenden, um beeinträchtigte Verfügbarkeitszonen zu minimieren. Weitere Informationen finden Sie unter [the section called “Erfahren Sie mehr über Zonal Shift”](#).
6. Geben Sie auf der Seite „Cluster konfigurieren“ im Bereich Clusterzugriff die folgenden Felder ein:

- Bootstrap-Cluster-Administratorzugriff — Der Cluster-Ersteller ist automatisch ein Kubernetes-Administrator. Wenn Sie dies deaktivieren möchten, wählen Sie Clusteradministratorzugriff verbieten aus.
- Cluster-Authentifizierungsmodus — Legen Sie fest, wie Sie IAM-Benutzern und -Rollen Zugriff auf Kubernetes gewähren möchten. APIs Weitere Informationen finden Sie unter [the section called “Stellen Sie den Cluster-Authentifizierungsmodus ein”](#).

Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

7. Wählen Sie auf der Seite Specify networking (Netzwerk angeben) die Werte für die folgenden Felder aus:

- VPC – Wählen Sie eine vorhandene VPC aus, die die [Anforderungen für Amazon EKS VPC](#) erfüllt, um Ihren Cluster zu erstellen. Bevor Sie sich für eine VPC entscheiden, empfehlen wir Ihnen, sich mit allen Anforderungen und Überlegungen in [the section called “VPC- und Subnetz-Anforderungen”](#) vertraut zu machen. Sie können nach der Clustererstellung nicht ändern, welche VPC Sie verwenden möchten. Wenn keine aufgeführt VPCs sind, müssen Sie zuerst eine erstellen. Weitere Informationen finden Sie unter [the section called “Erstellen einer VPC”](#).
- Subnetze – Standardmäßig sind alle im vorherigen Feld angegebenen Subnetze in der VPC vorausgewählt. Sie müssen mindestens zwei auswählen.

Die von Ihnen gewählten Subnetze müssen die [Anforderungen für Amazon-EKS-Subnetze](#) erfüllen. Bevor Sie Subnetze auswählen, empfehlen wir, dass Sie mit allen [Anforderungen und Überlegungen zu Amazon EKS VPC und Subnetzen](#) vertraut sind.

Security groups (Sicherheitsgruppen) – (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die Amazon EKS den erstellten Netzwerkschnittstellen zuordnen soll.

Unabhängig davon, ob Sie Sicherheitsgruppen wählen oder nicht, erstellt Amazon EKS eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der Cluster-Sicherheitsgruppe, die Amazon EKS erstellt, finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Sie können die Regeln in der von Amazon EKS erstellten Cluster-Sicherheitsgruppe ändern.

- Cluster-IP-Adressfamilie wählen — Sie können entweder und wählen. IPv4IPv6

Kubernetes weist Pods und Diensten standardmäßig IPv4 Adressen zu. Bevor Sie sich für die Verwendung der IPv6 Produktfamilie entscheiden, sollten Sie sicherstellen, dass Sie mit allen Überlegungen und Anforderungen in den [VPC-Anforderungen und Überlegungen](#), [the](#)

[section called “Subnetz-Anforderungen und -Überlegungen”](#) [the section called “Anforderungen an Sicherheitsgruppen”](#), und [the section called “IPv6”](#) Themen vertraut sind. Wenn Sie sich für die IPv6 Familie entscheiden, können Sie keinen Adressbereich angeben, aus dem Kubernetes IPv6 Dienstadressen zuweisen soll, wie Sie es für die Familie tun können. IPv4 Kubernetes weist Dienstadressen aus dem eindeutigen lokalen Adressbereich zu (). fc00::/7

- (Optional) Wählen Sie Configure Kubernetes Service IP address range (IP-Adressbereich des Kubernetes-Diensts konfigurieren) und geben Sie einen **IPv4**-Bereich für den Service an.

Wenn Sie Ihren eigenen Bereich angeben, können Sie Konflikte zwischen Kubernetes-Diensten und anderen Netzwerken vermeiden, die über Peering oder Verbindungen mit Ihrer VPC verbunden sind. Geben Sie einen Bereich in CIDR-Notation ein. Beispiel: 10.2.0.0/16.

Der CIDR-Block muss die folgenden Anforderungen erfüllen:

- Verwendet einen der folgenden Bereiche: 10.0.0.0/8, 172.16.0.0/12, oder 192.168.0.0/16.
- Hat eine Mindestgröße von /24 und eine maximale Größe von /12.
- Überschneidet sich nicht mit dem Bereich der VPC für Ihre Amazon-EKS-Ressourcen.

Sie können diese Option nur angeben, wenn Sie die IPv4-Adressfamilie verwenden, und nur bei Erstellen des Clusters. Wenn Sie dies nicht angeben, weist Kubernetes Dienst-IP-Adressen entweder aus den oder den CIDR-Blöcken zu. 10.100.0.0/16 172.20.0.0/16

- Wählen Sie eine Option für den Cluster-Endpunktzugriff aus. Nachdem Ihr Cluster erstellt wurde, können Sie diese Option ändern. Bevor Sie eine nicht standardmäßige Option auswählen, sollten Sie sich mit den Optionen und deren Auswirkungen vertraut machen. Weitere Informationen finden Sie unter [the section called “Cluster-Endpunktzugriff”](#).

Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

8. (Optional) Auf der Seite Beobachtbarkeit konfigurieren können Sie Metriken und Optionen zur Steuerebenen-Protokollierung aktivieren. Standardmäßig sind alle Protokollierungstypen deaktiviert.

- Weitere Informationen zur Option Prometheus-Metriken finden Sie unter. [the section called “Schritt 1: Prometheus-Metriken aktivieren”](#)
- Weitere Informationen zu den Optionen für die Steuerebenen-Protokollierung finden Sie unter [the section called “Protokolle der Kontrollebene”](#).

Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

9. Wählen Sie auf der Seite **Select add-ons (Add-Ons auswählen)** die Add-Ons aus, die Sie Ihrem Cluster hinzufügen möchten. Bestimmte Add-Ons sind vorausgewählt. Sie können so viele Amazon EKS-Add-Ons und AWS Marketplace-Add-Ons auswählen, wie Sie benötigen. Wenn die AWS Marketplace-Add-Ons, die Sie installieren möchten, nicht aufgeführt sind, können Sie auf die Seitennummerierung klicken, um zusätzliche Seitenergebnisse anzuzeigen, oder nach verfügbaren AWS Marketplace-Add-Ons suchen, indem Sie Text in das Suchfeld eingeben. Sie können auch nach Kategorie, Anbieter oder Preismodell filtern und dann die Add-Ons aus den Suchergebnissen auswählen. Beim Erstellen eines Clusters können Sie jedes Add-on, das EKS Pod Identities unterstützt, anzeigen, auswählen und installieren, wie unter beschrieben [the section called “Pod-Identität”](#).

Wenn Sie mit dieser Seite fertig sind, wählen Sie **Weiter** aus.

Einige Add-Ons, wie Amazon VPC CNI, CoreDNS und kube-proxy, sind standardmäßig installiert. Wenn Sie eines der Standard-Add-Ons deaktivieren, kann dies Ihre Fähigkeit beeinträchtigen, Kubernetes-Anwendungen auszuführen.

10. Wählen Sie auf der Seite **Einstellungen für ausgewählte Add-ons konfigurieren** die Version aus, die Sie installieren möchten. Sie können nach der Clustererstellung jederzeit auf eine neuere Version aktualisieren.

Bei Add-Ons, die EKS Pod Identities unterstützen, können Sie die Konsole verwenden, um die Rolle automatisch zu generieren, wobei der Name, die AWS verwaltete Richtlinie und die Vertrauensrichtlinie speziell für das Add-on vorausgefüllt sind. Sie können vorhandene Rollen wiederverwenden oder neue Rollen für unterstützte Add-Ons erstellen. Die Schritte zur Verwendung der Konsole zum Erstellen von Rollen für Add-Ons, die EKS Pod Identities unterstützen, finden Sie unter [the section called “Add-on erstellen \(AWS Konsole\)”](#). Wenn ein Add-On EKS Pod Identity nicht unterstützt, wird eine Meldung mit Anweisungen zur Verwendung des Assistenten zum Erstellen der IAM-Rollen für Dienstkonten (IRSA) angezeigt, nachdem der Cluster erstellt wurde.

Sie können die Konfiguration jedes Add-Ons nach der Cluster-Erstellung aktualisieren. Weitere Informationen zum Konfigurieren eines Add-Ons finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#). Wenn Sie mit dieser Seite fertig sind, wählen Sie **Weiter** aus.

11. Überprüfen Sie auf der Seite **Review and create (Überprüfen und erstellen)** die Informationen, die Sie auf den vorherigen Seiten eingegeben oder ausgewählt haben. Wenn Sie Änderungen vornehmen müssen, wählen Sie **Edit (Bearbeiten)**. Wenn Sie zufrieden sind, wählen Sie **Create**. Das Feld **Status** zeigt **CREATING (WIRD ERSTELLT)** an, während der Cluster bereitgestellt wird.

 Note

Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called “Unzureichende Kapazität”](#).

Die Clusterbereitstellung dauert mehrere Minuten.

12 Fahren Sie fort mit [the section called “Schritt 3: Kubeconfig aktualisieren”](#)

Cluster erstellen — AWS CLI

1. Erstellen Sie den Cluster mit dem folgenden Befehl. Nehmen Sie vor der Ausführung des Befehls die folgenden Ersetzungen vor:

- *region-code* Ersetzen Sie es durch die AWS Region, in der Sie Ihren Cluster erstellen möchten.
- Ersetzen Sie *my-cluster* durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (Groß- und Kleinschreibung beachten), Bindestriche und Unterstriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
- Ersetzen Sie *1.33* durch eine von [Amazon EKS unterstützte Version](#).
- Ersetzen Sie *111122223333* durch Ihre Konto-ID und *myAmazonEKSClusterRole* durch den Namen Ihres IAM-Rollen-Clusters.
- Ersetzen Sie *subnetIds* durch Ihre eigenen Werte. Sie können auch weitere hinzufügen IDs. Sie müssen mindestens zwei Subnetze IDs angeben.

Die von Ihnen gewählten Subnetze müssen die [Anforderungen für Amazon-EKS-Subnetze](#) erfüllen. Bevor Sie Subnetze auswählen, empfehlen wir, dass Sie mit allen [Anforderungen und Überlegungen zu Amazon EKS VPC und Subnetzen](#) vertraut sind.

- Wenn Sie keine Sicherheitsgruppen-ID angeben möchten, entfernen Sie sie , `securityGroupIds=sg-<ExampleID1>` aus dem Befehl. Wenn Sie eine oder mehrere Sicherheitsgruppen angeben möchten IDs, ersetzen Sie die Werte für `securityGroupIds` durch Ihre eigenen. Sie können auch weitere hinzufügen IDs.

Unabhängig davon, ob Sie Sicherheitsgruppen wählen oder nicht, erstellt Amazon EKS eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der Cluster-Sicherheitsgruppe, die Amazon EKS erstellt, finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Sie können die Regeln in der von Amazon EKS erstellten Cluster-Sicherheitsgruppe ändern.

```
aws eks create-cluster --region region-code --name my-cluster --kubernetes-version
1.33 \
  --role-arn arn:aws: iam::111122223333:role/myAmazonEKSClusterRole \
  --resources-vpc-config subnetIds=subnet-ExampleID1,subnet-
ExampleID2,securityGroupIds=sg-ExampleID1
```

Note

Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called “Unzureichende Kapazität”](#).

Im Folgenden finden Sie optionale Einstellungen, die bei Bedarf dem vorherigen Befehl hinzugefügt werden müssen. Sie können diese Optionen nur aktivieren, wenn Sie den Cluster erstellen, nicht danach.

- Standardmäßig installiert EKS während der Clustererstellung mehrere Netzwerk-Add-Ons. Dazu gehören Amazon VPC CNI, CoreDNS und Kube-Proxy.

Wenn Sie die Installation dieser Standard-Netzwerk-Add-Ons deaktivieren möchten, verwenden Sie den folgenden Parameter. Dies kann für alternative CNIs Anwendungen wie Cilium verwendet werden. Weitere Informationen finden Sie in der [EKS-API-Referenz](#).

```
aws eks create-cluster --bootstrapSelfManagedAddons false
```

- Wenn Sie angeben möchten welchem IPv4 CIDR-Block (Classless Inter-Domain Routing) Kubernetes Service-IP-Adressen zuweist, geben Sie die Option `--kubernetes-network-config serviceIpv4Cidr=<cidr-block>` für den folgenden Befehl an.

Wenn Sie Ihren eigenen Bereich angeben, können Sie Konflikte zwischen Kubernetes-Diensten und anderen Netzwerken vermeiden, die über Peering oder Verbindungen mit Ihrer VPC verbunden sind. Geben Sie einen Bereich in CIDR-Notation ein. Beispiel: `10.2.0.0/16`.

Der CIDR-Block muss die folgenden Anforderungen erfüllen:

- Verwendet einen der folgenden Bereiche: `10.0.0.0/8`, `172.16.0.0/12`, oder `192.168.0.0/16`.
- Hat eine Mindestgröße von `/24` und eine maximale Größe von `/12`.
- Überschneidet sich nicht mit dem Bereich der VPC für Ihre Amazon-EKS-Ressourcen.

Sie können diese Option nur angeben, wenn Sie die IPv4-Adressfamilie verwenden, und nur bei Erstellen des Clusters. Wenn Sie dies nicht angeben, weist Kubernetes Dienst-IP-Adressen entweder aus den oder den CIDR-Blöcken zu. `10.100.0.0/16` `172.20.0.0/16`

- Wenn Sie einen Cluster erstellen und möchten, dass der Cluster Pods und Diensten IPv6 Adressen anstelle von IPv4 Adressen zuweist, fügen Sie den folgenden Befehl `--kubernetes-network-config ipFamily=ipv6` hinzu.

Kubernetes weist Pods und Diensten standardmäßig IPv4 Adressen zu. Bevor Sie sich für die Verwendung der IPv6 Produktfamilie entscheiden, sollten Sie sicherstellen, dass Sie mit allen Überlegungen und Anforderungen in den [VPC-Anforderungen und Überlegungen](#), [the section called “Subnetz-Anforderungen und -Überlegungen”](#), [the section called “Anforderungen an Sicherheitsgruppen”](#), und [the section called “IPv6”](#) Themen vertraut sind. Wenn Sie sich für die IPv6 Familie entscheiden, können Sie keinen Adressbereich angeben, aus dem Kubernetes IPv6 Dienstadressen zuweisen soll, wie Sie es für die Familie tun können. IPv4 Kubernetes weist Dienstadressen aus dem eindeutigen lokalen Adressbereich zu (`fc00::/7`

2. Die Bereitstellung des Clusters dauert mehrere Minuten. Sie können den Status Ihres Clusters mit dem folgenden Befehl überprüfen.

```
aws eks describe-cluster --region region-code --name my-cluster --query  
"cluster.status"
```

Fahren Sie erst mit dem nächsten Schritt fort, wenn die zurückgegebene Ausgabe ACTIVE

3. Fahren Sie fort mit [the section called “Schritt 3: Kubeconfig aktualisieren”](#)

Schritt 3: Kubeconfig aktualisieren

1. Wenn Sie Ihren Cluster mit `eksctl` erstellt haben, können Sie diesen Schritt überspringen. Das liegt daran, dass `eksctl` diesen Schritt bereits für Sie durchgeführt hat. Aktivieren Sie `kubectl`, um mit Ihrem Cluster zu kommunizieren, indem Sie einen neuen Kontext zur Datei `kubeconfig` hinzufügen. Weitere Informationen zum Erstellen und Aktualisieren der Datei finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```
Added new context arn:aws:eks:region-code:111122223333:cluster/my-cluster to /home/  
username/.kube/config
```

2. Bestätigen Sie die Kommunikation mit Ihrem Cluster, indem Sie den folgenden Befehl ausführen.

```
kubectl get svc
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	28h

Schritt 4: Cluster-Setup

1. (Empfohlen) Um einige Amazon EKS-Add-Ons zu verwenden oder einzelnen Kubernetes-Workloads bestimmte AWS Identity and Access Management (IAM) -Berechtigungen zuzuweisen, [erstellen Sie einen IAM OpenID Connect \(OIDC\)](#) -Anbieter für Ihren Cluster. Sie müssen einen

IAM-OIDC-Anbieter für Ihren Cluster nur einmal erstellen. Weitere Informationen zu Amazon EKS-Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#). Weitere Informationen zum Zuweisen bestimmter IAM-Berechtigungen zu Ihren Workloads finden Sie unter [the section called “Referenzen bei IRSA”](#).

2. (Empfohlen) Konfigurieren Sie Ihren Cluster für das Amazon VPC CNI-Plug-In für Kubernetes, bevor Sie EC2 Amazon-Knoten in Ihrem Cluster bereitstellen. Standardmäßig wurde das Plugin mit Ihrem Cluster installiert. Wenn Sie EC2 Amazon-Knoten zu Ihrem Cluster hinzufügen, wird das Plugin automatisch auf jedem EC2 Amazon-Knoten bereitgestellt, den Sie hinzufügen. Das Plugin erfordert, dass Sie einer IAM-Rolle eine der folgenden IAM-Richtlinien zuordnen. Wenn Ihr Cluster die IPv4 Familie verwendet, verwenden Sie die von [Amazoneks_CNI_Policy](#) verwaltete IAM-Richtlinie. [Wenn Ihr Cluster die IPv6 Familie verwendet, verwenden Sie eine von Ihnen erstellte IAM-Richtlinie.](#)

Die IAM-Rolle, an die Sie die Richtlinie anhängen, kann die IAM-Rolle des Knotens oder eine dedizierte Rolle sein, die nur für das Plugin verwendet wird. Wir empfehlen, die Richtlinie an diese Rolle anzuhängen. Weitere Informationen zum Erstellen der Rolle finden Sie unter [the section called “Für IRSA konfigurieren”](#) oder [Amazon EKS node IAM role](#).

3. Wenn Sie Ihren Cluster mit dem bereitgestellt haben AWS Management Console, können Sie diesen Schritt überspringen. Der AWS Management Console stellt standardmäßig das Amazon VPC CNI-Plug-In für Kubernetes-, CoreDNS- und kube-proxy Amazon EKS-Add-Ons bereit.

Wenn Sie Ihren Cluster entweder mit der CLI `eksctl` oder mit der AWS CLI bereitstellen, werden das Amazon VPC CNI-Plug-In für Kubernetes, CoreDNS und selbstverwaltete Add-Ons bereitgestellt. kube-proxy Sie können das Amazon VPC CNI-Plug-In für Kubernetes, CoreDNS und kube-proxy selbstverwaltete Add-Ons, die mit Ihrem Cluster bereitgestellt werden, zu Amazon EKS-Add-Ons migrieren. Weitere Informationen finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

4. (Optional) Falls Sie dies noch nicht getan haben, können Sie Prometheus-Metriken für Ihren Cluster aktivieren. Weitere Informationen finden Sie unter [Erstellen eine Scrapers](#) im Benutzerhandbuch von Amazon Managed Service für Prometheus.
5. Wenn Sie planen, Workloads in Ihrem Cluster bereitzustellen, die Amazon EBS-Volumes verwenden, müssen Sie [Amazon EBS CSI](#) auf Ihrem Cluster installieren, bevor Sie die Workloads bereitstellen.

Nächste Schritte

- Der [IAM-Prinzipal](#), der den Cluster erstellt hat, ist der einzige Prinzipal, der Zugriff auf den Cluster hat. Erteilen [Sie anderen IAM-Prinzipalen Berechtigungen](#), damit diese auf Ihren Cluster zugreifen können.
- Wenn der IAM-Prinzipal, der den Cluster erstellt hat, nur über die Mindest-IAM-Berechtigungen verfügt, auf die in den Voraussetzungen verwiesen wird, dann möchten Sie vielleicht weitere Amazon-EKS-Berechtigungen für diesen Prinzipal hinzufügen. Weitere Informationen über das Erteilen von Amazon-EKS-Berechtigungen für IAM-Prinzipals finden Sie unter [the section called "IAM-Referenz"](#).
- Wenn Sie möchten, dass der IAM-Prinzipal, der den Cluster erstellt hat, oder andere Prinzipale Kubernetes-Ressourcen in der Amazon EKS-Konsole anzeigen, gewähren Sie den Entitäten die [erforderlichen Berechtigungen](#).
- Wenn Sie möchten, dass Knoten und IAM-Prinzipalen von Ihrer VPC aus auf Ihren Cluster zugreifen können, aktivieren Sie den privaten Endpunkt für Ihren Cluster. Standardmäßig ist der öffentliche Endpunkt aktiviert. Sie können den öffentlichen Endpunkt deaktivieren, sobald Sie den privaten Endpunkt aktiviert haben, falls gewünscht. Weitere Informationen finden Sie unter [the section called "Cluster-Endpunktzugriff"](#).
- [Aktivieren Sie die Secrets-Verschlüsselung für Ihren Cluster](#).
- [Konfigurieren Sie die Protokollierung für Ihren Cluster](#).
- [Fügen Sie Ihrem Cluster Knoten hinzu](#).

Bereiten Sie sich mit Cluster-Erkenntnissen auf Kubernetes-Versionsupgrades vor und beheben Sie Fehlkonfigurationen

Amazon EKS-Cluster-Einblicke bieten die Erkennung von Problemen und Empfehlungen zu deren Lösung, um Sie bei der Verwaltung Ihres Clusters zu unterstützen. Für jeden Amazon-EKS-Cluster werden automatisch wiederkehrende Überprüfungen anhand einer von Amazon EKS zusammengestellten Liste von Erkenntnissen durchgeführt. Diese Insight-Checks werden vollständig von Amazon EKS verwaltet und bieten Empfehlungen, wie mit etwaigen Ergebnissen umgegangen werden kann.

Amazon EKS bietet zwei Arten von Erkenntnissen: Einblicke in die Konfiguration und Einblicke in Upgrades. Anhand von Konfigurationsinformationen werden Fehlkonfigurationen in Ihrem EKS-Hybridknoten-Setup identifiziert, die die Funktionalität Ihres Clusters oder Ihrer Workloads

beeinträchtigen könnten. Mithilfe von Upgrade-Erkenntnissen werden Probleme identifiziert, die sich auf Ihre Fähigkeit auswirken könnten, auf neue Versionen von Kubernetes aufzurüsten.

Um die Liste der durchgeführten Insight-Checks und alle relevanten Probleme, die Amazon EKS identifiziert hat, zu sehen, können Sie den Vorgang „Look in the“ AWS Management Console, „AWS CLI“ und „Amazon EKS ListInsights API“ aufrufen. AWS SDKs Informationen zu den erforderlichen Schritten finden Sie unter [the section called “Cluster-Einblicke anzeigen”](#).

Häufigkeit Amazon EKS aktualisiert Cluster-Einblicke alle 24 Stunden. Sie können Cluster-Insights nicht manuell aktualisieren. Wenn Sie ein Cluster-Problem beheben, dauert es einige Zeit, bis die Cluster-Erkenntnisse aktualisiert sind. Um festzustellen, ob ein Fix erfolgreich war, vergleichen Sie den Zeitpunkt, zu dem die Änderung implementiert wurde, mit der „letzten Aktualisierungszeit“ der Insight-Prüfung.

Berechtigungen Amazon EKS erstellt automatisch einen Cluster-Zugriffseintrag für Cluster-Einblicke in jeden EKS-Cluster. Dieser Eintrag gibt EKS die Erlaubnis, Informationen über Ihren Cluster einzusehen. EKS verwendet diese Informationen, um die Erkenntnisse zu generieren. Weitere Informationen finden Sie unter [the section called “Amazon EKSCluster InsightsPolicy”](#).

Bereiten Sie sich mit Cluster-Erkenntnissen auf Kubernetes-Versionsupgrades vor

Important

Amazon EKS hat vorübergehend eine Funktion zurückgesetzt, bei der Sie bei bestimmten Cluster-Insight-Problemen ein `--force` Flag verwenden müssten, um Ihren Cluster zu aktualisieren. Weitere Informationen finden Sie unter [Vorübergehendes Rollback der Durchsetzung von Upgrade-Erkenntnissen bei der Aktualisierung der Cluster-Version auf GitHub](#)

Weitere Informationen zur Aktualisierung Ihres Clusters finden Sie unter [the section called “Schritt 3: Aktualisieren Sie die Cluster-Steuerebene”](#)

Bei Upgrade-Insights handelt es sich um eine spezielle Art von Insight-Checks innerhalb von Cluster Insights. Diese Prüfungen liefern Erkenntnisse über die Bereitschaft zum Upgrade der Kubernetes-Version. Amazon EKS führt Upgrade-Insight-Checks auf jedem EKS-Cluster durch.

- Bevor Sie Ihre Cluster-Kubernetes-Version aktualisieren, überprüfen Sie den Tab Cluster-Einblicke des Observability-Dashboards in der [Amazon](#) EKS-Konsole.

- Wenn in Ihrem Cluster Probleme festgestellt wurden, überprüfen Sie diese und nehmen Sie entsprechende Korrekturen vor. Zu den Problemen gehören Links zur Amazon EKS- und Kubernetes-Dokumentation.
- Warten Sie nach der Behebung der Probleme, bis die Cluster-Einblicke aktualisiert sind. Wenn alle Probleme behoben wurden, [aktualisieren Sie Ihren Cluster](#).

Amazon EKS gibt Einblicke in die Bereitschaft zum Upgrade der Kubernetes-Version. Upgrade-Einblicke identifizieren mögliche Probleme, die sich auf Kubernetes-Cluster-Upgrades auswirken könnten. Dies minimiert den Aufwand, den Administratoren für die Vorbereitung von Upgrades aufwenden müssen, und erhöht die Zuverlässigkeit von Anwendungen auf neueren Kubernetes-Versionen. Cluster werden automatisch von Amazon EKS anhand einer Liste möglicher Probleme mit dem Upgrade der Kubernetes-Version geprüft, die sich auf die Aktualisierung auswirken könnten. Amazon EKS aktualisiert die Liste der Insight-Checks häufig auf der Grundlage von Überprüfungen der Änderungen, die in den einzelnen Kubernetes-Versionen vorgenommen wurden.

Upgrade-Erkenntnisse von Amazon EKS beschleunigen den Test- und Überprüfungsprozess für neue Versionen. Sie ermöglichen es Clusteradministratoren und Anwendungsentwicklern auch, die neuesten Kubernetes-Funktionen zu nutzen, indem sie Bedenken hervorheben und Ratschläge zur Behebung geben.

Beheben Sie Fehlkonfigurationen mit Cluster-Erkenntnissen

EKS Cluster Insights scannt automatisch Amazon EKS-Cluster mit Hybridknoten, um Konfigurationsprobleme zu identifizieren, die die plane-to-webhook Kubernetes-Steuerungskommunikation, kubectl-Befehle wie exec und logs und mehr beeinträchtigen. Durch Einblicke in die Konfiguration werden Probleme aufgedeckt und Empfehlungen zur Problembehebung gegeben, wodurch die Zeit bis zur Einrichtung eines voll funktionsfähigen Hybridknotens beschleunigt wird.

Cluster-Einblicke anzeigen

Amazon EKS bietet zwei Arten von Erkenntnissen: Einblicke in die Konfiguration und Einblicke in Upgrades. Anhand von Konfigurationsinformationen werden Fehlkonfigurationen in Ihrem EKS-Hybridknoten-Setup identifiziert, die die Funktionalität Ihres Clusters oder Ihrer Workloads beeinträchtigen könnten. Mithilfe von Upgrade-Erkenntnissen werden Probleme identifiziert, die sich auf Ihre Fähigkeit auswirken könnten, auf neue Versionen von Kubernetes aufzurüsten.

Um die Liste der durchgeführten Insight-Checks und alle relevanten Probleme, die Amazon EKS identifiziert hat, zu sehen, können Sie den Vorgang Look in the AWS Management Console AWS SDKs, AWS CLI und Amazon EKS ListInsights API aufrufen.

Einblicke in die Konfiguration anzeigen (Konsole)

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie in der Clusterliste den Namen des Amazon-EKS-Clusters aus, für den Sie die Erkenntnisse anzeigen möchten.
3. Wählen Sie Cluster überwachen aus.
4. Wählen Sie die Registerkarte Clusterstatus.
5. In der Tabelle Configuration Insights sehen Sie die folgenden Spalten:
 - Name: Die Überprüfung, die von Amazon EKS für den Cluster durchgeführt wurde.
 - Insight-Status — Ein Einblick mit dem Status von `Error` bedeutet, dass eine Fehlkonfiguration vorliegt, die sich wahrscheinlich auf die Cluster-Funktionalität auswirkt. Ein Einblick mit dem Status von `Warning` bedeutet, dass die Konfiguration nicht dem dokumentierten Ansatz entspricht, dass die Cluster-Funktionalität jedoch möglicherweise funktioniert, wenn Sie sie absichtlich konfiguriert haben. Ein Einblick mit dem Status `Passing` bedeutet, dass Amazon EKS keine Probleme im Zusammenhang mit dieser Insight-Prüfung in Ihrem Cluster gefunden hat.
 - Beschreibung: Informationen der letzten Erkenntnisüberprüfung (einschließlich der Warnung und der empfohlenen Behandlungsmaßnahmen).
 - Zeitpunkt der letzten Aktualisierung — Der Zeitpunkt, zu dem der Status des Insights für diesen Cluster zuletzt aktualisiert wurde.

Upgrade-Einblicke anzeigen (Konsole)

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie in der Clusterliste den Namen des Amazon-EKS-Clusters aus, für den Sie die Erkenntnisse anzeigen möchten.
3. Wählen Sie „Dashboard anzeigen“.
4. Wählen Sie den Tab Cluster Insights.
5. In der Tabelle Upgrade Insights sehen Sie die folgenden Spalten:
 - Name — Die Prüfung, die Amazon EKS für den Cluster durchgeführt hat.

- **Insight-Status** — Ein Insight mit dem Status „Fehler“ bedeutet in der Regel, dass die betroffene Kubernetes-Version N+1 der aktuellen Cluster-Version ist, während der Status „Warnung“ bedeutet, dass der Einblick für eine future Kubernetes-Version N+2 oder höher gilt. Eine Erkenntnis mit dem Status „Bestanden“ bedeutet, dass Amazon EKS keine Probleme im Zusammenhang mit dieser Erkenntnisüberprüfung in Ihrem Cluster festgestellt hat. Bei einer Erkenntnis mit dem Status „Unbekannt“ kann Amazon EKS nicht feststellen, ob Ihr Cluster von dieser Erkenntnisüberprüfung betroffen ist.
- **Version** — Die Kubernetes-Version, bei der Insight auf mögliche Probleme überprüft wurde.
- **Zeitpunkt der letzten Aktualisierung** — Der Zeitpunkt, zu dem der Status des Insights für diesen Cluster zuletzt aktualisiert wurde.
- **Zeitpunkt des letzten Übergangs** — Der Zeitpunkt, zu dem sich der Status dieses Insights zuletzt geändert hat.
- **Beschreibung**: Informationen der letzten Erkenntnisüberprüfung (einschließlich der Warnung und der empfohlenen Behandlungsmaßnahmen).

Cluster-Einblicke anzeigen (AWS CLI)

1. Bestimmen Sie, welchen Cluster Sie auf Erkenntnisse überprüfen möchten. Der folgende Befehl listet die Erkenntnisse für einen angegebenen Cluster auf. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:

- ***region-code*** Ersetzen Sie es durch den Code für Ihre AWS Region.
- Ersetzen Sie ***my-cluster*** mit dem Namen Ihres Clusters.

```
aws eks list-insights --region region-code --cluster-name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "insights":
    [
      {
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "name": "Deprecated APIs removed in Kubernetes vX.XX",
        "category": "UPGRADE_READINESS",
        "kubernetesVersion": "X.XX",
        "lastRefreshTime": 1734557315.000,
```



```

        "lastTransitionTime": 1734557309.000,
        "description": "Checks for usage of deprecated APIs that are scheduled
for removal in Kubernetes vX.XX. Upgrading your cluster before migrating to the
updated APIs supported by vX.XX could cause application impact.",
        "insightStatus":
        {
            "status": "PASSING",
            "reason": "No deprecated API usage detected within the last 30
days.",
        },
    },
    {
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "name": "Kubelet version skew",
        "category": "UPGRADE_READINESS",
        "kubernetesVersion": "X.XX",
        "lastRefreshTime": 1734557309.000,
        "lastTransitionTime": 1734557309.000,
        "description": "Checks for kubelet versions of worker nodes in the
cluster to see if upgrade would cause non compliance with supported Kubernetes
kubelet version skew policy.",
        "insightStatus":
        {
            "status": "UNKNOWN",
            "reason": "Unable to determine status of node kubelet versions.",
        },
    },
    {
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "name": "Deprecated APIs removed in Kubernetes vX.XX",
        "category": "UPGRADE_READINESS",
        "kubernetesVersion": "X.XX",
        "lastRefreshTime": 1734557315.000,
        "lastTransitionTime": 1734557309.000,
        "description": "Checks for usage of deprecated APIs that are scheduled
for removal in Kubernetes vX.XX. Upgrading your cluster before migrating to the
updated APIs supported by vX.XX could cause application impact.",
        "insightStatus":
        {
            "status": "PASSING",
            "reason": "No deprecated API usage detected within the last 30
days.",
        },
    },
}

```

```

{
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
  "name": "Cluster health issues",
  "category": "UPGRADE_READINESS",
  "kubernetesVersion": "X.XX",
  "lastRefreshTime": 1734557314.000,
  "lastTransitionTime": 1734557309.000,
  "description": "Checks for any cluster health issues that prevent
successful upgrade to the next Kubernetes version on EKS.",
  "insightStatus":
  {
    "status": "PASSING",
    "reason": "No cluster health issues detected.",
  },
},
{
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
  "name": "EKS add-on version compatibility",
  "category": "UPGRADE_READINESS",
  "kubernetesVersion": "X.XX",
  "lastRefreshTime": 1734557314.000,
  "lastTransitionTime": 1734557309.000,
  "description": "Checks version of installed EKS add-ons to ensure they
are compatible with the next version of Kubernetes. ",
  "insightStatus": { "status": "PASSING", "reason": "All installed EKS
add-on versions are compatible with next Kubernetes version."},
},
{
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEccccc",
  "name": "kube-proxy version skew",
  "category": "UPGRADE_READINESS",
  "kubernetesVersion": "X.XX",
  "lastRefreshTime": 1734557314.000,
  "lastTransitionTime": 1734557309.000,
  "description": "Checks version of kube-proxy in cluster to see if
upgrade would cause non compliance with supported Kubernetes kube-proxy version
skew policy.",
  "insightStatus":
  {
    "status": "PASSING",
    "reason": "kube-proxy versions match the cluster control plane
version.",
  },
},
},

```

```

{
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEddddd",
  "name": "Deprecated APIs removed in Kubernetes vX.XX",
  "category": "UPGRADE_READINESS",
  "kubernetesVersion": "X.XX",
  "lastRefreshTime": 1734557315.000,
  "lastTransitionTime": 1734557309.000,
  "description": "Checks for usage of deprecated APIs that are scheduled
for removal in Kubernetes vX.XX. Upgrading your cluster before migrating to the
updated APIs supported by vX.XX could cause application impact.",
  "insightStatus":
  {
    "status": "PASSING",
    "reason": "No deprecated API usage detected within the last 30
days.",
  },
},
],
"nextToken": null,
}

```

2. Führen Sie den folgenden Befehl aus, um beschreibende Informationen zu der Erkenntnis zu erhalten. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:

- Ersetze es *region-code* durch den Code für deine AWS Region.
- *a1b2c3d4-5678-90ab-cdef-EXAMPLE22222* Ersetzen Sie es durch eine Insight-ID, die aus der Auflistung der Cluster-Insights abgerufen wurde.
- Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-insight --region region-code --id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 --cluster-name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```

{
  "insight":
  {
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "name": "Kubelet version skew",
    "category": "UPGRADE_READINESS",
    "kubernetesVersion": "1.27",

```

```

    "lastRefreshTime": 1734557309.000,
    "lastTransitionTime": 1734557309.000,
    "description": "Checks for kubelet versions of worker nodes in the cluster
to see if upgrade would cause non compliance with supported Kubernetes kubelet
version skew policy.",
    "insightStatus":
    {
        "status": "UNKNOWN",
        "reason": "Unable to determine status of node kubelet versions.",
    },
    "recommendation": "Upgrade your worker nodes to match the Kubernetes version
of your cluster control plane.",
    "additionalInfo":
    {
        "Kubelet version skew policy": "https://kubernetes.io/releases/version-
skew-policy/#kubelet",
        "Updating a managed node group": "https://docs.aws.amazon.com/eks/latest/
userguide/update-managed-node-group.html",
    },
    "resources": [],
    "categorySpecificSummary":
    { "deprecationDetails": [], "addonCompatibilityDetails": [] },
},
}

```

Aktualisieren Sie den vorhandenen Cluster auf die neue Kubernetes-Version

Wenn eine neue Kubernetes-Version in Amazon EKS verfügbar ist, können Sie Ihren Amazon-EKS-Cluster auf die neueste Version aktualisieren.

Important

Sobald Sie einen Cluster aktualisiert haben, können Sie kein Downgrade auf eine frühere Version durchführen. Bevor Sie auf eine neue Kubernetes-Version aktualisieren, empfehlen wir Ihnen, die Informationen [the section called “Kubernetes-Versionen”](#) und die Aktualisierungsschritte in diesem Thema zu lesen.

Neue Kubernetes-Versionen führen oft bedeutende Änderungen ein. Daher empfehlen wir Ihnen, das Verhalten Ihrer Anwendungen mit einer neuen Kubernetes-Version zu testen, bevor Sie Ihre Produktionscluster aktualisieren. Hierzu erstellen Sie einen kontinuierlichen Integrations-Workflow, um das Verhalten Ihrer Anwendungen zu testen, bevor Sie auf eine neue Kubernetes-Version aktualisieren.

Der Aktualisierungsprozess besteht darin, dass Amazon EKS neue API-Serverknoten mit der aktualisierten Kubernetes-Version startet, um die vorhandenen zu ersetzen. Amazon EKS führt standardmäßige Integritätsprüfungen für den Netzwerkverkehr auf diesen neuen Knoten durch, um sicherzustellen, dass sie erwartungsgemäß funktionieren. Sobald Sie das Cluster-Upgrade gestartet haben, können Sie es jedoch weder anhalten noch beenden. Wenn eine dieser Prüfungen fehlschlägt, macht Amazon EKS die Infrastruktur-Bereitstellung rückgängig und der Cluster verbleibt in der vorherigen Kubernetes-Version. Laufende Anwendungen sind davon nicht betroffen, und Ihr Cluster befindet sich nie in einem Zustand, der nicht deterministisch ist oder nicht wiederhergestellt werden kann. Amazon EKS sichert regelmäßig alle verwalteten Cluster, und es gibt Mechanismen, um Cluster bei Bedarf wiederherzustellen. Wir evaluieren und verbessern ständig unsere Prozesse für das Kubernetes-Infrastrukturmanagement.

Um den Cluster zu aktualisieren, benötigt Amazon EKS bis zu fünf verfügbare IP-Adressen aus den Subnetzen, die beim Erstellen des Clusters bereitgestellt wurden. Amazon EKS erstellt in jedem der von Ihnen angegebenen Subnetze neue Elastic-Network-Schnittstellen für den Cluster (Netzwerkschnittstellen). Die Netzwerkschnittstellen können in anderen Subnetzen erstellt werden als Ihre vorhandenen Netzwerkschnittstellen. Stellen Sie daher sicher, dass Ihre Sicherheitsgruppenregeln die [erforderliche Cluster-Kommunikation](#) für jedes der Subnetze zulassen, die Sie bei der Erstellung Ihres Clusters angegeben haben. Wenn eines der Subnetze, die Sie bei der Erstellung des Clusters angegeben haben, nicht vorhanden ist, nicht über genügend verfügbare IP-Adressen verfügt oder es keine Sicherheitsgruppenregeln gibt, die die erforderliche Cluster-Kommunikation ermöglichen, kann das Update fehlschlagen.

Um sicherzustellen, dass der API-Serverendpunkt für Ihren Cluster immer zugänglich ist, bietet Amazon EKS eine hochverfügbare Kubernetes-Steuerebene und führt während der Aktualisierungsvorgänge fortlaufende Updates von API-Server-Instances durch. Um den sich ändernden IP-Adressen von API-Server-Instances, die Ihren Kubernetes-API-Serverendpunkt unterstützen, Rechnung zu tragen, müssen Sie sicherstellen, dass Ihre API-Serverclients Wiederverbindungen effektiv verwalten. Neuere Versionen von `kubectl` und die offiziell unterstützten [Kubernetes-Clientbibliotheken](#) führen diesen Wiederverbindungsprozess transparent durch.

 Note

Weitere Informationen darüber, was in einem Cluster-Update enthalten ist, finden Sie unter [Best Practices for Cluster Upgrades](#) im EKS Best Practices Guide. Diese Ressource hilft Ihnen dabei, ein Upgrade zu planen und die Strategie für das Upgrade eines Clusters zu verstehen.

Überlegungen zum Amazon EKS Auto Mode

- Die Rechenkapazität von Amazon EKS Auto Mode steuert die Kubernetes-Version der Knoten. Nach dem Upgrade der Steuerungsebene beginnt der automatische Modus von EKS mit der schrittweisen Aktualisierung der verwalteten Knoten. Der EKS-Automatikmodus berücksichtigt die Budgets für Pod-Unterbrechungen.
- Sie müssen die Funktionen von Amazon EKS Auto Mode, einschließlich der Funktionen für automatische Rechenskalierung, Blockspeicher und Lastenausgleich, nicht manuell aktualisieren.

Übersicht

Die allgemeine Zusammenfassung des Amazon EKS-Cluster-Upgrade-Prozesses lautet wie folgt:

1. Stellen Sie sicher, dass sich Ihr Cluster in einem Zustand befindet, der ein Upgrade unterstützt. Dazu gehört die Überprüfung der Kubernetes-Werte, die von den im Cluster bereitgestellten Ressourcen APIs verwendet werden, um sicherzustellen, dass der Cluster frei von Gesundheitsproblemen ist. Sie sollten Amazon EKS Upgrade Insights verwenden, um die Upgrade-Bereitschaft Ihres Clusters zu bewerten.
2. Führen Sie ein Upgrade der Steuerungsebene auf die nächste Nebenversion durch (z. B. von 1.32 auf 1.33).
3. Aktualisieren Sie die Knoten in der Datenebene so, dass sie denen der Steuerungsebene entsprechen.
4. Aktualisieren Sie alle zusätzlichen Anwendungen, die auf dem Cluster ausgeführt werden (z. B. `cluster-autoscaler`).
5. Aktualisieren Sie die von Amazon EKS bereitgestellten Add-Ons, z. B. die standardmäßig enthaltenen:
 - [Empfohlene Version von Amazon VPC CNI](#)

- [CoreDNS empfohlene Version](#)
- [kube-proxyempfohlene Version](#)

6. Aktualisieren Sie alle Clients, die mit dem Cluster kommunizieren (z. B. `kubectl`).

Schritt 1: Bereiten Sie das Upgrade vor

Vergleichen Sie die Kubernetes-Version Ihrer Cluster-Steuerebene mit der Kubernetes-Version Ihrer Knoten.

- Holen Sie sich die Kubernetes-Version Ihrer Cluster-Steuerebene.

```
kubectl version
```

- Holen Sie sich die Kubernetes-Version Ihrer Knoten. Dieser Befehl gibt alle selbstverwalteten und verwalteten Amazon- EC2, Fargate- und Hybridknoten zurück. Jeder Fargate-Pod ist als eigener Knoten aufgeführt.

```
kubectl get nodes
```

Bevor Sie Ihre Kontrollebene auf eine neue Kubernetes-Version aktualisieren, stellen Sie sicher, dass die Kubernetes-Nebenversion sowohl der verwalteten Knoten als auch der Fargate-Knoten in Ihrem Cluster mit der Version Ihrer Kontrollebene identisch ist. Wenn auf Ihrer Kontrollebene beispielsweise die Version ausgeführt wird 1.28 und auf einem Ihrer Knoten die Version ausgeführt wird, müssen Sie Ihre Knoten auf Version aktualisieren 1.28, 1.29 bevor Sie Ihre Kontrollebene auf Version 1.30 aktualisieren. Wir empfehlen Ihnen außerdem, Ihre selbstverwalteten Knoten und Hybridknoten auf dieselbe Version wie Ihre Kontrollebene zu aktualisieren, bevor Sie die Kontrollebene aktualisieren. Weitere Informationen finden Sie unter [the section called “Aktualisierung”](#), [the section called “Update-Methoden”](#) und [the section called “Aktualisieren Sie Hybridknoten”](#). Wenn Sie Fargate-Knoten mit einer niedrigeren Nebenversion als der Version auf der Kontrollebene haben, löschen Sie zuerst den Pod, der durch den Knoten repräsentiert wird. Aktualisieren Sie dann Ihre Steuerebene. Alle verbleibenden Pods werden auf die neue Version aktualisiert, nachdem Sie sie erneut bereitgestellt haben.

Schritt 2: Überprüfen Sie die Überlegungen zum Upgrade

Amazon EKS Cluster Insights scannt Cluster automatisch anhand einer Liste potenzieller Kubernetes-Versionsupgrades, die sich auf Probleme wie die veraltete Kubernetes-API-Nutzung auswirken. Amazon EKS aktualisiert regelmäßig die Liste der durchzuführenden Insight-Checks auf der Grundlage von Bewertungen von Änderungen im Kubernetes-Projekt. Amazon EKS aktualisiert auch die Liste der Insight-Checks, sobald Änderungen am Amazon EKS-Service zusammen mit neuen Versionen eingeführt werden. Weitere Informationen finden Sie unter [the section called "Cluster-Erkenntnisse"](#).

Lesen Sie den [Leitfaden zur Migration veralteter APIs](#) in den Kubernetes-Dokumenten.

Lesen Sie Cluster Insights

Verwenden Sie Amazon EKS-Cluster-Einblicke, um Probleme zu identifizieren wi

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie in der Clusterliste den Namen des Amazon-EKS-Clusters aus, für den Sie die Erkenntnisse anzeigen möchten.
3. Wählen Sie Dashboard anzeigen.
4. Wählen Sie den Tab Cluster Insights.
5. In der Tabelle Upgrade Insights sehen Sie die folgenden Spalten:
 - Name: Die Überprüfung, die von Amazon EKS für den Cluster durchgeführt wurde.
 - Insight-Status — Ein Insight mit dem Status „Fehler“ bedeutet in der Regel, dass die betroffene Kubernetes-Version N+1 der aktuellen Cluster-Version ist, während der Status „Warnung“ bedeutet, dass der Einblick für eine future Kubernetes-Version N+2 oder höher gilt. Eine Erkenntnis mit dem Status „Bestanden“ bedeutet, dass Amazon EKS keine Probleme im Zusammenhang mit dieser Erkenntnisüberprüfung in Ihrem Cluster festgestellt hat. Bei einer Erkenntnis mit dem Status „Unbekannt“ kann Amazon EKS nicht feststellen, ob Ihr Cluster von dieser Erkenntnisüberprüfung betroffen ist.
 - Version — Die Kubernetes-Version, bei der Insight auf mögliche Probleme überprüft wurde.
 - Zeitpunkt der letzten Aktualisierung — Der Zeitpunkt, zu dem der Status des Insights für diesen Cluster zuletzt aktualisiert wurde.
 - Zeitpunkt des letzten Übergangs — Der Zeitpunkt, zu dem sich der Status dieses Insights zuletzt geändert hat.

- Beschreibung: Informationen der letzten Erkenntnisüberprüfung (einschließlich der Warnung und der empfohlenen Behandlungsmaßnahmen).

Detaillierte Überlegungen

- Da Amazon EKS eine hoch verfügbare Steuerebene ausführt, dürfen Sie jeweils nur um eine Unterversion aktualisieren. Weitere Informationen zu dieser Anforderung finden Sie unter [Kubernetes-Version und Version-Skew-Supportrichtlinie](#). Angenommen, Ihre aktuelle Cluster-Version ist Version 1.28 und Sie möchten sie auf Version 1.30 aktualisieren. Sie müssen zuerst Ihren Version 1.28-Cluster auf Version 1.29 und dann Ihren Version 1.29-Cluster auf Version 1.30 aktualisieren.
- Prüfen Sie den Versionsunterschied zwischen Kubernetes kube-apiserver und dem kubelet auf Ihren Nodes.
 - Ausgehend von der Kubernetes-Version 1.28 kubelet können bis zu drei Nebenversionen älter sein als kube-apiserver. Weitere Informationen finden Sie in der [Richtlinie zum Unterschied bei der Kubernetes-Upstream-Version](#).
 - Wenn der Knoten kubelet auf Ihrem verwalteten Knoten und auf Fargate auf einer Kubernetes-Version 1.25 oder neuer ist, können Sie Ihren Cluster bis zu drei Versionen im Voraus aktualisieren, ohne die Version zu aktualisieren. kubelet Wenn das kubelet also beispielsweise über die Version 1.25 verfügt, können Sie die Version Ihres Amazon EKS-Clusters von 1.25 auf 1.26, auf 1.27 und auf 1.28 aktualisieren und für kubelet die Version 1.25 beibehalten.
- Als bewährte Methode sollten Sie vor dem Start eines Updates sicherstellen, dass kubelet auf Ihren Knoten dieselbe Kubernetes-Version wie auf Ihrer Kontrollebene installiert ist.
- Wenn Ihr Cluster mit einer älteren Version des Amazon VPC CNI-Plug-ins für Kubernetes konfiguriert ist als 1.8.0, empfehlen wir Ihnen, das Plug-in auf die neueste Version zu aktualisieren, bevor Sie Ihren Cluster aktualisieren. Informationen zum Aktualisieren des Plugins finden Sie unter [the section called "Amazon VPC CNI"](#).

Schritt 3: Aktualisieren Sie die Cluster-Steuerebene

Important

Amazon EKS hat vorübergehend eine Funktion zurückgesetzt, bei der Sie bei bestimmten Cluster-Insight-Problemen ein `--force` Flag verwenden müssten, um Ihren Cluster zu

aktualisieren. Weitere Informationen finden Sie unter [Vorübergehendes Rollback der Durchsetzung von Upgrade-Erkenntnissen bei der Aktualisierung der Cluster-Version auf](#).

GitHub

Amazon EKS aktualisiert einen Cluster-Einblick 24 Stunden nach der „letzten Aktualisierungszeit“. Sie können die Zeit, zu der Sie ein Problem behoben haben, mit der „letzten Aktualisierungszeit“ von Cluster Insight vergleichen.

Darüber hinaus kann es bis zu 30 Tage dauern, bis der Insight-Status aktualisiert wird, nachdem die veraltete API-Nutzung behoben wurde. Upgrade Insights sucht immer über einen fortlaufenden Zeitraum von 30 Tagen nach veralteter API-Nutzung.

Sie können die Anfrage für ein Upgrade Ihrer EKS-Steuerebenenversion wie folgt einreichen:

- [eksctl](#)
- [die Konsole AWS](#)
- [die AWS CLI](#)

Cluster aktualisieren - eksctl

Für diesen Vorgang ist eksctl Version 0.210.0 oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Eine Installations- und Aktualisierungsanleitung für eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).

Aktualisieren Sie die Kubernetes-Version Ihrer Amazon EKS-Kontrollebene. Ersetzen Sie `<cluster-name>` mit Ihrem Clusternamen. `<version-number>` Ersetzen Sie es durch die von Amazon EKS unterstützte Versionsnummer, auf die Sie Ihren Cluster aktualisieren möchten. Eine Liste der unterstützten Versionsnummern finden Sie unter [the section called “Kubernetes-Versionen”](#).

```
eksctl upgrade cluster --name <cluster-name> --version <version-number> --approve
```

Die Aktualisierung dauert einige Minuten.

Fahren Sie fort mit [the section called “Schritt 4: Clusterkomponenten aktualisieren”](#).

Cluster aktualisieren — AWS Konsole

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie für einen Cluster, den Sie aktualisieren möchten, die Option Jetzt aktualisieren aus.
3. Wählen Sie die Version aus, auf die Sie Ihren Cluster aktualisieren möchten, und wählen Sie Upgrade.
4. Die Aktualisierung dauert einige Minuten. Fahren Sie fort mit [the section called “Schritt 4: Clusterkomponenten aktualisieren”](#).

Cluster aktualisieren — AWS CLI

1. Stellen Sie sicher, dass die AWS CLI installiert ist und ob Sie angemeldet sind. Weitere Informationen finden Sie unter [Installation oder Aktualisierung auf die neueste Version der AWS CLI](#).
2. Aktualisieren Sie Ihren Amazon EKS-Cluster mit dem folgenden AWS CLI-Befehl. Ersetzen Sie `<cluster-name>` und `<region-code>` des Clusters, den Sie aktualisieren möchten. `<version-number>` Ersetzen Sie es durch die von Amazon EKS unterstützte Versionsnummer, auf die Sie Ihren Cluster aktualisieren möchten. Eine Liste der unterstützten Versionsnummern finden Sie unter [the section called “Kubernetes-Versionen”](#).

```
aws eks update-cluster-version --name <cluster-name> \
  --kubernetes-version <version-number> --region <region-code>
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "update": {
    "id": "<update-id>",
    "status": "InProgress",
    "type": "VersionUpdate",
    "params": [
      {
        "type": "Version",
        "value": "<version-number>"
      },
      {
        "type": "PlatformVersion",
        "value": "eks.1"
      }
    ]
  }
}
```

```
    }  
  ],  
  [...]  
  "errors": []  
}
```

3. Die Aktualisierung dauert einige Minuten. Überwachen Sie den Status Ihres Cluster-Updates mit dem folgenden Befehl. Verwenden Sie nicht nur dasselbe `<cluster-name>` und `<region-code>`, sondern auch das, `<update-id>` das der vorherige Befehl zurückgegeben hat.

```
aws eks describe-update --name <cluster-name> \  
  --region <region-code> --update-id <update-id>
```

Wenn der Status `Successful` angezeigt wird, ist das Update abgeschlossen.

4. Fahren Sie fort mit [the section called “Schritt 4: Clusterkomponenten aktualisieren”](#).

Schritt 4: Clusterkomponenten aktualisieren

1. Nachdem Ihre Cluster-Aktualisierung abgeschlossen wurde, aktualisieren Sie Ihre Knoten auf dieselbe Kubernetes-Nebenversion wie Ihr aktualisierter Cluster. Weitere Informationen finden Sie unter [the section called “Update-Methoden”](#), [the section called “Aktualisierung”](#) und [the section called “Aktualisieren Sie Hybridknoten”](#). Alle neuen Pods, die auf Fargate gestartet werden, haben eine `kubelet` Version, die Ihrer Cluster-Version entspricht. Bestehende Fargate Pods werden nicht geändert.
2. (Optional) Wenn Sie den Kubernetes Cluster Autoscaler in Ihrem Cluster bereitgestellt haben, bevor Sie den Cluster aktualisiert haben, aktualisieren Sie den Cluster Autoscaler auf die neueste Version, die der Kubernetes-Haupt- und Nebenversion entspricht, auf die Sie aktualisiert haben.
 - a. Öffnen Sie die Seite mit den Cluster [Autoscaler-Releases](#) in einem Webbrowser und suchen Sie nach der neuesten Cluster Autoscaler-Version, die der Kubernetes-Haupt- und Nebenversion Ihres Clusters entspricht. Wenn es sich bei der Kubernetes-Version Ihres Clusters beispielsweise um die neueste Version von Cluster Autoscaler handelt, die `1.30` mit beginnt. `1.30` Notieren Sie die semantische Versionsnummer (z. B. `1.30.n`) für diese Version, um sie im nächsten Schritt zu verwenden.
 - b. Legen Sie das Cluster Autoscaler-Abbild-Tag mit dem folgenden Befehl auf die Version fest, die Sie im vorherigen Schritt notiert haben. Ersetzen Sie ggf. `X.XX.X` durch Ihren eigenen Wert.

```
kubectl -n kube-system set image deployment.apps/cluster-autoscaler cluster-autoscaler=registry.k8s.io/autoscaling/cluster-autoscaler:vX.XX.X
```

3. (Nur Cluster mit GPU-Knoten) Wenn Ihr Cluster Knotengruppen mit GPU-Unterstützung hat (z. B. p3.2xlarge), müssen Sie das [NVIDIA-Geräte-Plugin für DaemonSet Kubernetes](#) auf Ihrem Cluster aktualisieren. Ersetzen Sie es <vX.X.X> durch die gewünschte [s-device-pluginNVIDIA/K8-Version](#), bevor Sie den folgenden Befehl ausführen.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/<vX.X.X>/deployments/static/nvidia-device-plugin.yml
```

4. Aktualisieren Sie das Amazon VPC CNI-Plugin für Kubernetes, CoreDNS und Add-Ons. kube-proxy Wir empfehlen, die Add-Ons auf die Mindestversionen zu aktualisieren, die unter [Servicekonto-Tokens](#) aufgeführt sind.
- Wenn Sie Amazon-EKS-Add-Ons verwenden, wählen Sie Clusters (Cluster) in der Amazon-EKS-Konsole und dann im linken Navigationsbereich den Namen des Clusters aus, den Sie aktualisiert haben. In der Konsole werden Benachrichtigungen angezeigt. Diese informieren Sie darüber, dass für jedes Add-On, für das eine Aktualisierung verfügbar ist, eine neue Version verfügbar ist. Um ein Add-on zu aktualisieren, wählen Sie die Registerkarte Add-ons aus. Wählen Sie in einem der Felder für ein Add-on, für das eine Aktualisierung verfügbar ist, Jetzt aktualisieren aus, wählen Sie eine verfügbare Version aus, und wählen Sie dann Aktualisieren aus.
 - Alternativ können Sie die AWS CLI verwenden oder eksctl Add-Ons aktualisieren. Weitere Informationen finden Sie unter [the section called "Aktualisieren Sie ein Add-on"](#).
5. Sofern erforderlich, aktualisieren Sie Ihre Version von kubectl. Sie müssen eine kubectl-Version verwenden, die nur in der Minor-Version von Ihrer Amazon-EKS-Cluster-Steuerebene abweicht.

Downgrade der Kubernetes-Version für einen Amazon EKS-Cluster

Sie können die Kubernetes eines Amazon EKS-Clusters nicht herunterstufen. Erstellen Sie stattdessen einen neuen Cluster auf einer früheren Amazon EKS-Version und migrieren Sie die Workloads.

Einen Cluster löschen

Wenn Sie einen Amazon EKS-Cluster nicht mehr verwenden, sollten Sie die damit verbundenen Ressourcen löschen, damit Ihnen keine unnötigen Kosten entstehen.

Sie können einen Cluster mit `eksctl` AWS Management Console, der oder der AWS CLI löschen.

Überlegungen

- Wenn noch Services in Ihrem Cluster aktiv sind, die einem Load Balancer zugeordnet sind, müssen Sie diese Services löschen, bevor Sie den Cluster löschen können, damit die Load Balancer korrekt gelöscht werden können. Andernfalls bleiben in Ihrer VPC eventuell verwaiste Ressourcen zurück, die verhindern, dass Sie die VPC löschen können.
- Wenn Sie eine Fehlermeldung erhalten, weil der Cluster-Ersteller entfernt wurde, lesen Sie [diesen Artikel](#).
- Die Ressourcen von Amazon Managed Service for Prometheus befinden sich außerhalb des Cluster-Lebenszyklus und müssen unabhängig vom Cluster verwaltet werden. Wenn Sie Ihren Cluster löschen, stellen Sie sicher, dass Sie auch alle entsprechenden Scraper löschen, um die anfallenden Kosten zu stoppen. Weitere Informationen [finden Sie unter Suchen und Löschen von Scrapern](#) im Amazon Managed Service for Prometheus Benutzerhandbuch.
- Informationen zum Entfernen eines verbundenen Clusters finden Sie unter [the section called “Einen Cluster abmelden”](#).

Überlegungen zum automatischen Modus von EKS

- Alle EKS-Automodus-Knoten werden gelöscht, einschließlich der EC2 verwalteten Instanzen
- Alle Load Balancer werden gelöscht

Weitere Informationen finden Sie unter [the section called “Deaktivieren Sie den EKS-Automatikmodus”](#).

Cluster löschen (eksctl)

Für diesen Vorgang ist `eksctl` Version `0.210.0` oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Eine Installations- und Upgrade-Anleitung für eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).

1. Listen Sie alle in Ihrem Cluster ausgeführten Services auf.

```
kubectl get svc --all-namespaces
```

- a. Löschen Sie alle Services, die dem Wert EXTERNAL-IP zugeordnet sind. Diese Services werden hinter einem Elastic-Load-Balancing-Load-Balancer ausgeführt und müssen in Kubernetes gelöscht werden, damit der Load Balancer und die zugeordneten Ressourcen korrekt freigegeben werden können. *service-name* Ersetzen Sie es durch die Namen der einzelnen Dienste, die wie beschrieben aufgeführt sind.

```
kubectl delete svc service-name
```

2. Löschen Sie den Cluster und die zugehörigen Knoten mit dem folgenden Befehl. Ersetzen Sie dabei *prod* durch den Namen Ihres Clusters.

```
eksctl delete cluster --name prod
```

Ausgabe:

```
[#] using region region-code
[#] deleting EKS cluster "prod"
[#] will delete stack "eksctl-prod-nodegroup-standard-nodes"
[#] waiting for stack "eksctl-prod-nodegroup-standard-nodes" to get deleted
[#] will delete stack "eksctl-prod-cluster"
[#] the following EKS cluster resource(s) for "prod" will be deleted: cluster. If in
doubt, check CloudFormation console
```

Cluster löschen (AWS Konsole)

1. Listen Sie alle in Ihrem Cluster ausgeführten Services auf.

```
kubectl get svc --all-namespaces
```

2. Löschen Sie alle Services, die dem Wert EXTERNAL-IP zugeordnet sind. Diese Services werden hinter einem Elastic-Load-Balancing-Load-Balancer ausgeführt und müssen in Kubernetes gelöscht werden, damit der Load Balancer und die zugeordneten Ressourcen korrekt freigegeben werden können. `service-name` Ersetzen Sie es durch den Namen der einzelnen Dienste, die wie beschrieben aufgeführt sind.

```
kubectl delete svc service-name
```

3. Alle Knotengruppen und Fargate-Profil löschen.
 - a. Öffnen Sie die [Amazon-EKS-Konsole](#).
 - b. Wählen Sie im linken Navigationsbereich Clusters (Cluster) für Amazon EKS aus, und wählen Sie dann in der Registerkartenliste der Cluster den Namen des zu löschenden Clusters aus.
 - c. Wählen Sie auf der Registerkarte Compute (Datenverarbeitung) eine zu löschende Knotengruppe aus. Klicken Sie auf Delete (Löschen), geben Sie den Namen der Knotengruppe ein und wählen Sie anschließend Delete (Löschen) aus. Alle Knotengruppen im Cluster löschen.

**Note**

Die aufgelisteten Knotengruppen sind nur [verwaltete Knotengruppen](#).

- d. Wählen Sie ein zu löschendes Fargate-Profil aus, wählen Sie Delete (Löschen) aus, geben Sie den Namen des Profils ein und wählen Sie dann Delete (Löschen). Alle Fargate-Profile im Cluster löschen.
4. Löschen Sie alle selbstverwalteten AWS CloudFormation Knotenstapel.
 - a. Öffnen Sie die [AWS CloudFormation -Konsole](#).
 - b. Wählen Sie den Knoten-Stack aus, den Sie löschen möchten, und wählen Sie Delete (Löschen) aus.
 - c. Wählen Sie im Bestätigungsdialogfeld Stack löschen Stack löschen aus. Löschen Sie alle selbstverwalteten Knoten-Stacks im Cluster.
5. Löschen Sie den Cluster.
 - a. Öffnen Sie die [Amazon-EKS-Konsole](#).
 - b. Wählen Sie den Cluster aus, der gelöscht werden soll, und klicken Sie auf Delete (Löschen).
 - c. Klicken Sie auf dem Bestätigungsbildschirm zum Löschen des Clusters auf Delete (Löschen).
6. (Optional) Löschen Sie den AWS CloudFormation VPC-Stack.
 - a. Öffnen Sie die [AWS CloudFormation -Konsole](#).

- b. Wählen Sie den zu löschenden VPC-Stack und dann Löschen aus.
- c. Wählen Sie im Bestätigungsdialogfeld Stack löschen Stack löschen aus.

Cluster löschen (AWS CLI)

1. Listen Sie alle in Ihrem Cluster ausgeführten Services auf.

```
kubectl get svc --all-namespaces
```

2. Löschen Sie alle Services, die dem Wert EXTERNAL-IP zugeordnet sind. Diese Services werden hinter einem Elastic-Load-Balancing-Load-Balancer ausgeführt und müssen in Kubernetes gelöscht werden, damit der Load Balancer und die zugeordneten Ressourcen korrekt freigegeben werden können. *service-name* Ersetzen Sie es durch den Namen der einzelnen Dienste, die wie beschrieben aufgeführt sind.

```
kubectl delete svc service-name
```

3. Alle Knotengruppen und Fargate-Profil löschen.

- a. Listen Sie die Knotengruppen in Ihrem Cluster mit dem folgenden Befehl auf.

```
aws eks list-nodegroups --cluster-name my-cluster
```

Note

Die aufgelisteten Knotengruppen sind nur [verwaltete Knotengruppen](#).

- b. Löschen Sie jede Knotengruppe mit folgendem Befehl. Alle Knotengruppen im Cluster löschen.

```
aws eks delete-nodegroup --nodegroup-name my-nodegroup --cluster-name my-cluster
```

- c. Listen Sie die Fargate-Profil in Ihrem Cluster mit dem folgenden Befehl auf.

```
aws eks list-fargate-profiles --cluster-name my-cluster
```

- d. Löschen Sie jedes Fargate-Profil mit dem folgenden Befehl. Alle Fargate-Profil im Cluster löschen.

```
aws eks delete-fargate-profile --fargate-profile-name my-fargate-profile --  
cluster-name my-cluster
```

4. Löschen Sie alle selbstverwalteten AWS CloudFormation Knotenstapel.

- a. Listen Sie Ihre verfügbaren AWS CloudFormation Stacks mit dem folgenden Befehl auf. Suchen Sie den Vorlagennamen des Knotens in der sich daraus ergebenden Ausgabe.

```
aws cloudformation list-stacks --query "StackSummaries[].StackName"
```

- b. Löschen Sie jeden Knoten-Stack mit dem folgenden Befehl und ersetzen Sie dabei *node-stack* durch den Namen Ihres Knoten-Stacks. Löschen Sie alle selbstverwalteten Knoten-Stacks im Cluster.

```
aws cloudformation delete-stack --stack-name node-stack
```

5. Löschen Sie den Cluster mit dem folgenden Befehl und ersetzen Sie dabei *my-cluster* durch den Namen Ihres Clusters.

```
aws eks delete-cluster --name my-cluster
```

6. (Optional) Löschen Sie den AWS CloudFormation VPC-Stack.

- a. Listen Sie Ihre verfügbaren AWS CloudFormation Stacks mit dem folgenden Befehl auf. Suchen Sie die VPC-Vorlage in der sich daraus ergebenden Ausgabe.

```
aws cloudformation list-stacks --query "StackSummaries[].StackName"
```

- b. Löschen Sie den VPC-Stack mit dem folgenden Befehl und ersetzen Sie dabei *my-vpc-stack* durch den Namen Ihres VPC-Stacks.

```
aws cloudformation delete-stack --stack-name my-vpc-stack
```

Cluster-API-Serverendpunkt

In diesem Thema können Sie den privaten Zugriff für den Kubernetes-API-Serverendpunkt Ihres Amazon EKS-Clusters aktivieren und den öffentlichen Zugriff über das Internet einschränken oder vollständig deaktivieren.

Wenn Sie einen neuen Cluster erstellen, erstellt Amazon EKS einen Endpunkt für den verwalteten Kubernetes-API-Server, über den Sie mit Ihrem Cluster kommunizieren (mit Kubernetes-Verwaltungswerkzeugen wie `kubectl`). Standardmäßig ist dieser API-Serverendpunkt im Internet öffentlich, und der Zugriff auf den API-Server wird mithilfe einer Kombination aus AWS Identity and Access Management (IAM) und nativer Kubernetes [Role Based Access Control](#) (RBAC) gesichert. Dieser Endpunkt wird als öffentlicher Cluster-Endpunkt bezeichnet. Außerdem gibt es einen privaten Cluster-Endpunkt. Weitere Informationen zum privaten Cluster-Endpunkt finden Sie im folgenden Abschnitt [the section called “Privater Cluster-Endpunkt”](#).

IPv6Format des Cluster-Endpunkts

EKS erstellt einen eindeutigen Dual-Stack-Endpunkt im folgenden Format für neue IPv6 Cluster, die nach Oktober 2024 erstellt wurden. Ein IPv6 Cluster ist ein Cluster, den Sie IPv6 in der IP-Familie (ipFamily) -Einstellung des Clusters auswählen.

Example

AWS

Öffentlicher/privater Endpunkt des EKS-Clusters: `eks-cluster.region.api.aws`

AWS GovCloud (US)

Öffentlicher/privater Endpunkt des EKS-Clusters: `eks-cluster.region.api.aws`

Amazon Web Services in China

Öffentlicher/privater Endpunkt des EKS-Clusters: `eks-cluster.region.api.amazonwebservices.com.cn`

Note

Der Dual-Stack-Cluster-Endpunkt wurde im Oktober 2024 eingeführt. Weitere Informationen zu IPv6 Clustern finden Sie unter [the section called “IPv6”](#). Cluster, die vor Oktober 2024 erstellt wurden, verwenden stattdessen das folgende Endpunktformat.

IPv4Cluster-Endpunktformat

EKS erstellt für jeden Cluster, der in der Einstellung IP-Familie (IPFamily) des Clusters ausgewählt wird, einen eindeutigen Endpunkt IPv4 im folgenden Format:

Example

AWS

Öffentlicher/privater Endpunkt des EKS-Clusters `eks-cluster.region.eks.amazonaws.com`

AWS GovCloud (US)

Öffentlicher/privater Endpunkt des EKS-Clusters `eks-cluster.region.eks.amazonaws.com`

Amazon Web Services in China

Öffentlicher/privater Endpunkt des EKS-Clusters `eks-cluster.region.amazonwebservices.com.cn`

Note

Vor Oktober 2024 verwendeten IPv6 Cluster dieses Endpunktformat ebenfalls. Bei diesen Clustern haben sowohl der öffentliche als auch der private Endpunkt nur IPv4 Adressen, die von diesem Endpunkt aus aufgelöst wurden.

Privater Cluster-Endpunkt

Sie können den privaten Zugriff auf den Kubernetes-API-Server aktivieren, sodass die gesamte Kommunikation zwischen Ihren Knoten und dem API-Server innerhalb Ihrer VPC bleibt. Sie können die IP-Adressen einschränken, die über das Internet auf Ihren API-Server zugreifen können, oder den Internetzugriff auf den API-Server vollständig deaktivieren.

Note

Da dieser Endpunkt für den Kubernetes-API-Server und kein herkömmlicher AWS PrivateLink Endpunkt für die Kommunikation mit einer AWS API ist, wird er in der Amazon VPC-Konsole nicht als Endpunkt angezeigt.

Wenn Sie privaten Endpunktzugriff für Ihren Cluster aktivieren, erstellt Amazon EKS in Ihrem Namen eine private gehostete Route 53-Zone und ordnet sie der VPC Ihres Clusters zu. Diese privat gehostete Zone wird von Amazon EKS verwaltet und erscheint nicht in den Route 53-Ressourcen

Ihres Kontos. Damit die private gehostete Zone Datenverkehr ordnungsgemäß an Ihren API-Server weiterleiten kann, müssen `enableDnsHostnames` und `enableDnsSupport` für Ihre VPC auf `true` gesetzt sein und die DHCP-Optionen für Ihre VPC müssen `AmazonProvidedDNS` in ihrer Domainnamen-Serverliste enthalten. Weitere Informationen finden Sie unter [Aktualisieren der DNS-Unterstützung für Ihre VPC](#) im Amazon-VPC-Benutzerhandbuch.

Sie können Ihre Anforderungen für den Zugriff auf Ihre API-Server-Endpunkte definieren, wenn Sie einen neuen Cluster erstellen. Sie können den Zugriff auf die API-Server-Endpunkte für einen Cluster jederzeit aktualisieren.

Ändern des Cluster-Endpunktzugriffs

Verwenden Sie die Verfahren in diesem Abschnitt, um den Endpunktzugriff für einen bestehenden Cluster zu ändern. Die folgende Tabelle zeigt die unterstützten Kombinationen von API-Server-Endpunktzugriffen und das damit verbundene Verhalten.

Endpunkt für öffentlichen Zugriff	Endpunkt für privaten Zugriff	Behavior
Enabled	Disabled	• Dies ist das Standardverhalten für neue Amazon-EKS-Cluster. • Kubernetes-API-Anfragen, die aus der VPC Ihres Clusters stammen (z. B. die Kommunikation zwischen Knoten und Kontrollebene), verlassen die VPC, aber nicht das Amazon-Netzwerk. • Ihr Cluster-API-Server ist über das Internet erreichbar. Optional können Sie die CIDR-Blöcke einschränken, die auf den öffentlichen Endpunkt zugreifen können. Wenn Sie den Zugriff auf bestimmte CIDR-Blöcke beschränken, wird empfohlen, auch den privaten Endpunkt zu aktivieren oder sicherzustellen, dass die von Ihnen angegebenen CIDR-Blöcke die Adressen enthalten, von denen Knoten und Fargate-Pods (falls Sie sie verwenden) auf den öffentlichen Endpunkt zugreifen.

Endpunkt für öffentlichen Zugriff	Endpunkt für privaten Zugriff	Behavior
Enabled	Aktiviert	• Kubernetes-API-Anfragen innerhalb der VPC Ihres Clusters (z. B. Kommunikation zwischen Knoten und Kontrollebene) verwenden den privaten VPC-Endpunkt. • Ihr Cluster-API-Server ist über das Internet erreichbar. Optional können Sie die CIDR-Blöcke einschränken, die auf den öffentlichen Endpunkt zugreifen können. • Wenn Sie Hybridknoten mit Ihrem Amazon EKS-Cluster verwenden, wird nicht empfohlen, sowohl den öffentlichen als auch den privaten Cluster-Endpunktzugriff zu aktivieren. Da Ihre Hybridknoten außerhalb Ihrer VPC laufen, lösen sie den Cluster-Endpunkt in die öffentlichen IP-Adressen auf. Es wird empfohlen, für Cluster mit Hybridknoten entweder den öffentlichen oder den privaten Cluster-Endpunktzugriff zu verwenden.

Endpunkt für öffentlichen Zugriff	Endpunkt für privaten Zugriff	Behavior
Disabled	Aktiviert	- Der gesamte Datenverkehr zu Ihrem Cluster-API-Server muss aus der VPC Ihres Clusters oder einem verbundenen Netzwerk stammen. - Es gibt keinen öffentlichen Zugriff auf Ihren API-Server aus dem Internet. Alle <code>kubectl</code>-Befehle müssen aus der VPC oder einem verbundenen Netzwerk stammen. Die Verbindungsoptionen finden Sie unter the section called “Zugriff auf einen privaten API-Server”. - Der API-Serverendpunkt des Clusters wird von öffentlichen DNS-Servern in eine private IP-Adresse von der VPC aufgelöst. In der Vergangenheit konnte der Endpunkt nur innerhalb der VPC aufgelöst werden. Wenn Ihr Endpunkt nicht in eine private IP-Adresse innerhalb der VPC für einen vorhandenen Cluster aufgelöst wird, können Sie: - Den öffentlichen Zugriff aktivieren und ihn dann erneut deaktivieren. Sie müssen dies nur einmal für einen Cluster tun und der Endpunkt wird von diesem Punkt an zu einer privaten IP-Adresse aufgelöst. Aktualisieren Sie Ihren Cluster.

CIDR-Blöcke im öffentlichen Endpunkt (Cluster) **IPv6**

Sie können IPv4 CIDR-Blöcke zum öffentlichen Endpunkt eines IPv6 Clusters hinzufügen IPv6, da es sich bei dem öffentlichen Endpunkt um einen Dual-Stack-Endpunkt handelt. Dies gilt nur für neue Cluster mit der `ipFamily` Einstellung IPv6, die Sie im Oktober 2024 oder später vorgenommen haben. Sie können diese Cluster anhand des neuen Endpunktdomännennamens identifizieren `api.aws`.

CIDR-Blöcke auf dem öffentlichen Endpunkt (**IPv4** Cluster)

Sie können IPv4 CIDR-Blöcke zum öffentlichen Endpunkt eines IPv4 Clusters hinzufügen. Sie können dem öffentlichen Endpunkt eines Clusters keine IPv6 CIDR-Blöcke hinzufügen. IPv4 Wenn Sie es versuchen, gibt EKS die folgende Fehlermeldung zurück: `The following CIDRs are invalid in publicAccessCidrs`

CIDR-Blöcke auf dem öffentlichen Endpunkt (**IPv6**Cluster, der vor Oktober 2024 erstellt wurde)

Sie können IPv4 CIDR-Blöcke zum öffentlichen Endpunkt der alten IPv6 Cluster hinzufügen, die Sie vor Oktober 2024 erstellt haben. Sie können diese Cluster anhand des `eks.amazonaws.com` Endpunkts identifizieren. Sie können dem öffentlichen Endpunkt dieser alten IPv6 Cluster, die Sie vor Oktober 2024 erstellt haben, keine IPv6 CIDR-Blöcke hinzufügen. Wenn Sie es versuchen, gibt EKS die folgende Fehlermeldung zurück: `The following CIDRs are invalid in publicAccessCidrs`

Zugriff auf einen privaten API-Server

Wenn Sie den öffentlichen Zugriff für den Kubernetes-API-Serverendpunkt Ihres Clusters deaktiviert haben, können Sie nur von Ihrer VPC oder einem verbundenen Netzwerk aus auf den API-Server zugreifen. Hier sind einige Möglichkeiten, um auf den Kubernetes-API-Server-Endpunkt zuzugreifen:

Verbundenes Netzwerk

Verbinden Sie Ihr Netzwerk über ein [AWS -Transit-Gateway](#) oder eine andere [Konnektivitätsoption](#) mit der VPC und verwenden Sie dann einen Computer im verbundenen Netzwerk. Sie müssen sicherstellen, dass Ihre Amazon-EKS-Steuerebenen-Sicherheitsgruppe Regeln enthält, die den eingehenden Datenverkehr auf Port 443 von Ihrem verbundenen Netzwerk zulassen.

Gastgeber bei Amazon EC2 Bastion

Sie können eine EC2 Amazon-Instance in einem öffentlichen Subnetz in der VPC Ihres Clusters starten und sich dann über SSH bei dieser Instance anmelden, um Befehle auszuführen. `kubectl` Weitere Informationen finden Sie unter [Linux-Bastion-Hosts in AWS](#). Sie müssen sicherstellen, dass Ihre Amazon-EKS-Steuerebenen-Sicherheitsgruppe Regeln enthält, die den eingehenden Datenverkehr auf Port 443 von Ihrem Bastion-Host zulassen. Weitere Informationen finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#).

Achten Sie bei der Konfiguration `kubectl` für Ihren Bastion-Host darauf, AWS Anmeldeinformationen zu verwenden, die bereits der RBAC-Konfiguration Ihres Clusters

zugeordnet sind, oder fügen Sie den [IAM-Prinzipal](#), den Ihre Bastion verwendet wird, zur RBAC-Konfiguration hinzu, bevor Sie den öffentlichen Zugriff auf Endgeräte entfernen. Weitere Informationen erhalten Sie unter [the section called “Kubernetes-API-Zugriff”](#) und [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#).

AWS Cloud9 IDE

AWS Cloud9 ist eine cloudbasierte integrierte Entwicklungsumgebung (IDE), mit der Sie Ihren Code mit nur einem Browser schreiben, ausführen und debuggen können. Sie können eine AWS Cloud9-IDE in der VPC Ihres Clusters erstellen und die IDE für die Kommunikation mit Ihrem Cluster verwenden. Weitere Informationen finden Sie unter [Umgebung in AWS Cloud9 erstellen](#). Sie müssen sicherstellen, dass Ihre Amazon-EKS-Steuerebenen-Sicherheitsgruppe Regeln enthält, die den eingehenden Datenverkehr auf Port 443 von Ihrer IDE-Sicherheitsgruppe zulassen. Weitere Informationen finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#).

Achten Sie bei der Konfiguration `kubectl` für Ihre AWS Cloud9-IDE darauf, AWS Anmeldeinformationen zu verwenden, die bereits der RBAC-Konfiguration Ihres Clusters zugeordnet sind, oder fügen Sie den IAM-Prinzipal, den Ihre IDE verwendet wird, zur RBAC-Konfiguration hinzu, bevor Sie den öffentlichen Endpunktzugriff entfernen. Weitere Informationen erhalten Sie unter [the section called “Kubernetes-API-Zugriff”](#) und [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#).

[# Bearbeiten Sie diese Seite auf GitHub](#)

Netzwerkzugriff auf den Cluster-API-Serverendpunkt konfigurieren

Sie können den Endpunktzugriff Ihres Cluster-API-Servers mithilfe der AWS Management Console oder AWS CLI in den folgenden Abschnitten ändern.

Konfigurieren Sie den Endpunktzugriff — AWS Konsole

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, um Ihre Cluster-Informationen anzuzeigen.
3. Wählen Sie die Registerkarte Netzwerk und dann Endpunktzugriff verwalten aus.
4. Wählen Sie für den privaten Zugriff aus, ob Sie den privaten Zugriff für den Kubernetes API-Serverendpunkt Ihres Clusters aktivieren oder deaktivieren möchten. Wenn Sie privaten Zugriff aktivieren, verwenden Kubernetes API-Anfragen, die aus der VPC Ihres Clusters stammen, den

- privaten VPC-Endpunkt. Sie müssen den privaten Zugriff aktivieren, um den öffentlichen Zugriff zu deaktivieren.
5. Wählen Sie für den öffentlichen Zugriff aus, ob Sie den öffentlichen Zugriff für den Kubernetes API-Serverendpunkt Ihres Clusters aktivieren oder deaktivieren möchten. Wenn Sie den öffentlichen Zugriff deaktivieren, kann der Kubernetes API-Server Ihres Clusters nur Anfragen aus der Cluster-VPC empfangen.
 6. (Optional) Wenn Sie den öffentlichen Zugriff aktiviert haben, können Sie angeben, welche Adressen aus dem Internet mit dem öffentlichen Endpunkt kommunizieren können. Wählen Sie Erweiterte Einstellungen aus. Geben Sie einen CIDR-Block ein, z. B. **203.0.113.5/32**. Der Block darf keine [reservierten Adressen](#) enthalten. Sie können zusätzliche Blöcke eingeben, indem Sie Quelle hinzufügen auswählen. Es gibt eine maximale Anzahl von CIDR-Blöcken, die Sie angeben können. Weitere Informationen finden Sie unter [the section called "Servicekontingente"](#). Wenn Sie keine Blöcke angeben, empfängt der öffentliche API-Serverendpunkt Anfragen von allen IP-Adressen sowohl für () als auch zusätzlich IPv4 IPv6 (0.0.0.0/0::/0) für IPv6 Dual-Stack-Cluster. Wenn Sie den Zugriff auf Ihren öffentlichen Endpunkt mithilfe von CIDR-Blöcken einschränken, empfehlen wir Ihnen, auch den privaten Endpunktzugriff zu aktivieren, damit Knoten und Fargate Pods (falls Sie sie verwenden) mit dem Cluster kommunizieren können. Wenn der private Endpunkt nicht aktiviert ist, müssen die CIDR-Quellen des öffentlichen Zugriffs die Ausgangsquellen aus Ihrer VPC enthalten. Wenn Sie beispielsweise einen Knoten in einem privaten Subnetz haben, der über ein NAT-Gateway mit dem Internet kommuniziert, müssen Sie die ausgehende IP-Adresse des NAT-Gateways als Teil eines erlaubten CIDR-Blocks auf Ihrem öffentlichen Endpunkt hinzufügen.
 7. Wählen Sie zum Abschluss Update (Aktualisieren) aus.

Endpunktzugriff konfigurieren — AWS CLI

Führen Sie die folgenden Schritte mit der AWS CLI-Version 1.27.160 oder höher aus. Sie können Ihre aktuelle Version mit `aws --version` überprüfen. Informationen zur Installation oder zum Upgrade der AWS CLI finden Sie unter [AWS CLI installieren](#).

1. Aktualisieren Sie den Endpunktzugriff Ihres Cluster-API-Servers mit dem folgenden AWS CLI-Befehl. Verwenden Ihre eigenen Werte für den Clusternamen und den gewünschten Endpunkt. Wenn Sie `endpointPublicAccess=true` festlegen, können Sie (optional) einen einzelnen CIDR-Block oder eine kommagetrennte Liste von CIDR-Blöcken für `publicAccessCidrs` eingeben. Die Blöcke dürfen keine [reservierten Adressen](#) enthalten. Wenn Sie CIDR-Blöcke angeben, empfängt der öffentliche API-Server-Endpunkt nur Anforderungen von den aufgelisteten

Blöcken. Es gibt eine maximale Anzahl von CIDR-Blöcken, die Sie angeben können. Weitere Informationen finden Sie unter [the section called "Servicekontingente"](#). Wenn Sie den Zugriff auf Ihren öffentlichen Endpunkt mithilfe von CIDR-Blöcken einschränken, wird empfohlen, dass Sie auch den privaten Endpunktzugriff aktivieren, damit Knoten und Fargate-Pods (falls Sie diese verwenden) mit dem Cluster kommunizieren können. Wenn der private Endpunkt nicht aktiviert ist, müssen die CIDR-Quellen des öffentlichen Zugriffs die Ausgangsquellen aus Ihrer VPC enthalten. Wenn Sie beispielsweise einen Knoten in einem privaten Subnetz haben, der über ein NAT-Gateway mit dem Internet kommuniziert, müssen Sie die ausgehende IP-Adresse des NAT-Gateways als Teil eines erlaubten CIDR-Blocks auf Ihrem öffentlichen Endpunkt hinzufügen. Wenn Sie keine CIDR-Blöcke angeben, empfängt der öffentliche API-Serverendpunkt Anfragen von allen (0.0.0.0/0) IP-Adressen und zusätzlich IPv6 (:::/0) für Dual-Stack-Cluster. IPv6

Note

Der folgende Befehl ermöglicht den privaten Zugriff und den öffentlichen Zugriff von einer einzelnen IP-Adresse für den API-Server-Endpunkt. Ersetzen Sie **203.0.113.5/32** durch einen einzelnen CIDR-Block oder eine kommasetrennte Liste von CIDR-Blöcken, auf die Sie den Netzwerkzugriff beschränken möchten.

```
aws eks update-cluster-config \
  --region region-code \
  --name my-cluster \
  --resources-vpc-config
endpointPublicAccess=true,publicAccessCidrs="203.0.113.5/32",endpointPrivateAccess=true
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "update": {
    "id": "e6f0905f-a5d4-4a2a-8c49-EXAMPLE000000",
    "status": "InProgress",
    "type": "EndpointAccessUpdate",
    "params": [
      {
        "type": "EndpointPublicAccess",
        "value": "true"
      },
      {

```

```

        "type": "EndpointPrivateAccess",
        "value": "true"
    },
    {
        "type": "publicAccessCidrs",
        "value": "[\"203.0.113.5/32\"]"
    }
],
"createdAt": 1576874258.137,
"errors": []
}
}

```

2. Überwachen Sie den Status des aktualisierten Endpunktzugriffs mit dem folgenden Befehl unter Verwendung des Cluster-Namens und der Update-ID, die vom vorherigen Befehl zurückgegeben wurden. Ihre Aktualisierung ist abgeschlossen, wenn als Status `Successful` angezeigt wird.

```

aws eks describe-update \
  --region region-code \
  --name my-cluster \
  --update-id e6f0905f-a5d4-4a2a-8c49-EXAMPLE000000

```

Eine Beispielausgabe sieht wie folgt aus.

```

{
  "update": {
    "id": "e6f0905f-a5d4-4a2a-8c49-EXAMPLE000000",
    "status": "Successful",
    "type": "EndpointAccessUpdate",
    "params": [
      {
        "type": "EndpointPublicAccess",
        "value": "true"
      },
      {
        "type": "EndpointPrivateAccess",
        "value": "true"
      },
      {
        "type": "publicAccessCidrs",
        "value": "[\"203.0.113.5/32\"]"
      }
    ]
  }
}

```

```
    ],  
    "createdAt": 1576874258.137,  
    "errors": []  
  }  
}
```

[# Bearbeiten Sie diese Seite auf GitHub](#)

Stellen Sie Windows-Knoten auf EKS-Clustern bereit

Erfahren Sie, wie Sie die Windows-Unterstützung für Ihren Amazon EKS-Cluster aktivieren und verwalten, um Windows-Container zusammen mit Linux-Containern auszuführen.

Überlegungen

Beachten Sie vor der Bereitstellung von Windows-Knoten die folgenden Überlegungen.

- Der automatische Modus von EKS unterstützt keine Windows-Knoten
- Sie können Host-Netzwerke auf Windows-Knoten mithilfe von HostProcess-Pods verwenden. Weitere Informationen finden Sie HostProcessPod in der Kubernetes-Dokumentation unter [Create a Windows](#).
- Amazon EKS-Cluster müssen einen oder mehrere Linux- oder Fargate-Knoten enthalten, um Kernsystem-Pods ausführen zu können, die nur unter Linux laufen, wie CoreDNS.
- Die kubelet kube-proxy Ereignisprotokolle werden in das EKS Windows Ereignisprotokoll umgeleitet und sind auf ein Limit von 200 MB festgelegt.
- Sie können nicht dieselbe IAM-Rolle sowohl für Linux- als auch für Windows-Knoten verwenden.
- Sie können die Option [Sicherheitsgruppen einzelnen Pods zuweisen nicht verwenden](#), wenn Pods auf Windows-Knoten ausgeführt werden.
- Sie können [benutzerdefinierte Netzwerke](#) nicht mit Windows-Knoten verwenden.
- Sie können es nicht IPv6 mit Windows-Knoten verwenden.
- Windows-Knoten unterstützen eine Elastic-Network-Schnittstelle pro Knoten. Standardmäßig entspricht die Anzahl der Pods, die Sie pro Windows-Knoten ausführen können, der Anzahl der IP-Adressen, die pro elastic network interface für den Instance-Typ des Knotens verfügbar sind, minus eins. Weitere Informationen finden Sie unter [IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ](#) im EC2 Amazon-Benutzerhandbuch.

- In einem Amazon EKS-Cluster kann ein einzelner Service mit einem Load Balancer bis zu 1024 Back-End-Pods unterstützen. Jeder Pod hat seine eigene eindeutige IP-Adresse. Das bisherige Limit von 64 Pods ist nach [einem Windows Server-Update](#), das mit [OS Build](#) 17763.2746 beginnt, nicht mehr der Fall.
- Windows-Container werden für Amazon EKS-Pods auf Fargate nicht unterstützt.
- Sie können Amazon EKS Hybrid Nodes nicht mit Windows als Betriebssystem für den Host verwenden.
- Sie können keine Protokolle vom `vpc-resource-controller` Pod abrufen. Dies war zuvor möglich, als Sie den Controller auf der Datenebene bereitgestellt haben.
- Es gibt eine Abkühlungsphase, bevor einem neuen Pod eine IPv4-Adresse zugewiesen wird. Dadurch wird verhindert, dass Datenverkehr aufgrund veralteter IPv4-Regeln an einen älteren Pod mit derselben `kube-proxy`-Adresse fließt.
- Die Quelle für den Controller wird auf verwaltet GitHub. Wenn Sie zum Controller beitragen oder Probleme gegen den Controller einreichen möchten, besuchen Sie das [Projekt](#) unter GitHub.
- Wenn Sie eine benutzerdefinierte AMI-ID für von Windows verwaltete Knotengruppen angeben, fügen Sie `eks:kube-proxy-windows` diese Ihrer AWS IAM Authenticator-Konfigurationsübersicht hinzu. Weitere Informationen finden Sie unter [the section called “Grenzen und Bedingungen bei der Angabe einer AMI-ID”](#).
- Wenn die Beibehaltung Ihrer verfügbaren IPv4 Adressen für Ihr Subnetz von entscheidender Bedeutung ist, finden Sie weitere Informationen im [EKS Best Practices Guide — Windows Networking IP Address Management](#).
- Überlegungen zu EKS Access-Einträgen
 - Zugriffseinträge für die Verwendung mit Windows-Knoten benötigen den Typ `vonEC2_WINDOWS`. Weitere Informationen finden Sie unter [the section called “Zugangseinträge erstellen”](#).

Um einen Zugriffseintrag für einen Windows-Knoten zu erstellen:

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/<role-name> --type EC2_Windows
```

Voraussetzungen

- Einen vorhandenen -Cluster.

- Ihr Cluster muss mindestens einen (wir empfehlen mindestens zwei) Linux-Knoten oder Fargate-Pod haben, um CoreDNS ausführen zu können. Wenn Sie die ältere Windows-Unterstützung aktivieren, müssen Sie einen Linux-Knoten verwenden (Sie können keinen Fargate-Pod verwenden), um CoreDNS auszuführen.
- Eine bestehende [Amazon EKS-Cluster-IAM-Rolle](#).

Aktivieren Sie die Windows-Unterstützung

1. Wenn Sie keine Amazon Linux-Knoten in Ihrem Cluster haben und Sicherheitsgruppen für Pods verwenden, fahren Sie mit dem nächsten Schritt fort. Ansonsten bestätigen Sie, dass die verwaltete Richtlinie AmazonEKSVPCResourceController Ihrer [Cluster-Rolle](#) angefügt ist. Ersetzen Sie den *eksClusterRole* durch Ihren Clusterrollennamen.

```
aws iam list-attached-role-policies --role-name eksClusterRole
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "AttachedPolicies": [
    {
      "PolicyName": "AmazonEKSClusterPolicy",
      "PolicyArn": "arn:aws: iam::aws:policy/AmazonEKSClusterPolicy"
    },
    {
      "PolicyName": "AmazonEKSVPCResourceController",
      "PolicyArn": "arn:aws: iam::aws:policy/AmazonEKSVPCResourceController"
    }
  ]
}
```

Wenn die Richtlinie wie in der vorherigen Ausgabe angehängt ist, überspringen Sie den nächsten Schritt.

2. Fügen Sie die von [Amazon EKSVPCResource Controller](#) verwaltete Richtlinie Ihrer [Amazon EKS-Cluster-IAM-Rolle](#) hinzu. Ersetzen Sie den *eksClusterRole* durch Ihren Clusterrollennamen.

```
aws iam attach-role-policy \
  --role-name eksClusterRole \
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSVPCResourceController
```

3. Aktualisieren Sie das VPC-CNI, um Windows ConfigMap IPAM zu aktivieren. Hinweis: Wenn das VPC-CNI mithilfe eines Helm-Charts oder als Amazon EKS-Add-on auf Ihrem Cluster installiert ist, können Sie das möglicherweise nicht direkt ändern. ConfigMap Informationen zur Konfiguration von Amazon EKS Add-ons finden Sie unter [the section called “Felder, die Sie anpassen können”](#).

- a. Erstellen Sie eine Datei mit dem Namen *vpc-resource-controller-configmap.yaml* und dem folgenden Inhalt.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: amazon-vpc-cni
  namespace: kube-system
data:
  enable-windows-ipam: "true"
```

- b. Anwendung der ConfigMap auf Ihren Cluster.

```
kubectl apply -f vpc-resource-controller-configmap.yaml
```

4. Wenn in Ihrem Cluster der Authentifizierungsmodus so eingestellt ist, dass er die aws-auth Configmap aktiviert:

- Stellen Sie sicher, dass Sie aws-auth ConfigMap eine Zuordnung für die Instanzrolle des Windows-Knotens enthalten, die die eks:kube-proxy-windows RBAC-Berechtigungsgruppe einschließt. Prüfen Sie dies durch Ausführung des folgenden Befehls.

```
kubectl get configmap aws-auth -n kube-system -o yaml
```

Eine Beispielausgabe sieht wie folgt aus.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: aws-auth
  namespace: kube-system
data:
  mapRoles: |
    - groups:
      - system:bootstrappers
      - system:nodes
```



```
- eks:kube-proxy-windows # This group is required for Windows DNS resolution
to work
  rolearn: arn:aws:iam::111122223333:role/eksNodeRole
  username: system:node:{{EC2PrivateDNSName}}
[...]
```

eks:kube-proxy-windows sollte unter „Gruppen“ aufgelistet sein. Wenn die Gruppe nicht angegeben ist, müssen Sie Ihre Gruppe aktualisieren ConfigMap oder sie so erstellen, dass sie die erforderliche Gruppe enthält. Weitere Informationen zur aws-auth ConfigMap finden Sie unter [the section called “Anwenden von aws-authConfigMap auf Ihren Cluster”](#).

5. Wenn in Ihrem Cluster der Authentifizierungsmodus so eingestellt ist, dass er die aws-auth Configmap deaktiviert, können Sie EKS Access Entries verwenden. Erstellen Sie eine neue Knotenrolle für die Verwendung mit Windows-Instanzen, und EKS erstellt automatisch einen Zugriffseintrag vom TypEC2_WINDOWS.

Stellen Sie Windows-Pods bereit

Wenn Sie Pods in Ihrem Cluster bereitstellen, müssen Sie das Betriebssystem angeben, das sie verwenden, wenn Sie eine Mischung aus verschiedenen Knotentypen ausführen.

Verwenden Sie für Linux-Pods den folgenden Text zur Knotenauswahl in Ihren Manifesten.

```
nodeSelector:
  kubernetes.io/os: linux
  kubernetes.io/arch: amd64
```

Verwenden Sie für Windows-Pods den folgenden Knotenauswahltext in Ihren Manifesten.

```
nodeSelector:
  kubernetes.io/os: windows
  kubernetes.io/arch: amd64
```

Sie können eine [Beispielanwendung](#) bereitstellen, um die verwendeten Knotenselektoren zu sehen.

Support eine höhere Pod-Dichte auf Windows-Knoten

In Amazon EKS wird jedem Pod eine IPv4 Adresse aus Ihrer VPC zugewiesen. Aus diesem Grund ist die Anzahl der Pods, die Sie auf einem Knoten bereitstellen können, durch die verfügbaren IP-

Adressen begrenzt, auch wenn genügend Ressourcen vorhanden sind, um mehr Pods auf dem Knoten auszuführen. Da von einem Windows-Knoten nur eine elastische Netzwerkschnittstelle unterstützt wird, entspricht die maximale Anzahl verfügbarer IP-Adressen auf einem Windows-Knoten standardmäßig:

```
Number of private IPv4 addresses for each interface on the node - 1
```

Eine IP-Adresse wird als primäre IP-Adresse der Netzwerkschnittstelle verwendet, sodass sie Pods nicht zugewiesen werden kann.

Sie können eine höhere Pod-Dichte auf Windows-Knoten aktivieren, indem Sie die IP-Präfix-Delegierung aktivieren. Mit diesem Feature können Sie der primären Netzwerkschnittstelle ein /28-IPv4-Präfix zuweisen, anstatt sekundäre IPv4-Adressen zuzuweisen. Durch die Zuweisung eines IP-Präfixes wird die maximale Anzahl verfügbarer IPv4-Adressen auf dem Knoten auf Folgendes erhöht:

```
(Number of private IPv4 addresses assigned to the interface attached to the node - 1) *  
16
```

Bei dieser deutlich größeren Anzahl verfügbarer IP-Adressen sollten die verfügbaren IP-Adressen Ihre Fähigkeit, die Anzahl der Pods auf Ihren Knoten zu skalieren, nicht einschränken. Weitere Informationen finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#).

Windows-Unterstützung deaktivieren

1. Wenn Ihr Cluster Amazon Linux-Knoten enthält und Sie mit ihnen [Sicherheitsgruppen für Pods](#) verwenden, überspringen Sie diesen Schritt.

Entfernen Sie die AmazonVPCResourceController-verwaltete IAM-Richtlinie von Ihrer [Cluster-Rolle](#). `eksClusterRole` Ersetzen Sie es durch den Namen Ihrer Clusterrolle.

```
aws iam detach-role-policy \  
  --role-name eksClusterRole \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSVPCResourceController
```

2. Deaktivieren Sie Windows IPAM in der amazon-vpc-cni ConfigMap.

```
kubectl patch configmap/amazon-vpc-cni \  
  -n kube-system \  
  --type Merge
```

```
--type merge \  
-p '{"data":{"enable-windows-ipam":"false"}}'
```

Stellen Sie private Cluster mit eingeschränktem Internetzugang bereit

In diesem Thema wird beschrieben, wie Sie einen Amazon EKS-Cluster bereitstellen, der in der AWS Cloud bereitgestellt wird, aber keinen ausgehenden Internetzugang hat. Wenn Sie einen lokalen Cluster auf AWS Outposts haben [the section called “Knoten”](#), finden Sie statt dieses Themas weitere Informationen unter.

Wenn Sie mit Amazon EKS-Netzwerken nicht vertraut sind, finden Sie weitere Informationen unter [Entmystifying Cluster Networking for Amazon EKS Worker Nodes](#). Wenn Ihr Cluster keinen ausgehenden Internetzugang hat, muss er die folgenden Anforderungen erfüllen:

- Ihr Cluster muss Images aus einer Container-Registry abrufen, die sich in Ihrer VPC befindet. Sie können eine Amazon Elastic Container Registry in Ihrer VPC erstellen und Container-Images dorthin kopieren, damit Ihre Knoten daraus abrufen können. Weitere Informationen finden Sie unter [the section called “Kopieren eines Images in ein Repository”](#).
- In Ihrem Cluster muss der private Endpunkt-Zugriff aktiviert sein. Dies ist erforderlich, damit sich Knoten beim Cluster-Endpoint registrieren können. Der Endpoint für öffentlichen Zugriff ist optional. Weitere Informationen finden Sie unter [the section called “Cluster-Endpointzugriff”](#).
- Selbstverwaltete Linux- und Windows-Knoten müssen die folgenden Bootstrap-Argumente enthalten, bevor sie gestartet werden. Diese Argumente umgehen die Amazon EKS-Introspektion und erfordern keinen Zugriff auf die Amazon EKS-API von der VPC aus.
 - a. Ermitteln Sie den Wert des Endpunkts Ihres Clusters mit dem folgenden Befehl. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-cluster --name my-cluster --query cluster.endpoint --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
https://EXAMPLE108C897D9B2F1B21D5EXAMPLE.sk1.region-code.eks.amazonaws.com
```

- b. Ermitteln Sie den Wert der Zertifizierungsstelle Ihres Clusters mit dem folgenden Befehl. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-cluster --name my-cluster --query cluster.certificateAuthority --output text
```

Die zurückgegebene Ausgabe ist eine lange Zeichenfolge.

- c. Ersetzen Sie *cluster-endpoint* und *certificate-authority* in den folgenden Befehlen durch die Werte, die in der Ausgabe der vorherigen Befehle zurückgegeben wurden. Weitere Informationen zur Angabe von Bootstrap-Argumenten beim Start von selbstverwalteten Knoten finden Sie unter [the section called “Amazon Linux”](#) und [the section called “Windows”](#).

- Für Linux-Knoten:

```
--apiserver-endpoint cluster-endpoint --b64-cluster-ca certificate-authority
```

Weitere Argumente finden Sie im [Bootstrap-Skript](#) unter GitHub.

- Für Windows-Knoten:

Note

Wenn Sie den benutzerdefinierten Dienst CIDR verwenden, müssen Sie ihn mithilfe des `-ServiceCIDR` Parameters angeben. Andernfalls schlägt die DNS-Auflösung für Pods im Cluster fehl.

```
-APIServerEndpoint cluster-endpoint -Base64ClusterCA certificate-authority
```

Weitere Argumente finden Sie unter [the section called “Bootstrap-Skript-Konfigurationsparameter”](#).

- Ihre Cluster `aws-auth` ConfigMap müssen in Ihrer VPC erstellt werden. Weitere Informationen zum Erstellen und Hinzufügen von Einträgen zu `aws-auth` ConfigMap erhalten Sie durch Eingabe von `eksctl create iamidentitymapping --help` in Ihrem Terminal. Wenn der auf Ihrem Server ConfigMap nicht vorhanden ist, `eksctl` wird er erstellt, wenn Sie den Befehl verwenden, um eine Identitätszuweisung hinzuzufügen.
- Pods, die mit [IAM-Rollen für Dienstkonten](#) konfiguriert sind, erhalten Anmeldeinformationen über einen API-Aufruf des AWS Security Token Service (AWS STS). Wenn es keinen ausgehenden Internetzugang gibt, müssen Sie einen AWS STS-VPC-Endpunkt in Ihrer VPC erstellen und verwenden. Die meisten AWS v1 SDKs verwenden standardmäßig den globalen AWS STS-

Endpoint (`sts.amazonaws.com`), der den AWS STS-VPC-Endpoint nicht verwendet. Um den AWS STS-VPC-Endpoint zu verwenden, müssen Sie Ihr SDK möglicherweise so konfigurieren, dass es den regionalen AWS STS-Endpoint (`sts.region-code.amazonaws.com`) verwendet. Weitere Informationen finden Sie unter [the section called “STS-Endpoints”](#).

- Die VPC-Subnetze Ihres Clusters müssen über einen VPC-Schnittstellenendpunkt für alle AWS Dienste verfügen, auf die Ihre Pods Zugriff benötigen. Weitere Informationen finden Sie unter [Zugreifen auf einen AWS Dienst über einen Schnittstellen-VPC-Endpoint](#). Einige häufig verwendete Services und Endpunkte sind in der folgenden Tabelle aufgeführt. eine vollständige Liste der Endpunkte finden Sie unter [AWS -Services, die mit AWS integriert sind](#) [PrivateLink](#) im [AWS PrivateLink -Handbuch](#).

Wir empfehlen Ihnen, [private DNS-Namen für Ihre VPC-Endpoints zu aktivieren](#), damit Workloads weiterhin ohne Probleme öffentliche AWS Dienstendpunkte verwenden können.

Service	Endpoint
Amazon EC2	<code>com.amazonaws.<i>region-code</i>.ec2</code>
Amazon Elastic Container Registry (zum Abrufen von Container-Images)	<code>com.amazonaws.<i>region-code</i>.ecr.api</code> , <code>com.amazonaws.<i>region-code</i>.ecr.dkr</code> und <code>com.amazonaws.<i>region-code</i>.s3</code>
Application Load Balancer und Network Load Balancer	<code>com.amazonaws.<i>region-code</i>.elastischer</code> Lastenausgleich
AWS X-Ray	<code>com.amazonaws.<i>region-code</i>.xray</code>
CloudWatch Amazon-Protokolle	<code>com.amazonaws.<i>region-code</i>.protokolle</code>
AWS Security Token Service (erforderlich, wenn IAM-Rollen für Dienstkonto verwendet werden)	<code>com.amazonaws.<i>region-code</i>.sts</code>
Amazon EKS Auth (erforderlich bei Verwendung von Pod Identity-Zuordnungen)	<code>com.amazonaws.<i>region-code</i>.eks-auth</code>
Amazon EKS	<code>com.amazonaws.<i>region-code</i>.eks</code>

- Alle selbstverwalteten Knoten müssen in Subnetzen bereitgestellt werden, die über die von Ihnen benötigten VPC-Schnittstellenendpunkte verfügen. Wenn Sie eine verwaltete Knotengruppe erstellen, muss die Endpunktsicherheitsgruppe der VPC-Schnittstelle das CIDR für die Subnetze zulassen, oder Sie müssen die erstellte Knotensicherheitsgruppe zur Endpunktsicherheitsgruppe der VPC-Schnittstelle hinzufügen.
- Wenn Ihre Pods Amazon EFS-Volumes verwenden, muss vor der Bereitstellung von [Store an elastic file system with Amazon EFS](#) die Datei [kustomization.yaml](#) des Treibers so geändert werden, dass die Container-Images dieselbe AWS Region wie der Amazon EKS-Cluster verwenden.
- Route53 unterstützt nicht. AWS PrivateLink Sie können Route53-DNS-Einträge nicht von einem privaten Amazon EKS-Cluster aus verwalten. [Dies wirkt sich auf das externe DNS von Kubernetes aus.](#)
- Wenn Sie das EKS-optimierte AMI verwenden, sollten Sie den ec2 Endpunkt in der obigen Tabelle aktivieren. Alternativ können Sie den Knoten-DNS-Namen manuell festlegen. Das optimierte AMI verwendet EC2 APIs , um den DNS-Namen des Knotens automatisch festzulegen.
- Sie können den [Load AWS Balancer Controller](#) verwenden, um AWS Application Load Balancers (ALB) und Network Load Balancers in Ihrem privaten Cluster bereitzustellen. Beim Bereitstellen sollten Sie [Befehlszeilen-Flags](#) verwenden, um `enable-shield`, `enable-waf` und `enable-wafv2` auf falsch zu setzen. [Die Zertifikatserkennung](#) mit Hostnamen aus Ingress-Objekten wird nicht unterstützt. Dies liegt daran, dass der Controller AWS Certificate Manager erreichen muss, der keinen VPC-Schnittstellenendpunkt hat.

Der Controller unterstützt Network Load Balancer mit IP-Zielen, die für die Verwendung mit Fargate erforderlich sind. Weitere Informationen erhalten Sie unter [the section called "Application Load Balancing"](#) und [the section called "Erstellen eines Network Load Balancers"](#).

- [Cluster Autoscaler](#) wird unterstützt. Stellen Sie bei der Bereitstellung von Cluster Autoscaler Pods sicher, dass die Befehlszeile Folgendes umfasst: `--aws-use-static-instance-list=true` Weitere Informationen finden Sie unter [Statische Instanzliste verwenden](#) auf GitHub Die Worker-Node-VPC muss auch den AWS STS-VPC-Endpunkt und den VPC-Endpunkt für Autoscaling enthalten.
- Einige Container-Softwareprodukte verwenden API-Aufrufe, die auf den AWS Marketplace Metering Service zugreifen, um die Nutzung zu überwachen. Private Cluster lassen diese Aufrufe nicht zu, sodass Sie diese Containertypen nicht in privaten Clustern verwenden können.

Verstehen Sie den Lebenszyklus der Kubernetes-Version auf EKS

Kubernetes entwickelt sich mit neuen Funktionen, Design-Updates und Bugfixes schnell weiter. Die Community veröffentlicht im Durchschnitt alle vier Monate neue Kubernetes-Nebenversionen (z. B. 1.33). Amazon EKS folgt für Nebenversionen dem Upstream-Release- und Einstellungszyklus. Wenn neue Kubernetes-Versionen in Amazon EKS verfügbar werden, empfehlen wir Ihnen, Ihre Cluster proaktiv auf die neueste verfügbare Version zu aktualisieren.

Eine Nebenversion wird in den ersten 14 Monaten nach ihrer Veröffentlichung standardmäßig in Amazon EKS unterstützt. Sobald das Ende des Standard-Supportdatums für eine Version überschritten ist, gilt für sie der erweiterte Support für die nächsten 12 Monate. Mit dem erweiterten Support können Sie gegen Aufpreis pro Cluster-Stunde länger bei einer bestimmten Kubernetes-Version bleiben. Wenn Sie Ihren Cluster vor Ablauf des verlängerten Supportzeitraums nicht aktualisiert haben, wird Ihr Cluster automatisch auf die älteste derzeit unterstützte erweiterte Version aktualisiert.

Der erweiterte Support ist standardmäßig aktiviert. [the section called “Deaktivieren Sie den erweiterten Support”](#)

Wir empfehlen Ihnen, Ihren Cluster mit der neuesten verfügbaren Kubernetes-Version zu erstellen, die von Amazon EKS unterstützt wird. Wenn für Ihre Anwendung eine bestimmte Version von Kubernetes erforderlich ist, können Sie ältere Versionen auswählen. Sie können neue Amazon-EKS-Cluster auf jeder Version erstellen, die mit Standard- oder verlängertem Support angeboten wird.

Verfügbare Versionen mit Standard-Support

Die folgenden Kubernetes-Versionen sind derzeit im Amazon EKS-Standardsupport verfügbar:

- 1.33
- 1.32
- 1.31
- 1.30

Wichtige Änderungen, die Sie für jede Version des Standard-Supports beachten sollten, finden Sie unter [the section called “Standard-Supportversionen”](#).

Verfügbare Versionen mit verlängertem Support

Die folgenden Kubernetes-Versionen sind derzeit im erweiterten Support von Amazon EKS verfügbar:

- 1.29
- 1.28
- 1.27

Wichtige Änderungen, die Sie für jede Version des verlängerten Supports beachten sollten, finden Sie unter [the section called “Versionen mit verlängerten Support”](#).

Amazon-EKS-Kubernetes-Veröffentlichungskalender

Die folgende Tabelle zeigt wichtige Veröffentlichungs- und Supportdaten, die für jede Kubernetes-Version zu berücksichtigen sind. Die Abrechnung für erweiterten Support beginnt zu Beginn des Tages, an dem die Version das Ende des Standardsupports erreicht.

 Note

Daten mit nur einem Monat und einem Jahr sind ungefähre Angaben und werden mit einem genauen Datum aktualisiert, wenn es bekannt ist.

Um Benachrichtigungen über alle Änderungen an der Quelldatei auf dieser speziellen Dokumentationsseite zu erhalten, können Sie die folgende URL mit einem RSS-Reader abonnieren:

```
https://github.com/awsdocs/amazon-eks-user-guide/commits/mainline/latest/ug/clusters/kubernetes-versions.adoc.atom
```

Kubernetes-Version	Upstream-Release	Amazon-EKS-Version	Ende des Standard-Supports	Ende des verlängerten Supports
1.33	23. April 2025	29. Mai 2025	29. Juli 2026	29. Juli 2027
1.32	11. Dezember 2024	23. Januar 2025	23. März 2026	23. März 2027

Kubernetes-Version	Upstream-Release	Amazon-EKS-Version	Ende des Standard-Supports	Ende des verlängerten Supports
1.31	13. August 2024	26. September 2024	26. November 2025	26. November 2026
1.30	17. April 2024	23. Mai 2024	23. Juli 2025	23. Juli 2026
1.29	13. Dezember 2023	23. Januar 2024	23. März 2025	23. März 2026
1.28	15. August 2023	26. September 2023	26. November 2024	26. November 2025
1.27	11. April 2023	24. Mai 2023	24. Juli 2024	24. Juli 2025

Versionsinformationen mit AWS CLI abrufen

Sie können die AWS CLI verwenden, um Informationen zu den auf EKS verfügbaren Kubernetes-Versionen abzurufen, z. B. das Enddatum des Standardsupports.

So rufen Sie mithilfe der CLI Informationen zu verfügbaren Kubernetes-Versionen auf EKS ab AWS

1. Öffnen Sie Ihr Terminal.
2. Stellen Sie sicher, dass die AWS CLI installiert und konfiguriert ist. Weitere Informationen finden Sie unter [Installation oder Aktualisierung auf die neueste Version der CLI](#).
3. Führen Sie den folgenden Befehl aus:

```
aws eks describe-cluster-versions
```

4. Der Befehl gibt eine JSON-Ausgabe mit Details zu den verfügbaren Cluster-Versionen zurück. Hier ist ein Beispiel für die Ausgabe:

```
{
  "clusterVersions": [
    {
```

```
    "clusterVersion": "1.31",
    "clusterType": "eks",
    "defaultPlatformVersion": "eks.21",
    "defaultVersion": true,
    "releaseDate": "2024-09-25T17:00:00-07:00",
    "endOfStandardSupportDate": "2025-11-25T16:00:00-08:00",
    "endOfExtendedSupportDate": "2026-11-25T16:00:00-08:00",
    "status": "STANDARD_SUPPORT",
    "kubernetesPatchVersion": "1.31.3"
  }
]
```

Die Ausgabe enthält die folgenden Informationen für jede Cluster-Version:

- `clusterVersion`: Die Kubernetes-Version des EKS-Clusters
- `clusterType`: Der Clustertyp (z. B. „eks“)
- `defaultPlatformVersion`: Die Standardversion der EKS-Plattform
- `defaultVersion`: Ob dies die Standardversion ist
- `releaseDate`: Das Datum, an dem diese Version veröffentlicht wurde
- `endOfStandardSupportDate`: Das Datum, an dem der Standardsupport endet
- `endOfExtendedSupportDate`: Das Datum, an dem der erweiterte Support endet
- `status`: Der aktuelle Support-Status der Version, z. B. `STANDARD_SUPPORT` oder `EXTENDED_SUPPORT`
- `kubernetesPatchVersion`: Die spezifische Kubernetes-Patch-Version

Amazon EKS-Version FAQs

Wie viele Kubernetes-Versionen sind im Standardsupport verfügbar?

Im Einklang mit der Unterstützung der Kubernetes-Community für Kubernetes-Versionen verpflichtet sich Amazon EKS, jederzeit Unterstützung für drei Kubernetes-Versionen anzubieten. Wir werden das Ende des Standard-Supportdatums für eine bestimmte Kubernetes-Nebenversion mindestens 60 Tage im Voraus bekannt geben. Aufgrund des Qualifizierungs- und Veröffentlichungsprozesses von Amazon EKS für neue Kubernetes-Versionen endet der

Standardsupport einer Kubernetes-Version auf Amazon EKS nach dem Datum, an dem das Kubernetes-Projekt die Unterstützung der Upstream-Version einstellt.

Wie lange erhält ein Kubernetes Standardsupport von Amazon EKS?

Eine Kubernetes-Version erhielt 14 Monate lang Standardunterstützung, nachdem sie erstmals auf Amazon EKS verfügbar war. Dies gilt auch dann, wenn Upstream-Kubernetes eine Version, die auf Amazon EKS verfügbar ist, nicht mehr unterstützt. Wir führen Sicherheitspatches zurück, die für die Kubernetes-Versionen gelten, die auf Amazon EKS unterstützt werden.

Werde ich benachrichtigt, wenn der Standardsupport für eine Kubernetes-Version auf Amazon EKS endet?

Ja. Wenn auf Clustern in Ihrem Konto die Version ausgeführt wird, die sich dem Ende des Supports nähert, sendet Amazon EKS etwa 12 Monate nach der Veröffentlichung der Kubernetes-Version auf Amazon EKS eine Benachrichtigung über das AWS Health Dashboard. Die Mitteilung enthält das Datum des Support-Laufzeitendes. Dies ist mindestens 60 Tage ab dem Datum der Benachrichtigung.

Welche Kubernetes-Funktionen werden von Amazon EKS unterstützt?

Amazon EKS unterstützt alle allgemein verfügbaren (GA) Funktionen der Kubernetes-API. Neue APIs Betaversionen sind in Clustern standardmäßig nicht aktiviert. Zuvor vorhandene Betaversionen APIs und neue Versionen vorhandener Betaversionen sind jedoch APIs weiterhin standardmäßig aktiviert. Alpha-Funktionen werden nicht unterstützt.

Werden von Amazon EKS verwaltete Knotengruppen automatisch zusammen mit der Version der Cluster-Kontrollebene aktualisiert?

Nein. Eine verwaltete Knotengruppe erstellt EC2 Amazon-Instances in Ihrem Konto. Diese Instances werden nicht automatisch aktualisiert, wenn Sie oder Amazon EKS Ihre Kontrollebene aktualisieren. Weitere Informationen finden Sie unter [the section called “Aktualisierung”](#). Wir empfehlen, dieselbe Kubernetes-Version auf Ihrer Steuerungsebene und Ihren Knoten beizubehalten.

Werden selbstverwaltete Knotengruppen automatisch zusammen mit der Version der Cluster-Kontrollebene aktualisiert?

Nein. Eine selbstverwaltete Knotengruppe umfasst EC2 Amazon-Instances in Ihrem Konto. Diese Instances werden nicht automatisch aktualisiert, wenn Sie oder Amazon EKS die Version der Kontrollebene in Ihrem Namen aktualisieren. Bei einer selbstverwalteten Knotengruppe gibt es in der Konsole keinen Hinweis darauf, dass sie aktualisiert werden muss. Sie können die auf einem

Knoten installierte kubelet-Version anzeigen, indem Sie den Knoten in der Liste Knoten auf der Registerkarte Übersicht Ihres Clusters auswählen, um zu bestimmen, welche Knoten aktualisiert werden müssen. Sie müssen die Knoten manuell aktualisieren. Weitere Informationen finden Sie unter [the section called “Update-Methoden”](#).

Das Kubernetes-Projekt testet die Kompatibilität zwischen der Kontrollebene und den Knoten für bis zu drei Nebenversionen. 1.30-Knoten funktionieren beispielsweise weiterhin, wenn sie von einer 1.33-Steuerebene orchestriert werden. Es wird jedoch nicht empfohlen, einen Cluster mit Knoten auszuführen, bei denen sich dauerhaft drei Nebenversionen hinter der Kontrollebene befinden. Weitere Informationen finden Sie unter [Kubernetes Version and Version Skew Support Policy](#) in der Kubernetes-Dokumentation. Wir empfehlen, dieselbe Kubernetes-Version auf Ihrer Steuerungsebene und Ihren Knoten beizubehalten.

Werden Pods, die auf Fargate laufen, automatisch mit einem automatischen Versionsupgrade der Clustersteuerungsebene aktualisiert?

Nein. Wir empfehlen dringend, Fargate Pods als Teil eines Replikationscontrollers, z. B. einer Kubernetes-Bereitstellung, auszuführen. Führen Sie dann einen fortlaufenden Neustart aller Fargate Pods durch. Die neue Version des Fargate Pod wird mit einer kubelet Version bereitgestellt, die mit Ihrer aktualisierten Version der Cluster-Steuerebene identisch ist. Weitere Informationen finden Sie unter [Bereitstellungen](#) in der Kubernetes-Dokumentation.

 Important

Wenn Sie die Steuerebene aktualisieren, müssen Sie die Fargate-Knoten nach wie vor selbst aktualisieren. Um Fargate-Knoten zu aktualisieren, löschen Sie den Fargate-Pod, der durch den Knoten repräsentiert wird, und stellen Sie den Pod erneut bereit. Der neue Pod wird mit einer kubelet Version bereitgestellt, die der Version Ihres Clusters entspricht.

Welche Kubernetes-Versionen werden für Hybridknoten unterstützt?

Amazon EKS Hybrid Nodes unterstützt dieselben Kubernetes-Versionen wie Amazon EKS-Cluster mit anderen Knotenberechnungstypen, einschließlich standardmäßiger und erweiterter Kubernetes-Versionsunterstützung. Hybridknoten werden nicht automatisch aktualisiert, wenn Sie Ihre Version der Steuerungsebene aktualisieren, und Sie sind für das Upgrade Ihrer Hybridknoten verantwortlich. Weitere Informationen finden Sie unter [the section called “Aktualisieren Sie Hybridknoten”](#).

Erweiterter Support für Amazon EKS FAQs

Die Terminologie für Standardsupport und erweiterten Support ist für mich neu. Was bedeuten diese Begriffe?

Die Standardunterstützung für eine Kubernetes-Version in Amazon EKS beginnt mit der Veröffentlichung einer Kubernetes-Version auf Amazon EKS und endet 14 Monate nach dem Veröffentlichungsdatum. Der erweiterte Support für eine Kubernetes-Version beginnt unmittelbar nach dem Ende des Standardsupports und endet nach den nächsten 12 Monaten. Beispielsweise endete der Standardsupport für die Version 1.23 in Amazon EKS am 11. Oktober 2023. Der erweiterte Support für die Version 1.23 begann am 12. Oktober 2023 und endete am 11. Oktober 2024.

Was muss ich tun, um erweiterten Support für Amazon EKS-Cluster zu erhalten?

Sie müssen den erweiterten Support (siehe [the section called “Aktivieren Sie den erweiterten Support”](#)) für Ihren Cluster aktivieren, indem Sie die Cluster-Upgrade-Richtlinie auf ERWEITERT ändern. Standardmäßig ist die Upgrade-Richtlinie für alle neuen und vorhandenen Cluster auf ERWEITERT festgelegt, sofern nicht anders angegeben. Informationen [the section called “Upgrade-Richtlinie anzeigen”](#) zur Upgrade-Richtlinie für Ihren Cluster finden Sie unter. Der Standardsupport beginnt, wenn eine Kubernetes-Version auf Amazon EKS veröffentlicht wird, und endet 14 Monate nach dem Veröffentlichungsdatum. Der erweiterte Support für eine Kubernetes-Version beginnt unmittelbar nach dem Ende des Standardsupports und endet nach den nächsten 12 Monaten.

Für welche Kubernetes-Versionen kann ich erweiterten Support erhalten?

Sie können Cluster auf jeder Version bis zu 12 Monate nach dem Ende des Standard-Supports für diese Version ausführen. Das bedeutet, dass jede Version 26 Monate lang in Amazon EKS unterstützt wird (14 Monate Standard-Support plus 12 Monate verlängerter Support).

Was ist, wenn ich den erweiterten Support nicht nutzen möchte?

Wenn Sie nicht automatisch für den erweiterten Support registriert werden möchten, können Sie Ihren Cluster auf eine Kubernetes-Version aktualisieren, die standardmäßig von Amazon EKS unterstützt wird. Weitere Informationen [the section called “Deaktivieren Sie den erweiterten Support”](#) zum Deaktivieren des erweiterten Supports finden Sie unter. Hinweis: Wenn Sie den erweiterten Support deaktivieren, wird Ihr Cluster am Ende des Standardsupports automatisch aktualisiert.

Was passiert nach Ablauf von 12 Monaten des erweiterten Supports?

Cluster, die auf einer Kubernetes-Version laufen, die ihren 26-monatigen Lebenszyklus (14 Monate Standardsupport plus 12 Monate erweiterter Support) abgeschlossen hat, werden automatisch auf die nächste Version aktualisiert. Das automatische Upgrade umfasst nur die Kubernetes-Steuerebene. Wenn Sie über EKS-Automodus-Knoten verfügen, werden diese möglicherweise automatisch aktualisiert. Selbstverwaltete Knoten und von EKS verwaltete Knotengruppen bleiben in der vorherigen Version erhalten.

Nach Ablauf des verlängerten Supports können Sie mit der nicht unterstützten Version keine neuen Amazon-EKS-Cluster mehr erstellen. Vorhandene Steuerebenen werden von Amazon EKS durch einen schrittweisen Bereitstellungsprozess nach dem Datum des Support-Laufzeitendes automatisch auf die älteste unterstützte Version aktualisiert. Stellen Sie nach dem automatischen Update der Steuerungsebene sicher, dass Sie die Cluster-Add-Ons und EC2 Amazon-Knoten manuell aktualisieren. Weitere Informationen finden Sie unter [the section called “Kubernetes-Version aktualisieren”](#).

Wann genau wird meine Steuerungsebene nach Ablauf des Extended Support Datums automatisch aktualisiert?

Amazon EKS kann keine bestimmten Zeitrahmen bereitstellen. Automatische Updates können jederzeit nach Ablauf des verlängerten Supports erfolgen. Sie erhalten vor dem Update keine Benachrichtigung. Wir empfehlen Ihnen, dass Sie Ihre Steuerebene proaktiv aktualisieren, ohne sich auf den automatischen Aktualisierungsprozess von Amazon EKS zu verlassen. Weitere Informationen finden Sie unter [the section called “Kubernetes-Version aktualisieren”](#).

Kann ich meine Kontrollebene auf einer Kubernetes-Version auf unbestimmte Zeit verlassen?

Nein. Cloud-Sicherheit AWS hat höchste Priorität. Ab einem bestimmten Zeitpunkt (normalerweise ein Jahr) veröffentlicht die Kubernetes-Community keine Patches mehr für allgemeine Sicherheitslücken und Exposure (CVE) und rät von der Einreichung von CVE-Dateien für nicht unterstützte Versionen ab. Das bedeutet, dass Sicherheitslücken, die für eine ältere Version von Kubernetes spezifisch sind, möglicherweise nicht einmal gemeldet werden. Daher können Cluster im Falle einer Schwachstelle ohne Vorankündigung und ohne Behebungsoptionen offengelegt werden. Aus diesem Grund erlaubt Amazon EKS nicht, dass Kontrollebenen auf einer Version verbleiben, für die der erweiterte Support abgelaufen ist.

Fallen zusätzliche Kosten für die Inanspruchnahme von erweitertem Support an?

Ja, es fallen zusätzliche Kosten für Amazon EKS-Cluster an, die im erweiterten Support ausgeführt werden. Preisinformationen finden Sie im AWS Blog oder auf unserer [Preisseite](#) unter [Erweiterte Unterstützung für Kubernetes-Versionen von Amazon EKS](#).

Was ist im erweiterten Support enthalten?

Amazon EKS-Cluster mit erweitertem Support erhalten fortlaufend Sicherheitspatches für die Kubernetes-Steuerebene. Darüber hinaus wird Amazon EKS Patches für die Amazon VPC CNI- und CoreDNS-Add-Ons für Extended Support-Versionen veröffentlichen. kube-proxy Amazon EKS wird auch Patches für AWS veröffentlichte Amazon EKS veröffentlichen, die AMIs für Amazon Linux, Bottlerocket und Windows optimiert sind, sowie für Amazon EKS Fargate-Knoten für diese Versionen. Alle Cluster im erweiterten Support erhalten weiterhin Zugriff auf technischen Support von AWS.

Gibt es Einschränkungen bei Patches für Komponenten, die nicht zu Kubernetes gehören, im Rahmen des erweiterten Supports?

Extended Support deckt zwar alle Kubernetes-spezifischen Komponenten von ab AWS, bietet aber jederzeit nur Support für Amazon EKS, AWS das AMIs für Amazon Linux, Bottlerocket und Windows optimiert ist. Das bedeutet, dass Sie möglicherweise neuere Komponenten (wie Betriebssystem oder Kernel) auf Ihrem für Amazon EKS optimierten AMI haben werden, während Sie den verlängerten Support verwenden. Sobald Amazon Linux 2 beispielsweise [im Jahr 2025 das Ende seines Lebenszyklus](#) erreicht, AMIs wird das für Amazon EKS optimierte Amazon Linux mit einem neueren Amazon Linux-Betriebssystem erstellt. Amazon EKS wird wichtige Abweichungen im Support-Lebenszyklus wie diese für jede Kubernetes-Version bekannt geben und dokumentieren.

Kann ich mit einer Version mit erweitertem Support neue Cluster erstellen?

Ja.

Lesen Sie die Versionshinweise für Kubernetes-Versionen zur Standardunterstützung

Dieses Thema enthält wichtige Änderungen, die Sie für jede Kubernetes-Version im Standardsupport beachten sollten. Überprüfen Sie beim Upgrade sorgfältig die Änderungen, die zwischen der alten und der neuen Version für Ihren Cluster vorgenommen wurden.

Kubernetes 1.33

Kubernetes 1.33 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.33 Versionsankündigung.](#)

Important

- Die Beta-Kubernetes-API für dynamische Ressourcenzuweisung ist aktiviert.
 - Diese Beta-API verbessert die Erfahrung bei der Planung und Überwachung von Workloads, die Ressourcen erfordern, wie z. GPUs
 - Die Beta-API wird von der Kubernetes-Community definiert und kann sich in future Versionen von Kubernetes ändern.
 - Lesen Sie die [einzelnen Funktionsphasen](#) in der Kubernetes-Dokumentation sorgfältig durch, um die Auswirkungen der Beta-Version zu verstehen. APIs
 - AWS veröffentlicht kein EKS-optimiertes Amazon Linux 2-AMI für Kubernetes 1.33.
 - AWS fordert Sie auf, zu Amazon Linux 2023 zu migrieren. Weitere Informationen erhalten Sie unter [the section called “Führen Sie ein Upgrade auf Version AL2 023 durch”](#).
 - Weitere Informationen finden Sie unter [the section called “Veraltete Amazon Linux 2-AMI-Unterstützung”](#).
-
- Direkte Änderung der Größe von Pod-Ressourcen (Beta): Die direkte Änderung der Größe von Ressourcen wurde zur Beta-Version hochgestuft und ermöglicht dynamische Aktualisierungen der CPU- und Speicherressourcen für bestehende Pods ohne Neustarts. Dies ermöglicht die vertikale Skalierung von statusbehafteten Workloads ohne Ausfallzeiten und nahtlose Ressourcenanpassungen auf der Grundlage von Verkehrsmustern.
 - Sidecar-Container sind jetzt stabil: Sidecar-Container sind auf Stable umgestiegen und implementieren Sidecars als spezielle Init-Container, `restartPolicy: Always` die vor Anwendungscontainern starten, während des gesamten Pod-Lebenszyklus laufen und Sonden für die Signalisierung des Betriebszustands unterstützen.
 - [Weitere Informationen finden Sie unter Sidecar-Container in der Kubernetes-Dokumentation.](#)
 - Veraltete Endpunkt-API: Die Endpoint-API ist nun offiziell veraltet und gibt beim Zugriff Warnungen zurück. Migrieren Sie Workloads und Skripts, um stattdessen die EndpointSlices API zu

verwenden, die moderne Funktionen wie Dual-Stack-Netzwerke unterstützt und mehrere pro Service verarbeitet. EndpointSlices

- Weitere Informationen finden Sie im Kubernetes-Blog unter [Kubernetes v1.33](#): Fortsetzung des Übergangs von Endpoints zu. EndpointSlice
- Elastic Fabric Adapter-Unterstützung: Die Standardsicherheitsgruppe für Amazon EKS-Cluster unterstützt jetzt Elastic Fabric Adapter (EFA) -Verkehr. Die Standardsicherheitsgruppe verfügt über eine neue ausgehende Regel, die EFA-Verkehr mit dem Ziel derselben Sicherheitsgruppe zulässt. Dies ermöglicht EFA-Verkehr innerhalb des Clusters.
- Weitere Informationen finden Sie unter [Elastic Fabric Adapter für KI/ML- und HPC-Workloads auf Amazon EC2 im Amazon Elastic Compute Cloud-Benutzerhandbuch](#).

Das vollständige 1.33 Kubernetes-Changelog finden Sie unter -1.33.md <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG>

Kubernetes 1.32

Kubernetes 1.32 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.32 Versionsankündigung.](#)

Important

- Die `flowcontrol.apiserver.k8s.io/v1beta3` API-Version von FlowSchema und PriorityLevelConfiguration wurde in Version entfernt. 1.32 Wenn Sie diese verwenden APIs, müssen Sie Ihre Konfigurationen aktualisieren, um die neueste unterstützte Version zu verwenden, bevor Sie das Upgrade durchführen.
 - `ServiceAccount metadata.annotations[kubernetes.io/enforce-mountable-secrets]` ist in der Version veraltet 1.32 und wird in einer future Kubernetes-Nebenversion entfernt. Es wird empfohlen, separate Namespaces zu verwenden, um den Zugriff auf bereitgestellte Geheimnisse zu isolieren.
 - Die Kubernetes-Version 1.32 ist die letzte Version, für die Amazon EKS Amazon Linux 2 () AL2 veröffentlichen wird. AMIs 1.33 Ab Version 2 wird Amazon EKS weiterhin Amazon Linux 2023 (AL2023) und Bottlerocket auf Basis von Amazon veröffentlichen. AMIs
-
- Die Memory Manager-Funktion wurde in der Kubernetes-Version auf den Status Allgemein verfügbar (GA) umgestellt. 1.32 Diese Erweiterung ermöglicht eine effizientere und

vorhersehbarere Speicherzuweisung für containerisierte Anwendungen, was insbesondere für Workloads mit spezifischen Speicheranforderungen von Vorteil ist.

- PersistentVolumeClaims (PVCs), die StatefulSets inzwischen erstellt wurden, enthalten automatische Bereinigungsfunktionen. Wenn sie nicht mehr benötigt werden, werden sie automatisch gelöscht, wobei die Datenpersistenz bei StatefulSet Updates und Knotenwartungsvorgängen erhalten bleibt. Diese Funktion vereinfacht die Speicherverwaltung und verhindert, dass PVCs in Ihrem Cluster verwaiste Speicher entstehen.
- Es wurde eine Funktion zur Feldauswahl für benutzerdefinierte Ressourcen eingeführt, die es Entwicklern ermöglicht, benutzerdefinierten Ressourcen Feldselektoren hinzuzufügen. Diese Funktion bietet dieselben Filterfunktionen, die für integrierte Kubernetes-Objekte verfügbar sind, auch für benutzerdefinierte Ressourcen. Dadurch wird eine genauere und effizientere Ressourcenfilterung ermöglicht und bessere API-Entwurfspraktiken gefördert.

[Das vollständige 1.32 Kubernetes-Changelog finden Sie unter -1.32.md https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG](https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.32.md)

Anonyme Authentifizierungsänderungen

Ab Amazon EKS 1.32 ist die anonyme Authentifizierung auf die folgenden Endpunkte für die Zustandsprüfung von API-Servern beschränkt:

- /healthz
- /livez
- /readyz

Anfragen an jeden anderen Endpunkt, die den `system:unauthenticated` Benutzer verwenden, erhalten eine 401 Unauthorized HTTP-Antwort. Diese Sicherheitsverbesserung trägt dazu bei, unbeabsichtigten Clusterzugriffen zu verhindern, die aufgrund falsch konfigurierter RBAC-Richtlinien auftreten könnten.

Note

Die `public-info-viewer` RBAC-Rolle gilt weiterhin für die oben aufgeführten Health Check-Endpunkte.

Veraltete Amazon Linux 2-AMI-Unterstützung

Für Kubernetes-Versionen 1.33 und höher stellt EKS keine vorgefertigten optimierten Amazon Linux 2 (AL2) Amazon Machine Images () bereit. AMIs

AWS schlägt vor, den EKS-Automatikmodus zu übernehmen oder auf ein neueres Betriebssystem wie Amazon Linux 2023 (AL2023) oder Bottlerocket zu migrieren.

- [the section called “Migrieren Sie von MNGs”](#)
- [the section called “Führen Sie ein Upgrade auf Version AL2 023 durch”](#)
- [the section called “Bottlerocket”](#)

Note

Dieses Update gilt für EKS-Optimized. AL2 AMIs Weitere Informationen zum Betriebssystem selbst finden Sie unter [Amazon Linux FAQs 2](#).

Kubernetes 1.31

Kubernetes 1.31 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.31 Versionsankündigung](#).

Important

- Das seit 2017 --keep-terminated-pod-volumes veraltete Kubelet-Flag wurde im Rahmen der Versionsveröffentlichung entfernt. 1.31 Diese Änderung wirkt sich darauf aus, wie beendete Pod-Volumes vom Kubelet behandelt werden. Wenn Sie dieses Flag in Ihren Knotenkonfigurationen verwenden, müssen Sie Ihre Bootstrap-Skripte und Startvorlagen aktualisieren, um es vor dem Upgrade zu entfernen.
- Das VolumeAttributesClass Beta-Feature-Gate und die API-Ressource sind in der Amazon EKS-Version aktiviert1.31. Mit dieser Funktion können Cluster-Betreiber veränderbare Eigenschaften von Persistent Volumes (PVs) ändern, die von kompatiblen CSI-Treibern verwaltet werden, einschließlich des Amazon EBS CSI-Treibers. Um diese Funktion nutzen zu können, stellen Sie sicher, dass Ihr CSI-Treiber die VolumeAttributesClass Funktion unterstützt

(für den Amazon EBS CSI-Treiber aktualisieren Sie auf Version 1.35.0 oder höher, um die Funktion automatisch zu aktivieren). Sie können `VolumeAttributesClass` Objekte erstellen, um die gewünschten Volumenattribute wie Volumentyp und Durchsatz zu definieren und sie Ihren Persistent Volume Claims (PVCs) zuzuordnen. Weitere Informationen finden Sie in der [offiziellen Kubernetes-Dokumentation](#) sowie in der Dokumentation Ihres CSI-Treibers.

- Weitere Informationen zum Amazon EBS CSI-Treiber finden Sie unter [the section called “Amazon EBS”](#).
- Die Kubernetes-Unterstützung für [AppArmor](#) wurde auf Stable umgestellt und ist nun allgemein für die öffentliche Nutzung verfügbar. Mit dieser Funktion können Sie Ihre Container schützen, AppArmor indem Sie das `appArmorProfile.type` Feld in den Containern festlegen. `securityContext` Vor der Kubernetes-Version AppArmor wurde 1.30 es durch Anmerkungen gesteuert. Beginnend mit der Version 1.30 wird sie mithilfe von Feldern gesteuert. Um diese Funktion nutzen zu können, empfehlen wir, statt Anmerkungen zu migrieren und das `appArmorProfile.type` Feld zu verwenden, um sicherzustellen, dass Ihre Workloads kompatibel sind.
- Die Funktion für die Übergangszeit in der PersistentVolume letzten Phase wurde auf Stable umgestellt und ist nun in der Kubernetes-Version allgemein für die öffentliche Nutzung verfügbar. 1.31 Mit dieser Funktion wird ein neues Feld eingeführt, `.status.lastTransitionTime`, in dem ein Zeitstempel angegeben wird PersistentVolumeStatus, wann das PersistentVolume letzte Mal in eine andere Phase übergegangen ist. Diese Erweiterung ermöglicht eine bessere Nachverfolgung und Verwaltung von PersistentVolumes, insbesondere in Szenarien, in denen es wichtig ist, den Lebenszyklus von Volumen zu verstehen.

[Das vollständige 1.31 Kubernetes-Changelog finden Sie unter -1.31.md https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG](#)

Kubernetes 1.30

Kubernetes 1.30 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.30 Versionsankündigung.](#)

Important

- Ab der Amazon EKS-Version 1.30 oder neuer verwenden alle neu erstellten verwalteten Knotengruppen automatisch standardmäßig Amazon Linux 2023 (AL2023) als Knotenbetriebssystem. Bisher wurde für neue Knotengruppen standardmäßig Amazon

Linux 2 (AL2) verwendet. Sie können ihn weiterhin verwenden, AL2 indem Sie ihn beim Erstellen einer neuen Knotengruppe als AMI-Typ auswählen.

- Informationen zur Migration von AL2 zu AL2 023 finden Sie unter [the section called “Führen Sie ein Upgrade auf Version AL2 023 durch”](#)
- Weitere Informationen zu Amazon Linux finden Sie unter [AL2 Comparing und AL2 023](#) im Amazon Linux-Benutzerhandbuch.
- Weitere Informationen zur Angabe des Betriebssystems für eine verwaltete Knotengruppe finden Sie unter [the section called “Erstellen”](#)

- Mit Amazon EKS 1.30 wird das `topology.k8s.aws/zone-id` Label zu Worker-Knoten hinzugefügt. Sie können die Availability Zone IDs (AZ IDs) verwenden, um den Standort von Ressourcen in einem Konto im Verhältnis zu den Ressourcen in einem anderen Konto zu bestimmen. Weitere Informationen finden Sie im AWS RAM-Benutzerhandbuch unter [Availability Zone IDs für Ihre AWS Ressourcen](#).
- Ab sofort enthält Amazon EKS die default Anmerkung zur `gp2 StorageClass` Ressource 1.30, die auf neu erstellte Cluster angewendet wurde, nicht mehr. Dies hat keine Auswirkungen, wenn Sie diese Speicherklasse namentlich referenzieren. Sie müssen Maßnahmen ergreifen, wenn Sie sich auf einen Standard `StorageClass` im Cluster verlassen haben. Sie sollten mit `StorageClass` dem Namen auf die `verweisengp2`. Alternativ können Sie die von Amazon EBS empfohlene Standardspeicherklasse bereitstellen, indem Sie den `defaultStorageClass.enabled` Parameter bei der Installation der `aws-ebs-csi-driver` add-on Version 1.31.0 oder höher von auf `true` setzen.
- Die mindestens erforderliche IAM-Richtlinie für die Amazon EKS-Cluster-IAM-Rolle hat sich geändert. Die Aktion `ec2:DescribeAvailabilityZones` ist erforderlich. Weitere Informationen finden Sie unter [the section called “Cluster-IAM-Rolle”](#).

[Das vollständige 1.30 Kubernetes-Changelog finden Sie unter -1.30.md. https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG](#)

Lesen Sie die Versionshinweise für Kubernetes-Versionen zum erweiterten Support

Amazon EKS unterstützt Kubernetes-Versionen länger als sie im Upstream-Modus unterstützt werden, mit Standardunterstützung für Kubernetes-Nebenversionen für 14 Monate ab dem

Zeitpunkt, an dem sie in Amazon EKS veröffentlicht werden, und erweiterter Support für Kubernetes-Nebenversionen für weitere 12 Monate Support (insgesamt 26 Monate pro Version).

Dieses Thema erläutert wichtige Änderungen, die Sie für jede Kubernetes-Version des verlängerten Supports beachten sollten. Überprüfen Sie beim Upgrade sorgfältig die Änderungen, die zwischen der alten und der neuen Version für Ihren Cluster vorgenommen wurden.

Kubernetes 1.29

Kubernetes 1.29 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.29 Versionsankündigung.](#)

Important

- Die veralteten `flowcontrol.apiserver.k8s.io/v1beta2` API-Versionen von `FlowSchema` und `PriorityLevelConfiguration` werden in der Kubernetes-Version nicht mehr bereitgestellt. 1.29 Wenn Sie Manifeste oder Clientsoftware haben, die die veraltete Beta-API-Gruppe verwendet, sollten Sie diese ändern, bevor Sie auf die Version aktualisieren. 1.29
- Das `.status.kubeProxyVersion` Feld für Knotenobjekte ist jetzt veraltet, und das Kubernetes-Projekt schlägt vor, dieses Feld in einer future Version zu entfernen. Das veraltete Feld ist nicht korrekt und wurde in der Vergangenheit von einer Organisation verwaltet, die weder `kubelet` die `kube-proxy` Version noch weiß, ob sie ausgeführt wird. `kube-proxy` Wenn Sie dieses Feld in der Client-Software verwendet haben, hören Sie auf. Die Informationen sind nicht zuverlässig und das Feld ist jetzt veraltet.
- Um die potenzielle Angriffsfläche 1.29 zu reduzieren, kennzeichnet die `LegacyServiceAccountTokenCleanUp` Funktion in Kubernetes veraltete, automatisch generierte geheime Token als ungültig, wenn sie lange Zeit nicht verwendet wurden (standardmäßig 1 Jahr), und entfernt sie automatisch, wenn sie lange Zeit nicht verwendet wurden, nachdem sie als ungültig markiert wurden (standardmäßig 1 zusätzliches Jahr). Um solche Token zu identifizieren, können Sie Folgendes ausführen:

```
kubectl get cm kube-apiserver-legacy-service-account-token-tracking -n kube-system
```

[Das vollständige 1.29 Kubernetes-Changelog finden Sie unter https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.29.md#1280.changelog-since-v1.29](https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.29.md#1280.changelog-since-v1.29)

Kubernetes 1.28

Kubernetes 1.28 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.28 Versionsankündigung.](#)

- Kubernetes v1.28 erweiterte den unterstützten Unterschied zwischen den Komponenten des Kernknotens und der Steuerungsebene um eine Nebenversion, von n-2 bis n-3, sodass die Knotenkomponenten (kubelet und kube-proxy) für die älteste unterstützte Nebenversion mit den Komponenten der Steuerungsebene (kube-apiserver, kube-scheduler, kube-controller-manager, cloud-controller-manager) für die neueste unterstützte Nebenversion zusammenarbeiten können.
- Die Metriken `force_delete_pods_total` und `force_delete_pod_errors_total` im Pod GC Controller wurden dahingehend verbessert, dass alle erzwungenen Löschungen von Pods berücksichtigt werden. Der Metrik wird ein Grund hinzugefügt, der angibt, ob der Pod gewaltsam gelöscht wurde, weil er beendet wurde, verwaist ist, mit dem out-of-service Makel endet oder weil er beendet wurde und nicht geplant wurde.
- Der PersistentVolume (PV)-Controller wurde dahingehend geändert, dass allen ungebundenen PersistentVolumeClaim, bei denen der `storageClassName` nicht gesetzt ist, automatisch eine standardmäßige StorageClass zugewiesen wird. Darüber hinaus wurde der Mechanismus zur Überprüfung der PersistentVolumeClaim Zulassung innerhalb des API-Servers so angepasst, dass Werte von einem nicht festgelegten Status in einen tatsächlichen Namen geändert werden können. StorageClass

[Das vollständige 1.28 Kubernetes-Changelog finden Sie unter -1.28.md#1270. https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.28.md#1270.changelog-since-v1.28](https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.28.md#1270.changelog-since-v1.28)

Kubernetes 1.27

Kubernetes 1.27 ist jetzt in Amazon EKS verfügbar. [Weitere Informationen zu Kubernetes finden Sie in der offiziellen 1.27 Versionsankündigung.](#)

Important

- Die Unterstützung für die Alpha-seccomp-Anmerkungen und die Anmerkungen `seccomp.security.alpha.kubernetes.io/pod` und

`container.seccomp.security.alpha.kubernetes.io` wurde entfernt. Die Alpha-seccomp-Anmerkungen sind seit 1.19 veraltet. Aufgrund ihrer Entfernung in 1.27 werden seccomp-Felder für Pods nicht mehr automatisch mit seccomp-Anmerkungen gefüllt. Verwenden Sie stattdessen das Feld `securityContext.seccompProfile` für Pods oder Container, um seccomp-Profile zu konfigurieren. Um zu überprüfen, ob Sie die veralteten Alpha-seccomp-Anmerkungen im Cluster verwenden, führen Sie den folgenden Befehl aus:

```
kubectl get pods --all-namespaces -o json | grep  
-E 'seccomp.security.alpha.kubernetes.io/pod|  
container.seccomp.security.alpha.kubernetes.io'
```

- Das Befehlszeilenargument `--container-runtime` für das `kubelet` wurde entfernt. `containerd` Seitdem ist die Standard-Container-Laufzeit für Amazon EKS gültig 1.24, sodass die Container-Laufzeit nicht mehr angegeben werden muss. Ab 1.27 ignoriert Amazon EKS das Argument `--container-runtime`, das an Bootstrap-Skripte übergeben wird. Es ist wichtig, dass Sie dieses Argument nicht an übergeben, um `--kubelet-extra-args` Fehler während des Knoten-Bootstrap-Vorgangs zu vermeiden. Sie müssen das Argument `--container-runtime` aus allen Workflows und Build-Skripten zur Knotenerstellung entfernen.
- `kubelet` In Kubernetes 1.27 wurde die Standardeinstellung auf und `kubeAPIQPS` auf 50 erhöht. `kubeAPIBurst` 100 Dank dieser Verbesserungen kann das `kubelet` eine größere Menge an API-Abfragen verarbeiten, wodurch die Antwortzeiten und die Leistung verbessert werden. Wenn der Bedarf an Pods aufgrund von Skalierungsanforderungen steigt, stellen die überarbeiteten Standardwerte sicher, dass das `kubelet` die höhere Workload effizient bewältigen kann. Infolgedessen sind Pod-Starts schneller und Clustervorgänge effektiver.
- Zur Verteilung von Richtlinien wie `minDomain` können Sie eine detailliertere Pod-Topologie verwenden. Mit diesem Parameter können Sie die Mindestanzahl von Domains angeben, auf die die Pods verteilt werden sollen. `nodeAffinityPolicy` und `nodeTaintPolicy` ermöglichen ein zusätzliches Maß an Granularität bei der Steuerung der Pod-Verteilung. Dies entspricht den Knotenaffinitäten, den Taints und dem Feld `matchLabelKeys` in den `topologySpreadConstraints` der Spezifikation Ihres Pod's. Das ermöglicht die Auswahl von Pods für Verteilungsberechnungen nach einem fortlaufenden Upgrade.
- Kubernetes hat einen neuen Richtlinienmechanismus zur Beta-Version 1.27 befördert, der `StatefulSets` die Lebensdauer ihrer () steuert. `PersistentVolumeClaims` PVCs Mit der

neuen PVC-Aufbewahrungsrichtlinie können Sie angeben, ob die anhand der Spezifikationsvorlage `StatefulSet` generierten PVCs automatisch gelöscht oder beibehalten werden, wenn das `StatefulSet` gelöscht wird oder die Replikate im `StatefulSet` herunterskaliert werden.

- Die [Goaway-Chance-Option](#) im Kubernetes-API-Server verhindert, dass HTTP/2 Client-Verbindungen auf einer einzelnen API-Serverinstanz hängen bleiben, indem eine Verbindung nach dem Zufallsprinzip geschlossen wird. Wenn die Verbindung geschlossen wird, versucht der Client erneut, eine Verbindung herzustellen, und landet wahrscheinlich aufgrund des Load Balancers auf einem anderen API-Server. Die Amazon-EKS-Version 1.27 hat das `goaway-chance`-Flag aktiviert. Wenn Ihr Workload, der auf dem Amazon EKS-Cluster ausgeführt wird, einen Client verwendet, der nicht mit [HTTP GOAWAY](#) kompatibel ist, empfehlen wir Ihnen, Ihren Client so zu aktualisieren, dass er bei Verbindungsabbruch erneut eine Verbindung herstellt. GOAWAY

Das vollständige 1.27 Kubernetes-Changelog finden Sie unter [-1.27.md# 1260](#). <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-changelog-since-v>

Den aktuellen Cluster-Supportzeitraum anzeigen

Im Abschnitt Cluster-Supportzeitraum der AWS Konsole wird angezeigt, ob für Ihren Cluster derzeit Standard- oder erweiterter Support verfügbar ist. Wenn Ihr Cluster-Supportzeitraum „Erweiterter Support“ lautet, wird Ihnen der erweiterte EKS-Support in Rechnung gestellt.

Weitere Informationen zum Standard- und erweiterten Support finden Sie unter [the section called “Kubernetes-Versionen”](#).

1. Navigieren Sie im EKS-Bereich der AWS Konsole zur Seite Cluster. Vergewissern Sie sich, dass die Konsole auf dieselbe AWS Region eingestellt ist wie der Cluster, den Sie überprüfen möchten.
2. Sehen Sie sich die Spalte Support-Zeitraum an. Wenn der Wert `Standardsupport bis...` lautet, wird Ihnen derzeit kein erweiterter Support in Rechnung gestellt. Sie befinden sich innerhalb des Standard-Supportzeitraums. Wenn der Wert `Erweiterter Support...` lautet, wird für diesen Cluster derzeit der erweiterte Support in Rechnung gestellt.

Note

Der Support-Zeitraum kann nicht mit der AWS API oder CLI abgerufen werden.

Aktuelle Cluster-Upgrade-Richtlinie anzeigen

Die Cluster-Upgrade-Richtlinie legt fest, was mit Ihrem Cluster passiert, wenn der Standard-Supportzeitraum abgelaufen ist. Wenn Ihre Upgrade-Richtlinie `EXTENDED` gilt, wird der Cluster nicht automatisch aktualisiert und erhält stattdessen den erweiterten Support. Wenn Ihre Upgrade-Richtlinie `STANDARD` ist, wird der Server automatisch aktualisiert.

Die Versionsrichtlinie von Amazon EKS Controls for Kubernetes ermöglicht es Ihnen, das Ende des Standard-Supportverhaltens für Ihre EKS-Cluster festzulegen. Mit diesen Kontrollen können Sie entscheiden, für welche Cluster der erweiterte Support gewährt werden soll und für welche Cluster am Ende der Standardunterstützung für eine Kubernetes-Version automatisch ein Upgrade durchgeführt werden soll.

Eine Nebenversion wird in den ersten 14 Monaten nach ihrer Veröffentlichung standardmäßig in Amazon EKS unterstützt. Sobald das Ende des Standard-Supportdatums für eine Version überschritten ist, gilt für sie der erweiterte Support für die nächsten 12 Monate. Mit dem erweiterten Support können Sie gegen Aufpreis pro Cluster-Stunde länger bei einer bestimmten Kubernetes-Version bleiben. Sie können den erweiterten Support für einen EKS-Cluster aktivieren oder deaktivieren. Wenn Sie den erweiterten Support deaktivieren, AWS wird Ihr Cluster am Ende des Standardsupports automatisch auf die nächste Version aktualisiert. Wenn Sie den erweiterten Support aktivieren, können Sie gegen eine zusätzliche Gebühr für einen begrenzten Zeitraum bei der aktuellen Version bleiben. Planen Sie, Ihren Kubernetes-Cluster regelmäßig zu aktualisieren, auch wenn Sie den erweiterten Support nutzen.

Mithilfe der Eigenschaft können Sie die Versionsrichtlinie sowohl für neue als auch für bestehende Cluster festlegen. `supportType` Es gibt zwei Optionen, mit denen die Richtlinie für die Versionsunterstützung festgelegt werden kann:

- **STANDARD** — Ihr EKS-Cluster ist nach Ablauf des Standard-Supports für ein automatisches Upgrade geeignet. Bei dieser Einstellung fallen keine Gebühren für erweiterten Support an, aber Ihr EKS-Cluster wird automatisch auf die nächste unterstützte Kubernetes-Version im Standardsupport aktualisiert.
- **EXTENDED** — Ihr EKS-Cluster erhält den erweiterten Support, sobald der Standardsupport für die Kubernetes-Version ausläuft. Bei dieser Einstellung fallen Gebühren für den erweiterten Support an. Sie können Ihren Cluster auf eine standardmäßig unterstützte Kubernetes-Version aktualisieren, damit keine Gebühren für erweiterten Support anfallen. Cluster, die mit erweitertem Support ausgeführt werden, können am Ende des erweiterten Supports automatisch aktualisiert werden.

Extended Support ist standardmäßig für neue Cluster und bestehende Cluster aktiviert. Sie können in der oder mithilfe der AWS CLI überprüfen AWS Management Console, ob der erweiterte Support für einen Cluster aktiviert ist.

Important

Wenn Sie möchten, dass Ihr Cluster weiterhin die aktuelle Kubernetes-Version verwendet, um den erweiterten Support-Zeitraum nutzen zu können, müssen Sie die Upgrade-Richtlinie für den erweiterten Support vor dem Ende des Standard-Supportzeitraums aktivieren.

Sie können die Versionsunterstützungsrichtlinie für Ihre Cluster nur festlegen, wenn sie auf der Kubernetes-Version im Standardsupport ausgeführt werden. Sobald die Version in den erweiterten Support aufgenommen wurde, können Sie diese Einstellung erst ändern, wenn Sie eine Version mit Standardsupport verwenden.

Wenn Sie beispielsweise Ihre Richtlinie für die Versionsunterstützung auf „standard“ festgelegt haben, können Sie diese Einstellung nicht mehr ändern, nachdem die Kubernetes-Version, die auf Ihrem Cluster ausgeführt wird, das Ende des Standardsupports erreicht hat. Wenn Sie Ihre Versionsunterstützungsrichtlinie auf „extended“ festgelegt haben, können Sie diese Einstellung nicht mehr ändern, nachdem die auf Ihrem Cluster ausgeführte Kubernetes-Version das Ende der Standardunterstützung erreicht hat. Um die Richtlinieneinstellung für die Versionsunterstützung zu ändern, muss Ihr Cluster auf einer standardmäßig unterstützten Kubernetes-Version ausgeführt werden.

Cluster-Upgrade-Richtlinie anzeigen (Konsole)AWS

1. Navigieren Sie im EKS-Bereich der AWS Konsole zur Seite Cluster. Vergewissern Sie sich, dass die Konsole auf dieselbe AWS Region eingestellt ist wie der Cluster, den Sie überprüfen möchten.
2. Überprüfen Sie die Spalte Upgrade-Richtlinie. Wenn der Wert Standard Support ist, wird Ihr Cluster nicht in den erweiterten Support aufgenommen. Wenn der Wert Extended Support lautet, wird Ihr Cluster in den erweiterten Support aufgenommen.

Cluster-Upgrade-Richtlinie (AWS CLI) anzeigen

1. Stellen Sie sicher, dass die AWS CLI installiert ist und Sie angemeldet sind. [Erfahren Sie, wie Sie die AWS CLI aktualisieren und installieren.](#)

2. Ermitteln Sie den Namen Ihres EKS-Clusters. Stellen Sie die CLI auf dieselbe AWS Region wie Ihr EKS-Cluster ein.
3. Führen Sie den folgenden Befehl aus:

```
aws eks describe-cluster \
--name <cluster-name> \
--query "cluster.upgradePolicy.supportType"
```

4. Wenn der Wert ist `STANDARD`, wird Ihr Cluster nicht in den erweiterten Support aufgenommen. Wenn der Wert „ist“ `EXTENDED`, wird Ihr Cluster in den erweiterten Support aufgenommen.

Erhöhen Sie die Flexibilität bei der Planung von Kubernetes-Versionsupgrades, indem Sie den erweiterten EKS-Support aktivieren

In diesem Thema wird beschrieben, wie Sie die Upgrade-Richtlinie für einen EKS-Cluster festlegen, um erweiterten Support zu aktivieren. Die Upgrade-Richtlinie eines EKS-Clusters bestimmt, was passiert, wenn ein Cluster das Ende des Standard-Supportzeitraums erreicht. Wenn für eine Cluster-Upgrade-Richtlinie der erweiterte Support aktiviert ist, wird der erweiterte Supportzeitraum am Ende des Standard-Supportzeitraums aktiviert. Der Cluster wird am Ende des Standard-Supportzeitraums nicht automatisch aktualisiert.

Cluster, die sich tatsächlich im erweiterten Supportzeitraum befinden, sind mit höheren Kosten verbunden. Wenn für einen Cluster lediglich die Upgrade-Richtlinie zur Aktivierung des erweiterten Supports festgelegt ist und er sich ansonsten im Standard-Supportzeitraum befindet, fallen Standardkosten an.

Wenn Sie in der AWS Konsole einen Cluster erstellen, ist die Upgrade-Richtlinie so eingestellt, dass der erweiterte Support deaktiviert wird. Wenn Sie einen Cluster auf andere Weise erstellen, wird die Upgrade-Richtlinie so eingestellt, dass der erweiterte Support aktiviert wird. Bei Clustern, die mit der AWS API erstellt wurden, ist beispielsweise der erweiterte Support aktiviert.

Weitere Informationen zu Upgrade-Richtlinien finden Sie unter [the section called “Upgrade-Richtlinie anzeigen”](#).

 Important

Wenn Sie möchten, dass Ihr Cluster weiterhin die aktuelle Kubernetes-Version verwendet, um den erweiterten Supportzeitraum nutzen zu können, müssen Sie die Upgrade-Richtlinie für den erweiterten Support vor dem Ende des Standard-Supportzeitraums aktivieren. Wenn Sie den erweiterten Support nicht aktivieren, wird Ihr Cluster automatisch aktualisiert.

Aktivieren Sie den erweiterten EKS-Support (AWS Konsole)

1. Navigieren Sie in der AWS Konsole zu Ihrem EKS-Cluster. Wählen Sie auf der Cluster-Informationssseite die Registerkarte Overview aus.
2. Wählen Sie im Abschnitt Kubernetes-Versionseinstellungen die Option Verwalten aus.
3. Wählen Sie Erweiterter Support und dann Änderungen speichern aus.

Aktivieren Sie die erweiterte EKS-Unterstützung (AWS CLI)

1. Stellen Sie sicher, dass die AWS CLI installiert ist und Sie angemeldet sind. [Erfahren Sie, wie Sie die AWS CLI aktualisieren und installieren.](#)
2. Ermitteln Sie den Namen Ihres EKS-Clusters.
3. Führen Sie den folgenden Befehl aus:

```
aws eks update-cluster-config \
--name <cluster-name> \
--upgrade-policy supportType=EXTENDED
```

Vermeiden Sie erhöhte Cluster-Kosten, indem Sie den erweiterten EKS-Support deaktivieren

In diesem Thema wird beschrieben, wie Sie die Upgrade-Richtlinie eines EKS-Clusters so einrichten, dass der erweiterte Support deaktiviert wird. Die Upgrade-Richtlinie eines EKS-Clusters bestimmt, was passiert, wenn ein Cluster das Ende des Standard-Supportzeitraums erreicht. Wenn für eine Cluster-Upgrade-Richtlinie der erweiterte Support deaktiviert ist, wird sie automatisch auf die nächste Kubernetes-Version aktualisiert.

Weitere Informationen zu Upgrade-Richtlinien finden Sie unter. [the section called “Upgrade-Richtlinie anzeigen”](#)

 Important

Sie können den erweiterten Support nicht mehr deaktivieren, sobald Ihr Cluster ihn hinzugefügt hat. Sie können den erweiterten Support für Cluster nur im Standard-Support deaktivieren.

AWS empfiehlt, Ihren Cluster auf eine Version im Standard-Supportzeitraum zu aktualisieren.

Deaktivieren Sie den erweiterten EKS-Support (AWS Konsole)

1. Navigieren Sie in der AWS Konsole zu Ihrem EKS-Cluster. Wählen Sie auf der Cluster-Informationssseite die Registerkarte Overview aus.
2. Wählen Sie im Abschnitt Kubernetes-Versionseinstellungen die Option Verwalten aus.
3. Wählen Sie Standardsupport und dann Änderungen speichern aus.

Deaktivieren Sie die erweiterte EKS-Unterstützung (AWS CLI)

1. Stellen Sie sicher, dass die AWS CLI installiert ist und Sie angemeldet sind. [Erfahren Sie, wie Sie die AWS CLI aktualisieren und installieren.](#)
2. Ermitteln Sie den Namen Ihres EKS-Clusters.
3. Führen Sie den folgenden Befehl aus:

```
aws eks update-cluster-config \
--name <cluster-name> \
--upgrade-policy supportType=STANDARD
```

Amazon EKS-Plattformversionen für jede Kubernetes-Version anzeigen

Amazon-EKS-Plattformversionen definieren die Funktionalitäten der Amazon-EKS-Cluster-Steuerebene (z. B. welche Kubernetes-API-Server-Flags aktiviert sind) sowie die aktuelle Kubernetes-Patch-Version. Jede Kubernetes-Minor-Version hat eine oder mehrere zugehörige

Amazon-EKS-Plattformversionen. Die Plattformversionen für verschiedene Kubernetes-Minor-Versionen sind voneinander unabhängig. Sie können die [aktuelle Plattformversion Ihres Clusters mit der AWS CLI oder abrufen](#) AWS Management Console. Wenn Sie einen lokalen Cluster auf AWS Outposts haben, lesen Sie [the section called “Versionen der EKS-Plattform”](#) statt dieses Themas weiter.

Wenn eine neue Kubernetes-Nebenversion in Amazon EKS verfügbar ist, z. B. 1.33, beginnt die erste Amazon EKS-Plattformversion für diese Kubernetes-Nebenversion bei. eks . 1 Allerdings veröffentlicht Amazon EKS regelmäßig neue Plattformversionen, um neue Einstellungen für die Kubernetes-Steuerebene und Sicherheitsfixes bereitzustellen.

Wenn neue Amazon-EKS-Plattformversionen für eine Minor-Version verfügbar werden:

- Die Versionsnummer der Amazon-EKS-Plattform wird erhöht (eks . <n+1>).
- Amazon EKS aktualisiert automatisch alle bestehenden Cluster auf die neueste Amazon-EKS-Plattformversion für die entsprechende Kubernetes-Minor-Version. Automatische Upgrades bestehender Amazon-EKS-Plattformversionen werden schrittweise durchgeführt. Der Rollout-Prozess kann einige Zeit in Anspruch nehmen. Wenn Sie die neuesten Funktionen der Amazon-EKS-Plattformversion sofort benötigen, sollten Sie einen neuen Amazon-EKS-Cluster erstellen.

Wenn Ihr Cluster mehr als zwei Plattformversionen hinter der aktuellen Plattformversion zurückliegt, war Amazon EKS möglicherweise nicht in der Lage, Ihren Cluster automatisch zu aktualisieren. Einzelheiten dazu, was dies verursachen kann, finden Sie unter [the section called “Die Amazon-EKS-Plattformversion liegt mehr als zwei Versionen hinter der aktuellen Plattformversion”](#).

- Amazon EKS veröffentlicht möglicherweise ein neues Knoten-AMI mit einer entsprechenden Patch-Version. Alle Patch-Versionen sind jedoch zwischen der EKS-Steuerebene und dem Knoten AMIs für eine bestimmte Kubernetes-Nebenversion kompatibel.

Neue Versionen der Amazon EKS-Plattform führen nicht zu grundlegenden Änderungen oder Betriebsunterbrechungen.

Cluster werden immer mit der neuesten verfügbaren Amazon-EKS-Plattformversion (eks . <n>) für die angegebene Kubernetes-Version erstellt. Wenn Sie Ihren Cluster auf eine neue Kubernetes-Minor-Version aktualisieren, erhält Ihr Cluster die aktuelle Amazon-EKS-Plattformversion für die Kubernetes-Minor-Version, auf die Sie aktualisiert haben.

Die aktuellen und kürzlichen Amazon-EKS-Plattformversionen sind in den folgenden Tabellen beschrieben.

 Note

AWS hat kürzlich einige Plattformversionen deaktiviert, die im Juni 2024 veröffentlicht wurden. Die Plattformversionen hatten Stabilitätsprobleme. Keine Aktion erforderlich.

Um Benachrichtigungen über alle Änderungen an der Quelldatei auf dieser speziellen Dokumentationsseite zu erhalten, können Sie die folgende URL mit einem RSS-Reader abonnieren:

```
https://github.com/awsdocs/amazon-eks-user-guide/commits/mainline/latest/ug/clusters/platform-versions.adoc.atom
```

Kubernetes-Version **1.33**

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.33-Plattformversionen: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.33.1	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025
1.33.1	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025
1.33.1	eks.4	Erste Veröffentlichung der Kubernete	28. Mai 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
		s-Version 1.33 für EKS. Weitere Informationen finden Sie unter the section called “Kubernetes 1.33” .	

Kubernetes-Version 1.32

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.32-Plattformversionen:

NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.32.5	eks.13	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025
1.32.5	eks.12	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025
1.32.5	eks.11	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.32.3	eks.10	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025
1.32.3	eks.9	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.32.3	eks.8	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.32.3	eks.7	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.32.3	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.32.2	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.32.2	eks.4	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.32.1	eks.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.32.0	eks.2	Erste Veröffentlichung der Kubernetes-Version 1.32 für EKS. Weitere Informationen finden Sie unter the section called “Kubernetes 1.32” .	Januar 2025

Kubernetes-Version 1.31

Die folgenden Zugangssteuerungen sind für alle 1.31-Plattformversionen aktiviert: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota, ObjectCount.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.31.9	eks.29	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025
1.31.9	eks.28	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.31.9	eks.27	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai 2025
1.31.7	eks.26	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025
1.31.7	eks.25	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.31.7	eks.24	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.31.7	eks.23	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.31.7	eks.22	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.31.6	eks.21	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.31.6	eks.20	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.31.5	eks.19	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.31.5	eks.18	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025
1.31.4	eks.17	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2025
1.31.2	eks.12	Neue Plattformversion mit Unterstützung für Amazon EKS Hybrid Nodes und Verbesserungen der Beobachtbarkeit der Kontrollebene. Erfahren Sie the section called “Hybridknoten” , wie Amazon EKS die Leistungsbeobachtbarkeit entsprechend verbessert.	15. November 2024
1.31.1	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	21. Oktober 2024
1.31.0	eks.4	Erste Veröffentlichung der Kubernetes-Version 1.31 für EKS. Weitere Informationen finden Sie unter the section called “Kubernetes 1.31” .	26. September 2024

Kubernetes-Version 1.30

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.30-Plattformversionen:

NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.30.13	eks.37	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025
1.30.13	eks.36	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025
1.30.13	eks.35	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai 2025
1.30.11	eks.34	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025
1.30.11	eks.33	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.30.11	eks.32	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.30.11	eks.31	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.30.11	eks.30	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.30.10	eks.29	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.30.10	eks.28	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.30.9	eks.27	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025
1.30.8	eks.25	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2025
1.30.8	eks.24	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. Januar 2025
1.30.7	eks.23	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.30.6	eks.22	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.30.6	eks.21	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.30.6	eks.20	Neue Plattformversion mit Unterstützung für Amazon EKS Hybrid Nodes und Verbesserungen der Beobachtbarkeit der Kontrollebene. Erfahren Sie the section called “Hybridknoten” , wie Amazon EKS die Leistungsbeobachtbarkeit entsprechend verbessert .	15. November 2024
1.30.5	eks.12	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	21. Oktober 2024
1.30.4	eks.8	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. September 2024
1.30.3	eks.7	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	28. August 2024
1.30.3	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. August 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.30.2	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. Juli 2024
1.30.0	eks.2	Erste Veröffentlichung der Kubernetes-Version 1.30 für EKS. Weitere Informationen finden Sie unter the section called “Kubernetes 1.30” .	23. Mai 2024

Kubernetes-Version 1.29

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.29-Plattformversionen: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.29.15	eks.40	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025
1.29.15	eks.39	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.29.15	eks.38	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai 2025
1.29.15	eks.37	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025
1.29.15	eks.36	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.29.15	eks.35	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.29.15	eks.34	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.29.15	eks.33	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.29.14	eks.32	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.29.14	eks.31	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.29.13	eks.30	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.29.13	eks.29	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025
1.29.12	eks.28	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	20. Januar 2025
1.29.12	eks.27	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. Januar 2025
1.29.11	eks.26	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.29.10	eks.25	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.29.10	eks.24	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.29.10	eks.23	Neue Plattformversion mit Unterstützung für Amazon EKS Hybrid Nodes und Verbesserungen der Beobachtbarkeit der Kontrollebene. Erfahren Sie the section called “Hybridknoten” , wie Amazon EKS die Leistungsbeobachtbarkeit entsprechend verbessert .	15. November 2024
1.29.9	eks.17	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	21. Oktober 2024
1.29.8	eks.13	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. September 2024
1.29.7	eks.12	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	28. August 2024
1.29.7	eks.11	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. August 2024
1.29.6	eks.10	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. Juli 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.29.4	eks.7	Neue Plattformversion mit CoreDNS-Autoscaling, Sicherheitskorrekturen und Verbesserungen. Weitere Informationen zur automatischen CoreDNS-Skalierung finden Sie unter. the section called “Skalieren Sie für hohen Traffic”	16. Mai 2024
1.29.3	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2024
1.29.1	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. März 2024
1.29.1	eks.4	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	20. März 2024
1.29.1	eks.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. März 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.29.0	eks.1	Erste Veröffentlichung der Kubernetes-Version 1.29 für EKS. Weitere Informationen finden Sie unter the section called “Kubernetes 1.29” .	23. Januar 2024

Kubernetes-Version 1.28

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.28-Plattformversionen:

NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.28.15	eks.46	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025
1.28.15	eks.45	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025
1.28.15	eks.44	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai. 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.28.15	eks.43	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025
1.28.15	eks.42	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.28.15	eks.41	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.28.15	eks.40	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.28.15	eks.39	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.28.15	eks.38	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.28.15	eks.37	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.28.15	eks.36	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025
1.28.15	eks.34	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.28.15	eks.33	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. Januar 2025
1.28.15	eks.32	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.28.15	eks.31	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.28.15	eks.30	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.28.15	eks.29	Neue Plattformversion mit Unterstützung für Amazon EKS Hybrid Nodes und Verbesserungen der Beobachtbarkeit der Kontrollebene. Erfahren Sie the section called “Hybridknoten” , wie Amazon EKS die Leistungsbeobachtbarkeit entsprechend verbessert .	15. November 2024
1.28.14	eks.23	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	21. Oktober 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.28.13	eks.19	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. September 2024
1.28.12	eks.18	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	28. August 2024
1.28.11	eks.17	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. August 2024
1.28.11	eks.16	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. Juli 2024
1.28.9	eks.13	Neue Plattformversion mit CoreDNS-Autoscaling, Sicherheitskorrekturen und Verbesserungen. Weitere Informationen zur automatischen CoreDNS-Skalierung finden Sie unter the section called “Skalieren Sie für hohen Traffic”	16. Mai 2024
1.28.8	eks.12	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.28.7	eks.11	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. März 2024
1.28.7	eks.10	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	20. März 2024
1.28.6	eks.9	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. März 2024
1.28.5	eks.7	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2024
1.28.4	eks.6	Neue Plattformversion mit Zugangseinträgen , Sicherheitskorrekturen und Verbesserungen.	14. Dezember 2023
1.28.4	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. Dezember 2023
1.28.3	eks.4	Neue Plattformversion mit Erfahren Sie, wie EKS Pod Identity Pods Zugriff auf AWS Dienste, Sicherheitskorrekturen und Verbesserungen gewährt.	10. November 2023

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.28.3	eks.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. November 2023
1.28.2	eks.2	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Oktober 2023
1.28.1	eks.1	Erste Veröffentlichung der Kubernetes-Version 1.28 für EKS. Weitere Informationen finden Sie unter the section called "Kubernetes 1.28" .	26. September 2023

Kubernetes-Version 1.27

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.27-Plattformversionen: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.16	eks.50	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	26. Juni 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.16	eks.49	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025
1.27.16	eks.48	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai 2025
1.27.16	eks.47	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025
1.27.16	eks.46	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.27.16	eks.45	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.27.16	eks.44	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.27.16	eks.43	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.27.16	eks.42	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.27.16	eks.41	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.16	eks.40	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.27.16	eks.38	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2025
1.27.16	eks.37	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. Januar 2025
1.27.16	eks.36	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.27.16	eks.35	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.27.16	eks.34	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.27.16	eks.33	Neue Plattformversion mit Unterstützung für Amazon EKS Hybrid Nodes, Sicherheitskorrekturen und Verbesserungen. Weitere Informationen zu Amazon EKS-Hybridknoten finden Sie unter the section called “Hybridknoten” .	15. November 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.16	eks.27	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	21. Oktober 2024
1.27.16	eks.23	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. September 2024
1.27.16	eks.22	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	28. August 2024
1.27.16	eks.21	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. August 2024
1.27.15	eks.20	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. Juli 2024
1.27.13	eks.17	Neue Plattformversion mit CoreDNS-Autoscaling, Sicherheitskorrekturen und Verbesserungen. Weitere Informationen zur automatischen CoreDNS-Skalierung finden Sie unter the section called “Skalieren Sie für hohen Traffic”	16. Mai 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.12	eks.16	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2024
1.27.11	eks.15	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. März 2024
1.27.11	eks.14	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	20. März 2024
1.27.10	eks.13	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. März 2024
1.27.9	eks.11	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2024
1.27.8	eks.10	Neue Plattformversion mit Zugangseinträgen , Sicherheitskorrekturen und Verbesserungen.	14. Dezember 2023
1.27.8	eks.9	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. Dezember 2023

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.7	eks.8	Neue Plattformversion mit Erfahren Sie, wie EKS Pod Identity Pods Zugriff auf AWS Dienste, Sicherheitskorrekturen und Verbesserungen gewährt.	10. November 2023
1.27.7	eks.7	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. November 2023
1.27.6	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Oktober 2023
1.27.4	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. August 2023
1.27.4	eks.4	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Juli 2023
1.27.3	eks.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Juni 2023
1.27.2	eks.2	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. Juni 2023

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.27.1	eks.1	Erste Veröffentlichung der Kubernetes-Version 1.27 für EKS. Weitere Informationen finden Sie unter the section called “Kubernetes 1.27” .	24. Mai 2023

Kubernetes-Version 1.26

Die folgenden Zugangssteuerungen sind für alle aktiviert 1.26-Plattformversionen:

NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.26.15	eks.51	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	11. Juni 2025
1.26.15	eks.50	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Mai 2025
1.26.15	eks.49	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Mai 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.26.15	eks.48	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. April 2025
1.26.15	eks.47	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.26.15	eks.46	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2025
1.26.15	eks.45	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2025
1.26.15	eks.44	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. März 2025
1.26.15	eks.43	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	4. März 2025
1.26.15	eks.42	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	24. Februar 2025
1.26.15	eks.40	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2025
1.26.15	eks.39	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. Januar 2025

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.26.15	eks.38	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.26.15	eks.37	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.26.15	eks.36	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	13. Dezember 2024
1.26.15	eks.35	Neue Plattformversion mit Unterstützung für Amazon EKS Hybrid Nodes, Sicherheitskorrekturen und Verbesserungen. Weitere Informationen zu Amazon EKS-Hybridknoten finden Sie unter the section called “Hybridknoten” .	15. November 2024
1.26.15	eks.28	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	21. Oktober 2024
1.26.15	eks.24	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. September 2024
1.26.15	eks.23	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	28. August 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.26.15	eks.22	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. August 2024
1.26.15	eks.21	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. Juli 2024
1.26.15	eks.18	Neue Plattformversion mit CoreDNS-Autoscaling, Sicherheitskorrekturen und Verbesserungen. Weitere Informationen zur automatischen CoreDNS-Skalierung finden Sie unter. the section called “Skalieren Sie für hohen Traffic”	16. Mai 2024
1.26.15	eks.17	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	18. April 2024
1.26.14	eks.16	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	29. März 2024
1.26.14	eks.15	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	20. März 2024

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.26.13	eks.14	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. März 2024
1.26.12	eks.12	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	17. Januar 2024
1.26.11	eks.11	Neue Plattformversion mit Zugangseinträgen , Sicherheitskorrekturen und Verbesserungen.	14. Dezember 2023
1.26.11	eks.10	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	12. Dezember 2023
1.26.10	eks.9	Neue Plattformversion mit Erfahren Sie, wie EKS Pod Identity Pods Zugriff auf AWS Dienste, Sicherheitskorrekturen und Verbesserungen gewährt.	10. November 2023
1.26.10	eks.8	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	3. November 2023
1.26.9	eks.7	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	16. Oktober 2023

Kubernetes-Version	EKS-Plattformversionen	Versionshinweise	Datum der Veröffentlichung
1.26.7	eks.6	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. August 2023
1.26.7	eks.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Juli 2023
1.26.6	eks.4	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Juni 2023
1.26.5	eks.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	9. Juni 2023
1.26.4	eks.2	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	5. Mai 2023
1.26.2	eks.1	Erste Veröffentlichung der Kubernetes-Version 1.26 für EKS.	11. April 2023

Holen Sie sich die aktuelle Plattformversion

1. Öffnen Sie die Amazon-EKS-Konsole.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie in der Clusterliste den Clusternamen aus, von dem Sie die Plattformversion überprüfen möchten.
4. Wählen Sie die Übersicht-Registerkarte.
5. Die Plattformversion ist unter im Abschnitt Details verfügbar.

6. Ermitteln Sie den Namen des Clusters, dessen Plattformversion Sie überprüfen möchten.
7. Führen Sie den folgenden Befehl aus:

```
aws eks describe-cluster --name my-cluster --query cluster.platformVersion
```

Eine Beispielausgabe sieht wie folgt aus.

```
"eks.10"
```

Plattformversion ändern

Sie können die Plattformversion eines EKS-Clusters nicht ändern. Wenn neue Amazon EKS-Plattformversionen für eine Kubernetes-Version verfügbar werden, aktualisiert EKS automatisch alle vorhandenen Cluster auf die neueste Amazon EKS-Plattformversion für die entsprechende Kubernetes-Version. Automatische Upgrades bestehender Amazon-EKS-Plattformversionen werden schrittweise durchgeführt. Sie können die AWS Konsole oder CLI nicht verwenden, um die Plattformversion zu ändern.

Wenn Sie Ihre Kubernetes-Version aktualisieren, wechselt Ihr Cluster auf die neueste Plattformversion für die Kubernetes-Version.

Skalieren Sie Cluster-Computing mit Karpenter und Cluster Autoscaler

Die automatische Skalierung ist eine Funktion, die Ihre Ressourcen automatisch nach oben oder unten skaliert, um wechselnden Anforderungen gerecht zu werden. Dies ist eine wichtige Kubernetes-Funktion, die ansonsten umfangreiche Personalressourcen erfordern würde, um manuell zu arbeiten.

Automatischer EKS-Modus

Amazon EKS Auto Mode skaliert die Cluster-Rechenressourcen automatisch. Wenn ein Pod nicht auf vorhandene Knoten passt, erstellt der automatische Modus von EKS einen neuen. Der EKS-Automatikmodus konsolidiert auch Workloads und löscht Knoten. Der EKS Auto Mode baut auf Karpenter auf.

Weitere Informationen finden Sie unter:

- [Automatischer EKS-Modus](#)
- [the section called “Erstellen Sie einen Knotenpool”](#)
- [the section called “Stellen Sie einen aufgeblasenen Workload bereit”](#)

Zusätzliche Lösungen

Amazon EKS unterstützt zwei zusätzliche Autoscaling-Produkte:

Karpenter

Karpenter ist ein flexibler, leistungsstarker Kubernetes-Cluster-Autoscaler, der zur Verbesserung der Anwendungsverfügbarkeit und Cluster-Effizienz beiträgt. Karpenter startet Rechenressourcen in der richtigen Größe (z. B. EC2 Amazon-Instances) als Reaktion auf die sich ändernde Anwendungslast in weniger als einer Minute. Durch die Integration von Kubernetes mit kann Karpenter just-in-time Rechenressourcen bereitstellen AWS, die genau den Anforderungen Ihrer Arbeitslast entsprechen. Karpenter stellt automatisch neue Rechenressourcen basierend auf den spezifischen Anforderungen von Cluster-Workloads bereit. Dazu gehören Rechen-, Speicher-, Beschleunigungs- und Planungsanforderungen. Amazon EKS unterstützt Cluster, die Karpenter verwenden, obwohl Karpenter mit jedem konformierten Kubernetes-Cluster zusammenarbeitet. Weitere Informationen finden Sie in der [Karpenter](#)-Dokumentation.

Important

Karpenter ist Open-Source-Software, für deren Installation, Konfiguration und Verwaltung die AWS Kunden in ihren Kubernetes-Clustern verantwortlich sind. AWS bietet technischen Support, wenn Karpenter unverändert mit einer kompatiblen Version in Amazon EKS-Clustern ausgeführt wird. Es ist wichtig, dass Kunden die Verfügbarkeit und Sicherheit des Karpenter Controllers sowie die entsprechenden Testverfahren beibehalten, wenn sie ihn oder den Kubernetes-Cluster, in dem er läuft, aktualisieren, genau wie jede andere vom Kunden verwaltete Software. Für Karpenter gibt es kein AWS Service Level Agreement (SLA), und die Kunden sind dafür verantwortlich, sicherzustellen, dass die von Karpenter gestarteten EC2 Instanzen ihren Geschäftsanforderungen entsprechen.

Cluster-Autoscaler

Der Kubernetes Cluster Autoscaler passt die Anzahl der Knoten in Ihrem Cluster automatisch an, wenn Pods ausfallen oder auf andere Knoten umgeplant werden. Der Cluster Autoscaler verwendet Auto-Scaling-Gruppen. Weitere Informationen finden Sie unter [Cluster Autoscaler on AWS](#).

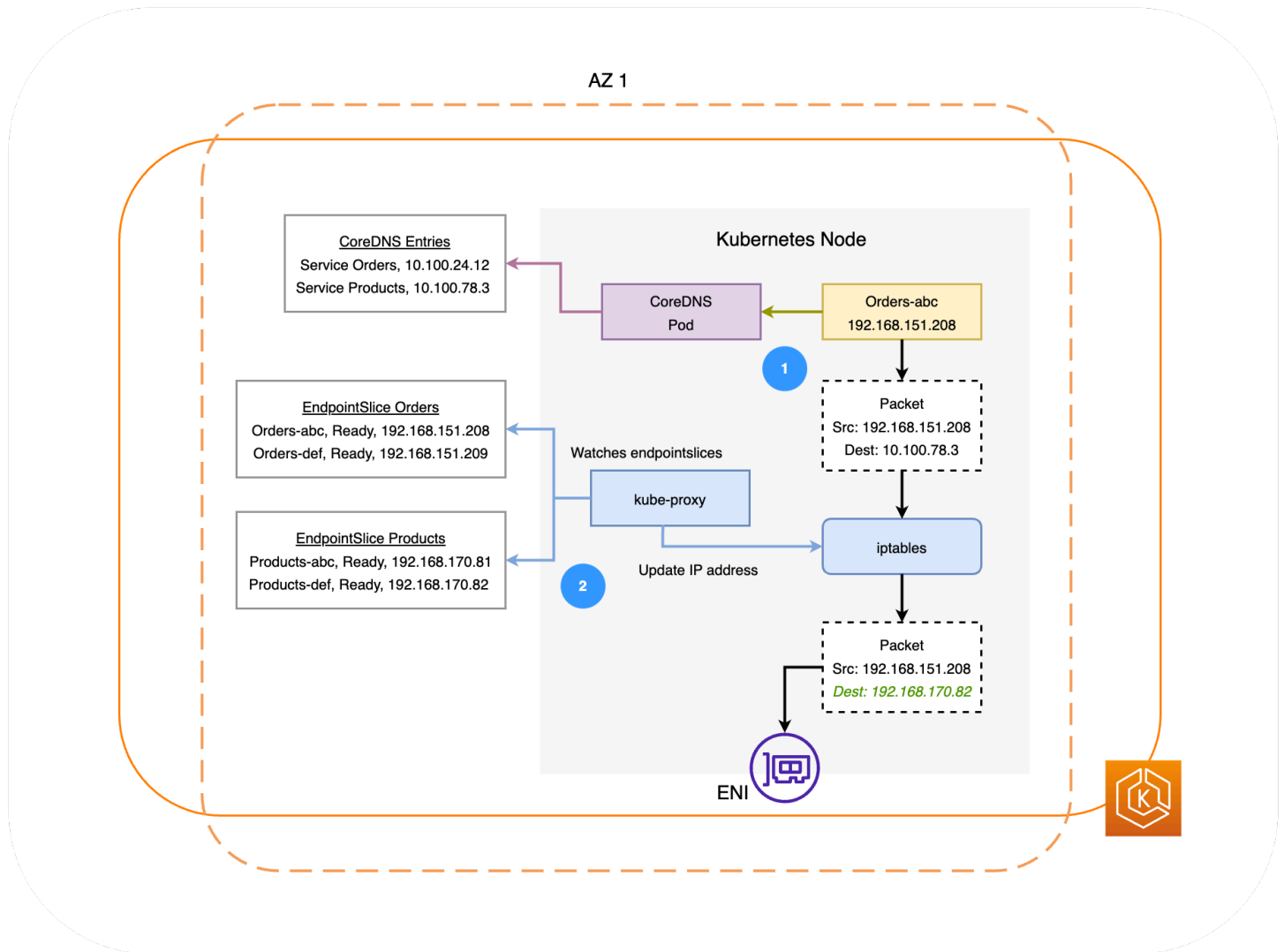
Erfahren Sie mehr über Zonal Shift von Amazon Application Recovery Controller (ARC) in Amazon EKS

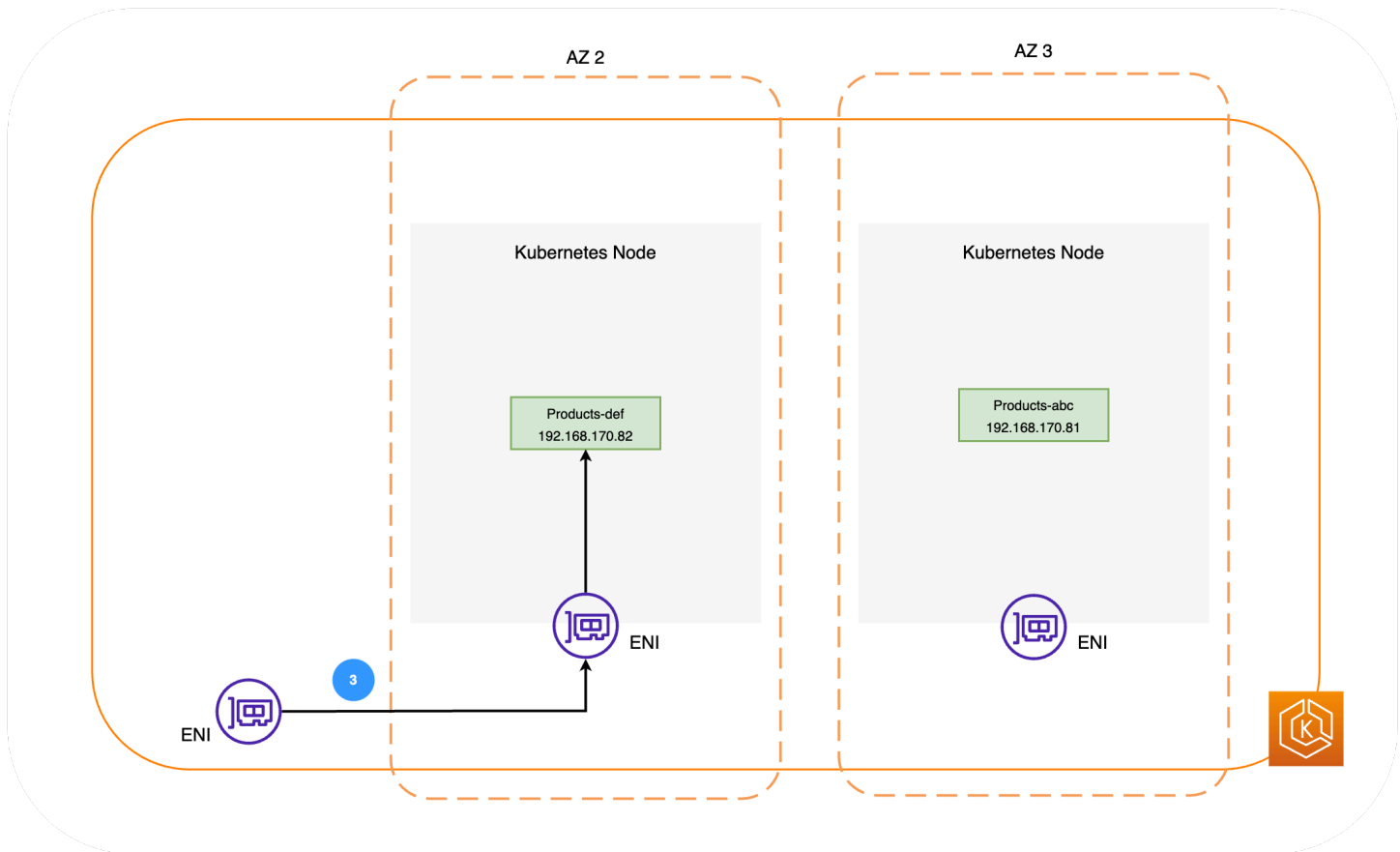
Kubernetes verfügt über native Funktionen, mit denen Sie Ihre Anwendungen widerstandsfähiger gegen Ereignisse wie den verschlechterten Zustand oder die Beeinträchtigung einer Availability Zone (AZ) machen können. Wenn Sie Ihre Workloads in einem Amazon EKS-Cluster ausführen, können Sie die Fehlertoleranz und Anwendungswiederherstellung Ihrer Anwendungsumgebung mit [Zonal Shift oder Zonal Autoshift von Amazon Application Recovery Controller \(ARC\)](#) weiter verbessern. ARC Zonal Shift ist als vorübergehende Maßnahme konzipiert, mit der Sie den Verkehr für eine Ressource von einer beeinträchtigten AZ wegverlagern können, bis die Zonenverschiebung abläuft oder Sie sie stornieren. Sie können die Zonenverschiebung bei Bedarf verlängern.

Sie können eine Zonenverschiebung für einen EKS-Cluster starten, oder Sie können es für AWS sich selbst erledigen lassen, indem Sie Zonal Autoshift aktivieren. Durch diese Verschiebung wird der east-to-west Netzwerkdatenverkehr in Ihrem Cluster aktualisiert, sodass nur Netzwerkendpunkte für Pods berücksichtigt werden, die auf Worker-Knoten ausgeführt werden, die fehlerfrei sind. AZs Darüber hinaus leitet jeder ALB oder NLB, der den eingehenden Datenverkehr für Anwendungen in Ihrem EKS-Cluster verarbeitet, den Datenverkehr automatisch an fehlerfreie Ziele weiter. AZs Für Kunden, die die höchsten Verfügbarkeitsziele anstreben, kann es für den Fall, dass eine AZ beeinträchtigt wird, wichtig sein, den gesamten Datenverkehr von der beeinträchtigten AZ fernzuhalten, bis er wieder hergestellt ist. Zu diesem Zweck können Sie auch [eine ALB oder NLB mit ARC-Zonenverschiebung aktivieren](#).

Grundlegendes zum Ost-West-Netzwerkdatenverkehr zwischen Pods

Das folgende Diagramm zeigt zwei Beispiele für Workloads: Bestellungen und Produkte. In diesem Beispiel soll gezeigt werden, wie Workloads und Pods in verschiedenen AZs Umgebungen miteinander kommunizieren.





1. Damit Bestellungen mit Produkten kommunizieren können, muss zuerst der DNS-Name des Zieldienstes aufgelöst werden. Bestellungen kommunizieren mit CoreDNS, um die virtuelle IP-Adresse (Cluster-IP) für diesen Dienst abzurufen. Sobald Orders den Servicenamen des Produkts aufgelöst hat, wird Datenverkehr an diese Ziel-IP gesendet.
2. Der Kube-Proxy läuft auf jedem Knoten im Cluster und überwacht kontinuierlich nach Diensten. [EndpointSlices](#) Wenn ein Service erstellt wird, EndpointSlice wird ein Service im Hintergrund vom Controller erstellt und verwaltet. EndpointSlice Jeder EndpointSlice hat eine Liste oder Tabelle mit Endpunkten, die eine Teilmenge von Pod-Adressen zusammen mit den Knoten enthält, auf denen sie ausgeführt werden. Der Kube-Proxy richtet Routing-Regeln für jeden dieser Pod-Endpunkte ein, die auf den Knoten verwendet werden. `iptables` Der Kube-Proxy ist auch für eine grundlegende Form des Lastenausgleichs verantwortlich, indem er den an die Cluster-IP eines Dienstes gerichteten Datenverkehr umleitet, sodass er stattdessen direkt an die IP-Adresse eines Pods gesendet wird. Der Kube-Proxy tut dies, indem er die Ziel-IP auf der ausgehenden Verbindung neu schreibt.
3. Die Netzwerkpakete werden dann über die jeweiligen Knoten an den Products-Pod in AZ 2 gesendet (wie in der Abbildung oben dargestellt). ENIs

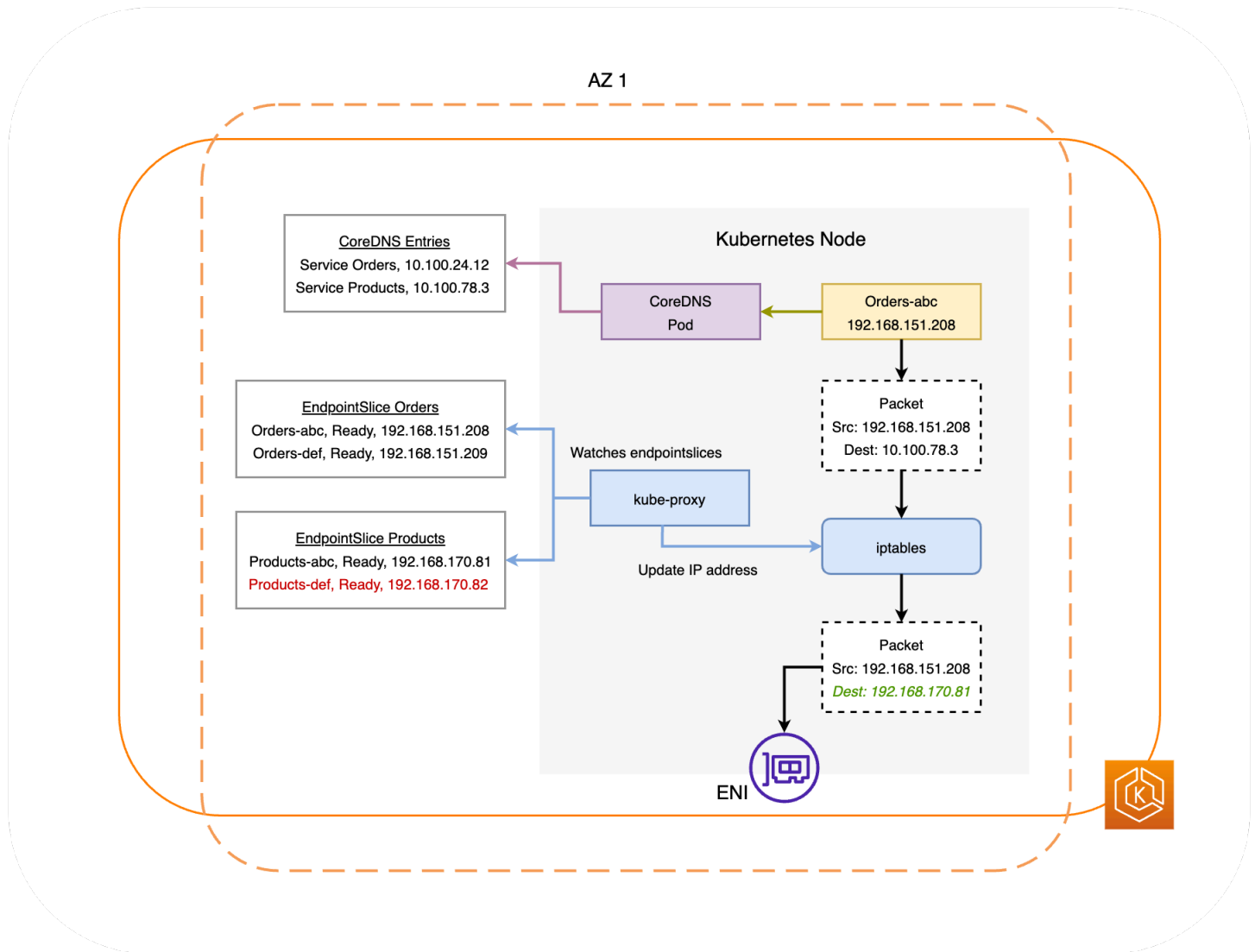
Grundlegendes zu ARC Zonal Shift in Amazon EKS

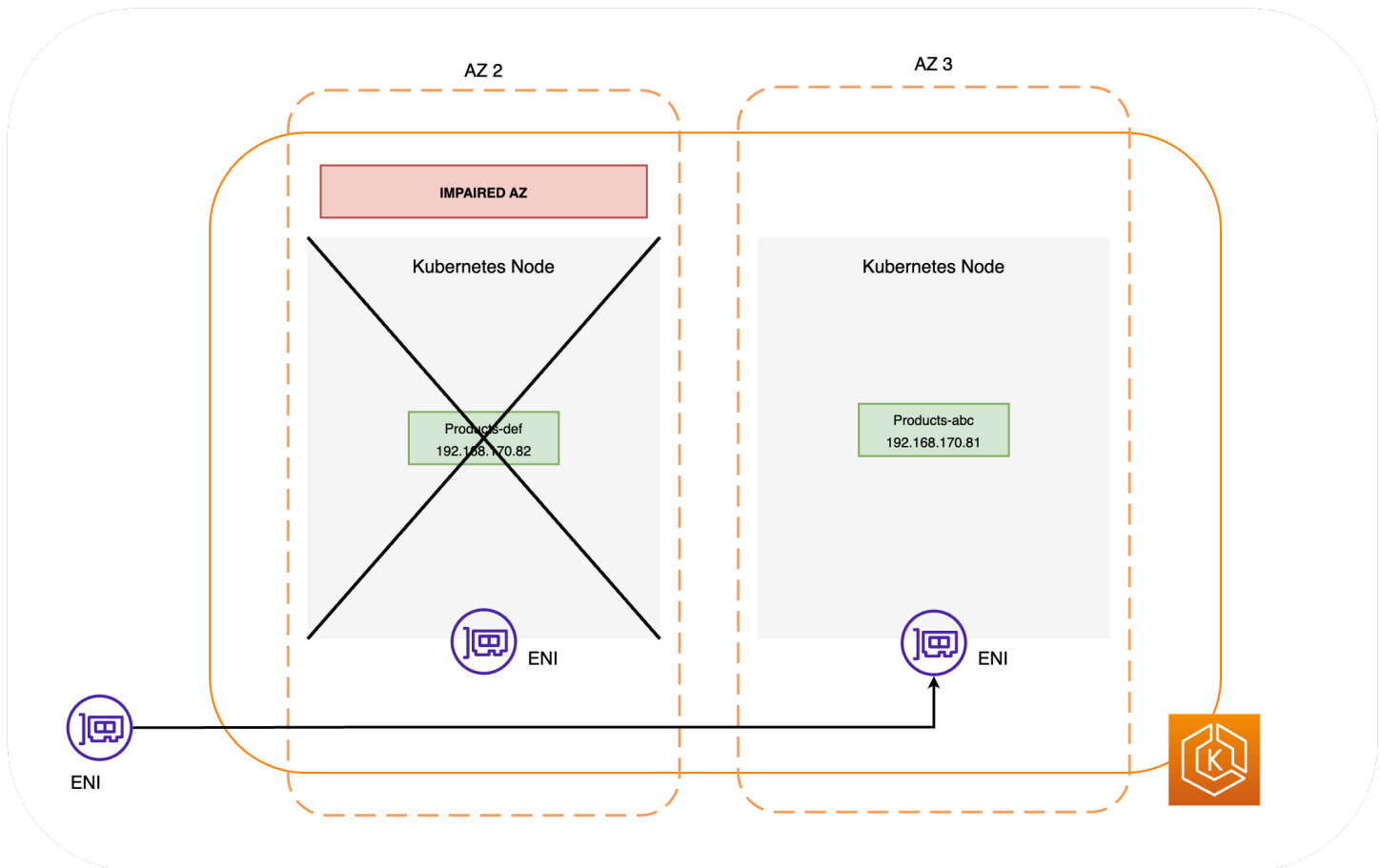
Falls es in Ihrer Umgebung zu einer Beeinträchtigung der AZ-Verfügbarkeit kommt, können Sie eine Zonenverschiebung für Ihre EKS-Cluster-Umgebung einleiten. Alternativ können AWS Sie sich dies mit Zonal Autoshift selbst vornehmen lassen. Mit Zonal Autoshift AWS wird der gesamte Zustand der AZ überwacht und auf eine mögliche Beeinträchtigung der AZ reagiert, indem der Verkehr in Ihrer Cluster-Umgebung automatisch von der beeinträchtigten AZ weggeleitet wird.

Sobald Ihr Amazon EKS-Cluster Zonal Shift mit ARC aktiviert hat, können Sie mit der ARC-Konsole, der AWS CLI oder Zonal Shift und Zonal Autoshift eine Zonal Shift auslösen oder Zonal Autoshift aktivieren. APIs Während einer EKS-Zonenverschiebung findet automatisch Folgendes statt:

- Alle Knoten in der betroffenen AZ werden gesperrt. Dadurch wird verhindert, dass der Kubernetes Scheduler neue Pods auf den Knoten in der fehlerhaften AZ plant.
- Wenn Sie [Managed Node Groups](#) verwenden, wird das [Rebalancing der Availability Zone](#) ausgesetzt und Ihre Auto Scaling Group (ASG) wird aktualisiert, um sicherzustellen, dass neue EKS-Datenplane-Knoten nur im fehlerfreien Zustand gestartet werden. AZs
- Die Knoten in der fehlerhaften AZ werden nicht beendet und die Pods werden nicht aus diesen Knoten entfernt. Auf diese Weise soll sichergestellt werden, dass Ihr Datenverkehr nach Ablauf oder Ausfall einer Zonenschicht sicher an die AZ zurückgesendet werden kann, wo immer noch die volle Kapazität vorhanden ist
- Der EndpointSlice Controller findet alle Pod-Endpunkte in der beeinträchtigten AZ und entfernt sie aus der entsprechenden Zone. EndpointSlices Dadurch wird sichergestellt, dass nur Pod-Endpunkte, die sich in einem fehlerfreien AZs Zustand befinden, gezielt Netzwerkverkehr empfangen. Wenn eine Zonenverschiebung storniert wird oder abläuft, aktualisiert der EndpointSlice Controller das so, dass die EndpointSlices Endpunkte in die wiederhergestellte AZ aufgenommen werden.

Die folgenden Diagramme zeigen auf grober Ebene, wie EKS Zonal Shift sicherstellt, dass nur funktionsfähige Pod-Endpunkte in Ihrer Cluster-Umgebung ins Visier genommen werden.





Anforderungen an EKS Zonal Shift

Damit Zonal Shift in EKS erfolgreich funktioniert, müssen Sie Ihre Cluster-Umgebung zuvor so einrichten, dass sie gegen eine Beeinträchtigung der AZ resistent ist. Im Folgenden finden Sie eine Liste der Schritte, die Sie befolgen müssen.

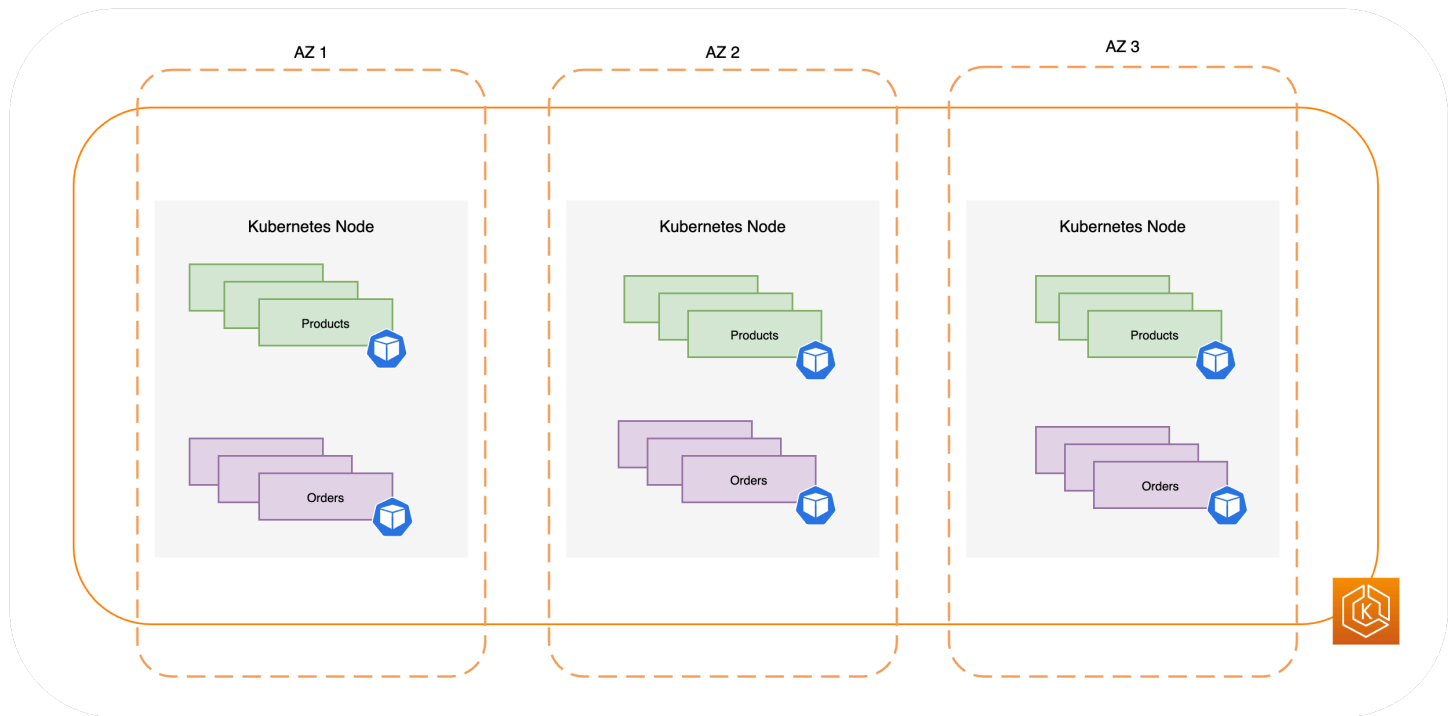
- Stellen Sie die Worker-Knoten Ihres Clusters über mehrere AZs
- Stellen Sie genügend Rechenkapazität bereit, um der Entfernung einer einzelnen AZ standzuhalten
- Skalieren Sie Ihre Pods (einschließlich CoreDNS) in jeder AZ vorab
- Verteilen Sie mehrere Pod-Repliken auf alle, AZs um sicherzustellen, dass Sie durch die Umstellung von einer einzigen AZ über ausreichend Kapazität verfügen
- Platzieren Sie voneinander abhängige oder verwandte Pods in derselben AZ
- Testen Sie, ob Ihre Cluster-Umgebung mit einer AZ weniger erwartungsgemäß funktioniert, indem Sie manuell eine Zonenverschiebung starten. Alternativ können Sie zonales Autoshift aktivieren und auf die Autoshift-Übungsläufe antworten. Dies ist nicht erforderlich, damit Zonal Shift in EKS funktioniert, wird aber dringend empfohlen.

Stellen Sie Ihre EKS-Worker-Knoten auf mehreren bereit AZs

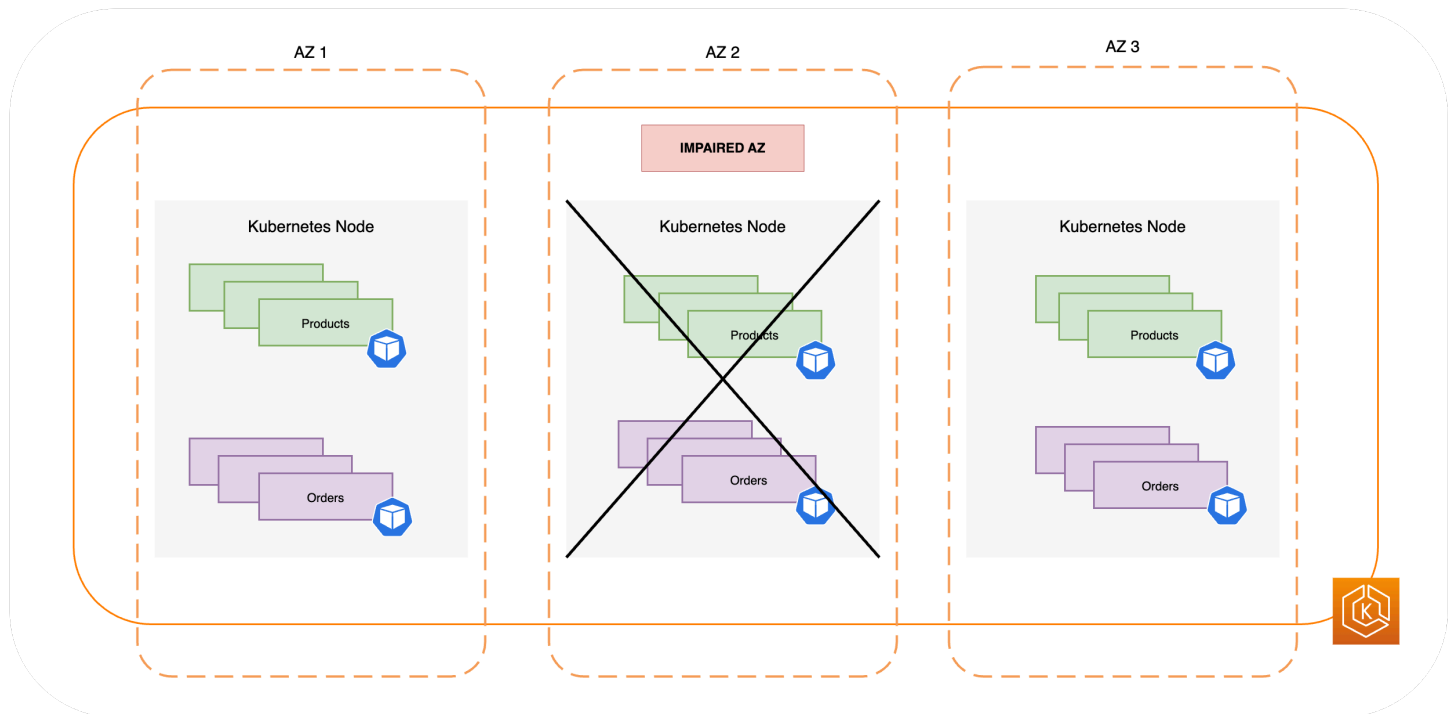
AWS Regionen haben mehrere, separate Standorte mit physischen Rechenzentren, die als Availability Zones (AZs) bezeichnet werden. AZs sind so konzipiert, dass sie physisch voneinander isoliert sind, um gleichzeitige Auswirkungen zu vermeiden, die sich auf eine gesamte Region auswirken könnten. Bei der Bereitstellung eines EKS-Clusters sollten Sie Ihre Worker-Knoten auf mehreren Knoten AZs in einer Region bereitstellen. Dadurch wird Ihre Cluster-Umgebung widerstandsfähiger gegen Beeinträchtigungen durch eine einzelne AZ und Sie können die Hochverfügbarkeit (HA) Ihrer Anwendungen, die in der anderen AZs ausgeführt werden, aufrechterhalten. Wenn Sie mit einer Zonenverlagerung weg von der betroffenen AZ beginnen, wird das Cluster-Netzwerk Ihrer EKS-Umgebung automatisch aktualisiert AZs, sodass es nur noch fehlerfrei verwendet und gleichzeitig eine hohe Verfügbarkeit für Ihren Cluster beibehält.

Wenn Sie sicherstellen, dass Sie über ein solches Multi-AZ-Setup für Ihre EKS-Umgebung verfügen, wird die allgemeine Zuverlässigkeit Ihres Systems verbessert. Multi-AZ-Umgebungen können jedoch eine wichtige Rolle bei der Übertragung und Verarbeitung von Anwendungsdaten spielen, was sich wiederum auf die Netzwerkgebühren Ihrer Umgebung auswirken wird. Insbesondere häufiger ausgehender zonenübergreifender Verkehr (zwischen den einzelnen Zonen verteilter Verkehr AZs) kann erhebliche Auswirkungen auf Ihre Netzwerkkosten haben. Sie können verschiedene Strategien anwenden, um den Umfang des zonenübergreifenden Datenverkehrs zwischen Pods in Ihrem EKS-Cluster zu kontrollieren und die damit verbundenen Kosten zu senken. Weitere Informationen zur Optimierung der Netzwerkkosten bei der Ausführung hochverfügbarer EKS-Umgebungen finden Sie in [diesem Best-Practice-Leitfaden](#).

Das folgende Diagramm zeigt eine hochverfügbare EKS-Umgebung mit drei AZs fehlerfreien Umgebungen.



Das folgende Diagramm zeigt, wie eine EKS-Umgebung mit 3 AZs eine AZ-Beeinträchtigung aushält und aufgrund der beiden anderen AZs fehlerfreien Umgebungen weiterhin hochverfügbar ist.



Stellen Sie genügend Rechenkapazität bereit, um der Entfernung einer einzigen AZ standzuhalten

Um die Ressourcennutzung und die Kosten für Ihre Recheninfrastruktur in der EKS-Datenebene zu optimieren, empfiehlt es sich, die Rechenkapazität an Ihren Workload-Anforderungen auszurichten. Wenn jedoch alle Ihre Worker-Knoten voll ausgelastet sind, sind Sie darauf angewiesen, dass der EKS-Datenebene neue Worker-Knoten hinzugefügt werden, bevor neue Pods geplant werden können. Bei der Ausführung kritischer Workloads empfiehlt es sich im Allgemeinen immer, mit redundanter Kapazität online zu arbeiten, um Eventualitäten wie plötzlichen Lastanstieg, Probleme mit dem Zustand der Knoten usw. zu bewältigen. Wenn Sie planen, Zonal Shift zu verwenden, planen Sie, eine gesamte AZ an Kapazität zu entfernen, sodass Sie Ihre redundante Rechenkapazität anpassen müssen, sodass sie ausreicht, um die Last auch dann zu bewältigen, wenn eine AZ offline ist.

Bei der Skalierung Ihrer Rechenleistung wird der Prozess des Hinzufügens neuer Knoten zur EKS-Datenebene einige Zeit in Anspruch nehmen, was sich auf die Echtzeitleistung und Verfügbarkeit Ihrer Anwendungen auswirken kann, insbesondere im Falle einer zonalen Beeinträchtigung. Ihre EKS-Umgebung sollte widerstandsfähig sein, um die Belastung durch den Verlust einer AZ zu verkraften, um eine Beeinträchtigung der Benutzererfahrung für Ihre Endbenutzer oder Kunden zu vermeiden. Dies bedeutet, dass jegliche Verzögerung zwischen dem Zeitpunkt, zu dem ein neuer Pod benötigt wird, und dem Zeitpunkt, zu dem er tatsächlich auf einem Worker-Knoten geplant ist, minimiert oder beseitigt werden muss.

Darüber hinaus sollten Sie bei einer Beeinträchtigung der Zonen das Risiko einer möglichen Einschränkung der Rechenkapazität minimieren, die verhindern würde, dass neu benötigte Knoten in einem fehlerfreien Zustand zu Ihrer EKS-Datenebene hinzugefügt werden. AZs

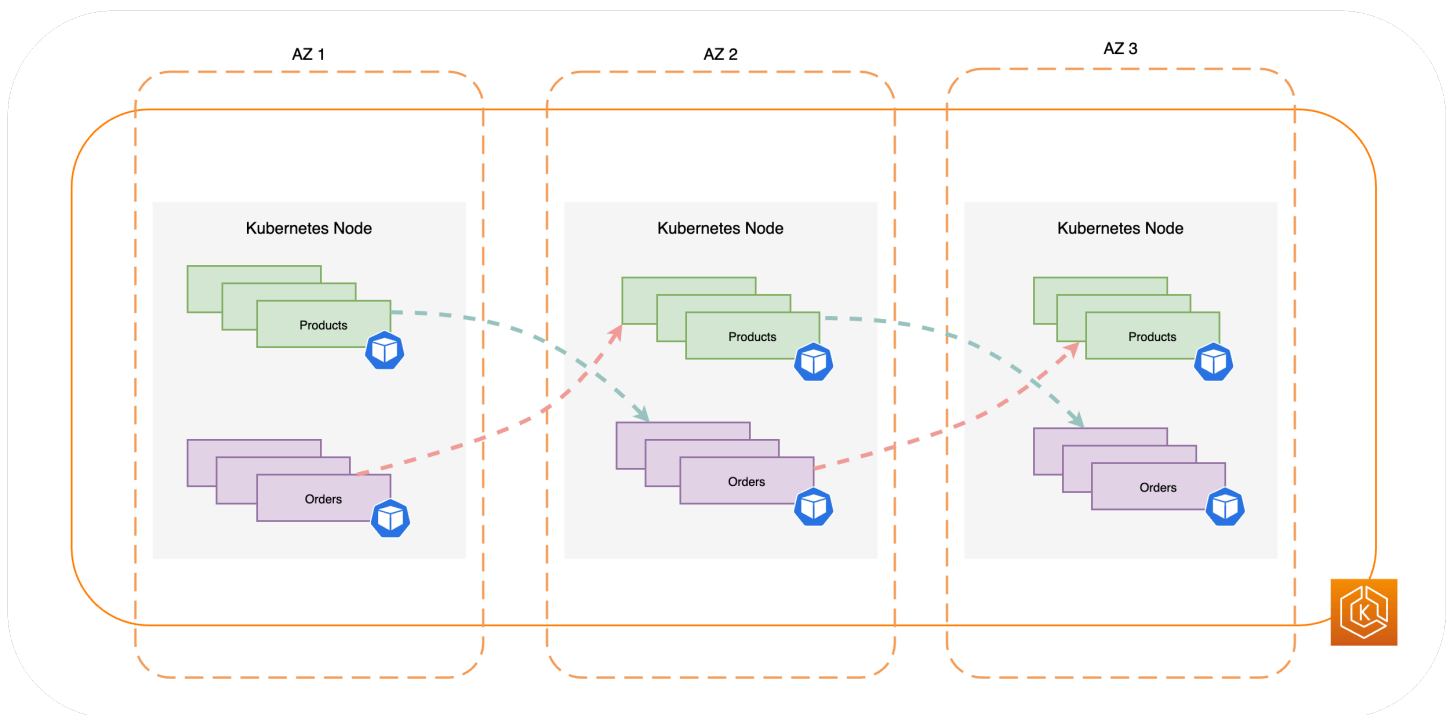
Um dies zu erreichen, sollten Sie in einigen der Worker-Knoten in jedem der beiden Workerknoten zu viel Rechenkapazität bereitstellen, AZs sodass der Kubernetes Scheduler über bereits vorhandene Kapazität für neue Pod-Platzierungen verfügt, insbesondere wenn Sie eine AZ weniger in Ihrer Umgebung haben.

Führen Sie mehrere Pod-Repliken aus und verteilen Sie sie auf AZs

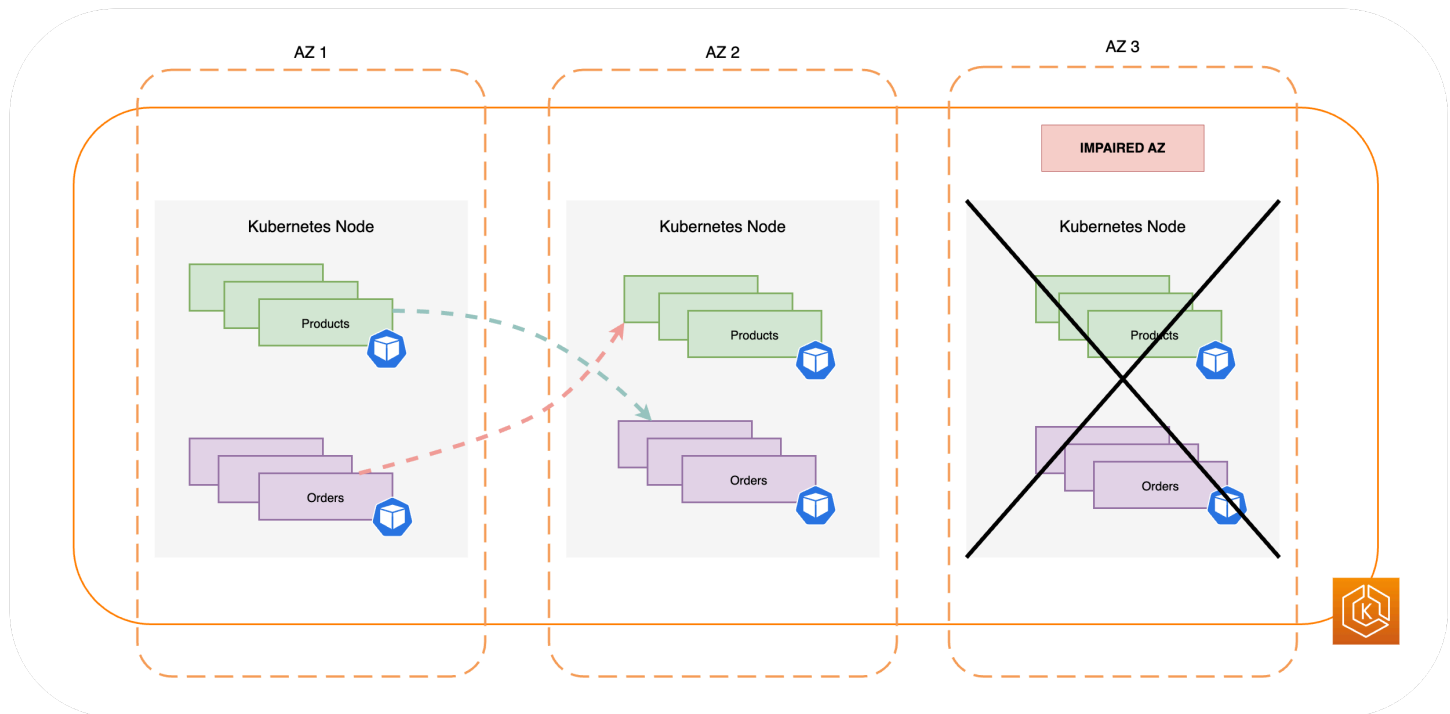
Mit Kubernetes können Sie Ihre Workloads vorab skalieren, indem Sie mehrere Instanzen (Pod-Repliken) einer einzigen Anwendung ausführen. Durch die Ausführung mehrerer Pod-Replikat für eine Anwendung wird ein einziger Fehlerpunkt vermieden und die Gesamtleistung erhöht, indem die Ressourcenbelastung für ein einzelnes Replikat reduziert wird. Um jedoch sowohl eine

hohe Verfügbarkeit als auch eine bessere Fehlertoleranz für Ihre Anwendungen zu gewährleisten, sollten Sie in diesem Fall mehrere Replikate einer Anwendung ausführen und auf verschiedene Fehlerdomänen (auch als Topologiedomänen bezeichnet) verteilen. AZs Mit [Einschränkungen der Topologieverteilung](#) können Sie Ihre Anwendungen so einrichten, dass sie bereits über statische Stabilität verfügen, sodass Sie im Falle einer Beeinträchtigung der Verfügbarkeit von AZ über genügend Replikate verfügen, AZs um zusätzliche Datenverkehrsspitzen oder -anstiege, die bei ihnen auftreten könnten, sofort bewältigen zu können.

Das folgende Diagramm zeigt eine EKS-Umgebung mit east-to-west Datenverkehrsfluss, wenn alle fehlerfrei sind. AZs



Das folgende Diagramm zeigt eine EKS-Umgebung mit east-to-west Verkehrsfluss, wenn eine einzelne AZ ausfällt und Sie eine Zonenverschiebung einleiten.



Der folgende Codeausschnitt ist ein Beispiel dafür, wie Sie Ihren Workload mit dieser Kubernetes-Funktion einrichten.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: orders
spec:
  replicas: 9
  selector:
    matchLabels:
      app: orders
  template:
    metadata:
      labels:
        app: orders
        tier: backend
    spec:
      topologySpreadConstraints:
        - maxSkew: 1
          topologyKey: "topology.kubernetes.io/zone"
          whenUnsatisfiable: ScheduleAnyway
          labelSelector:
            matchLabels:
```

`app: orders`

Am wichtigsten ist, dass Sie mehrere Replikate Ihrer DNS-Serversoftware (CoreDNS/Kube-DNS) ausführen und ähnliche Einschränkungen für die Topologieverteilung anwenden sollten, falls sie nicht bereits standardmäßig konfiguriert sind. Auf diese Weise können Sie sicherstellen, dass genügend DNS-Pods fehlerfrei sind, AZs um weiterhin Service Discovery-Anfragen für andere kommunizierende Pods im Cluster bearbeiten zu können, falls eine einzelne AZ-Beeinträchtigung vorliegt. Das [CoreDNS EKS-Add-On](#) verfügt über Standardeinstellungen für die CoreDNS-Pods, die über die Availability Zones Ihres Clusters verteilt werden, wenn mehrere Knoten verfügbar sind. AZs Sie können diese Standardeinstellungen auch durch Ihre eigenen benutzerdefinierten Konfigurationen ersetzen.

Bei der Installation von [CoreDNS mit Helm](#) können Sie die [Datei values.yaml](#) aktualisieren, um sicherzustellen, dass Sie replicaCount in jeder AZ über eine ausreichende Anzahl von Replikaten verfügen. Um sicherzustellen, dass diese Replikate auf die verschiedenen Replikate AZs in Ihrer Cluster-Umgebung verteilt sind, sollten Sie außerdem die Eigenschaft in derselben values.yaml-Datei aktualisieren. topologySpreadConstraints Der folgende Codeausschnitt zeigt, wie CoreDNS dafür konfiguriert wird.

CoreDNS Helm-Werte.yaml

```
replicaCount: 6
topologySpreadConstraints:
  - maxSkew: 1
    topologyKey: topology.kubernetes.io/zone
    whenUnsatisfiable: ScheduleAnyway
    labelSelector:
      matchLabels:
        k8s-app: kube-dns
```

Im Falle einer AZ-Beeinträchtigung können Sie die erhöhte Belastung der CoreDNS-Pods auffangen, indem Sie ein Autoscaling-System für CoreDNS verwenden. Die Anzahl der benötigten DNS-Instanzen hängt von der Anzahl der Workloads ab, die in Ihrem Cluster ausgeführt werden. CoreDNS ist CPU-gebunden, sodass es mithilfe des [Horizontal Pod Autoscaler](#) (HPA) je nach CPU skaliert werden kann. Im Folgenden finden Sie ein Beispiel, das Sie an Ihre Bedürfnisse anpassen können.

```
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
```

```
name: coredns
namespace: default
spec:
  maxReplicas: 20
  minReplicas: 2
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: coredns
  targetCPUUtilizationPercentage: 50
```

Alternativ kann EKS die automatische Skalierung der CoreDNS-Bereitstellung in der EKS-Add-On-Version von CoreDNS verwalten. Dieser CoreDNS-Autoscaler überwacht kontinuierlich den Clusterstatus, einschließlich der Anzahl der Knoten und CPU-Kerne. Basierend auf diesen Informationen passt der Controller die Anzahl der Replikate der CoreDNS-Bereitstellung in einem EKS-Cluster dynamisch an.

Um die [Autoscaling-Konfiguration im CoreDNS EKS-Add-On](#) zu aktivieren, sollten Sie die folgenden optionalen Konfigurationseinstellungen hinzufügen:

```
{
  "autoScaling": {
    "enabled": true
  }
}
```

Sie können auch [NodeLocal DNS](#) oder den [Cluster Proportional Autoscaler](#) verwenden, um CoreDNS zu skalieren. Weitere Informationen zur [horizontalen Skalierung von CoreDNS finden](#) Sie hier.

Stellen Sie voneinander abhängige Pods in derselben AZ zusammen

In den meisten Fällen führen Sie möglicherweise unterschiedliche Workloads aus, die miteinander kommunizieren müssen, damit ein Prozess erfolgreich ausgeführt werden kann. end-to-end Wenn die einzelnen Anwendungen auf verschiedene Anwendungen verteilt sind, sich AZs aber nicht in derselben AZ befinden, kann sich eine einzelne AZ-Beeinträchtigung auf den zugrunde liegenden Prozess auswirken. end-to-end Wenn Anwendung A beispielsweise mehrere Replikate in AZ 1 und AZ 2 hat, Anwendung B jedoch alle Replikate in AZ 3 hat, wirkt sich der Verlust von AZ 3 auf alle end-to-end Prozesse zwischen diesen beiden Workloads aus (Anwendung A und B). Durch die Kombination von Einschränkungen bei der Topologieverteilung mit der Pod-Affinität kann die Stabilität Ihrer Anwendung verbessert werden, indem Pods auf alle verteilt werden und eine Beziehung

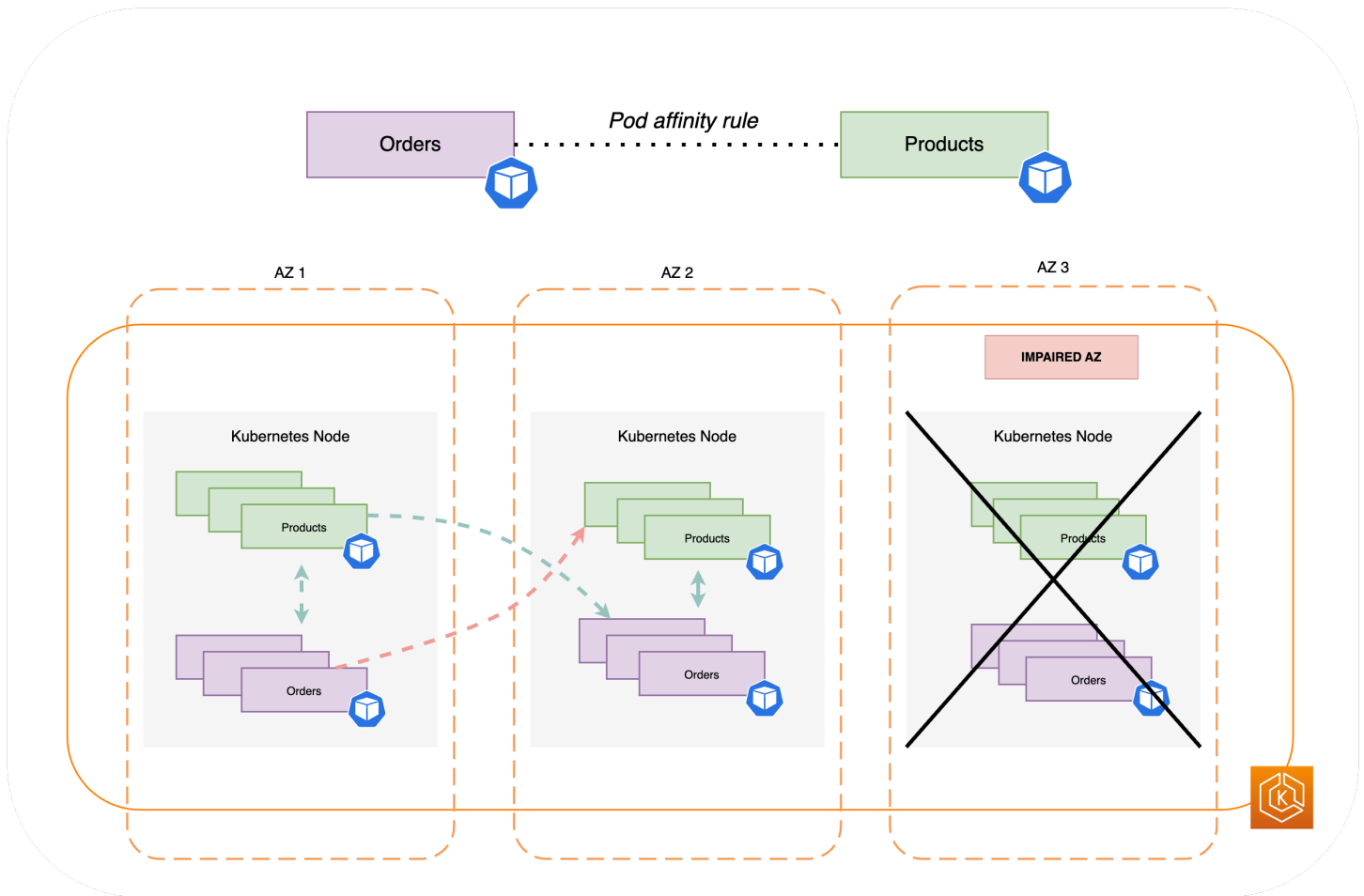
zwischen bestimmten Pods konfiguriert wird AZs, um sicherzustellen, dass sie gemeinsam platziert werden.

Mit [Pod-Affinitätsregeln](#) können Sie Beziehungen zwischen Workloads definieren, um das Verhalten des Kubernetes-Schedulers so zu beeinflussen, dass er Pods auf demselben Workerknoten oder in derselben AZ zusammenstellt. Sie können auch konfigurieren, wie streng diese Zeitplanungsbeschränkungen sein sollen.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: products
  namespace: ecommerce
  labels:
    app.kubernetes.io/version: "0.1.6"

spec:
  serviceName: graphql-service-account
  affinity:
    podAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
              - key: app
                operator: In
                values:
                  - orders
          topologyKey: "kubernetes.io/hostname"
```

Das folgende Diagramm zeigt Pods, die sich mithilfe von Pod-Affinitätsregeln auf demselben Knoten befinden.



Testen Sie, ob Ihre Cluster-Umgebung den Verlust einer AZ verkraften kann

Nachdem Sie die oben genannten Anforderungen erfüllt haben, besteht der nächste wichtige Schritt darin, zu testen, ob Sie über ausreichende Rechen- und Workload-Kapazität verfügen, um den Verlust einer AZ zu bewältigen. Sie können dies tun, indem Sie manuell eine Zonenverschiebung in EKS auslösen. Alternativ können Sie Zonal Autoshift aktivieren und Übungsläufe konfigurieren, um zu testen, ob Ihre Anwendungen mit einer AZ weniger in Ihrer Cluster-Umgebung erwartungsgemäß funktionieren.

Häufig gestellte Fragen

Warum sollte ich diese Funktion verwenden?

Durch die Verwendung von ARC Zonal Shift oder Zonal Autoshift in Ihrem EKS-Cluster können Sie die Verfügbarkeit von Kubernetes-Anwendungen besser aufrechterhalten, indem Sie den schnellen Wiederherstellungsprozess automatisieren, bei dem der Netzwerkverkehr innerhalb des Clusters weg

von einer beeinträchtigten AZ verlagert wird. Mit ARC können Sie lange und komplizierte Schritte vermeiden, die bei beeinträchtigten AZ-Ereignissen häufig zu einer längeren Erholungsphase führen.

Wie funktioniert diese Funktion mit anderen AWS Diensten?

EKS ist in ARC integriert, das die primäre Schnittstelle für die Durchführung von Wiederherstellungsvorgängen darstellt AWS. Um sicherzustellen, dass der Datenverkehr innerhalb des Clusters ordnungsgemäß von einer beeinträchtigten AZ weggeleitet wird, werden Änderungen an der Liste der Netzwerkendpunkte für Pods vorgenommen, die auf der Kubernetes-Datenebene ausgeführt werden. Wenn Sie AWS Load Balancer für die Weiterleitung von externem Datenverkehr in den Cluster verwenden, können Sie Ihre Load Balancer bereits bei ARC registrieren und eine Zonenverschiebung auf ihnen auslösen, um zu verhindern, dass Datenverkehr in die degradierte Zone fließt. Diese Funktion interagiert auch mit Amazon EC2 Auto Scaling Groups (ASG), die von EKS Managed Node Groups (MNG) erstellt wurden. Um zu verhindern, dass eine beeinträchtigte AZ für neue Kubernetes-Pods oder Node-Starts verwendet wird, entfernt EKS die beeinträchtigte AZ aus der ASG.

Wie unterscheidet sich diese Funktion von den standardmäßigen Kubernetes-Schutzmaßnahmen?

Diese Funktion arbeitet mit mehreren systemeigenen integrierten Schutzmaßnahmen von Kubernetes zusammen, die Kunden dabei unterstützen, widerstandsfähig zu bleiben. Sie können Tests zur Bereitschaft und Aktualität eines Pods konfigurieren, die entscheiden, wann ein Pod Traffic aufnehmen soll. Wenn diese Tests fehlschlagen, entfernt Kubernetes diese Pods als Ziele für einen Service und der Datenverkehr wird nicht mehr an den Pod gesendet. Das ist zwar nützlich, aber es ist für Kunden nicht trivial, diese Integritätsprüfungen so zu konfigurieren, dass sie garantiert fehlschlagen, wenn eine Zone heruntergefahren ist. Die ARC-Zonenverschiebungsfunktion bietet Ihnen ein zusätzliches Sicherheitsnetz, das ihnen hilft, eine heruntergestufte AZ vollständig zu isolieren, wenn die systemeigenen Schutzmaßnahmen von Kubernetes nicht ausreichend waren. Es bietet Ihnen auch eine einfache Möglichkeit, die Betriebsbereitschaft und Belastbarkeit Ihrer Architektur zu testen.

Kann ich in meinem Namen eine Zonenverschiebung AWS auslösen?

Ja, wenn Sie ARC Zonal Shift vollautomatisch nutzen möchten, können Sie ARC Zonal Autoshift aktivieren. Mit Zonal Autoshift können Sie sich darauf verlassen, AWS dass Sie den Zustand Ihres EKS-Clusters überwachen und automatisch eine Verschiebung auslösen, wenn eine AZ-Beeinträchtigung festgestellt wird. AZs

Was passiert, wenn ich diese Funktion verwende und meine Worker-Knoten und Workloads nicht vorkaliert sind?

Wenn Sie nicht vorkaliert sind und darauf angewiesen sind, während einer Zonenverschiebung zusätzliche Knoten oder Pods bereitzustellen, besteht die Gefahr einer verzögerten Wiederherstellung. Das Hinzufügen neuer Knoten zur Kubernetes-Datenebene wird einige Zeit in Anspruch nehmen, was sich auf die Echtzeitleistung und Verfügbarkeit Ihrer Anwendungen auswirken kann, insbesondere im Falle einer zonalen Beeinträchtigung. Darüber hinaus kann es bei einer Beeinträchtigung der Zonen zu einer potenziellen Einschränkung der Rechenkapazität kommen, die verhindern würde, dass neu benötigte Knoten zu den fehlerfreien Knoten hinzugefügt werden. AZs

Wenn Ihre Workloads nicht vorab skaliert und auf alle Bereiche Ihres Clusters verteilt sind, kann sich eine zonale Beeinträchtigung auf die Verfügbarkeit einer Anwendung auswirken, die nur auf Worker-Knoten AZs in einer betroffenen AZ ausgeführt wird. Um das Risiko eines vollständigen Verfügbarkeitsausfalls für Ihre Anwendung zu minimieren, verfügt EKS über eine Ausfallsicherung für den Datenverkehr, der an Pod-Endpunkte in einer beeinträchtigten Zone gesendet wird, falls sich alle Endpunkte des Workloads in der fehlerhaften AZ befinden. Es wird jedoch dringend empfohlen, Ihre Anwendungen vorab zu skalieren und auf alle AZs zu verteilen, um die Verfügbarkeit im Falle eines zonalen Problems aufrechtzuerhalten.

Was passiert, wenn ich eine statusbehaftete Anwendung ausführe?

Wenn Sie eine statusbehaftete Anwendung ausführen, müssen Sie ihre Fehlertoleranz je nach Anwendungsfall und Architektur bewerten. Wenn Sie über eine Aktiv-/Standby-Architektur oder ein Muster verfügen, kann es Fälle geben, in denen sich die aktive Komponente in einer beeinträchtigten AZ befindet. Wenn der Standby-Modus auf Anwendungsebene nicht aktiviert ist, können Probleme mit Ihrer Anwendung auftreten. Probleme können auch auftreten, wenn neue Kubernetes-Pods im fehlerfreien Zustand gestartet werden, AZs da sie dann nicht in der Lage sind, eine Verbindung zu den persistenten Volumes herzustellen, die auf die beeinträchtigte AZ beschränkt sind.

Funktioniert diese Funktion mit Karpenter?

Die Unterstützung von Karpenter ist derzeit für ARC Zonal Shift und Zonal Autoshift in EKS nicht verfügbar. Wenn eine AZ beeinträchtigt ist, können Sie die entsprechende NodePool Konfiguration von Karpenter anpassen, indem Sie die fehlerhafte AZ entfernen, sodass neue Worker-Knoten nur im fehlerfreien Zustand gestartet werden. AZs

Funktioniert diese Funktion mit EKS Fargate?

Diese Funktion funktioniert nicht mit EKS Fargate. Wenn EKS Fargate ein zonales Gesundheitsereignis erkennt, ziehen es Pods standardmäßig vor, in dem anderen System ausgeführt zu werden. AZs

Wird die von EKS verwaltete Kubernetes-Steuerebene beeinträchtigt?

Nein, Amazon EKS führt standardmäßig die Kubernetes-Steuerebene aus und skaliert sie über mehrere, AZs um eine hohe Verfügbarkeit zu gewährleisten. ARC Zonal Shift und Zonal Autoshift wirken nur auf der Kubernetes-Datenebene.

Sind mit dieser neuen Funktion irgendwelche Kosten verbunden?

Sie können ARC Zonal Shift und Zonal Autoshift in Ihrem EKS-Cluster ohne zusätzliche Kosten verwenden. Sie zahlen jedoch weiterhin für bereitgestellte Instances. Es wird dringend empfohlen, Ihre Kubernetes-Datenebene vorab zu skalieren, bevor Sie diese Funktion nutzen. Sie sollten das richtige Gleichgewicht zwischen Kosten und Anwendungsverfügbarkeit in Betracht ziehen.

Weitere Ressourcen

- [Wie funktioniert eine Zonenverschiebung](#)
- [Bewährte Methoden für zonale Verschiebungen in ARC](#)
- [Unterstützte Ressourcen und Szenarien für Zonal Shift und Zonal Autoshift](#)
- [Betrieb belastbarer Workloads auf Amazon EKS](#)
- [Eliminieren Sie Verzögerungen bei der Skalierung von Kubernetes-Knoten durch Pod-Priorität und Over-Provisioning](#)
- [Skalieren Sie CoreDNS-Pods für hohen DNS-Verkehr](#)

Aktivieren Sie EKS Zonal Shift, um beeinträchtigte Availability Zones zu vermeiden

Amazon Application Recovery Controller (ARC) unterstützt Sie bei der Verwaltung und Koordination der Wiederherstellung Ihrer Anwendungen in allen Availability Zones (AZs) und funktioniert mit vielen Services, einschließlich Amazon EKS. Mit der EKS-Unterstützung für ARC Zonal Shift können Sie den Netzwerkverkehr innerhalb des Clusters von einer beeinträchtigten AZ wegverlagern. Sie können auch autorisieren AWS, den Zustand Ihrer AZ zu überwachen und den Netzwerkverkehr in Ihrem Namen vorübergehend von einer fehlerhaften AZ zu verlagern.

So verwenden Sie EKS Zonal Shift:

1. Aktivieren Sie Ihren EKS-Cluster mit Amazon Application Recovery Controller (ARC). Dies erfolgt auf Cluster-Ebene mithilfe der Amazon EKS-Konsole, der AWS CLI oder eksctl. CloudFormation

2. Nach der Aktivierung können Sie Zonal Shifts oder Zonal Autoshift mit der ARC-Konsole, der AWS CLI oder Zonal Shift und Zonal Autoshift verwalten. APIs

Beachten Sie, dass Sie ARC nach der Registrierung eines EKS-Clusters bei ARC noch konfigurieren müssen. Sie können beispielsweise die ARC-Konsole verwenden, um Zonal Autoshift zu konfigurieren.

Ausführlichere Informationen zur Funktionsweise von EKS Zonal Shift und zur Gestaltung Ihrer Workloads für eingeschränkte Verfügbarkeitszonen finden Sie unter [the section called “Erfahren Sie mehr über Zonal Shift”](#)

Überlegungen

- Der EKS-Automatikmodus unterstützt Amazon Application Recovery Controller, Zonal Shift und Zonal Autoshift nicht.
- Wir empfehlen, zwischen den Vorgängen in Zonal Shift mindestens 60 Sekunden zu warten, um sicherzustellen, dass jede Anfrage ordnungsgemäß bearbeitet wird.

Wenn Sie versuchen, Zonenschichten schnell hintereinander (innerhalb von 60 Sekunden) durchzuführen, verarbeitet der Amazon EKS-Service möglicherweise nicht alle Schichtanfragen ordnungsgemäß. Dies ist auf den aktuellen Abfragemechanismus zurückzuführen, der den zonalen Status des Clusters aktualisiert. Wenn Sie mehrere Zonenverschiebungen durchführen müssen, stellen Sie sicher, dass zwischen den Vorgängen genügend Zeit liegt, damit das System jede Änderung verarbeiten kann.

Was ist Amazon Application Recovery Controller?

Amazon Application Recovery Controller (ARC) unterstützt Sie bei der Vorbereitung und Durchführung einer schnelleren Wiederherstellung von Anwendungen, die auf ausgeführt AWS werden. Zonal Shift ermöglicht es Ihnen, sich schnell von Beeinträchtigungen der Availability Zone (AZ) zu erholen, indem Sie den Datenverkehr für eine unterstützte Ressource vorübergehend von einer AZ auf eine fehlerfreie Ressource AZs in der AWS Region verlagern.

[Erfahren Sie mehr über Amazon Application Recovery Controller \(ARC\)](#)

Was ist Zonenverschiebung?

Zonal Shift ist eine Funktion in ARC, mit der Sie den Traffic für eine Ressource wie einen EKS-Cluster oder einen Elastic Load Balancer von einer Availability Zone in einer AWS Region wegverlagern können, um ein Problem schnell zu beheben und Ihre Anwendung schnell wiederherzustellen. Sie könnten sich dafür entscheiden, den Datenverkehr zu verlagern, z. B. weil eine fehlerhafte Bereitstellung Latenzprobleme verursacht oder weil die Availability Zone beeinträchtigt ist. Für eine Zonenverschiebung sind keine weiteren Konfigurationsschritte erforderlich.

[Erfahren Sie mehr über ARC Zonal Shift](#)

Was ist Zonal Autoshift?

Zonal Autoshift ist eine Funktion in ARC, mit der Sie autorisieren AWS können, den Verkehr in Ihrem Namen von einer AZ für unterstützte Ressourcen auf gesunde Ressourcen in der Region zu verlagern. AWS startet eine automatische Verschiebung, wenn die interne Telemetrie anzeigt, dass in einer AZ in einer Region eine Beeinträchtigung vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Die interne Telemetrie beinhaltet Metriken aus verschiedenen Quellen, darunter dem AWS Netzwerk und den Amazon- EC2 und Elastic Load Balancing Diensten.

AWS beendet Autoshifts, wenn Indikatoren anzeigen, dass kein Problem oder potenzielles Problem mehr besteht.

[Erfahren Sie mehr über ARC Zonal Autoshift](#)

Was macht EKS während eines Autoshifts?

EKS aktualisiert die Netzwerkkonfigurationen, um zu verhindern, dass der Datenverkehr an beeinträchtigte Personen weitergeleitet wird. Wenn Sie verwaltete Knotengruppen verwenden, startet EKS außerdem nur AZs während einer Zonenverschiebung neue Knoten im fehlerfreien Zustand. Wenn die Schicht abläuft oder storniert wird, werden die Netzwerkkonfigurationen so wiederhergestellt, dass sie die AZ enthalten, die zuvor als fehlerhaft erkannt wurde.

[Erfahren Sie mehr über EKS Zonal Shift.](#)

Registrieren Sie den EKS-Cluster beim Amazon Application Recovery Controller (ARC) (AWS Konsole)

1. Suchen Sie den Namen und die Region des EKS-Clusters, den Sie bei ARC registrieren möchten.

2. Navigieren Sie zur [EKS-Konsole](#) in dieser Region und wählen Sie Ihren Cluster aus.
3. Wählen Sie auf der Cluster-Informationsseite die Registerkarte Overview aus.
4. Wählen Sie unter der Überschrift Zonal Shift die Schaltfläche Verwalten aus.
5. Wählen Sie „Aktivieren“ oder „Deaktivieren“ für EKS Zonal Shift.

Jetzt ist Ihr EKS-Cluster bei ARC registriert.

Wenn Sie beeinträchtigte Verfügbarkeitszonen erkennen und vermeiden möchten AWS , müssen Sie ARC Zonal Autoshift konfigurieren. Sie können dies beispielsweise in der ARC-Konsole tun.

Nächste Schritte

- Erfahren Sie, wie Sie [Zonal Autoshift aktivieren](#).
- Erfahren Sie, wie Sie [eine zonale Verschiebung manuell starten](#).

Erfahren Sie, wie die Zugriffskontrolle in Amazon EKS funktioniert

Erfahren Sie, wie Sie den Zugriff auf Ihren Amazon EKS-Cluster verwalten. Die Verwendung von Amazon EKS erfordert Kenntnisse darüber, wie sowohl Kubernetes als auch AWS Identity and Access Management (AWS IAM) die Zugriffskontrolle handhaben.

Dieser Abschnitt beinhaltet:

[the section called “Kubernetes-API-Zugriff”](#)— Erfahren Sie, wie Sie Anwendungen oder Benutzern die Authentifizierung bei der Kubernetes-API ermöglichen. Sie können Zugriffseinträge, aws-auth ConfigMap oder einen externen OIDC-Anbieter verwenden.

[the section called “Auf Cluster-Ressourcen zugreifen”](#)— Erfahren Sie, wie Sie den AWS Management Console für die Kommunikation mit Ihrem Amazon EKS-Cluster konfigurieren. Verwenden Sie die Konsole, um Kubernetes-Ressourcen im Cluster wie Namespaces, Knoten und Pods anzuzeigen.

[the section called “Greifen Sie mit kubectl auf den Cluster zu”](#)— Erfahren Sie, wie Sie kubectl für die Kommunikation mit Ihrem Amazon EKS-Cluster konfigurieren. Verwenden Sie die AWS CLI, um eine kubeconfig-Datei zu erstellen.

[the section called “Workload-Zugriff auf AWS ”](#)— Erfahren Sie, wie Sie ein Kubernetes-Dienstkonto mit IAM-Rollen verknüpfen. AWS Sie können Pod Identity oder IAM-Rollen für Dienstkonten (IRSA) verwenden.

Allgemeine Aufgaben

- Gewähren Sie Entwicklern Zugriff auf die Kubernetes-API. Sehen Sie sich die Kubernetes-Ressourcen im an. AWS Management Console
 - Lösung: [Verwenden Sie Zugriffseinträge](#), um Kubernetes-RBAC-Berechtigungen IAM-Benutzern oder -Rollen zuzuordnen. AWS
- Konfigurieren Sie kubectl so, dass es mithilfe AWS von Anmeldeinformationen mit einem Amazon EKS-Cluster kommuniziert.
 - Lösung: Verwenden Sie die AWS CLI, um [eine kubeconfig-Datei zu erstellen](#).
- Verwenden Sie einen externen Identitätsanbieter wie Ping Identity, um Benutzer bei der Kubernetes-API zu authentifizieren.

- Lösung: [Verknüpfen Sie einen externen](#) OIDC-Anbieter.
- Gewähren Sie Workloads auf Ihrem Kubernetes-Cluster die Möglichkeit, Anrufe zu tätigen. AWS APIs
- Lösung: [Verwenden Sie Pod Identity](#), um eine AWS IAM-Rolle einem Kubernetes-Dienstkonto zuzuordnen.

Hintergrund

- [Erfahren Sie, wie Kubernetes-Dienstkonten funktionieren.](#)
- [Sehen Sie sich das RBAC-Modell \(Role Based Access Control\) von Kubernetes an](#)
- [Weitere Informationen zur Verwaltung des Zugriffs auf AWS Ressourcen finden Sie im AWS IAM-Benutzerhandbuch.](#) Alternativ können Sie an einer kostenlosen [Einführungsschulung zur Verwendung von AWS IAM](#) teilnehmen.

Überlegungen zum EKS-Automatikmodus

Der automatische EKS-Modus ist in die Zugriffseinträge EKS Pod Identity und EKS EKS integriert.

- Der EKS Auto Mode verwendet Zugriffseinträge, um der EKS-Steuerebene Kubernetes-Berechtigungen zu gewähren. Die Zugriffsrichtlinien ermöglichen es EKS Auto Mode beispielsweise, Informationen über Netzwerkendpunkte und Dienste zu lesen.
- Sie können Zugriffseinträge auf einem EKS-Auto-Modus-Cluster nicht deaktivieren.
- Sie können optional die aktivieren `aws-authConfigMap`.
- Die Zugriffseinträge für den EKS Auto Mode werden automatisch konfiguriert. Sie können diese Zugriffseinträge anzeigen, aber Sie können sie nicht ändern.
- Wenn Sie eine NodeClass benutzerdefinierte Node-IAM-Rolle verwenden, müssen Sie mithilfe der EKSAuto NodePolicy Amazon-Zugriffsrichtlinie einen Zugriffseintrag für die Rolle erstellen.
- Wenn Sie Workload-Berechtigungen für AWS Dienste gewähren möchten, verwenden Sie EKS Pod Identity.
- Sie müssen den Pod Identity-Agenten nicht auf EKS-Auto-Mode-Clustern installieren.

Gewähren Sie IAM-Benutzern und -Rollen Zugriff auf Kubernetes APIs

Ihr Cluster hat einen Kubernetes-API-Endpunkt. Kubectl verwendet diese API. Sie können sich mit zwei Arten von Identitäten bei dieser API authentifizieren:

- Ein AWS Identity and Access Management (IAM) -Prinzipal (Rolle oder Benutzer) — Dieser Typ erfordert eine Authentifizierung bei IAM. Benutzer können sich AWS als [IAM-Benutzer](#) oder mit einer [föderierten Identität anmelden, indem sie Anmeldeinformationen verwenden, die über eine Identitätsquelle](#) bereitgestellt wurden. Benutzer können sich nur dann mit einer Verbundidentität anmelden, wenn Ihr Administrator zuvor mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet hat. Wenn Benutzer AWS mithilfe eines Verbunds darauf zugreifen, [übernehmen sie indirekt eine Rolle](#). Wenn Benutzer diese Art von Identität verwenden, gilt Folgendes:
 - Kann ihnen Kubernetes-Berechtigungen zuweisen, sodass sie mit Kubernetes-Objekten in Ihrem Cluster arbeiten können. Weitere Informationen darüber, wie Sie Ihren IAM-Prinzipalen Berechtigungen zuweisen, sodass sie auf Kubernetes-Objekte in Ihrem Cluster zugreifen können, finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#)
 - Kann ihnen IAM-Berechtigungen zuweisen, sodass sie mithilfe der Amazon EKS-API, AWS CLI,, oder eksctl mit Ihrem Amazon EKS-Cluster und seinen Ressourcen arbeiten können. AWS CloudFormation AWS Management Console Weitere Informationen finden Sie in der Service-Authorization-Referenz unter [Von Amazon Elastic Kubernetes Service definierte Aktionen](#).
 - Wenn Knoten in Ihren Cluster eingebunden werden, nehmen sie eine IAM-Rolle an. Die Möglichkeit, mithilfe von IAM-Prinzipalen auf Ihren Cluster zuzugreifen, wird durch den [AWS IAM Authenticator for Kubernetes](#) bereitgestellt, der auf der Amazon EKS-Steuerebene ausgeführt wird.
- Ein Benutzer in Ihrem eigenen OpenID Connect (OIDC) -Anbieter — [Dieser Typ erfordert eine Authentifizierung bei Ihrem OIDC-Anbieter](#). Weitere Informationen zur Einrichtung Ihres eigenen OIDC-Anbieters mit Ihrem Amazon EKS-Cluster finden Sie unter [the section called “OIDC-Anbieter verknüpfen”](#) Wenn Benutzer diese Art von Identität verwenden, gilt Folgendes:
 - Kann ihnen Kubernetes-Berechtigungen zuweisen, sodass sie mit Kubernetes-Objekten in Ihrem Cluster arbeiten können.
 - Ihnen können keine IAM-Berechtigungen zugewiesen werden, sodass sie mithilfe der Amazon EKS-API, AWS CLI,, oder eksctl mit Ihrem Amazon EKS-Cluster und seinen Ressourcen arbeiten können. AWS CloudFormation AWS Management Console

Sie können beide Arten von Identitäten mit Ihrem Cluster verwenden. Die IAM-Authentifizierungsmethode kann nicht deaktiviert werden. Die OIDC-Authentifizierungsmethode ist optional.

Verknüpfen Sie IAM-Identitäten mit Kubernetes-Berechtigungen

Der [AWS IAM Authenticator für Kubernetes](#) ist auf der Steuerungsebene Ihres Clusters installiert. Es ermöglicht [AWS Identity and Access Management](#) (IAM) -Prinzipale (Rollen und Benutzer), denen Sie Zugriff auf Kubernetes-Ressourcen in Ihrem Cluster gewähren. Sie können IAM-Prinzipalen den Zugriff auf Kubernetes-Objekte in Ihrem Cluster mit einer der folgenden Methoden ermöglichen:

- Zugriffseinträge erstellen — Wenn Ihr Cluster die Plattformversion hat, die im Abschnitt [Voraussetzungen](#) für die Kubernetes-Version Ihres Clusters aufgeführt ist, oder höher ist, empfehlen wir Ihnen, diese Option zu verwenden.

Verwenden Sie Zugriffseinträge, um die Kubernetes-Berechtigungen von IAM-Prinzipalen von außerhalb des Clusters zu verwalten. Sie können den Zugriff auf den Cluster mithilfe der EKS-API, der AWS Befehlszeilenschnittstelle, AWS SDKs und hinzufügen und verwalten. AWS CloudFormation AWS Management Console Für die Benutzerverwaltung können also die gleichen Tools verwendet werden wie für die Clustererstellung.

Folgen Sie zunächst den Anweisungen [Authentifizierungsmodus zur Verwendung von Zugriffseinträgen ändern und anschließend Vorhandene aws-auth-Einträge zu ConfigMap Zugriffseinträgen migrieren](#).

- Hinzufügen von Einträgen zum **aws-auth ConfigMap** — Wenn die Plattformversion Ihres Clusters älter ist als die im Abschnitt [Voraussetzungen](#) aufgeführte Version, müssen Sie diese Option verwenden. Wenn die Plattformversion Ihres Clusters der Plattformversion entspricht, die im Abschnitt [Voraussetzungen](#) für die Kubernetes-Version Ihres Clusters aufgeführt ist, oder höher ist, und Sie Einträge zu der hinzugefügt haben, empfehlen wir Ihnen ConfigMap, diese Einträge zu Access-Einträgen zu migrieren. Sie können ConfigMap jedoch keine Einträge migrieren, die Amazon EKS dem hinzugefügt hat, z. B. Einträge für IAM-Rollen, die mit verwalteten Knotengruppen oder Fargate-Profilen verwendet werden. Weitere Informationen finden Sie unter [the section called “Kubernetes-API-Zugriff”](#).
- Wenn Sie aws-auth ConfigMap verwenden müssen, können Sie mithilfe des Befehls `eksctl create iamidentitymapping` Einträge zu ConfigMap hinzufügen. Weitere Informationen finden Sie in der Dokumentation zu eksctl unter [Manage IAM users and roles](#).

Stellen Sie den Cluster-Authentifizierungsmodus ein

Jeder Cluster hat einen Authentifizierungsmodus. Der Authentifizierungsmodus bestimmt, mit welchen Methoden Sie IAM-Prinzipalen den Zugriff auf Kubernetes-Objekte in Ihrem Cluster ermöglichen können. Es gibt drei Authentifizierungsmodi.

Important

Sobald die Zugriffseingabemethode aktiviert ist, kann sie nicht deaktiviert werden.

Wenn die ConfigMap Methode bei der Clustererstellung nicht aktiviert wurde, kann sie später nicht aktiviert werden. Bei allen Clustern, die vor der Einführung von Zugriffseinträgen erstellt wurden, ist die ConfigMap Methode aktiviert.

Wenn Sie Hybridknoten mit Ihrem Cluster verwenden, müssen Sie den Authentifizierungsmodus API oder den API_AND_CONFIG_MAP Cluster-Authentifizierungsmodus verwenden.

Das **aws-auth ConfigMap** Innere des Clusters

Dies ist der ursprüngliche Authentifizierungsmodus für Amazon-EKS-Cluster. Der IAM-Prinzipal, der den Cluster erstellt hat, ist zunächst der einzige Benutzer, der über `kubectl` auf den Cluster zugreifen kann. Dieser Benutzer muss der Liste in `aws-auth ConfigMap` weitere Benutzer hinzufügen und Berechtigungen zuweisen, die sich auf die anderen Benutzer innerhalb des Clusters auswirken. Diese anderen Benutzer können den ursprünglichen Benutzer nicht verwalten oder entfernen, da es im Bereich `Zu verwalten` keinen Eintrag gibt. `ConfigMap`

Sowohl der als **ConfigMap** auch der Zugriff auf Einträge

In diesem Authentifizierungsmodus können Sie beide Methoden verwenden, um dem Cluster IAM-Prinzipale hinzuzufügen. Beachten Sie, dass jede Methode separate Einträge speichert. Wenn Sie beispielsweise einen Zugriffseintrag über die AWS CLI hinzufügen, `aws-auth ConfigMap` wird dieser nicht aktualisiert.

Nur auf Einträge zugreifen

In diesem Authentifizierungsmodus können Sie die EKS-API, die AWS Befehlszeilenschnittstelle, und verwenden AWS SDKs AWS CloudFormation, AWS Management Console um den Zugriff auf den Cluster für IAM-Prinzipale zu verwalten.

Jeder Zugriffseintrag hat einen Typ und Sie können eine Kombination aus Zugriffsbereich und Zugriffsrichtlinie verwenden, um mithilfe des Zugriffsbereichs den Prinzipal auf einen bestimmten

Namespace zu beschränken und mithilfe der Zugriffsrichtlinie vorkonfigurierte, wiederverwendbare Berechtigungsrichtlinien festzulegen. Alternativ können Sie den Typ STANDARD und Kubernetes RBAC-Gruppen verwenden, um benutzerdefinierte Berechtigungen zuzuweisen.

Authentifizierungsmodus	Methoden
Nur ConfigMap (CONFIG_MAP)	aws-auth ConfigMap
EKS-API und ConfigMap (API_AND_CONFIG_MAP)	auf Einträge in der EKS-API, der AWS Befehlszeilenschnittstelle, und AWS SDKs zugreifen AWS CloudFormation AWS Management Console aws-auth ConfigMap
Nur EKS-API (API)	auf Einträge in der EKS-API, der AWS Befehlszeilenschnittstelle, AWS SDKs, AWS CloudFormation, zugreifen und AWS Management Console

Note

Amazon EKS Auto Mode erfordert Access-Einträge.

Gewähren Sie IAM-Benutzern Zugriff auf Kubernetes mit EKS-Zugriffseinträgen

Was sind EKS-Zugriffseinträge?

EKS-Zugriffseinträge sind der beste Weg, Benutzern Zugriff auf die Kubernetes-API zu gewähren. Sie können beispielsweise Zugriffseinträge verwenden, um Entwicklern Zugriff auf die Verwendung von kubectl zu gewähren.

Grundsätzlich verknüpft ein EKS-Zugriffseintrag eine Reihe von Kubernetes-Berechtigungen mit einer IAM-Identität, z. B. einer IAM-Rolle. Ein Entwickler kann beispielsweise eine IAM-Rolle annehmen und diese zur Authentifizierung bei einem EKS-Cluster verwenden.

Sie können Kubernetes-Berechtigungen auf zwei Arten an Zugriffseinträge anhängen:

- Verwenden Sie eine Zugriffsrichtlinie. Zugriffsrichtlinien sind vordefinierte Kubernetes-Berechtigungsvorlagen, die von verwaltet werden. AWS Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#).
- Verweisen Sie auf eine Kubernetes-Gruppe. Wenn Sie einer Kubernetes-Gruppe eine IAM-Identität zuordnen, können Sie Kubernetes-Ressourcen erstellen, die der Gruppe Berechtigungen gewähren. Weitere Informationen finden Sie unter [Using RBAC Authorization](#) in der Kubernetes-Dokumentation.

Vorteile

Mit dem Amazon EKS-Cluster-Zugriffsmanagement können Sie die Authentifizierung und Autorisierung für Ihre Kubernetes-Cluster direkt über Amazon EKS steuern. APIs Diese Funktion vereinfacht die Zugriffsverwaltung, da APIs bei der Verwaltung von Benutzerberechtigungen nicht zwischen Kubernetes AWS und Kubernetes gewechselt werden muss. Mithilfe von Zugriffseinträgen und Zugriffsrichtlinien können Sie detaillierte Berechtigungen für AWS IAM-Prinzipale definieren, einschließlich der Möglichkeit, Cluster-Admin-Berechtigungen vom Cluster-Ersteller zu ändern oder zu entziehen.

Die Funktion lässt sich in Infrastructure-as-Code-Tools (IaC) wie Terraform und AWS CDK integrieren AWS CloudFormation, sodass Sie bei der Clustererstellung Zugriffskonfigurationen definieren können. Wenn Fehlkonfigurationen auftreten, können Sie den Cluster-Zugriff über die Amazon EKS-API wiederherstellen, ohne direkten Kubernetes-API-Zugriff zu benötigen. Dieser zentralisierte Ansatz reduziert den betrieblichen Aufwand und verbessert die Sicherheit, indem bestehende AWS IAM-Funktionen wie CloudTrail Audit-Logging und Multi-Faktor-Authentifizierung genutzt werden.

Erste Schritte

1. Ermitteln Sie die IAM-Identitäts- und Zugriffsrichtlinie, die Sie verwenden möchten.
 - [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#)
2. Aktivieren Sie EKS Access Entries auf Ihrem Cluster. Vergewissern Sie sich, dass Sie über eine unterstützte Plattformversion verfügen.
 - [the section called “Authentifizierungsmodus”](#)
3. Erstellen Sie einen Zugriffseintrag, der eine IAM-Identität mit einer Kubernetes-Berechtigung verknüpft.
 - [the section called “Zugangseinträge erstellen”](#)
4. Authentifizieren Sie sich mit der IAM-Identität beim Cluster.

- [the section called “AWS CLI einrichten”](#)
- [the section called “Richten Sie kubectl und eksctl ein”](#)

Legacy-Cluster-Zugriffskonfiguration

Wenn Sie EKS-Zugriffseinträge auf Clustern aktivieren, die vor der Einführung dieser Funktion erstellt wurden (Cluster mit ersten Plattformversionen, die älter sind als die in den Anforderungen für die Plattformversion angegebenen), erstellt EKS automatisch einen Zugriffseintrag, der bereits bestehende Berechtigungen widerspiegelt. Dieser Zugriffseintrag zeigt:

- Die IAM-Identität, mit der der Cluster ursprünglich erstellt wurde
- Die Administratorberechtigungen, die dieser Identität bei der Clustererstellung gewährt wurden

Note

Bisher wurde dieser Administratorzugriff automatisch gewährt und konnte nicht geändert werden. Wenn die EKS-Zugriffseinträge aktiviert sind, können Sie diese ältere Zugriffskonfiguration jetzt anzeigen und löschen.

Zugriffsrichtlinien mit Zugriffseinträgen verknüpfen

Sie können Zugriffseinträgen vom Typ STANDARD eine oder mehrere Zugriffsrichtlinien zuweisen. Amazon EKS erteilt den anderen Arten von Zugriffseinträgen automatisch die erforderlichen Berechtigungen, damit sie in Ihrem Cluster ordnungsgemäß funktionieren. Die Amazon EKS-Zugriffsrichtlinien beinhalten Kubernetes-Berechtigungen, keine IAM-Berechtigungen. Bevor Sie einem Zugriffseintrag eine Zugriffsrichtlinie zuordnen, stellen Sie sicher, dass Sie mit den in den einzelnen Zugriffsrichtlinien enthaltenen Kubernetes-Berechtigungen vertraut sind. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#). Wenn keine der Zugriffsrichtlinien Ihren Anforderungen entspricht, ordnen Sie einem Zugriffseintrag keine Zugriffsrichtlinie zu. Geben Sie stattdessen einen oder mehrere Gruppennamen für den Zugriffseintrag an und erstellen und verwalten Sie rollenbasierte Zugriffskontrollobjekte von Kubernetes. Weitere Informationen finden Sie unter [the section called “Zugangseinträge erstellen”](#).

- Ein vorhandener Zugriffseintrag. Informationen zum Erstellen finden Sie unter [the section called “Zugangseinträge erstellen”](#).

- Eine AWS Identity and Access Management Zugriffsverwaltungsrolle oder ein Benutzer mit den folgenden Berechtigungen: `ListAccessEntries`, `DescribeAccessEntry`, `UpdateAccessEntry`, `ListAccessPolicies`, `AssociateAccessPolicy`, und `DisassociateAccessPolicy`. Weitere Informationen finden Sie unter [Von Amazon Elastic Kubernetes Service definierte Aktionen in der Service Authorization Reference](#).

Berücksichtigen Sie die folgenden Anforderungen, bevor Sie Zugriffsrichtlinien mit Zugriffseinträgen verknüpfen:

- Sie können jedem Zugriffseintrag mehrere Zugriffsrichtlinien zuordnen, aber Sie können jede Richtlinie nur einmal einem Zugriffseintrag zuordnen. Wenn Sie mehrere Zugriffsrichtlinien zuordnen, verfügt der IAM-Principal des Zugriffseintrags über alle Berechtigungen, die in allen zugehörigen Zugriffsrichtlinien enthalten sind.
- Sie können eine Zugriffsrichtlinie auf alle Ressourcen in einem Cluster beschränken oder indem Sie den Namen eines oder mehrerer Kubernetes-Namespaces angeben. Sie können Platzhalterzeichen für einen Namespace-Namen verwenden. Wenn Sie beispielsweise eine Zugriffsrichtlinie auf alle Namespaces ausrichten möchten, die mit `dev-` beginnen, können Sie `dev-*` als Namespace-Namen angeben. Stellen Sie sicher, dass die Namespaces in Ihrem Cluster vorhanden sind und dass Ihre Schreibweise dem tatsächlichen Namespace-Namen im Cluster entspricht. Amazon EKS bestätigt nicht die Schreibweise oder das Vorhandensein der Namespaces in Ihrem Cluster.
- Der Zugriffsbereich für eine Zugriffsrichtlinie kann geändert werden, nachdem sie einem Zugriffseintrag zugeordnet wurde. Wenn Sie die Zugriffsrichtlinie auf Kubernetes-Namespaces beschränkt haben, können Sie bei Bedarf Namespaces für die Zuordnung hinzufügen und entfernen.
- Wenn Sie eine Zugriffsrichtlinie einem Zugriffseintrag zuordnen, für den auch Gruppennamen angegeben sind, verfügt der IAM-Prinzipal über alle Berechtigungen in allen zugehörigen Zugriffsrichtlinien. Es verfügt außerdem über alle Berechtigungen für alle Kubernetes `Role`- oder `ClusterRole` Objekte, die in Kubernetes angegeben sind, sowie für Objekte, die die Gruppennamen angeben. `Role` `RoleBinding`
- Wenn Sie den `kubectl auth can-i --list` Befehl ausführen, werden Ihnen keine Kubernetes-Berechtigungen angezeigt, die durch Zugriffsrichtlinien zugewiesen wurden, die einem Zugriffseintrag für den IAM-Prinzipal zugeordnet sind, den Sie bei der Ausführung des Befehls verwenden. Der Befehl zeigt Kubernetes-Berechtigungen nur an, wenn Sie sie in Kubernetes `Role` oder in `ClusterRole` Objekten erteilt haben, die Sie an die Gruppennamen oder den Benutzernamen gebunden haben, die Sie für einen Zugriffseintrag angegeben haben.

- Wenn Sie sich bei der Interaktion mit Kubernetes-Objekten in Ihrem Cluster als ein Kubernetes-Benutzer oder eine Kubernetes-Gruppe ausgeben, z. B. wenn Sie den `kubectl` Befehl mit `--as username` oder `--as-group group-name` verwenden, erzwingen Sie die Verwendung der Kubernetes-RBAC-Autorisierung. Daher werden dem IAM-Prinzipal keine Berechtigungen durch eine Zugriffsrichtlinie zugewiesen, die dem Zugriffseintrag zugeordnet ist. Die einzigen Kubernetes-Berechtigungen, über die der Benutzer oder die Gruppe verfügt, für die sich der IAM-Prinzipal ausgibt, sind die Kubernetes-Berechtigungen, die Sie ihnen in Kubernetes erteilt haben, `Role` oder `ClusterRole` Objekte, die Sie an die Gruppennamen oder den Benutzernamen gebunden haben. Geben Sie sich nicht als ein Kubernetes-Benutzer oder eine Kubernetes-Gruppe aus, damit Ihr IAM-Prinzipal über die in den zugehörigen Zugriffsrichtlinien festgelegten Berechtigungen verfügt. Der IAM-Prinzipal verfügt weiterhin über alle Berechtigungen, die Sie ihm in Kubernetes `Role` oder `ClusterRole` Objekten erteilt haben, die Sie an die Gruppennamen oder den Benutzernamen gebunden haben, die Sie für den Zugriffseintrag angegeben haben. Weitere Informationen finden Sie unter [Benutzerimpersonation](#) in der Kubernetes-Dokumentation.

Sie können einem Zugriffseintrag mithilfe der AWS Management Console oder der AWS CLI eine Zugriffsrichtlinie zuordnen.

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, der über einen Zugriffseintrag verfügt, dem Sie eine Zugriffsrichtlinien zuordnen möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wenn es sich um einen Zugriffseintrag vom Typ Standard handelt, können Sie Zugriffsrichtlinien von Amazon EKS zuordnen oder deren Zuordnung aufheben. Wenn der Typ Ihres Zugriffseintrags etwas anderes als Standard ist, ist diese Option nicht verfügbar.
5. Wählen Sie Zugriffsrichtlinie zuordnen aus.
6. Wählen Sie unter Richtliniennamen die Richtlinie mit den Berechtigungen aus, über die der IAM-Prinzipal verfügen soll. Informationen zu den Berechtigungen, die in der jeweiligen Richtlinie enthalten sind, finden Sie unter [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#).
7. Wählen Sie unter Zugriffsbereich einen Zugriffsbereich aus. Wenn Sie Cluster wählen, werden die Berechtigungen in der Zugriffsrichtlinie dem IAM-Prinzipal für Ressourcen in allen Kubernetes-Namespaces gewährt. Wenn Sie den Kubernetes-Namespace wählen, können Sie anschließend Neuen Namespace hinzufügen wählen. In dem daraufhin angezeigten Feld Namespace können Sie den Namen eines Kubernetes-Namespaces in Ihrem Cluster eingeben. Wenn die

Berechtigungen für den IAM-Prinzipal in mehreren Namespaces gelten sollen, können Sie mehrere Namespaces eingeben.

8. Wählen Sie Zugriffsrichtlinie hinzufügen aus.

AWS CLI

1. Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yumapt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).

2. Sehen Sie sich die verfügbaren Zugriffsrichtlinien an.

```
aws eks list-access-policies --output table
```

Eine Beispielausgabe sieht wie folgt aus.

```
-----
|                                     ListAccessPolicies
|                                     |
+-----+
||                                     accessPolicies
||                                     ||
|+-----+-----+
+-----+-----+|
||                                     arn
name                                     ||
|+-----+-----+
+-----+-----+|
|| {arn-aws}eks::aws:cluster-access-policy/AmazonEKSAAdminPolicy |
AmazonEKSAAdminPolicy ||
|| {arn-aws}eks::aws:cluster-access-policy/AmazonEKSClusterAdminPolicy |
AmazonEKSClusterAdminPolicy ||
```



```

|| {arn-aws}eks::aws:cluster-access-policy/AmazonEKSEditPolicy      |
AmazonEKSEditPolicy      ||
|| {arn-aws}eks::aws:cluster-access-policy/AmazonEKSVIEWPolicy      |
AmazonEKSVIEWPolicy      ||
|+-----+
+-----+

```

Informationen zu den Berechtigungen, die in der jeweiligen Richtlinie enthalten sind, finden Sie unter [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#).

3. Sehen Sie sich Ihre vorhandenen Zugriffseinträge an. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks list-access-entries --cluster-name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```

{
  "accessEntries": [
    "arn:aws: iam::111122223333:role/my-role",
    "arn:aws: iam::111122223333:user/my-user"
  ]
}

```

4. Ordnen Sie eine Zugriffsrichtlinie einem Zugriffseintrag zu. Im folgenden Beispiel wird die Zugriffsrichtlinie AmazonEKSVIEWPolicy einem Zugriffseintrag zugeordnet. Immer wenn die *my-role* IAM-Rolle versucht, auf Kubernetes-Objekte im Cluster zuzugreifen, autorisiert Amazon EKS die Rolle, die Berechtigungen in der Richtlinie nur für den Zugriff auf Kubernetes-Objekte in den Kubernetes-Namespace und Kubernetes-Namespace zu verwenden. *my-namespace1 my-namespace2 my-cluster* Ersetzen Sie durch den Namen Ihres Clusters, *111122223333* durch Ihre AWS Konto-ID und *my-role* durch den Namen der IAM-Rolle, für die Amazon EKS den Zugriff auf Kubernetes-Clusterobjekte autorisieren soll.

```
aws eks associate-access-policy --cluster-name my-cluster --principal-arn arn:aws:
iam::111122223333:role/my-role \
  --access-scope type=namespace,namespaces=my-namespace1,my-namespace2 --policy-arn
arn:aws: eks::aws:cluster-access-policy/AmazonEKSVIEWPolicy

```

Wenn die Berechtigungen für den IAM-Prinzipal clusterweit gelten sollen, ersetzen Sie `type=namespace,namespaces=`*my-namespace1,my-namespace2* durch `type=cluster`.

Wenn Sie dem Zugriffseintrag mehrere Zugriffsrichtlinien zuordnen möchten, führen Sie den Befehl mehrmals aus und verwenden Sie dabei jeweils eine individuelle Zugriffsrichtlinie. Jede zugeordnete Zugriffsrichtlinie hat ihren eigenen Geltungsbereich.

Note

Wenn Sie später den Geltungsbereich einer zugehörigen Zugriffsrichtlinie ändern möchten, können Sie den vorherigen Befehl erneut ausführen und dabei den neuen Bereich angeben. Wenn Sie den Befehl beispielsweise entfernen *my-namespace2* möchten, führen Sie den Befehl erneut aus und verwenden dabei nur. `type=namespace, namespaces=my-namespace1` Wenn Sie den Gültigkeitsbereich von namespace bis ändern möchten `cluster`, führen Sie den Befehl erneut mit `type=cluster, remove austype=namespace, namespaces=my-namespace1, my-namespace2`.

5. Ermitteln Sie, welche Zugriffsrichtlinien einem Zugriffseintrag zugeordnet sind.

```
aws eks list-associated-access-policies --cluster-name my-cluster --principal-arn
arn:aws:iam::111122223333:role/my-role
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "clusterName": "my-cluster",
  "principalArn": "arn:aws:iam::111122223333",
  "associatedAccessPolicies": [
    {
      "policyArn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSVIEWPolicy",
      "accessScope": {
        "type": "cluster",
        "namespaces": []
      },
      "associatedAt": "2023-04-17T15:25:21.675000-04:00",
      "modifiedAt": "2023-04-17T15:25:21.675000-04:00"
    },
    {
      "policyArn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSAAdminPolicy",
      "accessScope": {
```

```

        "type": "namespace",
        "namespaces": [
            "my-namespace1",
            "my-namespace2"
        ]
    },
    "associatedAt": "2023-04-17T15:02:06.511000-04:00",
    "modifiedAt": "2023-04-17T15:02:06.511000-04:00"
}
]
}

```

Im vorherigen Beispiel hat der IAM-Prinzipal für diesen Zugriffseintrag Leseberechtigungen für alle Namespaces im Cluster und Administratorberechtigungen für zwei Kubernetes-Namespaces.

6. Heben Sie die Zuordnung zwischen einer Zugriffsrichtlinie und einem Zugriffseintrag auf. In diesem Beispiel wird die Zuordnung zwischen der Richtlinie `AmazonEKSAAdminPolicy` und einem Zugriffseintrag aufgehoben. Der IAM-Prinzipal behält jedoch die in der `AmazonEKSVIEWPolicy` Zugriffsrichtlinie enthaltenen Berechtigungen für Objekte in den *my-namespace2* Namespaces *my-namespace1* und bei, da diese Zugriffsrichtlinie nicht vom Zugriffseintrag getrennt ist.

```

aws eks disassociate-access-policy --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/my-role \
    --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSAAdminPolicy

```

Eine Liste der verfügbaren Zugriffsrichtlinien finden Sie unter. [the section called “Überprüfen Sie die Zugriffsrichtlinien”](#)

Migrieren vorhandener **aws-auth ConfigMap**-Einträge zu Zugriffseinträgen

Wenn Sie `aws-auth ConfigMap` auf Ihrem Cluster Einträge hinzugefügt haben, empfehlen wir Ihnen, Zugriffseinträge für die vorhandenen Einträge in Ihrem zu erstellen `aws-authConfigMap`. Nach der Erstellung der Zugriffseinträge können Sie die Einträge aus `ConfigMap` entfernen. Sie können keine [Zugriffsrichtlinien](#) Einträgen in der zuordnen `aws-authConfigMap`. Wenn Sie Ihren IAM-Prinzipalen Zugriffsrichtlinien zuordnen möchten, müssen Sie Zugriffseinträge erstellen.

Important

- Wenn sich ein Cluster im API_AND_CONFIGMAP Authentifizierungsmodus befindet und sowohl in den Zugriffseinträgen als auch in den ConfigMap-Einträgen eine Zuordnung für dieselbe IAM-Rolle vorhanden ist, verwendet die Rolle die Zuordnung des Zugriffseintrags zur Authentifizierung. aws-auth ConfigMap-Zugriffseinträge haben Vorrang vor ConfigMap-Einträgen für denselben IAM-Prinzipal.
- Bevor Sie bestehende aws-auth ConfigMap-Einträge entfernen, die von Amazon EKS für eine [verwaltete Knotengruppe](#) oder ein [Fargate-Profil](#) für Ihren Cluster erstellt wurden, überprüfen Sie, ob die richtigen Zugriffseinträge für diese spezifischen Ressourcen in Ihrem Amazon EKS-Cluster vorhanden sind. Wenn Sie Einträge entfernen, die Amazon EKS erstellt hat, funktioniert Ihr Cluster nicht ordnungsgemäß.

Voraussetzungen

- Vertrautheit mit Zugriffseinträgen und Zugriffsrichtlinien. Weitere Informationen erhalten Sie unter [the section called “Erteilen Sie Berechtigungen”](#) und [the section called “Ordnen Sie Zugriffsrichtlinien zu”](#).
- Ein vorhandener Cluster mit einer Plattformversion, die den in den Voraussetzungen des [the section called “Erteilen Sie Berechtigungen”](#) Themas aufgeführten Versionen entspricht oder höher ist.
- Version 0.210.0 oder höher des eksctl-Befehlszeilen-Tools, das auf Ihrem Computer oder in der AWS CloudShell installiert ist. Informationen zum Installieren und Aktualisieren von eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).
- Kubernetes-Berechtigungen zum Ändern von aws-auth ConfigMap im kube-system Namespace.
- Eine AWS Identity and Access Management Zugriffsverwaltungsrolle oder ein Benutzer mit den folgenden Berechtigungen: CreateAccessEntry und ListAccessEntries. Weitere Informationen finden Sie in der Service-Authorization-Referenz unter [Von Amazon Elastic Kubernetes Service definierte Aktionen](#).

eksctl

1. Sehen Sie sich die vorhandenen Einträge in `aws-auth ConfigMap` an. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
eksctl get iamidentitymapping --cluster my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

ARN	USERNAME	GROUPS	ACCOUNT
arn:aws:iam::111122223333:role/EKS-my-cluster-Admins	Admins	system:masters	
arn:aws:iam::111122223333:role/EKS-my-cluster-my-namespace-Viewers	my-namespace-Viewers	Viewers	
arn:aws:iam::111122223333:role/EKS-my-cluster-self-managed-ng-1	system:node:{{EC2PrivateDNSName}}	system:bootstrappers,system:nodes	
arn:aws:iam::111122223333:user/my-user	my-user		
arn:aws:iam::111122223333:role/EKS-my-cluster-fargateprofile1	system:node:{{SessionName}}		
	system:bootstrappers,system:nodes,system:node-proxier		
arn:aws:iam::111122223333:role/EKS-my-cluster-managed-ng	system:node:{{EC2PrivateDNSName}}	system:bootstrappers,system:nodes	

2. [the section called “Zugangseinträge erstellen”](#) für alle ConfigMap Einträge, die Sie in der vorherigen Ausgabe erstellt haben. Achten Sie beim Erstellen der Zugriffseinträge darauf, für ARN, USERNAME, GROUPS und ACCOUNT die gleichen Werte anzugeben, die in der Ausgabe zurückgegeben wurden. Im Falle der Beispielausgabe würden Sie Zugriffseinträge für alle Einträge außer den letzten beiden Einträgen erstellen, da diese von Amazon EKS für ein Fargate-Profil bzw. für eine verwaltete Knotengruppe erstellt wurden.
3. Löschen Sie die Einträge aus ConfigMap für alle von Ihnen erstellten Zugriffseinträge. Wenn Sie den Eintrag nicht aus dem `löschenConfigMap`, überschreiben die Einstellungen für den Zugriffseintrag für den IAM-Prinzipal-ARN den ConfigMap Eintrag. *111122223333* Ersetzen Sie es durch Ihre AWS Konto-ID und *EKS-my-cluster-my-namespace-Viewers* durch den Namen der Rolle im Eintrag in Ihrem ConfigMap. Wenn der Eintrag, den Sie entfernen möchten, für einen IAM-Benutzer und nicht für eine IAM-Rolle bestimmt ist, `role` ersetzen Sie ihn durch `user` und *EKS-my-cluster-my-namespace-Viewers* durch den Benutzernamen.

```
eksctl delete iamidentitymapping --arn arn:aws:iam::111122223333:role/EKS-my-cluster-my-namespace-Viewers --cluster my-cluster
```

Überprüfen Sie die Zugriffsrichtlinienberechtigungen

Zu den Zugriffsrichtlinien gehören `rules` solche, die Kubernetes verbs (Berechtigungen) und `resources` Die Zugriffsrichtlinien beinhalten keine IAM-Berechtigungen oder Ressourcen. Ähnlich wie bei Kubernetes Role und ClusterRole Objekten beinhalten die Zugriffsrichtlinien nur `allow rules` Sie können den Inhalt einer Zugriffsrichtlinie nicht ändern. Sie können keine eigenen Zugriffsrichtlinien erstellen. Wenn die Berechtigungen in den Zugriffsrichtlinien nicht Ihren Anforderungen entsprechen, erstellen Sie Kubernetes-RBAC-Objekte und geben Sie Gruppennamen für Ihre Zugriffseinträge an. Weitere Informationen finden Sie unter [the section called “Zugangseinträge erstellen”](#). Die in den Zugriffsrichtlinien enthaltenen Berechtigungen ähneln den Berechtigungen in den benutzerorientierten Kubernetes-Clusterrollen. Weitere Informationen finden Sie unter [Benutzerorientierte Rollen](#) in der Kubernetes-Dokumentation.

Wählen Sie eine beliebige Zugriffsrichtlinie aus, um ihren Inhalt anzuzeigen. Die Zeilen der einzelnen Tabellen in den Zugriffsrichtlinien sind jeweils separate Regeln.

EKSAdminAmazon-Richtlinie

Diese Zugriffsrichtlinie umfasst Berechtigungen, die einem IAM-Prinzipal die meisten Berechtigungen für Ressourcen erteilen. Wenn er einem Zugriffseintrag zugeordnet ist, umfasst sein Zugriffsbereich in der Regel einen oder mehrere Kubernetes-Namespace. Wenn ein IAM-Prinzipal über Administratorzugriff auf alle Ressourcen in Ihrem Cluster verfügen soll, ordnen Sie die Zugriffsrichtlinie [the section called “Amazon EKSCluster AdminPolicy”](#) stattdessen Ihrem Zugriffseintrag zu.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSAdminPolicy`

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
apps	daemonsets , deployments , deployments/rollback , deployments/scale , replicase	create, delete, deletecollection , patch, update

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
	ts , replicasets/ scale, statefulsets , statefulsets/scale	
apps	controllerrevisions , daemonsets , daemonset s/status , deployment s , deployments/scale , deployments/status , replicasets , replicase ts/scale , replicase ts/status , statefuls ets , statefulsets/ scale , statefulsets/ status	get, list, watch
authorization.k8s.io	localsubjectaccess reviews	create
autoscaling	horizontalpodautos calers	create, delete, deletecol lection , patch, update
autoscaling	horizontalpodautos calers , horizonta lpodautoscalers/st atus	get, list, watch
batch	cronjobs, jobs	create, delete, deletecol lection , patch, update
batch	cronjobs, cronjobs/ status , jobs, jobs/stat us	get, list, watch
discovery.k8s.io	endpointslices	get, list, watch

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
extensions	daemonsets , deployments , deployments/rollback , deployments/scale , ingresses , networkpolicies , replicaset , replicaset/scale , replicationcontrollers/scale	create, delete, deletecollection , patch, update
extensions	daemonsets , daemonsets/status , deployments , deployments/scale , deployments/status , ingresses , ingresses/status , networkpolicies , replicaset , replicaset/scale , replicaset/status , replicationcontrollers/scale	get, list, watch
networking.k8s.io	ingresses , ingresses/status , networkpolicies	get, list, watch
networking.k8s.io	ingresses , networkpolicies	create, delete, deletecollection , patch, update
policy	poddisruptionbudgets	create, delete, deletecollection , patch, update
policy	poddisruptionbudgets , poddisruptionbudgets/status	get, list, watch

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
rbac.authorization.k8s.io	rolebindings , roles	create, delete, deletecollection , get, list, patch, update, watch
	configmaps , endpoints , persistentvolumeclaims , persistentvolumeclaims/status , pods, replicationcontrollers , replicationcontrollers/scale , serviceaccounts , services, services/status	get, list, watch
	pods/attach , pods/exec , pods/portforward , pods/proxy , secrets, services/proxy	get, list, watch
	configmaps , events, persistentvolumeclaims , replicationcontrollers , replicationcontrollers/scale , secrets, serviceaccounts , services, services/proxy	create, delete, deletecollection , patch, update
	pods, pods/attach , pods/exec , pods/portforward , pods/proxy	create, delete, deletecollection , patch, update

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
	serviceaccounts	impersonate
	bindings, events, limitranges, namespaces/status, pods/log, pods/status, replicationcontrollers/status, resourcequotas, resourcequotas/status	get, list, watch
	namespaces	get, list, watch

Amazon EKSCluster AdminPolicy

Diese Zugriffsrichtlinie umfasst Berechtigungen, die einem IAM-Prinzipaladministrator Zugriff auf einen Cluster gewähren. Wenn er einem Zugriffseintrag zugeordnet ist, entspricht sein Zugriffsbereich in der Regel dem Cluster und nicht einem Kubernetes-Namespace. Wenn der Administratorbereich eines IAM-Prinzipals stärker eingeschränkt sein soll, können Sie stattdessen Ihrem Zugriffseintrag ggf. die Zugriffsrichtlinie [the section called “EKSClusterAdminAmazon-Richtlinie”](#) zuordnen.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSClusterAdminPolicy`

Kubernetes-API-Gruppen	Kubernetes, keine Ressource URLs	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
*		*	*
	*		*

Amazon EKSAAdmin ViewPolicy

Diese Zugriffsrichtlinie umfasst Berechtigungen, die einem IAM-Prinzipal Zugriff auf list/view alle Ressourcen in einem Cluster gewähren. Beachten Sie, dass dies auch [Kubernetes Secrets](#) beinhaltet.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSAAdminViewPolicy`

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
*	*	get, list, watch

EKSEditAmazon-Richtlinie

Diese Zugriffsrichtlinie beinhaltet Berechtigungen, die es einem IAM-Prinzipal ermöglichen, die meisten Kubernetes-Ressourcen zu bearbeiten.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSEditPolicy`

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
apps	daemonsets , deployments , deployments/rollback , deployments/scale , replicaset , replicaset/scale , statefulsets , statefulsets/scale	create, delete, deletecollection , patch, update
apps	controllerrevisions , daemonsets , daemonsets/status , deployments , deployments/scale , deployments/status , replicaset , replicaset/scale , replicaset	get, list, watch

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
	ts/status , statefulsets , statefulsets/scale , statefulsets/status	
autoscaling	horizontalpodautoscalers , horizontalpodautoscalers/status	get, list, watch
autoscaling	horizontalpodautoscalers	create, delete, deletecollection , patch, update
batch	cronjobs, jobs	create, delete, deletecollection , patch, update
batch	cronjobs, cronjobs/status , jobs, jobs/status	get, list, watch
discovery.k8s.io	endpointslices	get, list, watch
extensions	daemonsets , deployments , deployments/rollback , deployments/scale , ingresses , networkpolicies , replicaset , replicaset/scale , replicationcontrollers/scale	create, delete, deletecollection , patch, update

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
extensions	daemonsets , daemonsets/status , deployments , deployments/scale , deployments/status , ingresses , ingresses/status , networkpolicies , replicaset , replicaset/scale , replicaset/status , replicationcontrollers/scale	get, list, watch
networking.k8s.io	ingresses , networkpolicies	create, delete, deletecollection , patch, update
networking.k8s.io	ingresses , ingresses/status , networkpolicies	get, list, watch
policy	poddisruptionbudgets	create, delete, deletecollection , patch, update
policy	poddisruptionbudgets , poddisruptionbudgets/status	get, list, watch
	namespaces	get, list, watch
	pods/attach , pods/exec , pods/portforward , pods/proxy , secrets, services/proxy	get, list, watch
	serviceaccounts	impersonate

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
	pods, pods/attach , pods/exec , pods/port forward , pods/proxy	create, delete, deletecollection , patch, update
	configmaps , events, persistentvolumeclaims , replicationcontrollers , replicationcontrollers/scale , secrets, serviceaccounts , services, services/proxy	create, delete, deletecollection , patch, update
	configmaps , endpoints , persistentvolumeclaims , persistentvolumeclaims/status , pods, replicationcontrollers , replicationcontrollers/scale , serviceaccounts , services, services/status	get, list, watch
	bindings, events, limitranges , namespaces/status , pods/log, pods/status , replicationcontrollers/status , resourcequotas , resourcequotas/status	get, list, watch

EKSViewAmazon-Richtlinie

Diese Zugriffsrichtlinie beinhaltet Berechtigungen, die es einem IAM-Prinzipal ermöglichen, die meisten Kubernetes-Ressourcen einzusehen.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSViewPolicy`

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
apps	controllerrevisions , daemonsets , daemonsets/status , deployments , deployments/scale , deployments/status , replicaset , replicaset/scale , replicaset/status , statefulsets , statefulsets/scale , statefulsets/status	get, list, watch
autoscaling	horizontalpodautoscalers , horizontalpodautoscalers/status	get, list, watch
batch	cronjobs, cronjobs/status , jobs, jobs/status	get, list, watch
discovery.k8s.io	endpointslices	get, list, watch
extensions	daemonsets , daemonsets/status , deployments , deployments/scale , deployments/status , ingresses , ingresses/status , networkpo	get, list, watch

Kubernetes-API-Gruppen	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
	replicasets , replicasets/scale , replicasets/status , replicationcontrollers/scale	
networking.k8s.io	ingresses , ingresses/status , networkpolicies	get, list, watch
policy	poddisruptionbudgets , poddisruptionbudgets/status	get, list, watch
	configmaps , endpoints , persistentvolumeclaims , persistentvolumeclaims/status , pods, replicationcontrollers , replicationcontrollers/scale , serviceaccounts , services, services/status	get, list, watch
	bindings, events, limitranges , namespaces/status , pods/logpods/status , replicationcontrollers/status resourcequotas resourcequotas/status	get, list, watch
	namespaces	get, list, watch

Amazon EKSAuto NodePolicy

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSAutoNodePolicy`

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen Amazon EKS-Komponenten die folgenden Aufgaben ausführen können:

- `kube-proxy`— Überwachen Sie Netzwerkendpunkte und -dienste und verwalten Sie damit verbundene Ereignisse. Dies ermöglicht die clusterweite Netzwerk-Proxyfunktion.
- `ipamd`— Verwaltung von AWS VPC-Netzwerkressourcen und Container-Netzwerkschnittstellen (CNI). Auf diese Weise kann der IP-Adressverwaltungs-Daemon das Pod-Netzwerk verwalten.
- `coredns`— Greifen Sie auf Ressourcen zur Diensterkennung wie Endpunkte und Dienste zu. Dies ermöglicht die DNS-Auflösung innerhalb des Clusters.
- `ebs-csi-driver`— Arbeiten Sie mit speicherbezogenen Ressourcen für Amazon EBS-Volumes. Dies ermöglicht die dynamische Bereitstellung und das Anhängen persistenter Volumes.
- `neuron`— Überwachen Sie Knoten und Pods für AWS Neuron-Geräte. Dies ermöglicht die Verwaltung von AWS Inferentia- und Trainium-Beschleunigern.
- `node-monitoring-agent`— Zugriffsknotendiagnosen und Ereignisse. Dies ermöglicht die Überwachung des Clusterzustands und die Erfassung von Diagnosen.

Jede Komponente verwendet ein eigenes Dienstkonto und ist nur auf die Berechtigungen beschränkt, die für die jeweilige Funktion erforderlich sind.

Wenn Sie eine Node-IAM-Rolle in einem manuell angeben NodeClass, müssen Sie einen Zugriffseintrag erstellen, der die neue Node-IAM-Rolle dieser Zugriffsrichtlinie zuordnet.

Amazon EKSBLOCK StoragePolicy

Note

Diese Richtlinie ist nur für AWS dienstbezogene Rollen vorgesehen und kann nicht für vom Kunden verwaltete Rollen verwendet werden.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSBLOCKStoragePolicy`

Diese Richtlinie umfasst Berechtigungen, die es Amazon EKS ermöglichen, Ressourcen für die Wahl und Koordination von Führungskräften für Speicheroperationen zu verwalten:

- `coordination.k8s.io`— Erstellung und Verwaltung von Leasingobjekten für die Wahl des Leiters. Auf diese Weise können EKS-Speicherkomponenten ihre Aktivitäten im gesamten Cluster über einen Mechanismus zur Wahl des Leiters koordinieren.

Die Richtlinie ist auf bestimmte Leasing-Ressourcen beschränkt, die von den EKS-Speicherkomponenten verwendet werden, um widersprüchliche Zugriffe auf andere Koordinationsressourcen im Cluster zu verhindern.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Blockspeicherkapazität ordnungsgemäß funktioniert.

Amazon EKSLoad BalancingPolicy

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy`

Diese Richtlinie umfasst Berechtigungen, die es Amazon EKS ermöglichen, Ressourcen für die Wahl von Führungskräften für den Lastenausgleich zu verwalten:

- `coordination.k8s.io`— Erstellung und Verwaltung von Leasingobjekten für die Wahl von Führungskräften. Auf diese Weise können die EKS-Lastenausgleichskomponenten die Aktivitäten mehrerer Replikate koordinieren, indem sie einen Leiter wählen.

Die Richtlinie ist speziell auf den Lastenausgleich von Leasing-Ressourcen ausgerichtet, um eine ordnungsgemäße Koordination sicherzustellen und gleichzeitig den Zugriff auf andere Leasing-Ressourcen im Cluster zu verhindern.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Netzwerkfähigkeit ordnungsgemäß funktioniert.

EKSNetworkingAmazon-Richtlinie

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy`

Diese Richtlinie umfasst Berechtigungen, die es Amazon EKS ermöglichen, Ressourcen zur Wahl von Führungskräften für Netzwerke zu verwalten:

- `coordination.k8s.io`— Erstellung und Verwaltung von Leasingobjekten für die Wahl von Führungskräften. Auf diese Weise können die EKS-Netzwerkkomponenten die Aktivitäten zur Zuweisung von IP-Adressen koordinieren, indem sie einen Leiter wählen.

Die Richtlinie ist speziell auf Netzwerk-Leasing-Ressourcen ausgerichtet, um eine korrekte Koordination sicherzustellen und gleichzeitig den Zugriff auf andere Leasing-Ressourcen im Cluster zu verhindern.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Netzwerkfähigkeit ordnungsgemäß funktioniert.

EKSComputeAmazon-Richtlinie

Note

Diese Richtlinie ist nur für AWS dienstbezogene Rollen vorgesehen und kann nicht für vom Kunden verwaltete Rollen verwendet werden.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy`

Diese Richtlinie umfasst Berechtigungen, die es Amazon EKS ermöglichen, Ressourcen für die Wahl von Führungskräften für Rechenoperationen zu verwalten:

- `coordination.k8s.io`— Leasingobjekte für die Wahl des Leiters erstellen und verwalten. Auf diese Weise können EKS-Rechenkomponenten die Aktivitäten zur Knotenskalierung koordinieren, indem sie einen Leiter wählen.

Die Richtlinie ist speziell auf Leasing-Ressourcen für das Rechenmanagement ausgelegt und ermöglicht gleichzeitig einfachen Lesezugriff (`get`, `watch`) auf alle Leasing-Ressourcen im Cluster.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Netzwerkfähigkeit ordnungsgemäß funktioniert.

Amazon EKSBLOCK StorageClusterPolicy

Note

Diese Richtlinie ist nur für AWS dienstbezogene Rollen vorgesehen und kann nicht für vom Kunden verwaltete Rollen verwendet werden.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSBLOCKStorageClusterPolicy`

Diese Richtlinie gewährt die für die Blockspeicherfunktion von Amazon EKS Auto Mode erforderlichen Berechtigungen. Es ermöglicht die effiziente Verwaltung von Blockspeicherressourcen innerhalb von Amazon EKS-Clustern. Die Richtlinie umfasst die folgenden Berechtigungen:

CSI-Treiberverwaltung:

- CSI-Treiber speziell für Blockspeicher erstellen, lesen, aktualisieren und löschen.

Volume-Verwaltung:

- persistente Volumes auflisten, überwachen, erstellen, aktualisieren, patchen und löschen.
- Ansprüche auf persistente Volumes auflisten, überwachen und aktualisieren.
- Patchen Sie den Status persistenter Volumenansprüche.

Interaktion zwischen Knoten und Pod:

- Lesen Sie die Knoten- und Pod-Informationen.
- Verwalten Sie Ereignisse im Zusammenhang mit Speichervorgängen.

Speicherklassen und Attribute:

- Lesen Sie Speicherklassen und CSI-Knoten.
- Lesen Sie die Klassen von Volumenattributen.

Volumenanhänge:

- Volumenanhänge und deren Status auflisten, beobachten und ändern.

Snapshot-Operationen:

- Verwalten Sie Volume-Snapshots, Snapshot-Inhalte und Snapshot-Klassen.
- Verwaltet Operationen für Volumegruppen-Snapshots und zugehörige Ressourcen.

Diese Richtlinie wurde entwickelt, um eine umfassende Blockspeicherverwaltung innerhalb von Amazon EKS-Clustern zu unterstützen, die im Auto-Modus ausgeführt werden. Sie kombiniert Berechtigungen für verschiedene Operationen, einschließlich der Bereitstellung, des Anfügens, der Größenänderung und der Erstellung von Snapshots von Blockspeicher-Volumes.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Blockspeicherkapazität ordnungsgemäß funktioniert.

Amazon EKSCoordinate ClusterPolicy

Note

Diese Richtlinie ist nur für AWS dienstbezogene Rollen vorgesehen und kann nicht für vom Kunden verwaltete Rollen verwendet werden.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSCoordinateClusterPolicy`

Diese Richtlinie gewährt Berechtigungen, die für die Rechenverwaltungsfunktion von Amazon EKS Auto Mode erforderlich sind. Es ermöglicht eine effiziente Orchestrierung und Skalierung von Rechenressourcen innerhalb von Amazon EKS-Clustern. Die Richtlinie umfasst die folgenden Berechtigungen:

Knotenverwaltung:

- Den Status von und erstellen, lesen, aktualisieren, löschen NodePools und verwalten NodeClaims.
- Verwalten NodeClasses, einschließlich Erstellung, Änderung und Löschung.

Terminplanung und Ressourcenmanagement:

- Lesezugriff auf Pods, Knoten, persistente Volumes, persistente Volume Claims, Replikationscontroller und Namespaces.
- Lesezugriff auf Speicherklassen, CSI-Knoten und Volume-Anhänge.
- Listet Bereitstellungen, Daemon-Sets, Replikatgruppen und Stateful-Sets auf und beobachtet sie.
- Lesen Sie Budgets für Pod-Unterbrechungen.

Umgang mit Ereignissen:

- Cluster-Ereignisse erstellen, lesen und verwalten.

Deprovisionierung von Knoten und Pod-Räumung:

- Knoten aktualisieren, patchen und löschen.
- Erstellen Sie Pod-Räumungen und löschen Sie Pods, falls erforderlich.

Verwaltung benutzerdefinierter Ressourcendefinitionen (CRD):

- Neues CRDs erstellen.
- Spezifische Funktionen CRDs im Zusammenhang mit der Knotenverwaltung verwalten (NodeClasses NodePools NodeClaims,, und NodeDiagnostics).

Diese Richtlinie wurde entwickelt, um ein umfassendes Rechenmanagement innerhalb von Amazon EKS-Clustern zu unterstützen, die im Auto-Modus ausgeführt werden. Sie kombiniert Berechtigungen für verschiedene Operationen, einschließlich Knotenbereitstellung, Planung, Skalierung und Ressourcenoptimierung.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Rechenverwaltungsfunktion ordnungsgemäß funktioniert.

Amazon EKSLoad BalancingClusterPolicy

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingClusterPolicy`

Diese Richtlinie gewährt Berechtigungen, die für die Lastausgleichsfunktion von Amazon EKS Auto Mode erforderlich sind. Es ermöglicht die effiziente Verwaltung und Konfiguration von Lastausgleichsressourcen innerhalb von Amazon EKS-Clustern. Die Richtlinie umfasst die folgenden Berechtigungen:

Ereignis- und Ressourcenmanagement:

- Ereignisse erstellen und patchen.
- Lesezugriff auf Pods, Knoten, Endpunkte und Namespaces.
- Pod-Status aktualisieren.

Service- und Eingangsmanagement:

- Vollständige Verwaltung der Dienste und ihres Status.
- Umfassende Kontrolle über Zugriffe und deren Status.
- Lesezugriff auf Endpunkt-Slices und Ingress-Klassen.

Zielgruppenbindungen:

- Zielgruppenbindungen und deren Status erstellen und ändern.
- Lesezugriff auf Ingress-Klassenparameter.

Verwaltung benutzerdefinierter Ressourcendefinitionen (CRD):

- Alles CRDs erstellen und lesen.
- Spezifische Verwaltung von `targetgroupbindings.eks.amazonaws.com` und `ingressclassparams.eks.amazonaws.com`. CRDs

Webhook-Konfiguration:

- Erstellen und lesen Sie mutierende und validierende Webhook-Konfigurationen.
- Verwalte die Konfiguration. `eks-load-balancing-webhook`

Diese Richtlinie wurde entwickelt, um ein umfassendes Lastausgleichsmanagement innerhalb von Amazon EKS-Clustern zu unterstützen, die im Auto-Modus ausgeführt werden. Sie kombiniert

Berechtigungen für verschiedene Vorgänge, darunter die Bereitstellung von Diensten, das Routing eingehender Daten und die Integration mit AWS Lastausgleichsdiensten.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Lastausgleichsfunktion ordnungsgemäß funktioniert.

Amazon EKSNetworking ClusterPolicy

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy`

Amazon EKSNetworking ClusterPolicy

Diese Richtlinie gewährt Berechtigungen, die für die Netzwerkfähigkeit von Amazon EKS Auto Mode erforderlich sind. Es ermöglicht eine effiziente Verwaltung und Konfiguration von Netzwerkressourcen innerhalb von Amazon EKS-Clustern. Die Richtlinie umfasst die folgenden Berechtigungen:

Knoten- und Pod-Verwaltung:

- Lesezugriff auf NodeClasses und deren Status.
- Lesezugriff auf NodeClaims und deren Status.
- Lesezugriff auf Pods.

CNI-Knotenverwaltung:

- Berechtigungen für CNINodes und deren Status, einschließlich Erstellen, Lesen, Aktualisieren, Löschen und Patchen.

Verwaltung benutzerdefinierter Ressourcendefinitionen (CRD):

- Alles CRDs erstellen und lesen.
- Spezifische Verwaltung (aktualisieren, patchen, löschen) der `cninodes.eks.amazonaws.com` CRD.

Verwaltung von Veranstaltungen:

- Ereignisse erstellen und patchen.

Diese Richtlinie wurde entwickelt, um ein umfassendes Netzwerkmanagement innerhalb von Amazon EKS-Clustern zu unterstützen, die im Auto-Modus ausgeführt werden. Sie kombiniert Berechtigungen für verschiedene Operationen, darunter die Netzwerkkonfiguration von Knoten, die Verwaltung von CNI (Container Network Interface) und die damit verbundene benutzerdefinierte Ressourcenverwaltung.

Die Richtlinie ermöglicht es den Netzwerkkomponenten, mit knotenbezogenen Ressourcen zu interagieren, CNI-spezifische Knotenkonfigurationen zu verwalten und benutzerdefinierte Ressourcen zu verwalten, die für Netzwerkvorgänge im Cluster von entscheidender Bedeutung sind.

Amazon EKS erstellt automatisch einen Zugriffseintrag mit dieser Zugriffsrichtlinie für die Cluster-IAM-Rolle, wenn der automatische Modus aktiviert ist. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen vorhanden sind, damit die Netzwerkfähigkeit ordnungsgemäß funktioniert.

EKSHybridAmazon-Richtlinie



Note

Diese Richtlinie ist nur für AWS dienstbezogene Rollen vorgesehen und kann nicht für vom Kunden verwaltete Rollen verwendet werden.

Diese Zugriffsrichtlinie umfasst Berechtigungen, die EKS Zugriff auf die Knoten eines Clusters gewähren. Wenn sie einem Zugriffseintrag zugeordnet ist, entspricht sein Zugriffsbereich in der Regel dem Cluster und nicht einem Kubernetes-Namespace. Diese Richtlinie wird von Amazon EKS-Hybridknoten verwendet.

ARN – `arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy`

Kubernetes-API-Gruppen	Kubernetes, keine Ressource URLs	Kubernetes-Ressourcen	Kubernetes-Verben (Berechtigungen)
*		nodes	list

Amazon EKSCluster InsightsPolicy

 Note

Diese Richtlinie ist nur für AWS dienstbezogene Rollen vorgesehen und kann nicht für vom Kunden verwaltete Rollen verwendet werden.

ARN – `arn:aws: eks::aws:cluster-access-policy/AmazonEKSClusterInsightsPolicy`

Diese Richtlinie gewährt nur Leseberechtigungen für die Amazon EKS Cluster Insights-Funktionalität. Die Richtlinie umfasst die folgenden Berechtigungen:

Knotenzugriff: — Clusterknoten auflisten und anzeigen — Informationen zum Knotenstatus lesen

DaemonSet Zugriff: - Lesezugriff auf die Kube-Proxy-Konfiguration

Diese Richtlinie wird automatisch vom EKS-Dienst für Cluster Insights verwaltet. Weitere Informationen finden Sie unter [the section called “Cluster-Erkenntnisse”](#).

Aktualisierungen für Zugriffsrichtlinien

Sehen Sie sich an, welche Aktualisierungen für Zugriffsrichtlinien seit ihrer Einführung vorgenommen wurden. Abonnieren Sie den RSS-Feed in, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten[Dokumentverlauf](#).

Änderung	Beschreibung	Datum
Richtlinie für EKS Cluster Insights hinzufügen	Veröffentlichen AmazonEKS ClusterInsightsPolicy	2. Dezember 2024
Richtlinien für Amazon EKS Hybrid hinzufügen	Veröffentlichen AmazonEKS HybridPolicy	2. Dezember 2024
Richtlinien für Amazon EKS Auto Mode hinzufügen	Diese Zugriffsrichtlinien gewähren der Cluster-IAM-Rolle und der Node-IAM-Rolle die Erlaubnis,	2. Dezember 2024

Änderung	Beschreibung	Datum
	Kubernetes aufzurufen. APIs AWS verwendet diese, um Routineaufgaben für Speicher-, Rechen- und Netzwerkr Ressourcen zu automatisieren.	
Add AmazonEKSAAdminView Policy	Fügen Sie eine neue Richtlinie für erweiterten Anzeigegriff hinzu, einschließlich Ressourcen wie Secrets.	23. April 2024
Zugriffsrichtlinien wurden eingeführt.	In Amazon EKS wurden Zugriffsrichtlinien eingeführt.	29. Mai 2023

Ändern Sie den Authentifizierungsmodus, um Zugriffseinträge zu verwenden

Wenn Sie Zugriffseinträge verwenden möchten, müssen Sie zunächst den Authentifizierungsmodus des Clusters in API_AND_CONFIG_MAP oder API ändern. Dadurch wird die API für Zugriffseinträge hinzugefügt.

AWS Konsole

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, in dem Sie einen Zugriffseintrag erstellen möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Der Authentifizierungsmodus zeigt den aktuellen Authentifizierungsmodus des Clusters an. Wenn im Modus EKS-API angegeben ist, können Sie bereits Zugriffseinträge hinzufügen und die verbleibenden Schritte überspringen.
5. Wählen Sie Zugriff verwalten aus.
6. Wählen Sie für den Cluster-Authentifizierungsmodus einen Modus mit der EKS-API aus. Beachten Sie, dass Sie den Authentifizierungsmodus nicht wieder in einen Modus ändern können, der die EKS-API und die Zugriffseinträge entfernt.
7. Wählen Sie Änderungen speichern aus. Amazon EKS beginnt mit der Aktualisierung des Clusters, der Status des Clusters ändert sich in Aktualisierung, und die Änderung wird auf der Registerkarte Aktualisierungsverlauf aufgezeichnet.

8. Warten Sie, bis der Status des Clusters wieder Aktiv ist. Wenn der Cluster aktiv ist, können Sie die unter beschriebenen Schritte ausführen, [the section called “Zugangseinträge erstellen”](#) um IAM-Prinzipalen Zugriff auf den Cluster hinzuzufügen.

AWS CLI

1. Installieren Sie die AWS CLI, wie unter [Installation](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle beschrieben.
2. Führen Sie den folgenden Befehl aus. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Wenn Sie die ConfigMap-Methode dauerhaft deaktivieren möchten, ersetzen Sie `API_AND_CONFIG_MAP` durch `API`.

Amazon EKS beginnt mit der Aktualisierung des Clusters, der Status des Clusters ändert sich in `UPDATE`, und die Änderung wird in den `aws eks-list-updates` aufgezeichnet.

```
aws eks update-cluster-config --name my-cluster --access-config
authenticationMode=API_AND_CONFIG_MAP
```

3. Warten Sie, bis der Status des Clusters wieder Aktiv ist. Wenn der Cluster aktiv ist, können Sie die unter beschriebenen Schritte ausführen, [the section called “Zugangseinträge erstellen”](#) um IAM-Prinzipalen Zugriff auf den Cluster hinzuzufügen.

Erforderliche Plattformversion

Um Zugriffseinträge verwenden zu können, muss der Cluster über eine Plattformversion verfügen, die mit der in der folgenden Tabelle aufgeführten Version identisch oder höher ist, oder über eine Kubernetes-Version, die später als die in der Tabelle aufgeführten Versionen ist. Wenn Ihre Kubernetes-Version nicht aufgeführt ist, unterstützen alle Plattformversionen Zugriffseinträge.

Kubernetes-Version	Plattformversion
1.30	eks.2
1.29	eks.1
1.28	eks.6
1.27	eks.10

Kubernetes-Version	Plattformversion
1.26	eks.11

Weitere Informationen finden Sie unter [the section called “Plattformversionen”](#).

Zugangseinträge erstellen

Berücksichtigen Sie Folgendes, bevor Sie Zugriffseinträge erstellen:

- Ein ordnungsgemäß eingestellter Authentifizierungsmodus. Siehe [the section called “Authentifizierungsmodus”](#).
- Ein Zugriffseintrag enthält den Amazon-Ressourcennamen (ARN) genau eines vorhandenen IAM-Prinzips. Ein IAM-Prinzipal kann nicht in mehr als einem Zugriffseintrag enthalten sein. Zusätzliche Überlegungen zu dem von Ihnen angegebenen ARN:
 - In den bewährten Methoden für IAM wird empfohlen, für den Zugriff auf Ihren Cluster IAM-Rollen mit kurzfristigen Anmeldeinformationen zu verwenden anstatt IAM-Benutzer mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zuzugreifen](#).
 - Wenn der ARN für eine IAM-Rolle bestimmt ist, kann er einen Pfad enthalten. ARNs in aws-auth ConfigMap Einträgen darf kein Pfad enthalten sein. Ihr ARN kann beispielsweise `arn:aws:iam::<111122223333>:role/<development/apps/my-role>` oder `arn:aws:iam::<111122223333>:role/<my-role>` lauten.
 - Wenn der Typ des Zugriffseintrags etwas anderes ist als STANDARD (siehe nächste Überlegung zu Typen), muss sich der ARN in demselben AWS Konto befinden, in dem sich Ihr Cluster befindet. Wenn der Typ ist STANDARD, kann sich der ARN in demselben oder einem anderen Konto befinden als das AWS Konto, in dem sich Ihr Cluster befindet.
 - Sie können den IAM-Prinzipal nicht ändern, nachdem der Zugriffseintrag erstellt wurde.
 - Wenn Sie jemals den IAM-Prinzipal mit diesem ARN löschen, wird der Zugriffseintrag nicht automatisch gelöscht. Es empfiehlt sich, den Zugriffseintrag mit einem ARN für einen gelöschten IAM-Prinzipal zu löschen. Wenn Sie den Zugriffseintrag nicht löschen und den IAM-Prinzipal erneut erstellen, funktioniert der Zugriffseintrag nicht, auch wenn er denselben ARN hat. Dies liegt daran, dass, obwohl der ARN für den neu erstellten IAM-Prinzipal derselbe ist, der `roleID` oder `userID` (Sie können dies mit dem `aws sts get-caller-identity` AWS CLI-Befehl sehen) für den neu erstellten IAM-Prinzipal anders ist als für den ursprünglichen IAM-Prinzipal.

Auch wenn Sie den `roleID` oder `userID` für einen Zugriffseintrag des IAM-Prinzipals nicht sehen, speichert Amazon EKS ihn zusammen mit dem Zugriffseintrag.

- Jeder Zugriffseintrag hat einen Typ. Der Typ des Zugriffseintrags hängt von der Art der Ressource ab, der er zugeordnet ist, und definiert nicht die Berechtigungen. Wenn Sie keinen Typ angeben, setzt Amazon EKS den Typ automatisch auf STANDARD
 - EC2_LINUX— Für eine IAM-Rolle, die mit selbstverwalteten Linux- oder Bottlerocket-Knoten verwendet wird
 - EC2_WINDOWS— Für eine IAM-Rolle, die mit selbstverwalteten Windows-Knoten verwendet wird
 - FARGATE_LINUX- Für eine IAM-Rolle, die mit AWS Fargate (Fargate) verwendet wird
 - HYBRID_LINUX— Für eine IAM-Rolle, die mit Hybridknoten verwendet wird
 - STANDARD— Standardtyp, falls keiner angegeben ist
 - EC2- Für benutzerdefinierte Knotenklassen im EKS-Auto-Modus. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen Eintrag zum Zugriff auf die Knotenklasse”](#).
 - Sie können den Typ nicht ändern, nachdem der Zugriffseintrag erstellt wurde.
- Es ist nicht erforderlich, einen Zugriffseintrag für eine IAM-Rolle zu erstellen, die für eine verwaltete Knotengruppe oder ein Fargate-Profil verwendet wird. EKS erstellt Zugriffseinträge (falls aktiviert) oder aktualisiert die Authentifizierungskonfigurationsübersicht (falls Zugriffseinträge nicht verfügbar sind)
- Wenn der Typ des Zugriffseintrags STANDARD lautet, können Sie einen Benutzernamen für den Zugriffseintrag angeben. Wenn Sie keinen Wert für den Benutzernamen angeben, legt Amazon EKS einen der folgenden Werte für Sie fest, abhängig vom Typ des Zugriffseintrags und davon, ob es sich bei dem von Ihnen angegebenen IAM-Prinzipal um eine IAM-Rolle oder einen IAM-Benutzer handelt. Sofern Sie keinen bestimmten Grund für die Angabe Ihres eigenen Benutzernamens haben, empfehlen wir, keinen anzugeben und Amazon EKS ihn automatisch für Sie generieren zu lassen. Beachten Sie bei Angabe eines eigenen Benutzernamens Folgendes:
 - Es kann nicht mit `system:`, `eks:`, `aws:amazon:`, oder `iam:` beginnen.
 - Wenn der Benutzername für eine IAM-Rolle ist, empfehlen wir, dass Sie am Ende Ihres Benutzernamens `{{SessionName}}` oder `{{SessionNameRaw}}` hinzufügen. Wenn Sie Ihrem Benutzernamen eines `{{SessionName}}` oder `{{SessionNameRaw}}` hinzufügen, muss der Benutzername einen Doppelpunkt vor `{{SessionName}}` enthalten. Wenn diese Rolle übernommen wird, wird der Name der AWS STS-Sitzung, der bei der Übernahme der Rolle angegeben wurde, automatisch an den Cluster übergeben und erscheint in den CloudTrail Protokollen. Sie können beispielsweise keinen Benutzernamen von `habenjohn{{SessionName}}`. Er müsste `:john{{SessionName}}` oder

`jo:hn{{SessionName}}` lauten. Der Doppelpunkt muss sich nur vor `{{SessionName}}` befinden. Der von Amazon EKS generierte Benutzername in der folgenden Tabelle enthält einen ARN. Da ein ARN Doppelpunkte enthält, erfüllt er diese Anforderung. Der Doppelpunkt ist nicht erforderlich, wenn Sie ihn nicht `{{SessionName}}` in Ihrem Benutzernamen angeben. Beachten Sie, dass in `{{SessionName}}` dem Sonderzeichen „@“ im Sitzungsnamen durch „-“ ersetzt wird. `{{SessionNameRaw}}` behält alle Sonderzeichen im Sitzungsnamen bei.

IAM-Prinzipaltyp	Typ	Von Amazon EKS automatisch festgelegter Wert für den Benutzernamen
Benutzer	STANDARD	Der ARN des Benutzers . Beispiel: <code>arn:aws:iam::<111122223333>:user/<my-user></code>
Rolle	STANDARD	Der STS-ARN der Rolle, als sie übernommen wurde. Amazon EKS fügt am Ende der Rolle <code>{{SessionName}}</code> hinzu. Beispiel: <code>arn:aws:sts::<111122223333>:assumed-role/<my-role>/{{SessionName}}</code> Wenn der ARN der von Ihnen angegebenen Rolle einen Pfad enthalten hat, wird dieser von Amazon EKS im generierten Benutzernamen entfernt.
Rolle	EC2_LINUX oder EC2_Windows	<code>system:node:{{EC2PrivateDNSName}}</code>

IAM-Prinzipaltyp	Typ	Von Amazon EKS automatisch festgelegter Wert für den Benutzernamen
Rolle	FARGATE_LINUX	<code>system:node:{{SessionName}}</code>
Rolle	HYBRID_LINUX	<code>system:node:{{SessionName}}</code>

Sie können den Benutzernamen ändern, nachdem der Zugriffseintrag erstellt wurde.

- Wenn der Typ eines Zugriffseintrags ist STANDARD und Sie die Kubernetes-RBAC-Autorisierung verwenden möchten, können Sie dem Zugriffseintrag einen oder mehrere Gruppennamen hinzufügen. Gruppennamen können nach der Erstellung eines Zugriffseintrags hinzugefügt und entfernt werden. Damit der IAM-Prinzipal Zugriff auf Kubernetes-Objekte in Ihrem Cluster hat, müssen Sie Objekte für die rollenbasierte Autorisierung (RBAC) von Kubernetes erstellen und verwalten. Erstellen Sie Kubernetes RoleBinding oder ClusterRoleBinding Objekte in Ihrem Cluster, die den Gruppennamen als für angeben. `subject kind: Group` Kubernetes autorisiert den IAM-Prinzipalzugriff auf alle Clusterobjekte, die Sie in einem Kubernetes angegeben haben, `Role` oder auf Objekte, die Sie auch in Ihren `ClusterRole` Bindungen angegeben haben. `roleRef` Wenn Sie Gruppennamen angeben, empfehlen wir, dass Sie mit den Objekten für die rollenbasierte Autorisierung (RBAC) von Kubernetes vertraut sind. Weitere Informationen finden Sie unter [Using RBAC Authorization](#) in der Kubernetes-Dokumentation.

Important

Amazon EKS bestätigt nicht, dass alle Kubernetes-RBAC-Objekte, die in Ihrem Cluster vorhanden sind, einen der von Ihnen angegebenen Gruppennamen enthalten. Wenn Sie beispielsweise einen Zugriffseintrag für eine Gruppe erstellen, die derzeit nicht existiert, erstellt EKS die Gruppe, anstatt einen Fehler zurückzugeben.

Anstatt oder zusätzlich dazu, dass Kubernetes den IAM-Prinzipalzugriff auf Kubernetes-Objekte in Ihrem Cluster autorisiert, können Sie Amazon EKS-Zugriffsrichtlinien einem Zugriffseintrag zuordnen. Amazon EKS autorisiert IAM-Prinzipale für den Zugriff auf Kubernetes-Objekte in Ihrem Cluster mit den Berechtigungen in der Zugriffsrichtlinie. Sie können die Berechtigungen einer

Zugriffsrichtlinie auf die von Ihnen angegebenen Kubernetes-Namespaces beschränken. Für die Verwendung von Zugriffsrichtlinien müssen Sie Kubernetes-RBAC-Objekte nicht verwalten. Weitere Informationen finden Sie unter [the section called “Ordnen Sie Zugriffsrichtlinien zu”](#).

- Wenn Sie einen Zugriffseintrag mit dem Typ EC2_LINUX oder EC2_Windows erstellen, muss der IAM-Prinzipal, der den Zugriffseintrag erstellt, über die Berechtigung `iam:PassRole` verfügen. Weitere Informationen finden Sie im [IAM-Benutzerhandbuch unter Gewähren von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS Dienst](#).
- Ähnlich wie beim standardmäßigen [IAM-Verhalten](#) sind die Erstellung und Aktualisierung von Zugriffseinträgen letztlich konsistent und es kann mehrere Sekunden dauern, bis sie wirksam werden, nachdem der erste API-Aufruf erfolgreich abgeschlossen wurde. Sie müssen Ihre Anwendungen unter Berücksichtigung dieser potenziellen Verzögerungen konzipieren. Wir empfehlen, keine Erstellungen oder Aktualisierungen von Zugriffseinträgen in die kritischen, hochverfügbaren Codepfade Ihrer Anwendung aufzunehmen. Nehmen Sie -Änderungen stattdessen in einer separaten Initialisierungs- oder Einrichtungsroutine vor, die seltener ausgeführt wird. Vergewissern Sie sich auch, dass die Änderungen weitergegeben wurden, bevor die Produktionsarbeitsabläufe davon abhängen.
- Access-Einträge unterstützen keine [dienstbezogenen Rollen](#). Sie können keine Zugriffseinträge erstellen, bei denen der Prinzipal-ARN eine dienstverknüpfte Rolle ist. Sie können dienstverknüpfte Rollen anhand ihrer ARN identifizieren, die im folgenden Format angegeben ist `arn:aws:iam::*:role/aws-service-role/*`.

Sie können einen Zugriffseintrag mit der AWS Management Console oder der AWS CLI erstellen.

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, in dem Sie einen Zugriffseintrag erstellen möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie Zugriffseintrag erstellen aus.
5. Wählen Sie unter IAM-Prinzipal eine bereits vorhandene IAM-Rolle oder einen bereits vorhandenen IAM-Benutzer aus. In den bewährten Methoden für IAM wird empfohlen, für den Zugriff auf Ihren Cluster IAM-Rollen mit kurzfristigen Anmeldeinformationen zu verwenden anstatt IAM-Benutzer mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zuzugreifen](#).

6. Wenn sich der Zugriffseintrag auf die Knotenrolle bezieht, die für selbstverwaltete EC2 Amazon-Knoten verwendet wird, wählen Sie EC2 Linux oder EC2 Windows aus. Übernehmen Sie andernfalls die Standardeinstellung (Standard).
7. Wenn Sie unter Typ die Option Standard ausgewählt haben, können Sie bei Bedarf unter Benutzername einen Benutzernamen angeben.
8. Wenn Sie den Typ Standard ausgewählt haben und Sie die Kubernetes-RBAC-Autorisierung für den IAM-Prinzipal verwenden möchten, geben Sie einen oder mehrere Namen für Gruppen an. Wenn Sie keine Gruppennamen angeben und die Amazon EKS-Autorisierung verwenden möchten, können Sie in einem späteren Schritt oder nachdem der Zugriffseintrag erstellt wurde, eine Zugriffsrichtlinie zuordnen.
9. (Optional) Weisen Sie dem Zugriffseintrag unter Tags Beschriftungen zu. So können Sie beispielsweise ganz einfach nach allen Ressourcen mit dem gleichen Tag suchen.
10. Wählen Sie Weiter aus.
11. Wenn Sie auf der Seite Zugriffsrichtlinie hinzufügen den Typ Standard ausgewählt haben und Sie möchten, dass Amazon EKS den IAM-Prinzipal autorisiert, Berechtigungen für die Kubernetes-Objekte in Ihrem Cluster zu erhalten, führen Sie die folgenden Schritte aus. Klicken Sie andernfalls auf Next (Weiter).
 - a. Wählen Sie unter Richtlinienname eine Zugriffsrichtlinie aus. Sie können die Berechtigungen der Zugriffsrichtlinien nicht einsehen, sie enthalten jedoch ähnliche Berechtigungen wie die der Kubernetes-Benutzerobjekte. `ClusterRole` Weitere Informationen finden Sie unter [Benutzerorientierte Rollen](#) in der Kubernetes-Dokumentation.
 - b. Wählen Sie eine der folgenden Optionen:
 - Cluster — Wählen Sie diese Option, wenn Amazon EKS den IAM-Prinzipal autorisieren soll, die in der Zugriffsrichtlinie festgelegten Berechtigungen für alle Kubernetes-Objekte in Ihrem Cluster zu erhalten.
 - Kubernetes-Namespace — Wählen Sie diese Option, wenn Amazon EKS den IAM-Prinzipal autorisieren soll, die Berechtigungen in der Zugriffsrichtlinie für alle Kubernetes-Objekte in einem bestimmten Kubernetes-Namespace auf Ihrem Cluster zu erhalten. Geben Sie für Namespace den Namen des Kubernetes-Namespace in Ihrem Cluster ein. Wenn Sie zusätzliche Namespaces hinzufügen möchten, wählen Sie Neuen Namespace hinzufügen aus und geben Sie den Namespace-Namen ein.
 - c. Wenn Sie weitere Richtlinien hinzufügen möchten, wählen Sie Richtlinie hinzufügen aus. Sie können für jede Richtlinie unterschiedliche Geltungsbereiche festlegen, aber jede Richtlinie kann nur einmal hinzugefügt werden.

d. Wählen Sie Weiter aus.

12. Überprüfen Sie die Konfiguration für Ihren Zugriffseintrag. Sollten Sie einen Fehler entdecken, wählen Sie Zurück aus, um schrittweise zurück zu navigieren und den Fehler zu korrigieren. Ist die Konfiguration korrekt, wählen Sie Erstellen aus.

AWS CLI

1. Installieren Sie die AWS CLI, wie unter [Installation](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle beschrieben.
2. So erstellen Sie einen Zugriffseintrag Sie können eines der folgenden Beispiele verwenden, um Zugriffseinträge zu erstellen:
 - Erstellen Sie einen Zugriffseintrag für eine selbstverwaltete Amazon EC2 Linux-Knotengruppe. *my-cluster* Ersetzen Sie ihn durch den Namen Ihres Clusters, *111122223333* durch Ihre AWS Konto-ID und *EKS-my-cluster-self-managed-ng-1* durch den Namen Ihrer [Node-IAM-Rolle](#). Wenn es sich bei Ihrer Knotengruppe um eine Windows-Knotengruppe handelt, *EC2_LINUX* ersetzen EC2_Windows Sie sie durch.

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/EKS-my-cluster-self-managed-ng-1 --type EC2_LINUX
```

Sie können die `--kubernetes-groups` Option nicht verwenden, wenn Sie einen anderen Typ als `STANDARD` angeben. Sie können diesem Zugriffseintrag keine Zugriffsrichtlinie zuordnen, da es sich bei seinem Typ um einen anderen Wert als `STANDARD` handelt.

- Erstellen Sie einen Zugriffseintrag, der eine IAM-Rolle zulässt, die nicht für eine von Amazon EC2 selbst verwaltete Knotengruppe verwendet wird, mit der Kubernetes den Zugriff auf Ihren Cluster autorisieren soll. *my-cluster* Ersetzen Sie ihn durch den Namen Ihres Clusters, *111122223333* durch Ihre AWS Konto-ID und *my-role* durch den Namen Ihrer IAM-Rolle. *Viewers* Ersetzen Sie es durch den Namen einer Gruppe, die Sie in einem Kubernetes `RoleBinding` oder `ClusterRoleBinding` Objekt in Ihrem Cluster angegeben haben.

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/my-role --type STANDARD --user Viewers --kubernetes-groups Viewers
```

- Erstellen Sie einen Zugriffseintrag, der es einem IAM-Benutzer ermöglicht, sich bei Ihrem Cluster zu authentifizieren. Dieses Beispiel soll zeigen, dass es diese Möglichkeit gibt. In den

bewährten Methoden für IAM wird empfohlen, für den Zugriff auf Ihren Cluster IAM-Rollen mit kurzfristigen Anmeldeinformationen zu verwenden anstatt IAM-Benutzer mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu](#) können.

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:user/my-user --type STANDARD --username my-user
```

Wenn Sie möchten, dass dieser Benutzer mehr Zugriff auf Ihren Cluster hat als die Berechtigungen in den Kubernetes-API-Discovery-Rollen, müssen Sie dem Zugriffseintrag eine Zugriffsrichtlinie zuordnen, da die `--kubernetes-groups` Option nicht verwendet wird. Weitere Informationen finden Sie unter [the section called “Ordnen Sie Zugriffsrichtlinien zu” Rollen für API-Erkennung](#) in der Kubernetes-Dokumentation.

Zugangseinträge aktualisieren

Sie können einen Zugriffseintrag mit der AWS Management Console oder der AWS CLI aktualisieren.

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, in dem Sie einen Zugriffseintrag erstellen möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie den Zugriffseintrag aus, den Sie aktualisieren möchten.
5. Wählen Sie Edit (Bearbeiten) aus.
6. Unter Benutzername können Sie den vorhandenen Wert ändern.
7. Unter Gruppen können Sie Gruppennamen entfernen oder neue Gruppennamen hinzufügen. Wenn die folgenden Gruppennamen existieren, entfernen Sie sie nicht: `system:nodes` oder `system:bootstrappers`. Wenn Sie diese Gruppen entfernen, funktioniert Ihr Cluster unter Umständen nicht mehr ordnungsgemäß. Wenn Sie keine Gruppennamen angeben und die Amazon EKS-Autorisierung verwenden möchten, ordnen Sie in einem späteren Schritt eine [Zugriffsrichtlinie](#) zu.
8. Unter Tags können Sie dem Zugriffseintrag Beschriftungen zuweisen. So können Sie beispielsweise ganz einfach nach allen Ressourcen mit dem gleichen Tag suchen. Außerdem können Sie vorhandene Tags entfernen.

9. Wählen Sie Änderungen speichern.

10. Informationen zum Zuordnen einer Zugriffsrichtlinie zu dem Eintrag finden Sie unter [the section called “Ordnen Sie Zugriffsrichtlinien zu”](#).

AWS CLI

1. Installieren Sie die AWS CLI, wie unter [Installation](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle beschrieben.
2. Um einen Zugriffseintrag zu aktualisieren, *my-cluster* ersetzen Sie ihn durch den Namen Ihres Clusters, *111122223333* durch Ihre AWS Konto-ID und *EKS-my-cluster-my-namespace-Viewers* durch den Namen einer IAM-Rolle.

```
aws eks update-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/EKS-my-cluster-my-namespace-Viewers --kubernetes-groups Viewers
```

Sie können die `--kubernetes-groups` Option nicht verwenden, wenn der Typ des Zugriffseintrags ein anderer Wert als STANDARD ist. Sie können auch keine Zugriffsrichtlinie einem Zugriffseintrag zuordnen, der einen anderen Typ als STANDARD hat.

Zugangseinträge löschen

Wenn Sie einen Zugriffseintrag versehentlich gelöscht haben, können Sie ihn jederzeit erneut erstellen. Wenn der Zugriffseintrag, den Sie löschen, mit Zugriffsrichtlinien verknüpft ist, werden die Zuordnungen automatisch gelöscht. Sie müssen die Zuordnung von Zugriffsrichtlinien zu einem Zugriffseintrag nicht trennen, bevor Sie den Zugriffseintrag löschen.

Sie können einen Zugriffseintrag mit der AWS Management Console oder der AWS CLI löschen.

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, aus dem Sie einen Zugriffseintrag löschen möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie in der Liste Zugriffseinträge den Zugriffseintrag aus, den Sie löschen möchten.
5. Wählen Sie Löschen.

6. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).

AWS CLI

1. Installieren Sie die AWS CLI, wie unter [Installation](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle beschrieben.
2. Um einen Zugriffseintrag zu löschen, *my-cluster* ersetzen Sie ihn durch den Namen Ihres Clusters, *111122223333* durch Ihre AWS Konto-ID und *my-role* durch den Namen der IAM-Rolle, auf die Sie keinen Zugriff mehr auf Ihren Cluster haben möchten.

```
aws eks delete-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/my-role
```

Gewähren Sie IAM-Benutzern Zugriff auf Kubernetes mit einem ConfigMap

Important

Der `aws-auth` ConfigMap ist veraltet. Die empfohlene Methode zur Verwaltung des Zugriffs auf Kubernetes finden Sie unter APIs [the section called “Erteilen Sie Berechtigungen”](#)

Der Zugriff auf Ihren Cluster mithilfe von [IAM-Prinzipalen](#) wird durch den [AWS IAM Authenticator for Kubernetes](#) ermöglicht, der auf der Amazon EKS-Steuerebene ausgeführt wird. Der Authenticator erhält seine Konfigurationsinformationen von `aws-auth` ConfigMap. Alle `aws-auth` ConfigMap-Einstellungen finden Sie unter [Vollständiges Konfigurationsformat](#) auf GitHub.

Hinzufügen von IAM-Prinzipal zu Ihrem Amazon EKS-Cluster

Wenn Sie einen Amazon EKS-Cluster erstellen, erhält der [IAM-Principal](#), der den Cluster erstellt, automatisch `system:masters` Berechtigungen für die rollenbasierte Zugriffskontrolle (RBAC) des Clusters in der Amazon EKS-Kontrollebene. Dieser Principal erscheint in keiner sichtbaren Konfiguration. Vergewissern Sie sich daher, dass Sie stets im Auge behalten, welcher Prinzipal den Cluster ursprünglich erstellt hat. Um weiteren IAM-Prinzipalen die Möglichkeit zu geben, mit Ihrem Cluster zu interagieren, bearbeiten Sie die `aws-auth` ConfigMap in Kubernetes und erstellen Sie ein Kubernetes `rolebinding` oder `clusterrolebinding` mit dem Namen eines group, den Sie in der angeben. `aws-auth` ConfigMap

 Note

Weitere Informationen zur Konfiguration der rollenbasierten Zugriffskontrolle (RBAC) von Kubernetes finden Sie unter [Using RBAC Authorization in der Kubernetes-Dokumentation](#).

1. Bestimmen Sie, welche Anmeldeinformationen `kubectl` für den Zugriff auf Ihren Cluster verwendet. Amazon Resource Name (ARN) Auf Ihrem Computer können Sie mit dem folgenden Befehl sehen, welche Anmeldeinformationen `kubectl` verwendet. Ersetzen Sie ihn `~/.kube/config` durch den Pfad zu Ihrer kubeconfig Datei, wenn Sie nicht den Standardpfad verwenden.

```
cat ~/.kube/config
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
contexts:
- context:
  cluster: my-cluster.region-code.eksctl.io
  user: admin@my-cluster.region-code.eksctl.io
  name: admin@my-cluster.region-code.eksctl.io
current-context: admin@my-cluster.region-code.eksctl.io
[...]
```

In der vorherigen Beispielausgabe werden die Anmeldeinformationen für einen Benutzer mit dem Namen `admin` für einen Cluster mit dem Namen `my-cluster` konfiguriert. Wenn dies der Benutzer ist, der den Cluster erstellt hat, hat er bereits Zugriff auf Ihren Cluster. Wenn es nicht der Benutzer ist, der den Cluster erstellt hat, müssen Sie die verbleibenden Schritte ausführen, um den Clusterzugriff für andere IAM-Prinzipale zu aktivieren. [Bewährte Methoden für IAM](#) empfehlen, dass Sie Rollen statt Benutzern Berechtigungen gewähren. Mit dem folgenden Befehl können Sie sehen, welche anderen Prinzipale derzeit Zugriff auf Ihren Cluster haben:

```
kubectl describe -n kube-system configmap/aws-auth
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name:          aws-auth
```

```
Namespace:    kube-system
Labels:       <none>
Annotations:  <none>

Data
====
mapRoles:
----
- groups:
  - system:bootstrappers
  - system:nodes
  rolearn: arn:aws:iam::111122223333:role/my-node-role
  username: system:node:{{EC2PrivateDNSName}}

BinaryData
====

Events:    <none>
```

Das vorherige Beispiel ist ein standardmäßiger `aws-auth ConfigMap`. Nur die Knoten-Instance-Rolle hat Zugriff auf den Cluster.

2. Stellen Sie sicher, dass Sie bereits über Kubernetes und/oder andere verfügen `roles` `clusterroles` und `clusterrolebindings` dass Sie `rolebindings` IAM-Prinzipale zuordnen können. Weitere Informationen über diese Ressourcen finden Sie unter [Using RBAC Authorization](#) (RBAC-Autorisierung verwenden) in der Kubernetes-Dokumentation.
 - a. Zeigen Sie Ihre vorhandenen Kubernetes `roles` oder `clusterroles` an. Roles sind auf einen namespace ausgelegt, aber `clusterroles` sind auf den Cluster ausgelegt.

```
kubectl get roles -A
```

```
kubectl get clusterroles
```

- b. Zeigen Sie die Details einer beliebigen `role` oder `clusterrole` an, die in der vorherigen Ausgabe zurückgegeben wurden, und bestätigen Sie, dass Sie die Berechtigungen (`rules`) hat, die Ihre IAM-Prinzipale in Ihrem Cluster haben sollen.

Ersetzen Sie *role-name* durch einen `role`-Namen, den der vorherige Befehl zurückgegeben hat. Ersetzen Sie *kube-system* durch den Namespace der `role`.


```
kubectl describe role role-name -n kube-system
```

Ersetzen Sie *cluster-role-name* durch einen clusterrole-Namen, den der vorherige Befehl zurückgegeben hat.

```
kubectl describe clusterrole cluster-role-name
```

- c. Zeigen Sie Ihre vorhandenen Kubernetes `rolebindings` oder `clusterrolebindings` an. Rolebindings sind auf einen namespace ausgelegt, aber `clusterrolebindings` sind auf den Cluster ausgelegt.

```
kubectl get rolebindings -A
```

```
kubectl get clusterrolebindings
```

- d. Zeigen Sie die Details einer beliebigen `rolebinding` oder `clusterrolebinding` an und bestätigen Sie, dass sie eine `role` oder `clusterrole` aus dem vorherigen Schritt hat, die als `roleRef` aufgeführt wird, und einen Gruppennamen, der für `subjects` aufgeführt wird.

Ersetzen Sie *role-binding-name* durch einen rolebinding-Namen, den der vorherige Befehl zurückgegeben hat. Ersetzen Sie *kube-system* mit dem namespace der rolebinding.

```
kubectl describe rolebinding role-binding-name -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: eks-console-dashboard-restricted-access-role-binding
  namespace: default
subjects:
- kind: Group
  name: eks-console-dashboard-restricted-access-group
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
```

```
name: eks-console-dashboard-restricted-access-role
apiGroup: rbac.authorization.k8s.io
```

Ersetzen Sie *cluster-role-binding-name* durch einen clusterrolebinding-Namen, den der vorherige Befehl zurückgegeben hat.

```
kubectl describe clusterrolebinding cluster-role-binding-name
```

Eine Beispielausgabe sieht wie folgt aus.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: eks-console-dashboard-full-access-binding
subjects:
- kind: Group
  name: eks-console-dashboard-full-access-group
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: eks-console-dashboard-full-access-clusterrole
  apiGroup: rbac.authorization.k8s.io
```

3. Bearbeiten Sie aws-auth ConfigMap. Sie können ein Tool wie eksctl verwenden, um die ConfigMap zu aktualisieren, oder Sie können sie durch manuelle Bearbeitung aktualisieren.

Important

Wir empfehlen die Verwendung von eksctl oder einem anderen Tool, um die ConfigMap zu bearbeiten. Informationen zu anderen Tools, die Sie verwenden können, finden Sie unter [Use tools to make changes to the aws-auth ConfigMap](#) in den Amazon EKS-Best-Practices-Handbüchern. Ist aws-auth ConfigMap falsch formatiert, können Sie den Zugriff auf Ihren Cluster verlieren.

- Sehen Sie sich die Schritte zum [Bearbeiten der Configmap mit eksctl](#) an.
- Sehen Sie sich die Schritte zur manuellen [Bearbeitung](#) der Configmap an.

Bearbeiten Sie Configmap mit Eksctl

1. Sie benötigen eine Version 0.210.0 oder eine neuere Version des eksctl Befehlszeilentools, das auf Ihrem Gerät installiert ist oder. AWS CloudShell Informationen zum Installieren und Aktualisieren von eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).
2. Zeigen Sie die aktuellen Mappings in der ConfigMap an. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. *region-code* Ersetzen Sie durch die AWS Region, in der sich Ihr Cluster befindet.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

Eine Beispielausgabe sieht wie folgt aus.

ARN	USERNAME	GROUPS
ACCOUNT		
arn:aws: iam::111122223333:role/eksctl-my-cluster-my-nodegroup-		
NodeInstanceRole-1XLS7754U3ZPA	system:node:{{EC2PrivateDNSName}}	
system:bootstrappers,system:nodes		

3. Fügen Sie ein Mapping für eine Rolle hinzu. Ersetzen Sie *my-role* durch den Namen Ihrer Rolle. *eks-console-dashboard-full-access-group* Ersetzen Sie durch den Namen der Gruppe, die in Ihrem Kubernetes RoleBinding oder ClusterRoleBinding Objekt angegeben ist. Ersetzen Sie *111122223333* durch Ihre Konto-ID. Sie können *admin* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
eksctl create iamidentitymapping --cluster my-cluster --region=region-code \
    --arn arn:aws: iam::111122223333:role/my-role --username admin --group eks-
console-dashboard-full-access-group \
    --no-duplicate-arns
```

Important

Der Rollen-ARN darf keinen Pfad wie enthalten `role/my-team/developers/my-role`. Das Format des ARN muss `arn:aws: iam::111122223333:role/my-role` sein. In diesem Beispiel muss `my-team/developers/` entfernt werden.

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
2022-05-09 14:51:20 [#] adding identity "{arn-aws}iam::111122223333:role/my-role" to
auth ConfigMap
```

4. Fügen Sie ein Mapping für einen Benutzer hinzu. [Bewährte Methoden für IAM](#) empfehlen, dass Sie Rollen statt Benutzern Berechtigungen gewähren. Ersetzen Sie *my-user* durch den Benutzernamen. *eks-console-dashboard-restricted-access-group* Ersetzen Sie es durch den Namen der Gruppe, die in Ihrem Kubernetes RoleBinding oder ClusterRoleBinding Objekt angegeben ist. Ersetzen Sie *111122223333* durch Ihre Konto-ID. Sie können *my-user* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
eksctl create iamidentitymapping --cluster my-cluster --region=region-code \
    --arn arn:aws: iam::111122223333:user/my-user --username my-user --group eks-
console-dashboard-restricted-access-group \
    --no-duplicate-arns
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
2022-05-09 14:53:48 [#] adding identity "arn:aws: iam::111122223333:user/my-user" to
auth ConfigMap
```

5. Zeigen Sie wieder die Mappings in der ConfigMap an.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

Eine Beispielausgabe sieht wie folgt aus.

ARN	USERNAME	GROUPS
arn:aws: iam::111122223333:role/eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA	system:node:{{EC2PrivateDNSName}}	
	system:bootstrappers,system:nodes	
arn:aws: iam::111122223333:role/admin	my-role	eks-console-dashboard-full-access-group

```
arn:aws: iam::111122223333:user/my-user
                                my-user                                eks-console-dashboard-restricted-
access-group
```

Bearbeiten Sie Configmap manuell

1. Öffnen Sie ConfigMap zum Bearbeiten.

```
kubectl edit -n kube-system configmap/aws-auth
```

Note

Wenn Sie eine Fehlermeldung mit der Angabe "Error from server (NotFound): configmaps "aws-auth" not found" erhalten, wenden Sie das Verfahren unter [AWS-Auth auf Ihren Cluster anwenden ConfigMap an, um den Bestand anzuwenden.](#) ConfigMap

2. Fügen Sie Ihre IAM-Prinzipale zu der ConfigMap hinzu. Eine IAM-Gruppe ist kein IAM-Prinzipal und kann daher nicht zur hinzugefügt werden. ConfigMap

- So fügen Sie eine IAM-Rolle hinzu (z. B. für [Verbundbenutzer](#)): Fügen Sie die Rollendetails zum Abschnitt mapRoles der ConfigMap unter data hinzu. Fügen Sie diesen Abschnitt hinzu, wenn er nicht bereits in der Datei vorhanden sind. Jeder Eintrag unterstützt die folgenden Parameter:
 - rolearn: Der ARN der IAM-Rolle, den Sie hinzufügen möchten. Dieser Wert darf keinen Pfad enthalten. Sie können beispielsweise keinen ARN wie angeben `arn:aws: iam::111122223333:role/my-team/developers/role-name` . Der ARN muss stattdessen `arn:aws: iam::111122223333:role/role-name` sein.
 - username: Der Benutzername in Kubernetes für die Zuweisung zur IAM-Rolle.
 - Gruppen: Die Gruppe oder Liste der Kubernetes-Gruppen, denen die Rolle zugeordnet werden soll. Die Gruppe kann eine Standardgruppe oder eine Gruppe sein, die in einer clusterrolebinding oder rolebinding angegeben ist. Weitere Informationen finden Sie unter [Standardrollen und Rollenbindungen](#) in der Kubernetes-Dokumentation.
- Um einen IAM-Benutzer hinzuzufügen: [Bewährte Methoden von IAM](#) empfehlen, dass Sie Rollen statt Benutzern Berechtigungen gewähren. Fügen Sie die Benutzerdetails zum mapUsers-Abschnitt der ConfigMap unter data hinzu. Fügen Sie diesen Abschnitt hinzu, wenn er nicht bereits in der Datei vorhanden sind. Jeder Eintrag unterstützt die folgenden Parameter:

- `userarn`: Die ARN des IAM-Benutzers, den Sie hinzufügen möchten.
- `username`: Der Benutzername in Kubernetes für die Zuweisung zum IAM-Benutzer.
- `Gruppen`: Die Gruppe oder Liste der Kubernetes-Gruppen, denen der Benutzer zugeordnet werden soll. Die Gruppe kann eine Standardgruppe oder eine Gruppe sein, die in einer `clusterrolebinding` oder `rolebinding` angegeben ist. Weitere Informationen finden Sie unter [Standardrollen und Rollenbindungen](#) in der Kubernetes-Dokumentation.

3. Beispiel: Der folgende YAML-Block enthält:

- Einen `mapRoles`-Abschnitt, der die IAM-Knoten-Instance Kubernetes-Gruppen zuordnet, sodass sich Knoten selbst bei dem Cluster und der `my-console-viewer-role`-IAM-Rolle registrieren können, die einer Kubernetes-Gruppe zugeordnet ist, die alle Kubernetes-Ressourcen für alle Cluster anzeigen kann. Eine Liste der erforderlichen IAM- und Kubernetes-Gruppenberechtigungen für die `my-console-viewer-role`-IAM-Rolle finden Sie unter [the section called "Erforderliche Berechtigungen"](#).
- Ein `mapUsers` Abschnitt, der den `admin` IAM-Benutzer aus dem AWS Standardkonto der `system:masters` Kubernetes-Gruppe und den `my-user` Benutzer aus einem anderen AWS Konto zuordnet, das einer Kubernetes-Gruppe zugeordnet ist, die Kubernetes-Ressourcen für einen bestimmten Namespace anzeigen kann. Eine Liste der erforderlichen IAM- und Kubernetes-Gruppenberechtigungen für die `my-user`-IAM-Benutzer finden Sie unter [the section called "Erforderliche Berechtigungen"](#).

Fügen Sie nach Bedarf Zeilen hinzu oder entfernen Sie sie und ersetzen Sie alle *example values* durch eigene Werte.

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file
# will be
# reopened with the relevant failures.
#
apiVersion: v1
data:
  mapRoles: |
    - groups:
      - system:bootstrappers
      - system:nodes
      rolearn: arn:aws:iam::111122223333:role/my-role
      username: system:node:{{EC2PrivateDNSName}}
    - groups:
      - eks-console-dashboard-full-access-group
```

```
rolearn: arn:aws: iam::111122223333:role/my-console-viewer-role
username: my-console-viewer-role
mapUsers: |
- groups:
  - system:masters
  userarn: arn:aws: iam::111122223333:user/admin
  username: admin
- groups:
  - eks-console-dashboard-restricted-access-group
  userarn: arn:aws: iam::444455556666:user/my-user
  username: my-user
```

4. Speichern Sie die Datei und beenden Sie den Text-Editor.

Anwenden von **aws-authConfigMap** auf Ihren Cluster

aws-auth ConfigMap wird automatisch erstellt und auf Ihren Cluster angewendet, wenn Sie eine verwaltete Knotengruppe erstellen oder wenn Sie eine Knotengruppe mit `eksctl` erstellen. Sie wird anfänglich erstellt, um Knoten zu erlauben, Ihrem Cluster beizutreten, aber Sie verwenden diese ConfigMap auch, um rollenbasierten Zugriffssteuerungs(RBAC)-Zugriff auf IAM-Prinzipale hinzuzufügen. Wenn Sie selbstverwaltete Knoten gestartet und sie nicht auf Ihren Cluster angewendet haben, können Sie dies aws-auth ConfigMap mit dem folgenden Verfahren tun.

1. Prüfen Sie, ob Sie das bereits angewendet haben. aws-auth ConfigMap

```
kubectl describe configmap -n kube-system aws-auth
```

Wenn Sie eine Fehlermeldung mit der Angabe "Error from server (NotFound): configmaps "aws-auth" not found" erhalten, fahren Sie mit den folgenden Schritten fort, um die Aktie anzuwendenConfigMap.

2. Laden Sie die AWS Authenticator-Konfigurationsübersicht herunter, bearbeiten Sie sie und wenden Sie sie an.

a. Laden Sie die Konfigurationszuordnung herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/
aws-auth-cm.yaml
```

- b. Stellen Sie in der Datei `aws-auth-cm.yaml` `rolearn` auf den Amazon-Ressourcennamen (ARN) der IAM-Rolle ein, die Ihren Knoten zugeordnet ist. Hierzu können Sie einen Texteditor verwenden oder `my-node-instance-role` ersetzen und den folgenden Befehl ausführen:

```
sed -i.bak -e 's|<ARN of instance role (not instance profile)>|my-node-instance-role|' aws-auth-cm.yaml
```

Ändern Sie keine anderen Zeilen in dieser Datei.

 Important

Der Rollen-ARN darf keinen Pfad wie `enthaltenrole/my-team/developers/my-role`. Das Format des ARN muss `arn:aws:iam::111122223333:role/my-role` sein. In diesem Beispiel muss `my-team/developers/` entfernt werden.

Sie können die AWS CloudFormation Stack-Ausgaben für Ihre Knotengruppen überprüfen und nach den folgenden Werten suchen:

- `InstanceRoleARN` — Für Knotengruppen, die erstellt wurden mit `eksctl`
 - `NodeInstanceRole` — Für Knotengruppen, die mit von Amazon EKS bereitgestellten AWS CloudFormation Vorlagen erstellt wurden, in der AWS Management Console
- c. Wenden Sie die Konfiguration an. Die Ausführung dieses Befehls kann einige Minuten dauern.

```
kubectl apply -f aws-auth-cm.yaml
```

 Note

Wenn Sie Autorisierungs- oder Ressourcenfehler erhalten, finden Sie weitere Informationen unter [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#) im Thema zur Fehlerbehebung.

3. Sehen Sie sich den Status Ihrer Knoten an und warten Sie, bis diese in den Ready-Status eintreten.

```
kubectl get nodes --watch
```


Geben Sie `Ctrl+C` ein, um zu einer Shell-Eingabeaufforderung zurückzukehren.

Gewähren Sie Benutzern Zugriff auf Kubernetes mit einem externen OIDC-Anbieter

Amazon EKS unterstützt die Verwendung von OpenID-Connect(OIDC)-Identitätsanbietern als Methode zur Authentifizierung von Benutzern bei Ihrem Cluster. OIDC-Identitätsanbieter können zusammen mit oder als Alternative zu AWS Identity and Access Management (IAM) verwendet werden. Weitere Informationen zur Verwendung von IAM finden Sie unter [the section called “Kubernetes-API-Zugriff”](#). Nachdem Sie die Authentifizierung für Ihren Cluster konfiguriert haben, können Sie Kubernetes `roles` und `clusterroles` erstellen, um den Rollen Berechtigungen zuzuweisen, und dann die Rollen mithilfe von Kubernetes `rolebindings` und `clusterrolebindings` an die Identitäten binden. Weitere Informationen finden Sie unter [Using RBAC Authorization](#) in der Kubernetes-Dokumentation.

- Sie können Ihrem Cluster einen OIDC-Identitätsanbieter zuordnen.
- Kubernetes bietet keinen OIDC-Identitätsanbieter. Sie können einen vorhandenen öffentlichen OIDC-Identitätsanbieter verwenden oder Ihren eigenen Identitätsanbieter ausführen. Eine Liste zertifizierter Anbieter finden Sie unter [OpenID-Zertifizierung](#) auf der OpenID-Website.
- Die Aussteller-URL des OIDC-Identitätsanbieters muss öffentlich zugänglich sein, damit Amazon EKS die Signaturschlüssel erkennen kann. Amazon EKS unterstützt keine OIDC-Identitätsanbieter mit selbstsignierten Zertifikaten.
- Sie können die IAM-Authentifizierung für Ihren Cluster nicht deaktivieren, da sie immer noch erforderlich ist, um Knoten zu einem Cluster hinzuzufügen.
- Ein Amazon EKS-Cluster muss weiterhin von einem AWS [IAM-Prinzipal](#) erstellt werden und nicht von einem OIDC-Identitätsanbieter-Benutzer. Dies liegt daran, dass der Cluster-Ersteller mit Amazon EKS APIs und nicht mit APIs Kubernetes interagiert.
- Benutzer, die vom OIDC-Identitätsanbieter authentifiziert wurden, werden im Auditprotokoll des Clusters aufgeführt, wenn die CloudWatch Protokolle für die Kontrollebene aktiviert sind. Weitere Informationen finden Sie unter [the section called “Aktivieren oder deaktivieren Sie die Protokolle der Kontrollebene”](#).
- Sie können sich nicht AWS Management Console mit einem Konto eines OIDC-Anbieters bei der anmelden. Sie können dies nur [the section called “Auf Cluster-Ressourcen zugreifen”](#) tun, indem

Sie sich AWS Management Console mit einem AWS Identity and Access Management-Konto anmelden.

Verknüpfen Sie einen OIDC-Identitätsanbieter

Bevor Sie Ihrem Cluster einen OIDC-Identitätsanbieter zuordnen können, benötigen Sie die folgenden Informationen von Ihrem Anbieter:

URL des Ausstellers

Die URL des OIDC-Identitätsanbieters, die es dem API-Server ermöglicht, öffentliche Signierschlüssel zur Verifizierung von Token zu ermitteln. Die URL muss mit dem `iss` Anspruch in den OIDC-ID-Token des Anbieters beginnen `https://` und diesem entsprechen. Gemäß dem OIDC-Standard sind Pfadkomponenten erlaubt, Abfrageparameter jedoch nicht. Normalerweise besteht die URL nur aus einem Hostnamen wie <https://server.example.org> oder <https://example.com>. Diese URL sollte auf die Ebene unterhalb von `.well-known/openid-configuration` verweisen und muss über das Internet öffentlich zugänglich sein.

Client-ID (auch bekannt als Zielgruppe)

Die ID für die Client-Anwendung, die Authentifizierungsanforderungen an den OIDC-Identitätsanbieter stellt.

Sie können einen Identitätsanbieter mit `eksctl` oder AWS Management Console zuordnen.

Ordnen Sie mithilfe von `eksctl` einen Identitätsanbieter zu

1. Erstellen Sie eine Datei mit dem Namen *associate-identity-provider.yaml* und dem folgenden Inhalt. Ersetzen Sie das *example values* durch Ihr eigenes. Die Werte im Abschnitt `identityProviders` erhalten Sie von Ihrem OIDC-Identitätsanbieter. Werte werden nur für die `name`-, `type`-, `issuerUrl`- und `clientId`-Einstellungen unter `identityProviders` benötigt.

```
---
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: your-region-code
```

```
identityProviders:
  - name: my-provider
    type: oidc
    issuerUrl: https://example.com
    clientId: kubernetes
    usernameClaim: email
    usernamePrefix: my-username-prefix
    groupsClaim: my-claim
    groupsPrefix: my-groups-prefix
    requiredClaims:
      string: string
    tags:
      env: dev
```

Important

Geben Sie `system:` nicht oder einen Teil dieser Zeichenfolge für `groupsPrefix` oder `an.usernamePrefix`

2. Erstellen Sie den Anbieter.

```
eksctl associate identityprovider -f associate-identity-provider.yaml
```

3. Informationen `kubectl` zur Verwendung mit Ihrem Cluster und Ihrem OIDC-Identitätsanbieter finden Sie unter [Using kubectl in der Kubernetes-Dokumentation](#).

Ordnen Sie mithilfe der Konsole einen Identitätsanbieter zu AWS

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie Ihren Cluster und dann die Registerkarte Zugriff aus.
3. Wählen Sie im Abschnitt OIDC Identity Provider* Associate Identity Provider* aus.
4. Geben Sie auf der Seite OIDC-Identitätsanbieter zuordnen die folgenden Optionen ein oder wählen Sie sie aus, und wählen Sie dann Zuordnen aus.
 - Geben Sie für Name einen eindeutigen Namen für den Anbieter ein.
 - Geben Sie für Aussteller-URL die URL Ihres Anbieters ein. Diese URL muss über das Internet zugänglich sein.
 - Geben Sie als Client-ID die Client-ID des OIDC-Identitätsanbieters (auch bekannt als Audience) ein.

- Geben Sie für Benutzernamenanspruch den Anspruch ein, der als Benutzername verwendet werden soll.
- Geben Sie unter Gruppenanspruch den Anspruch ein, der als Benutzergruppe verwendet werden soll.
- (Optional) Wählen Sie Erweiterte Optionen, geben Sie die folgenden Informationen ein oder wählen Sie sie aus.
 - Benutzernamen-Präfix – Geben Sie ein Präfix ein, das den Benutzernamenansprüchen vorangestellt wird. Das Präfix wird den Benutzernamensansprüchen vorangestellt, um Konflikte mit bestehenden Namen zu vermeiden. Wenn Sie keinen Wert angeben und der Benutzername ein anderer Wert als `email` ist, wird als Präfix standardmäßig der Wert für die Aussteller-URL verwendet. Sie können den Wert `-` verwenden, um alle Präfixe zu deaktivieren. Geben Sie diese Zeichenfolge nicht `system:` oder nur einen Teil davon an.
 - Gruppen-Präfix – Geben Sie ein Präfix ein, um Gruppenansprüchen voranzustellen. Das Präfix wird Gruppenansprüchen vorangestellt, um Konflikte mit vorhandenen Namen (wie z. B. `system: groups`) zu vermeiden. Der Wert `oidc:` erstellt beispielsweise Gruppennamen wie `oidc:engineering` und `oidc:infra`. Geben Sie nicht `system:` oder nur einen Teil dieser Zeichenfolge an..
 - Erforderliche Ansprüche – Wählen Sie Anspruch hinzufügen aus, und geben Sie ein oder mehrere Schlüsselwertpaare ein, die erforderliche Ansprüche im Client-ID-Token beschreiben. Die Paare beschreiben die erforderlichen Ansprüche im ID-Token. Wenn festgelegt, wird überprüft, ob jeder Anspruch im ID-Token mit einem übereinstimmenden Wert vorhanden ist.
 - a. Informationen `kubectl` zur Verwendung mit Ihrem Cluster und Ihrem OIDC-Identitätsanbieter finden Sie unter [Using kubectl in der Kubernetes-Dokumentation](#).

Beispiel für eine IAM-Richtlinie

Wenn Sie verhindern möchten, dass ein OIDC-Identitätsanbieter mit einem Cluster verknüpft wird, erstellen Sie die folgende IAM-Richtlinie und verknüpfen Sie sie mit den IAM-Konten Ihrer Amazon-EKS-Administratoren. [Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien und Hinzufügen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch und unter Aktionen in der Referenz zur Serviceautorisierung.](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Sid": "denyOIDC",
        "Effect": "Deny",
        "Action": [
            "eks:AssociateIdentityProviderConfig"
        ],
        "Resource": "arn:aws: eks:us-west-2.amazonaws.com:111122223333:cluster/*"
    },
    {
        "Sid": "eksAdmin",
        "Effect": "Allow",
        "Action": [
            "eks:*"
        ],
        "Resource": "*"
    }
]
}

```

Die folgende Beispielrichtlinie lässt die Zuordnung von OIDC-Identitätsanbietern zu, wenn `clientID` `kubernetes` und `issuerUrl` [https://cognito-idp.us-west-2amazonaws.com/](https://cognito-idp.us-west-2.amazonaws.com/) ist.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCognitoOnly",
            "Effect": "Deny",
            "Action": "eks:AssociateIdentityProviderConfig",
            "Resource": "arn:aws: eks:us-west-2:111122223333:cluster/my-instance",
            "Condition": {
                "StringNotLikeIfExists": {
                    "eks:issuerUrl": "https://cognito-idp.us-west-2.amazonaws.com/*"
                }
            }
        },
        {
            "Sid": "DenyOtherClients",
            "Effect": "Deny",
            "Action": "eks:AssociateIdentityProviderConfig",
            "Resource": "arn:aws: eks:us-west-2:111122223333:cluster/my-instance",
            "Condition": {
                "StringNotEquals": {

```

```
        "eks:clientId": "kubernetes"
      }
    },
    {
      "Sid": "AllowOthers",
      "Effect": "Allow",
      "Action": "eks:*",
      "Resource": "*"
    }
  ]
}
```

Trennen Sie einen OIDC-Identitätsanbieter von Ihrem Cluster

Wenn Sie einen OIDC-Identitätsanbieter von Ihrem Cluster trennen, können Benutzer, die im Anbieter enthalten sind, nicht mehr auf den Cluster zugreifen. Sie können jedoch weiterhin mit [IAM-Prinzipalen](#) auf den Cluster zugreifen.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im Abschnitt OIDC-Identitätsanbieter die Option Zuordnung aufheben, geben Sie den Namen des Identitätsanbieters ein und wählen Sie dann Disassociate aus.

Sehen Sie sich die Kubernetes-Ressourcen an in der AWS Management Console

Mit der AWS Management Console können Sie die Kubernetes-Ressourcen anzeigen, die in Ihrem Cluster bereitgestellt sind. [Sie können Kubernetes-Ressourcen nicht mit der AWS CLI oder eksctl anzeigen. Um Kubernetes-Ressourcen mit einem Befehlszeilentool anzuzeigen, verwenden Sie kubectl.](#)

Note

Um die Registerkarte Ressourcen und den Abschnitt Knoten auf der Registerkarte Compute in der anzuzeigen AWS Management Console, muss der von Ihnen verwendete [IAM-Prinzipal über bestimmte IAM](#) - und Kubernetes-Berechtigungen verfügen. Weitere Informationen finden Sie unter [the section called "Erforderliche Berechtigungen"](#).

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie in der Liste Cluster den Cluster aus, der die Kubernetes-Ressourcen enthält, die Sie anzeigen möchten.
3. Wählen Sie die Registerkarte für Resources (Ressourcen).
4. Wählen Sie eine Resource type-Gruppe (Ressourcentyp) aus, für die Sie Ressourcen anzeigen möchten, z. B. Workloads. Ihnen wird eine Liste der Ressourcentypen in dieser Gruppe angezeigt.
5. Wählen Sie einen Ressourcentyp aus, z. B. Deployments (Bereitstellungen) in der Gruppe Workloads. Sie sehen eine Beschreibung des Ressourcentyps, einen Link zur Kubernetes-Dokumentation für weitere Informationen über den Ressourcentyp und eine Liste der Ressourcen dieses Typs, die in Ihrem Cluster bereitgestellt werden. Wenn die Liste leer ist, werden keine Ressourcen dieses Typs in Ihrem Cluster bereitgestellt.
6. Wählen Sie eine Ressource aus, um weitere Informationen dazu anzuzeigen. Probieren Sie die folgenden Beispiele aus:
 - Wählen Sie die Gruppe Workloads aus, dann den Ressourcentyp Deployments (Bereitstellungen) gefolgt von der Ressource coredns. Wenn Sie eine Ressource auswählen, befinden Sie sich standardmäßig in der strukturierten Ansicht. Für einige Ressourcentypen wird in der strukturierten Ansicht der Abschnitt Pods angezeigt. In diesem Abschnitt sind die Pods aufgeführt, die vom Workload verwaltet werden. Sie können einen beliebigen aufgelisteten Pod auswählen, um Informationen über den Pod anzuzeigen. Nicht für alle Ressourcentypen werden Informationen in der strukturierten Ansicht angezeigt. Wenn Sie die Ansicht Raw in der oberen rechten Ecke der Seite für die Ressource auswählen, sehen Sie die vollständige JSON-Antwort von der Kubernetes-API für die Ressource.
 - Wählen Sie die Cluster-Gruppe aus und dann den Ressourcentyp Nodes (Knoten). Eine Liste aller Knoten in Ihrem Cluster wird angezeigt. Die Knoten können von jedem [Amazon-EKS-Knoten-Typ](#) sein. Das ist die gleiche Liste, die Sie im Abschnitt Nodes (Knoten) sehen, wenn Sie die Registerkarte Compute (Datenverarbeitung) für Ihren Cluster auswählen. Wählen Sie eine Knotenressource aus der Liste aus. In der strukturierten Ansicht sehen Sie ebenfalls einen Abschnitt Pods. In diesem Abschnitt werden alle Pods angezeigt, die auf dem Knoten ausgeführt werden.

Erforderliche Berechtigungen

Um die Registerkarte Ressourcen und den Abschnitt Knoten auf der Registerkarte Compute in der anzeigen zu können AWS Management Console, muss der von Ihnen verwendete [IAM-Principal](#)

über bestimmte Mindestberechtigungen für IAM und Kubernetes verfügen. Führen Sie die folgenden Schritte aus, um Ihren IAM-Prinzipalen die erforderlichen Berechtigungen zuzuweisen.

1. Stellen Sie sicher, dass `eks:AccessKubernetesApi`, dass die und andere erforderliche IAM-Berechtigungen zum Anzeigen von Kubernetes-Ressourcen dem von Ihnen verwendeten IAM-Prinzipal zugewiesen sind. Weitere Informationen zum Bearbeiten von Berechtigungen für einen IAM-Prinzipal finden Sie unter [Zugriff für Prinzipale steuern](#) und im IAM-Benutzerhandbuch. Weitere Informationen zum Bearbeiten von Rollenberechtigungen finden Sie unter [Modifying a role permissions policy \(console\)](#) (Ändern einer Rollenberechtigungsrichtlinie (Konsole)) im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie umfasst die erforderlichen Berechtigungen für einen Prinzipal, um Kubernetes-Ressourcen für alle Cluster in Ihrem Konto anzuzeigen. Ersetzen Sie es **111122223333** durch Ihre AWS Konto-ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks:ListFargateProfiles",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
        "eks:ListUpdates",
        "eks:AccessKubernetesApi",
        "eks:ListAddons",
        "eks:DescribeCluster",
        "eks:DescribeAddonVersions",
        "eks:ListClusters",
        "eks:ListIdentityProviderConfigs",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ssm:GetParameter",
      "Resource": "arn:aws:ssm:*:111122223333:parameter/*"
    }
  ]
}
```



```
}
```

Um Knoten in [verbundenen Clustern](#) anzuzeigen, sollte die [IAM-Rolle des Amazon-EKS-Connectors](#) in der Lage sein, den Prinzipal im Cluster anzunehmen. Dadurch kann der [Amazon EKS-Connector](#) den Principal einem Kubernetes-Benutzer zuordnen.

2. Erstellen Sie ein Kubernetes `rolebinding` oder `clusterrolebinding`, das an ein Kubernetes `role` oder `clusterrole` gebunden ist, das über die erforderlichen Berechtigungen zum Anzeigen der Kubernetes-Ressourcen verfügt. Informationen zu Rollen und Rollenbindungen in Kubernetes finden Sie unter [Using RBAC Authorization](#) (Verwenden der RBAC-Autorisierung) in der Kubernetes-Dokumentation. Sie können eines der folgenden Manifeste auf Ihren Cluster anwenden, die eine `role` und eine `rolebinding` oder eine `clusterrole` und eine `clusterrolebinding` mit den erforderlichen Kubernetes-Berechtigungen erstellen:

Kubernetes-Ressourcen in allen Namespaces anzeigen

- Der Gruppenname in der Datei lautet `eks-console-dashboard-full-access-group`. Wenden Sie das Manifest mit dem folgenden Befehl auf Ihren Cluster an:

```
kubectl apply -f https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-full-access.yaml
```

Kubernetes-Ressourcen in einem bestimmten Namespace anzeigen

- Der Namespace in dieser Datei ist `default`. Der Gruppenname in der Datei lautet `eks-console-dashboard-restricted-access-group`. Wenden Sie das Manifest mit dem folgenden Befehl auf Ihren Cluster an:

```
kubectl apply -f https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-restricted-access.yaml
```

Wenn Sie den Namen, den Namespace, die Berechtigungen oder eine andere Konfiguration in der Datei der Kubernetes-Gruppe ändern müssen, laden Sie die Datei herunter und bearbeiten Sie sie, bevor Sie sie auf Ihren Cluster anwenden:

- a. Laden Sie die Datei mit einem der folgenden Befehle herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-full-access.yaml
```

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-restricted-access.yaml
```

- b. Bearbeiten Sie die Datei nach Bedarf.
- c. Wenden Sie das Manifest mit einem der folgenden Befehle auf Ihren Cluster an:

```
kubectl apply -f eks-console-full-access.yaml
```

```
kubectl apply -f eks-console-restricted-access.yaml
```

3. Ordnen Sie den [IAM-Prinzipal](#) dem Kubernetes-Benutzer oder der Kubernetes-Gruppe im zu. aws-auth ConfigMap Sie können ein Tool wie eksctl verwenden, um die ConfigMap zu aktualisieren, oder Sie können sie durch manuelle Bearbeitung aktualisieren.

Important

Wir empfehlen die Verwendung von eksctl oder einem anderen Tool, um die ConfigMap zu bearbeiten. Informationen zu anderen Tools, die Sie verwenden können, finden Sie unter [Use tools to make changes to the aws-auth ConfigMap](#) in den Amazon EKS-Best-Practices-Leitfäden. Ist aws-auth ConfigMap falsch formatiert, können Sie den Zugriff auf Ihren Cluster verlieren.

Mit eksctl bearbeiten

1. Sie benötigen eine Version 0.210.0 oder eine neuere Version des eksctl Befehlszeilentools, das auf Ihrem Gerät installiert ist oder. AWS CloudShell Informationen zum Installieren und Aktualisieren von eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).
2. Zeigen Sie die aktuellen Mappings in der ConfigMap an. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

Eine Beispielausgabe sieht wie folgt aus.

ARN	USERNAME	GROUPS
ACCOUNT		
arn:aws: iam::111122223333:role/eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA		system:node:{{EC2PrivateDNSName}}
		system:bootstrappers,system:nodes

3. Fügen Sie ein Mapping für eine Rolle hinzu. In diesem Beispiel wird davon ausgegangen, dass Sie die IAM-Berechtigungen im ersten Schritt einer Rolle namens *my-console-viewer-role* zuweisen. Ersetzen Sie **111122223333** durch Ihre Konto-ID.

```
eksctl create iamidentitymapping \
  --cluster my-cluster \
  --region=region-code \
  --arn arn:aws: iam::111122223333:role/my-console-viewer-role \
  --group eks-console-dashboard-full-access-group \
  --no-duplicate-arns
```

Important

Der Rollen-ARN darf keinen Pfad wie `enthaltenrole/my-team/developers/my-role`. Das Format des ARN muss `arn:aws: iam::111122223333:role/my-role` sein. In diesem Beispiel muss `my-team/developers/` entfernt werden.

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
2022-05-09 14:51:20 [#] adding identity "arn:aws: iam::111122223333:role/my-console-viewer-role" to auth ConfigMap
```

4. Fügen Sie ein Mapping für einen Benutzer hinzu. [Bewährte Methoden für IAM](#) empfehlen, dass Sie Rollen statt Benutzern Berechtigungen gewähren. In diesem Beispiel wird davon ausgegangen, dass Sie die IAM-Berechtigungen im ersten Schritt einem Benutzer *my-user* zuweisen. Ersetzen Sie **111122223333** durch Ihre Konto-ID.

```
eksctl create iamidentitymapping \
  --cluster my-cluster \
  --region=region-code \
```

```
--arn arn:aws: iam::111122223333:user/my-user \
--group eks-console-dashboard-restricted-access-group \
--no-duplicate-arns
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
2022-05-09 14:53:48 [#] adding identity "arn:aws: iam::111122223333:user/my-user" to
auth ConfigMap
```

5. Zeigen Sie wieder die Mappings in der ConfigMap an.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

Eine Beispielausgabe sieht wie folgt aus.

ARN	USERNAME	GROUPS
	ACCOUNT	
arn:aws: iam::111122223333:role/eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA	system:node:{{EC2PrivateDNSName}}	
arn:aws: iam::111122223333:role/my-console-viewer-role	system:bootstrappers,system:nodes	
		eks-console-dashboard-full-access-group
arn:aws: iam::111122223333:user/my-user		eks-console-dashboard-restricted-access-group

ConfigMap Manuell bearbeiten

Weitere Informationen zum Hinzufügen von Benutzern oder Rollen zur aws-auth ConfigMap finden Sie unter [the section called “Hinzufügen von IAM-Prinzipal zu Ihrem Amazon EKS-Cluster”](#).

1. Öffnen Sie die aws-auth ConfigMap zum Bearbeiten.

```
kubectl edit -n kube-system configmap/aws-auth
```

2. Fügen Sie die Zuordnungen zu den hinzu aws-authConfigMap, ersetzen Sie jedoch keine der vorhandenen Zuordnungen. Im folgenden Beispiel werden Zuordnungen zwischen [IAM-Prinzipalen](#)

mit im ersten Schritt hinzugefügten Berechtigungen und den im vorherigen Schritt erstellten Kubernetes-Gruppen hinzugefügt:

- Die *my-console-viewer-role*-Rolle und eks-console-dashboard-full-access-group.
- Der *my-user*-Benutzer und eks-console-dashboard-restricted-access-group.

In diesen Beispielen wird davon ausgegangen, dass Sie die IAM-Berechtigungen im ersten Schritt einer Rolle namens *my-console-viewer-role* und einem Benutzer namens *my-user* zuweisen. Ersetzen Sie es durch Ihre Konto-ID. **111122223333** AWS

```
apiVersion: v1
data:
mapRoles: |
  - groups:
    - eks-console-dashboard-full-access-group
    rolearn: arn:aws: iam::111122223333:role/my-console-viewer-role
    username: my-console-viewer-role
mapUsers: |
  - groups:
    - eks-console-dashboard-restricted-access-group
    userarn: arn:aws: iam::111122223333:user/my-user
    username: my-user
```

Important

Der Rollen-ARN darf keinen Pfad wie enthaltenrole/my-team/developers/my-console-viewer-role. Das Format des ARN muss arn:aws:iam::**111122223333**:role/*my-console-viewer-role* sein. In diesem Beispiel muss my-team/developers/ entfernt werden.

3. Speichern Sie die Datei und beenden Sie den Text-Editor.

Connect kubectl mit einem EKS-Cluster, indem Sie eine kubeconfig-Datei erstellen

In diesem Thema erstellen Sie eine kubeconfig-Datei für Ihren Cluster (oder aktualisieren eine vorhandene).

Das `kubectl`-Befehlszeilentool verwendet Konfigurationsinformationen in `kubeconfig`-Dateien für die Kommunikation mit dem API-Server eines Clusters. Weitere Informationen finden Sie unter [Organisieren des Clusterzugriffs mithilfe von kubeconfig-Dateien](#) in der Kubernetes-Dokumentation.

Amazon EKS verwendet den Befehl `aws eks get-token` mit `kubectl` für die Cluster-Authentifizierung. Standardmäßig verwendet die AWS CLI dieselben Anmeldeinformationen, die mit dem folgenden Befehl zurückgegeben werden:

```
aws sts get-caller-identity
```

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#).
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Ein IAM-Benutzer oder eine Rolle mit Berechtigung zur Verwendung der API-Aktion `eks:DescribeCluster` für den angegebenen Cluster. Weitere Informationen finden Sie unter [the section called “Identitätsbasierte Richtlinien”](#). Wenn Sie eine Identität Ihres eigenen OpenID Connect-Anbieters für den Zugriff auf Ihren Cluster verwenden, finden Sie weitere Informationen unter Using [kubectl in der Kubernetes-Dokumentation](#), um Ihre Datei zu erstellen oder zu aktualisieren. `kube config`

kubeconfig-Datei automatisch erstellen

- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit `aws configure`](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Berechtigung zur Nutzung der `eks:DescribeCluster`-API-Aktion für den Cluster, den Sie angeben. Weitere Informationen finden Sie unter [the section called “Identitätsbasierte Richtlinien”](#).
 1. Erstellen oder aktualisieren Sie eine kubeconfig-Datei für Ihren Cluster. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet, und *my-cluster* ersetzen Sie es durch den Namen Ihres Clusters.

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

Standardmäßig wird die resultierende Konfigurationsdatei im Standard kubeconfig-Pfad (`.kube`) in Ihrem Stammverzeichnis erstellt oder mit einer vorhandenen config-Datei an diesem Speicherort zusammengeführt. Sie können mit der Option `--kubeconfig` einen anderen Pfad angeben.

Sie können einen IAM-Rollen-ARN mit der Option `--role-arn` für die Authentifizierung verwenden, wenn Sie `kubectl`-Befehle ausgeben. Andernfalls wird der [IAM-Prinzipal](#) in Ihrer standardmäßigen AWS CLI- oder SDK-Anmeldeinformationskette verwendet. Sie können Ihre AWS Standard-CLI- oder SDK-Identität anzeigen, indem `aws sts get-caller-identity` Sie den Befehl ausführen.

Für alle verfügbaren Optionen führen Sie den `aws eks update-kubeconfig help` Befehl aus oder sehen Sie sich [update-kubeconfig](#) in der AWS CLI-Befehlsreferenz an.

2. Testen Sie Ihre Konfiguration.

```
kubectl get svc
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
svc/kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	1m

Wenn Sie Autorisierungs- oder Ressourcenfehler erhalten, finden Sie weitere Informationen unter [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#) im Thema zur Fehlerbehebung.

Kubernetes-Workloads Zugriff auf die AWS Nutzung von Kubernetes-Dienstkonten gewähren

A Kubernetes service account provides an identity for processes that run in a Pod. For more information see [Verwaltung von Dienstkonten](#) in the Kubernetes documentation. If your Pod needs access to AWS services, you can map the service account to an AWS Identity and Access Management identity to grant that access. For more information, see [the section called “Referenzen bei IRSA”](#) or [the section called “Pod-Identität”](#).

Servicekonto-Tokens

Die [BoundServiceAccountTokenVolume](#)Funktion ist in Kubernetes-Versionen standardmäßig aktiviert. Die Funktion verbessert die Sicherheit von Servicekonto-Tokens, indem sie es auf Kubernetes ausgeführten Workloads ermöglicht, JSON-Web-Tokens, die an Zielgruppen, Zeit und Schlüssel gebunden sind, anzufordern. Die Ablaufzeit für Servicekonto-Tokens beträgt eine Stunde. In früheren Kubernetes-Versionen hatten die Token kein Ablaufdatum. Clients, die diese Tokens verwenden, müssen die Tokens nun also innerhalb einer Stunde aktualisieren. Die folgenden [Kubernetes-Clients SDKs](#) aktualisieren die Token automatisch innerhalb des erforderlichen Zeitrahmens:

- Go-Version 0.15.7 und höher
- Python-Version 12.0.0 und höher
- Java-Version 9.0.0 und höher
- JavaScript Version 0.10.3 und später
- Ruby master-Branch
- Haskell-Version 0.3.0.0

- C#-Version 7.0.5 und höher

Wenn Ihre Workload eine frühere Client-Version verwendet, ist eine Aktualisierung erforderlich. Um eine reibungslose Migration von Clients zu den neueren zeitgebundenen Dienstkonto-Tokens zu ermöglichen, fügt Kubernetes dem Dienstkonto-Token eine verlängerte Ablaufzeit hinzu, die standardmäßig über eine Stunde liegt. Für Amazon-EKS-Cluster gilt eine verlängerte Ablaufzeit von 90 Tagen. Der Kubernetes-API-Server Ihres Amazon EKS-Clusters lehnt Anfragen mit Tokens ab, die älter als 90 Tage sind. Wir empfehlen Ihnen, Ihre Anwendungen und deren Abhängigkeiten zu überprüfen, um sicherzustellen, dass es sich bei den Kubernetes-Clients um dieselben oder eine neuere Version als die zuvor aufgeführten Versionen SDKs handelt.

Wenn der API-Server Anfragen mit Token erhält, die älter als eine Stunde sind, kommentiert er das Audit-Protokollereignis der API mit `annotations.authentication.k8s.io/stale-token`. Die Anmerkung sieht zum Beispiel wie folgt aus:

```
subject: system:serviceaccount:common:fluent-bit, seconds after warning threshold:
4185802.
```

Wenn für Ihren Cluster die [Steuerebenen-Protokollierung](#) aktiviert ist, dann befinden sich die Anmerkungen in den Überwachungsprotokollen. Sie können die folgende [CloudWatch Logs Insights-Abfrage](#) verwenden, um alle Pods in Ihrem Amazon EKS-Cluster zu identifizieren, die veraltete Token verwenden:

```
fields @timestamp
|filter @logStream like /kube-apiserver-audit/
|filter @message like /seconds after warning threshold/
|parse @message "subject: *, seconds after warning threshold:*\\"" as subject,
elapsedtime
```

Das `subject` bezieht sich auf das Dienstkonto, das der Pod verwendet hat. `elapsedtime` gibt die verstrichene Zeit (in Sekunden) nach dem Lesen des neuesten Tokens an. Die Anfragen an den API-Server werden abgelehnt, wenn `elapsedtime` 90 Tage (7 776 000 Sekunden) überschreitet. Sie sollten das Kubernetes-Client-SDK Ihrer Anwendungen proaktiv aktualisieren, sodass es eine der zuvor aufgeführten Versionen verwendet, die das Token automatisch aktualisieren. Wenn das verwendete Dienstkonto-Token fast 90 Tage dauert und Sie nicht genügend Zeit haben, um Ihre Client-SDK-Versionen vor Ablauf des Tokens zu aktualisieren, können Sie bestehende Pods beenden und neue erstellen. Dies führt dazu, dass das Dienstkonto-Tokens erneut abgerufen wird, sodass Sie weitere 90 Tage Zeit haben, um Ihre Client-Version zu aktualisieren. SDKs

Wenn der Pod Teil einer Bereitstellung ist, wird empfohlen, Pods zu beenden und gleichzeitig die hohe Verfügbarkeit aufrechtzuerhalten, indem Sie einen Rollout mit dem folgenden Befehl durchführen. Ersetzen Sie *my-deployment* mit dem Namen Ihrer Bereitstellung.

```
kubectl rollout restart deployment/my-deployment
```

Cluster-Add-ons

Die folgenden Cluster-Add-Ons wurden aktualisiert und verwenden nun den Kubernetes-Client SDKs, der Dienstkonto-Tokens automatisch erneut abrufen. Wir empfehlen Ihnen, sicherzustellen, dass die aufgeführten Versionen oder neuere Versionen auf Ihrem Cluster installiert sind.

- Version 1.8.0 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes und Metrik-Hilfs-Plugins. 1.8.0
Zum Überprüfen oder Aktualisieren Ihrer aktuellen Version siehe [the section called “Amazon VPC CNI”](#) und [cni-metrics-helper](#).
- CoreDNS-Version 1.8.4 und höher. Zum Überprüfen oder Aktualisieren Ihrer aktuellen Version siehe [the section called “CoreDNS”](#).
- AWS Load Balancer Controller-Version 2.0.0 und höher. Zum Überprüfen oder Aktualisieren Ihrer aktuellen Version siehe [the section called “AWS Load Balancer Controller”](#).
- Eine aktuelle kube-proxy-Version. Zum Überprüfen oder Aktualisieren Ihrer aktuellen Version siehe [the section called “kube-proxy”](#).
- AWS für Fluent Bit-Version 2.25.0 oder höher. Informationen zum Aktualisieren Ihrer aktuellen Version finden Sie unter [Veröffentlichungen](#) am GitHub.
- Fluentd-Imageversion [1.14.6-1.2](#) oder höher und Fluentd-Filter-Plugin für Kubernetes-Metadatenversion [2.11.1](#) oder höher.

Erteilen von AWS Identity and Access Management

Zugriffsverwaltungsberechtigungen für Workloads auf Amazon Elastic Kubernetes Service Clustern

Amazon EKS bietet zwei Möglichkeiten, AWS Identity and Access Management Zugriffsverwaltungsberechtigungen für Workloads zu gewähren, die in Amazon EKS-Clustern ausgeführt werden: IAM-Rollen für Dienstkonten und EKS-Pod-Identitäten.

IAM-Rollen für Servicekonten

IAM-Rollen für Dienstkonten (IRSA) konfiguriert Kubernetes-Anwendungen, auf denen sie ausgeführt werden, AWS mit detaillierten IAM-Berechtigungen für den Zugriff auf verschiedene andere AWS Ressourcen wie Amazon S3 S3-Buckets, Amazon DynamoDB-Tabellen und mehr. Sie können mehrere Anwendungen zusammen in demselben Amazon EKS-Cluster ausführen und sicherstellen, dass jede Anwendung nur über die erforderlichen Mindestberechtigungen verfügt. IRSA wurde entwickelt, um verschiedene Kubernetes-Bereitstellungsoptionen zu unterstützen, die von AWS Amazon EKS, Amazon EKS Anywhere, Red Hat OpenShift Service on und selbstverwaltete Kubernetes-Cluster auf AWS Amazon-Instances unterstützt werden. EC2 Daher wurde IRSA mithilfe grundlegender AWS Dienste wie IAM erstellt und war nicht direkt vom Amazon EKS-Service und der EKS-API abhängig. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#).

EKS-Pod-Identitäten

EKS Pod Identity bietet Clusteradministratoren einen vereinfachten Arbeitsablauf für die Authentifizierung von Anwendungen für den Zugriff auf verschiedene andere AWS Ressourcen wie Amazon S3 S3-Buckets, Amazon DynamoDB-Tabellen und mehr. EKS Pod Identity ist nur für EKS vorgesehen und vereinfacht Cluster-Administratoren so die Konfiguration von Kubernetes-Anwendungen, um IAM-Berechtigungen zu erhalten. Diese Berechtigungen können jetzt einfach mit weniger Schritten direkt über AWS Management Console die EKS-API und die AWS CLI konfiguriert werden, und es müssen keine Maßnahmen innerhalb des Clusters in Kubernetes-Objekten ergriffen werden. Clusteradministratoren müssen nicht zwischen den EKS- und IAM-Diensten wechseln oder privilegierte IAM-Operationen verwenden, um die für Ihre Anwendungen erforderlichen Berechtigungen zu konfigurieren. IAM-Rollen können jetzt in mehreren Clustern verwendet werden, ohne dass bei der Erstellung neuer Cluster die Rollenvertrauensrichtlinie aktualisiert werden muss. Die von EKS Pod Identity bereitgestellten IAM-Anmeldeinformationen umfassen Rollensitzungs-Tags mit Attributen wie Cluster-Name, Namespace und dem Namen des Servicekontos. Mithilfe von Rollensitzungs-Tags können Administratoren eine einzelne Rolle erstellen, die für alle Dienstkonten verwendet werden kann, indem sie den Zugriff auf AWS Ressourcen auf der Grundlage übereinstimmender Tags ermöglicht. Weitere Informationen finden Sie unter [the section called “Pod-Identität”](#).

Vergleich von EKS Pod Identity und IRSA

Ganz allgemein ermöglichen es Ihnen sowohl EKS Pod Identity als auch IRSA, Anwendungen, die auf Kubernetes-Clustern ausgeführt werden, IAM-Berechtigungen zu gewähren. Sie unterscheiden

sich jedoch grundlegend in ihrer Konfiguration, den unterstützten Grenzwerten und den aktivierten Features. Im Folgenden vergleichen wir einige der wichtigsten Aspekte beider Lösungen.

Attribut	EKS Pod Identity	IRSA
Erweiterbarkeit von Rollen	Sie müssen jede Rolle einmal einrichten, um das Vertrauen des neu eingeführten Amazon EKS-Service-Prinzipal zu erhalten <code> pods . eks . amazonaws . com </code> . Nach diesem einmaligen Schritt müssen Sie die Vertrauensrichtlinie der Rolle nicht jedes Mal aktualisieren, wenn sie in einem neuen Cluster verwendet wird.	Sie müssen die Vertrauensrichtlinie der IAM-Rolle jedes Mal mit dem neuen EKS-Cluster-OIDC-Provider-Endpunkt aktualisieren, wenn Sie die Rolle in einem neuen Cluster verwenden möchten.
Skalierbarkeit von Clustern	Bei EKS Pod Identity müssen Benutzer den IAM-OIDC-Anbieter nicht einrichten, sodass dieses Limit nicht gilt.	Jedem EKS-Cluster ist eine OpenID Connect (OIDC) - Emittenten-URL zugeordnet. Um IRSA verwenden zu können, muss für jeden EKS-Cluster in IAM ein eindeutiger OpenID Connect-Anbieter erstellt werden. IAM hat ein globales Standardlimit von 100 OIDC-Anbietern für jedes Konto. AWS Wenn Sie planen, mehr als 100 EKS-Cluster für jedes AWS Konto bei IRSA einzurichten, erreichen Sie das IAM-OIDC-Anbieterlimit.
Skalierbarkeit von Rollen	Bei EKS Pod Identity müssen Benutzer in der Vertrauensrichtlinie keine Vertrauens	In IRSA definieren Sie die Vertrauensbeziehung zwischen einer IAM-Rolle

Attribut	EKS Pod Identity	IRSA
	sbeziehung zwischen der IAM-Rolle und dem Dienstkonto definieren, sodass dieses Limit nicht gilt.	und einem Dienstkonto in der Vertrauensrichtlinie der Rolle. Standardmäßig beträgt die Größe der Vertrauensrichtlinie 2048. Das bedeutet, dass Sie in der Regel vier Vertrauensbeziehungen in einer Vertrauensrichtlinie definieren können. Sie können zwar das Limit für die maximale Größe der Vertrauensrichtlinie erhöhen, sind jedoch in der Regel auf maximal acht Vertrauensbeziehungen innerhalb einer Vertrauensrichtlinie beschränkt.

Attribut	EKS Pod Identity	IRSA
Wiederverwendbarkeit von Rollen	AWS Zu den temporären STS-Anmeldeinformationen, die von EKS Pod Identity bereitgestellt werden, gehören Rollensitzungs-Tags wie Clustername, Namespace und Dienstkontoname. Mithilfe von Rollensitzungs-Tags können Administratoren eine einzelne IAM-Rolle erstellen, die mit mehreren Dienstkonten mit unterschiedlichen effektiven Berechtigungen verwendet werden kann, indem sie den Zugriff auf AWS Ressourcen auf der Grundlage der ihnen zugewiesenen Tags ermöglichen. Dies wird auch als attributbasierte Zugriffskontrolle (ABAC) bezeichnet. Weitere Informationen finden Sie unter the section called “Gewähren Sie Pods Zugriff”.	AWS STS-Sitzungs-Tags werden nicht unterstützt. Sie können eine Rolle in verschiedenen Clustern wiederverwenden, aber jeder Pod erhält alle Berechtigungen der Rolle.
Unterstützte Umgebungen	EKS Pod Identity ist nur in Amazon EKS verfügbar.	IRSA kann wie Amazon EKS, Amazon EKS Anywhere, Red Hat OpenShift Service on und selbstverwaltete Kubernetes-Cluster auf AWS Amazon-Instances verwendet werden. EC2

Attribut	EKS Pod Identity	IRSA
Unterstützte EKS-Versionen	Alle unterstützten EKS-Cluster-Versionen. Informationen über die jeweiligen Plattformversionen finden Sie unter the section called “Cluster-Versionen von EKS Pod Identity” .	Alle unterstützten EKS-Cluster-Versionen.

IAM-Rollen für Servicekonten

Anwendungen in den Containern eines Pods können ein AWS SDK oder die AWS CLI verwenden, um API-Anfragen an AWS Dienste mithilfe von AWS Identity and Access Management (IAM) -Berechtigungen zu stellen. Anwendungen müssen ihre AWS API-Anfragen mit AWS Anmeldeinformationen signieren. IAM-Rollen für Servicekonten (IRSA) bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie EC2 Amazon-Instance-Profile Anmeldeinformationen für Amazon-Instances bereitstellen. EC2 Anstatt Ihre AWS Anmeldeinformationen zu erstellen und an die Container zu verteilen oder die Rolle der EC2 Amazon-Instance zu verwenden, verknüpfen Sie eine IAM-Rolle mit einem Kubernetes-Dienstkonto und konfigurieren Ihre Pods so, dass sie das Dienstkonto verwenden. Sie können IAM-Rollen nicht für Dienstkonten mit [lokalen Clustern für Amazon EKS auf AWS Outposts](#) verwenden.

IAM-Rollen für Servicekonten bietet die folgenden Vorteile:

- Geringste Rechte — Sie können IAM-Berechtigungen auf ein Dienstkonto beschränken, und nur Pods, die dieses Dienstkonto verwenden, haben Zugriff auf diese Berechtigungen. Mit diesem Feature entfällt auch die Notwendigkeit von Drittanbieterlösungen wie kiam oder kube2iam.
- Isolierung von Anmeldeinformationen — Wenn der Zugriff auf den [Amazon EC2 Instance Metadata Service \(IMDS\)](#) eingeschränkt ist, können die Container eines Pods nur Anmeldeinformationen für die IAM-Rolle abrufen, die dem Dienstkonto zugeordnet ist, das der Container verwendet. Ein Container hat niemals Zugriff auf Anmeldeinformationen, die von anderen Containern in anderen Pods verwendet werden. Wenn IMDS nicht eingeschränkt ist, haben die Container des Pods auch Zugriff auf die [IAM-Rolle des Amazon EKS-Knotens](#), und die Container können möglicherweise auf Anmeldeinformationen von IAM-Rollen anderer Pods auf demselben Knoten zugreifen. Weitere

Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

 Note

Pods, `hostNetwork: true` die mit konfiguriert sind, haben immer IMDS-Zugriff, aber die AWS SDKs AND-CLI verwendet IRSA-Anmeldeinformationen, wenn sie aktiviert sind.

- Überprüfbarkeit — Zugriffs- und Ereignisprotokollierung sind über verfügbar, um eine nachträgliche Prüfung AWS CloudTrail zu gewährleisten.

 Important

Container stellen keine Sicherheitsgrenze dar, und die Verwendung von IAM-Rollen für Dienstkonten ändert daran nichts. Pods, die demselben Knoten zugewiesen sind, teilen sich je nach Ihrer Pod-Konfiguration einen Kernel und möglicherweise weitere Ressourcen. Pods, die auf separaten Knoten laufen, werden zwar auf der Rechenebene isoliert, es gibt jedoch Knotenanwendungen, die über zusätzliche Berechtigungen in der Kubernetes-API verfügen, die über den Rahmen einer einzelnen Instanz hinausgehen. Einige Beispiele sind `kubelet` CSI-Speichertreiber oder Ihre eigenen Kubernetes-Anwendungen. `kube-proxy`

Aktivieren Sie IAM-Rollen für Servicekonten, indem Sie die folgenden Verfahren ausführen:

1. [Erstellen Sie einen IAM-OIDC-Anbieter für Ihren Cluster](#) — Sie führen dieses Verfahren für jeden Cluster nur einmal durch.

 Note

Wenn Sie den EKS-VPC-Endpoint aktiviert haben, konnte von dieser VPC aus nicht auf den EKS-OIDC-Dienstendpunkt zugegriffen werden. Folglich funktionieren Ihre Operationen wie das Erstellen eines OIDC-Anbieters mit `eksctl` in der VPC nicht und führen zu einem Timeout, wenn Sie versuchen, <https://oidc.eks.region.amazonaws.com> anzufordern. Es folgt ein Beispiel für eine Fehlermeldung:


```
server cant find oidc.eks.region.amazonaws.com: NXDOMAIN
```

Um diesen Schritt abzuschließen, können Sie den Befehl außerhalb der VPC ausführen, z. B. in AWS CloudShell oder auf einem Computer, der mit dem Internet verbunden ist. Alternativ können Sie in der VPC einen bedingten Split-Horizon-Resolver erstellen, z. B. den Route 53-Resolver, um einen anderen Resolver für die OIDC-Aussteller-URL zu verwenden und nicht das VPC-DNS dafür zu verwenden. Ein Beispiel für bedingte Weiterleitung in CoreDNS finden Sie in der [Amazon EKS-Funktionsanfrage](#) unter. GitHub

2. [Weisen Sie Kubernetes-Servicekonten IAM-Rollen zu](#) — Führen Sie dieses Verfahren für jeden eindeutigen Satz von Berechtigungen aus, über den eine Anwendung verfügen soll.
3. [Pods so konfigurieren, dass sie ein Kubernetes-Dienstkonto verwenden](#) — Führen Sie dieses Verfahren für jeden Pod durch, der Zugriff auf Dienste benötigt. AWS
4. [IRSA mit dem AWS SDK verwenden](#) — Vergewissern Sie sich, dass der Workload ein AWS SDK einer unterstützten Version verwendet und dass der Workload die standardmäßige Anmeldeinformationskette verwendet.

Hintergrundinformationen zu IAM, Kubernetes und OpenID Connect (OIDC)

2014 fügte AWS Identity and Access Management die Unterstützung für föderierte Identitäten mithilfe von OpenID Connect (OIDC) hinzu. Mit dieser Funktion können Sie AWS API-Aufrufe bei unterstützten Identitätsanbietern authentifizieren und ein gültiges OIDC-JSON-Webtoken (JWT) erhalten. Sie können dieses Token an den AWS AssumeRoleWithWebIdentity STS-API-Vorgang übergeben und temporäre IAM-Rollenanmeldedaten erhalten. Sie können diese Anmeldeinformationen verwenden, um mit jedem AWS Service zu interagieren, einschließlich Amazon S3 und DynamoDB.

Jedes JWT-Token ist mit einem Signaturschlüsselpaar signiert. Die Schlüssel werden für den von Amazon EKS verwalteten OIDC-Anbieter bereitgestellt und der private Schlüssel wechselt alle 7 Tage. Amazon EKS bewahrt die öffentlichen Schlüssel auf, bis sie ablaufen. Wenn Sie externe OIDC-Clients verbinden, beachten Sie, dass Sie die Signaturschlüssel aktualisieren müssen, bevor der öffentliche Schlüssel abläuft. Erfahren Sie, wie Sie [Signaturschlüssel abrufen, um OIDC-Token zu validieren](#).

Kubernetes verwendet seit langem Servicekonten als eigenes internes Identitätssystem. Pods können sich beim Kubernetes-API-Server mithilfe eines automatisch gemounteten Tokens

(ein Nicht-OIDC-JWT) authentifizieren, das nur der Kubernetes-API-Server validieren kann. Diese alten Dienstkonto-Tokens laufen nicht ab, und die Rotation des Signaturschlüssels ist ein schwieriger Prozess. In der Kubernetes-Version 1.12 wurde Unterstützung für eine neue `ProjectedServiceAccountToken` Funktion hinzugefügt. Bei dieser Funktion handelt es sich um ein OIDC-JSON-Webtoken, das auch die Identität des Dienstkontos enthält und eine konfigurierbare Zielgruppe unterstützt.

Amazon EKS hostet für jeden Cluster einen öffentlichen OIDC-Erkennungsendpunkt, der die Signaturschlüssel für die `ProjectedServiceAccountToken` JSON-Webtoken enthält, sodass externe Systeme wie IAM die von Kubernetes ausgegebenen OIDC-Token validieren und akzeptieren können.

Erstellen Sie einen IAM-OIDC-Anbieter für Ihren Cluster

Ihrem Cluster ist eine [OpenID Connect](#) (OIDC) -Emittenten-URL zugeordnet. Um AWS Identity and Access Management (IAM) -Rollen für Dienstkonten verwenden zu können, muss ein IAM-OIDC-Anbieter für die OIDC-Aussteller-URL Ihres Clusters vorhanden sein.

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#).
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit `aws configure`](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie `kubectl` und `eksctl` ein”](#).

- Eine vorhandene `kubectl` config-Datei, die Ihre Clusterkonfiguration enthält. Informationen zum Erstellen einer `kubectl` config-Datei finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).

Sie können einen IAM-OIDC-Anbieter für Ihren Cluster mithilfe von oder erstellen. `eksctl` AWS Management Console

Erstellen Sie einen OIDC-Anbieter (`eksctl`)

1. Version `0.210.0` oder höher des `eksctl`-Befehlszeilen-Tools, das auf Ihrem Computer oder in der AWS CloudShell installiert ist. Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).
2. Ermitteln Sie die OIDC-Aussteller-ID für Ihren Cluster.

Rufen Sie die OIDC-Aussteller-ID Ihres Clusters ab und speichern Sie sie in einer Variablen. Ersetzen Sie `<my-cluster>` durch Ihren eigenen Wert.

```
cluster_name=<my-cluster>
oidc_id=$(aws eks describe-cluster --name $cluster_name --query
  "cluster.identity.oidc.issuer" --output text | cut -d '/' -f 5)
echo $oidc_id
```

3. Stellen Sie fest, ob ein IAM-OIDC-Anbieter mit der Aussteller-ID Ihres Clusters bereits in Ihrem Konto vorhanden ist.

```
aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4
```

Wenn die Ausgabe zurückgegeben wird, haben Sie bereits einen IAM-OIDC-Anbieter für Ihren Cluster und können den nächsten Schritt überspringen. Wenn keine Ausgabe erfolgt, müssen Sie einen IAM-OIDC-Anbieter für Ihr Cluster erstellen.

4. Erstellen Sie einen IAM-OIDC-Identitätsanbieter für Ihren Cluster mit dem folgenden Befehl.

```
eksctl utils associate-iam-oidc-provider --cluster $cluster_name --approve
```

Note

Wenn Sie den EKS-VPC-Endpunkt aktiviert haben, konnte von dieser VPC aus nicht auf den EKS-OIDC-Dienstendpunkt zugegriffen werden. Folglich funktionieren Ihre

Operationen wie das Erstellen eines OIDC-Anbieters `eksctl` in der VPC nicht und führen zu einem Timeout. Es folgt ein Beispiel für eine Fehlermeldung:

```
** server cant find oidc.eks.<region-code>.amazonaws.com: NXDOMAIN
```

Um diesen Schritt abzuschließen, können Sie den Befehl außerhalb der VPC ausführen, z. B. in AWS CloudShell oder auf einem Computer, der mit dem Internet verbunden ist. Alternativ können Sie in der VPC einen bedingten Split-Horizon-Resolver erstellen, z. B. den Route 53-Resolver, um einen anderen Resolver für die OIDC-Aussteller-URL zu verwenden und nicht das VPC-DNS dafür zu verwenden. Ein Beispiel für bedingte Weiterleitung in CoreDNS finden Sie in der [Amazon EKS-Funktionsanfrage](#) unter. GitHub

OIDC-Anbieter erstellen (Konsole)AWS

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Bereich Cluster aus und wählen Sie dann den Namen Ihres Clusters auf der Seite Cluster.
3. Notieren Sie im Abschnitt Details der Registerkarte Overview (Übersicht) den Wert der OpenID-Connect-Provider-URL.
4. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
5. Wählen Sie im linken Navigationsbereich Identity Providers (Identitätsanbieter) unter Access management (Zugriffsverwaltung) aus. Wenn ein Anbieter aufgeführt ist, der mit der URL für Ihren Cluster übereinstimmt, haben Sie bereits einen Anbieter für Ihren Cluster. Wenn kein Anbieter aufgeführt ist, der der URL für Ihren Cluster entspricht, müssen Sie einen erstellen.
6. Um einen Anbieter zu erstellen, wählen Sie Add provider (Anbieter hinzufügen) aus.
7. Wählen Sie als Anbietertyp OpenID Connect aus.
8. Geben Sie unter Provider-URL die OIDC-Provider-URL für Ihren Cluster ein.
9. Geben Sie für Audience den Wert ein. `sts.amazonaws.com`
- 10.(Optional) Fügen Sie beliebige Tags hinzu, z. B. ein Tag, um zu identifizieren, welcher Cluster für diesen Anbieter bestimmt ist.
- 11.Wählen Sie Add provider (Anbieter hinzufügen) aus.

Nächster Schritt: [the section called "Weisen Sie eine IAM-Rolle zu"](#)

Zuweisen von IAM-Rollen zu Kubernetes-Dienstkonten

In diesem Thema wird beschrieben, wie Sie ein Kubernetes-Dienstkonto so konfigurieren, dass es eine AWS Identity and Access Management (IAM) -Rolle übernimmt. Alle Pods, die für die Verwendung des Dienstkontos konfiguriert sind, können dann auf jeden AWS Dienst zugreifen, für den die Rolle Zugriffsberechtigungen besitzt.

Voraussetzungen

- Einen vorhandenen -Cluster. Wenn Sie noch keinen haben, können Sie einen erstellen, indem Sie einer der Anleitungen unter folgen [Erste Schritte](#).
- Ein vorhandener Anbieter für IAM OpenID Connect (OIDC) für Ihren Cluster. Informationen zum Feststellen, ob Sie bereits einen haben oder wie Sie einen erstellen können, finden Sie unter [the section called “IAM OIDC-Anbieter”](#).
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie yumapt-get, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Das kubectl-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie kubectl-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von kubectl finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Eine vorhandene kubectl config-Datei, die Ihre Clusterkonfiguration enthält. Informationen zum Erstellen einer kubectl config-Datei finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).

Schritt 1: IAM-Richtlinie erstellen

Wenn Sie Ihrer IAM-Rolle eine vorhandene IAM-Richtlinie zuordnen möchten, fahren Sie mit dem nächsten Schritt fort.

1. Erstellen Sie eine IAM-Richtlinie. Sie können Ihre eigene Richtlinie erstellen oder eine AWS verwaltete Richtlinie kopieren, die bereits einige der benötigten Berechtigungen gewährt, und sie an Ihre spezifischen Anforderungen anpassen. Weitere Informationen finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.
2. Erstellen Sie eine Datei, die die Berechtigungen für die AWS Dienste enthält, auf die Ihre Pods zugreifen sollen. Eine Liste aller Aktionen für alle AWS Dienste finden Sie in der [Referenz zur Dienstautorisierung](#).

Sie können den folgenden Befehl ausführen, um eine Beispiel-Richtliniendatei zu erstellen, die schreibgeschützten Zugriff auf einen Amazon-S3-Bucket gewährt. Sie können optional Konfigurationsinformationen oder ein Bootstrap-Skript in diesem Bucket speichern, und die Container in Ihrem Pod können die Datei aus dem Bucket lesen und in Ihre Anwendung laden. Wenn Sie diese Beispielrichtlinie erstellen möchten, kopieren Sie den folgenden Inhalt auf Ihr Gerät. *my-pod-secrets-bucket* Ersetzen Sie es durch Ihren Bucket-Namen und führen Sie den Befehl aus.

```
cat >my-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws: s3::my-pod-secrets-bucket"
    }
  ]
}
EOF
```

3. Erstellen Sie die IAM-Richtlinie.

```
aws iam create-policy --policy-name my-policy --policy-document file://my-policy.json
```

Schritt 2: IAM-Rolle erstellen und zuordnen

Erstellen Sie eine IAM-Rolle und verknüpfen Sie sie mit einem Kubernetes-Dienstkonto. Sie können entweder `eksctl` oder die AWS CLI verwenden.

Rolle erstellen und zuordnen (`eksctl`)

Dieser `eksctl` Befehl erstellt ein Kubernetes-Dienstkonto im angegebenen Namespace, erstellt eine IAM-Rolle (falls sie nicht existiert) mit dem angegebenen Namen, fügt der Rolle einen vorhandenen IAM-Richtlinien-ARN hinzu und annotiert das Dienstkonto mit dem IAM-Rollen-ARN. Achten Sie darauf, die Beispiel-Platzhalterwerte in diesem Befehl durch Ihre spezifischen Werte zu ersetzen. Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).

```
eksctl create iamserviceaccount --name my-service-account --namespace default --cluster my-cluster --role-name my-role \
    --attach-policy-arn arn:aws:iam::111122223333:policy/my-policy --approve
```

Important

Wenn die Rolle oder das Servicekonto bereits vorhanden ist, schlägt der vorherige Befehl möglicherweise fehl. `eksctl` hat verschiedene Optionen, die Sie in diesen Situationen angeben können. Führen Sie `eksctl create iamserviceaccount --help` aus, um weitere Informationen zu erhalten.

Rolle erstellen und zuordnen (AWS CLI)

Wenn Sie bereits ein Kubernetes-Dienstkonto haben, dem Sie eine IAM-Rolle zuweisen möchten, können Sie diesen Schritt überspringen.

1. Erstellen Sie ein Kubernetes-Servicekonto. Kopieren Sie den folgenden Inhalt auf Ihr Gerät.
my-service-account Ersetzen Sie es durch Ihren gewünschten Namen und gegebenenfalls *default* durch einen anderen Namespace. Wenn Sie eine Änderung vornehmend *default*, muss der Namespace bereits existieren.

```
cat >my-service-account.yaml <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
```

```
name: my-service-account
namespace: default
EOF
kubectl apply -f my-service-account.yaml
```

2. Setzen Sie Ihre AWS Konto-ID mit dem folgenden Befehl auf eine Umgebungsvariable.

```
account_id=$(aws sts get-caller-identity --query "Account" --output text)
```

3. Stellen Sie den OIDC-Identitätsanbieter Ihres Clusters mit dem folgenden Befehl auf eine Umgebungsvariable ein. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
oidc_provider=$(aws eks describe-cluster --name my-cluster --region $AWS_REGION --
query "cluster.identity.oidc.issuer" --output text | sed -e "s/^https:\\/\\/\\/" )
```

4. Legen Sie Variablen für den Namespace und den Namen des Servicekontos fest. *my-service-account* Ersetzen Sie es durch das Kubernetes-Dienstkonto, das Sie die Rolle übernehmen möchten. Ersetzen Sie es *default* durch den Namespace des Dienstkontos.

```
export namespace=default
export service_account=my-service-account
```

5. Führen Sie den folgenden Befehl aus, um eine Vertrauensrichtlinie für die IAM-Rolle zu erstellen. Wenn Sie allen Servicekonten innerhalb eines Namespaces die Verwendung der Rolle erlauben möchten, kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetze *StringEquals* durch *StringLike* und ersetze *\$service_account* durch *. Sie können mehrere Einträge in den Bedingungen *StringEquals* und *StringLike* unten hinzufügen, um mehreren Servicekonten oder Namespaces das Annehmen der Rolle zu erlauben. Weitere Informationen dazu, wie Sie zulassen können, dass Rollen von einem anderen AWS Konto als dem Konto, in dem sich Ihr Cluster befindet, diese Rolle übernehmen können, finden Sie unter [the section called "Kontoübergreifendes IAM"](#).

```
cat >trust-relationship.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::$account_id:oidc-provider/$oidc_provider"
      },
    },
  ],
}
```



```

    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "$oidc_provider:aud": "sts.amazonaws.com",
        "$oidc_provider:sub": "system:serviceaccount:$namespace:$service_account"
      }
    }
  }
]
}
EOF

```

6. Erstellen Sie die -Rolle. Ersetzen Sie *my-role* durch einen Namen für Ihre IAM-Rolle und *my-role-description* durch eine Beschreibung für Ihre Rolle.

```
aws iam create-role --role-name my-role --assume-role-policy-document file://trust-relationship.json --description "my-role-description"
```

7. Hängen Sie eine IAM-Richtlinie an Ihre Rolle an. Ersetzen Sie *my-role* durch den Namen Ihrer IAM-Rolle und *my-policy* durch den Namen einer vorhandenen Richtlinie, die Sie erstellt haben.

```
aws iam attach-role-policy --role-name my-role --policy-arn=arn:aws:iam::
$account_id:policy/my-policy
```

8. Annotieren Sie Ihr Servicekonto mit dem Amazon-Ressourcennamen (ARN) der IAM-Rolle, die das Servicekonto annehmen soll. Ersetzen Sie *my-role* durch den Namen Ihrer bestehenden IAM-Rolle. Angenommen, Sie haben in einem vorherigen Schritt zugelassen, dass eine Rolle von einem anderen AWS Konto als dem Konto, in dem sich Ihr Cluster befindet, diese Rolle übernimmt. Stellen Sie dann sicher, dass Sie das AWS Konto und die Rolle des anderen Kontos angeben. Weitere Informationen finden Sie unter [the section called "Kontoübergreifendes IAM"](#).

```
kubectl annotate serviceaccount -n $namespace $service_account eks.amazonaws.com/
role-arn=arn:aws:iam::$account_id:role/my-role
```

9. (Optional) [Konfigurieren Sie den AWS Security Token Service-Endpunkt für ein Dienstkonto](#). AWS empfiehlt die Verwendung eines regionalen AWS STS-Endpunkts anstelle des globalen Endpunkts. Dies reduziert die Latenz, bietet integrierte Redundanz und erhöht die Gültigkeit der Sitzungstoken.

Schritt 3: Konfiguration bestätigen

1. Vergewissern Sie sich, dass die Vertrauensrichtlinie der IAM-Rolle korrekt konfiguriert ist.

```
aws iam get-role --role-name my-role --query Role.AssumeRolePolicyDocument
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:default:my-service-account",
          "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
        }
      }
    }
  ]
}
```

2. Stellen Sie sicher, dass die Richtlinie, die Sie in einem vorherigen Schritt an Ihre Rolle angehängt haben, an die Rolle angehängt ist.

```
aws iam list-attached-role-policies --role-name my-role --query "AttachedPolicies[].PolicyArn" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
arn:aws:iam::111122223333:policy/my-policy
```

3. Legen Sie eine Variable fest, um den Amazon-Ressourcennamen (ARN) der Richtlinie zu speichern, die Sie verwenden möchten. *my-policy* Ersetzen Sie es durch den Namen der Richtlinie, für die Sie die Berechtigungen bestätigen möchten.

```
export policy_arn=arn:aws: iam::111122223333:policy/my-policy
```

4. Zeigen Sie die Standardversion der Richtlinie an.

```
aws iam get-policy --policy-arn $policy_arn
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "Policy": {
    "PolicyName": "my-policy",
    "PolicyId": "EXAMPLEBIOWGLDEXAMPLE",
    "Arn": "arn:aws: iam::111122223333:policy/my-policy",
    "Path": "/",
    "DefaultVersionId": "v1",
    [...]
  }
}
```

5. Sehen Sie sich den Inhalt der Richtlinie an, um sicherzustellen, dass die Richtlinie alle Berechtigungen enthält, die Ihr Pod benötigt. Falls erforderlich, ersetzen Sie **1** den folgenden Befehl durch die Version, die in der vorherigen Ausgabe zurückgegeben wurde.

```
aws iam get-policy-version --policy-arn $policy_arn --version-id v1
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws: s3::my-pod-secrets-bucket"
    }
  ]
}
```

```
}
```

Wenn Sie die Beispielrichtlinie in einem vorherigen Schritt erstellt haben, ist Ihre Ausgabe dieselbe. Wenn Sie eine andere Richtlinie erstellt haben, ist der *example* Inhalt anders.

6. Vergewissern Sie sich, dass das Kubernetes-Dienstkonto mit der Rolle versehen ist.

```
kubectl describe serviceaccount my-service-account -n default
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name:                my-service-account
Namespace:           default
Annotations:         eks.amazonaws.com/role-arn: arn:aws:iam::111122223333:role/my-
                    role
Image pull secrets:   <none>
Mountable secrets:    my-service-account-token-qqjfl
Tokens:              my-service-account-token-qqjfl
[...]
```

Nächste Schritte

- [the section called “Dem Pod zuweisen”](#)

Pods für die Verwendung eines Kubernetes-Dienstkontos konfigurieren

Wenn ein Pod auf AWS Dienste zugreifen muss, müssen Sie ihn für die Verwendung eines Kubernetes-Dienstkontos konfigurieren. Das Dienstkonto muss einer AWS Identity and Access Management (IAM) -Rolle zugeordnet sein, die über Berechtigungen für den Zugriff auf die AWS Dienste verfügt.

- Einen vorhandenen -Cluster. Falls Sie noch keinen haben, können Sie ihn mithilfe einer der Anleitungen unter erstellen. [Erste Schritte](#)
- Ein vorhandener Anbieter für IAM OpenID Connect (OIDC) für Ihren Cluster. Informationen zum Feststellen, ob Sie bereits einen haben oder wie Sie einen erstellen können, finden Sie unter [the section called “IAM OIDC-Anbieter”](#).
- Ein vorhandenes Kubernetes-Dienstkonto, das einer IAM-Rolle zugeordnet ist. Das Servicekonto muss mit dem Amazon-Ressourcennamen (ARN) der IAM-Rolle versehen sein. Der Rolle muss

eine IAM-Richtlinie zugeordnet sein, die die Berechtigungen enthält, die Ihre Pods für die Nutzung von Diensten haben sollen. AWS Weitere Informationen zu Rollen, ihren Vorteilen sowie zu ihrer Erstellung und Konfiguration finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).

- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit `aws configure`](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
 - Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie `kubectl` und `eksctl` ein”](#).
 - Eine vorhandene `kubectl config`-Datei, die Ihre Clusterkonfiguration enthält. Informationen zum Erstellen einer `kubectl config`-Datei finden Sie unter [the section called “Greifen Sie mit `kubectl` auf den Cluster zu”](#).
1. Verwenden Sie den folgenden Befehl, um ein Bereitstellungsmanifest zu erstellen, mit dem Sie einen Pod bereitstellen können, um die Konfiguration zu bestätigen. Ersetzen Sie *example values* durch Ihre eigenen Werte.

```
cat >my-deployment.yaml <<EOF
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  selector:
    matchLabels:
      app: my-app
  template:
    metadata:
      labels:
```

```
    app: my-app
  spec:
    serviceAccountName: my-service-account
    containers:
    - name: my-app
      image: public.ecr.aws/nginx/nginx:X.XX
EOF
```

2. Stellen Sie das Manifest in Ihrem Cluster bereit.

```
kubectl apply -f my-deployment.yaml
```

3. Vergewissern Sie sich, dass die erforderlichen Umgebungsvariablen für Ihren Pod vorhanden sind.

- Sehen Sie sich die Pods an, die im vorherigen Schritt mit der Bereitstellung bereitgestellt wurden.

```
kubectl get pods | grep my-app
```

Eine Beispielausgabe sieht wie folgt aus.

```
my-app-6f4dfff6cb-76cv9    1/1      Running    0          3m28s
```

- Zeigen Sie den ARN der IAM-Rolle an, die der Pod verwendet.

```
kubectl describe pod my-app-6f4dfff6cb-76cv9 | grep AWS_ROLE_ARN:
```

Eine Beispielausgabe sieht wie folgt aus.

```
AWS_ROLE_ARN: arn:aws:iam::111122223333:role/my-role
```

Der Rollen-ARN muss mit dem Rollen-ARN übereinstimmen, mit dem Sie das vorhandene Servicekonto mit Anmerkungen versehen haben. Weitere Informationen zum Annotieren des Servicekontos finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).

- Vergewissern Sie sich, dass der Pod über eine Web-Identity-Token-Datei-Mount verfügt.

```
kubectl describe pod my-app-6f4dfff6cb-76cv9 | grep AWS_WEB_IDENTITY_TOKEN_FILE:
```

```
AWS_WEB_IDENTITY_TOKEN_FILE: /var/run/secrets/eks.amazonaws.com/serviceaccount/token
```

Der kubelet fordert das Token im Namen des Pods an und speichert es. Standardmäßig aktualisiert das kubelet das Token, wenn es älter als 80 Prozent seiner gesamten TTL ist oder wenn das Token älter als 24 Stunden ist. Sie können die Ablaufdauer für jedes Konto mit Ausnahme des Standarddienstkontos mithilfe der Einstellungen in Ihrer Pod-Spezifikation ändern. Weitere Informationen finden Sie unter [Service Account Token Volume Projection](#) in der Kubernetes-Dokumentation.

Der [Amazon EKS Pod Identity Webhook](#) auf dem Cluster sucht nach Pods, die ein Dienstkonto mit der folgenden Anmerkung verwenden:

```
eks.amazonaws.com/role-arn: arn:aws:iam::111122223333:role/my-role
```

Der Webhook wendet die vorherigen Umgebungsvariablen auf diese Pods an. Ihr Cluster muss den Webhook nicht verwenden, um die Umgebungsvariablen und Token-Datei-Mounts zu konfigurieren. Sie können Pods manuell so konfigurieren, dass sie diese Umgebungsvariablen haben. Die [unterstützten Versionen des AWS SDK](#) suchen zuerst im Credential Chain Provider nach diesen Umgebungsvariablen. Die Rollenmeldedaten werden für Pods verwendet, die diese Kriterien erfüllen.

4. Vergewissern Sie sich, dass Ihre Pods mithilfe der Berechtigungen, die Sie in der IAM-Richtlinie für Ihre Rolle zugewiesen haben, mit den AWS Diensten interagieren können.

Note

Wenn ein Pod AWS Anmeldeinformationen von einer IAM-Rolle verwendet, die mit einem Dienstkonto verknüpft ist, verwendet die AWS CLI oder andere SDKs in den Containern für diesen Pod die Anmeldeinformationen, die von dieser Rolle bereitgestellt werden. Wenn Sie den Zugriff auf die Anmeldeinformationen, die für die [IAM-Rolle des Amazon EKS-Knotens](#) bereitgestellt werden, nicht einschränken, hat der Pod weiterhin Zugriff auf diese Anmeldeinformationen. Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

Wenn Ihre Pods nicht wie erwartet mit den Diensten interagieren können, führen Sie die folgenden Schritte durch, um sicherzustellen, dass alles ordnungsgemäß konfiguriert ist.

- a. Vergewissern Sie sich, dass Ihre Pods eine AWS SDK-Version verwenden, die die Übernahme einer IAM-Rolle über eine OpenID Connect-Webidentitätstokendatei unterstützt. Weitere Informationen finden Sie unter [the section called "Wird unterstützt SDKs"](#).
- b. Stellen Sie sicher, dass die Bereitstellung das Servicekonto verwendet.

```
kubectl describe deployment my-app | grep "Service Account"
```

Eine Beispielausgabe sieht wie folgt aus.

```
Service Account: my-service-account
```

- c. Wenn Ihre Pods immer noch nicht auf Dienste zugreifen können, überprüfen Sie die unter [Zuweisen von IAM-Rollen zu Kubernetes-Dienstkonten beschriebenen Schritte, um](#) sicherzustellen, dass Ihre Rolle und Ihr Dienstkonto ordnungsgemäß konfiguriert sind.

Den AWS Security Token Service-Endpunkt für ein Dienstkonto konfigurieren

Wenn Sie ein Kubernetes-Dienstkonto mit [IAM-Rollen für Dienstkonten](#) verwenden, können Sie den Typ des AWS Security Token Service-Endpunkts konfigurieren, der vom Dienstkonto verwendet wird, wenn Ihr Cluster und Ihre Plattformversion mit den in der folgenden Tabelle aufgeführten Versionen identisch oder höher sind. Wenn Ihre Kubernetes- oder Plattformversion älter ist als die in der Tabelle aufgeführten, können Ihre Dienstkonten nur den globalen Endpunkt verwenden.

Kubernetes-Version	Plattformversion	Standardtyp für Endpunkt
1.31	eks.4	Regional
1.30	eks.2	Regional
1.29	eks.1	Regional
1.28	eks.1	Regional
1.27	eks.1	Regional

Kubernetes-Version	Plattformversion	Standardtyp für Endpunkt
1.26	eks.1	Regional

AWS empfiehlt die Verwendung der regionalen AWS STS-Endpunkte anstelle des globalen Endpunkts. Dies reduziert die Latenz, bietet integrierte Redundanz und erhöht die Gültigkeit der Sitzungstoken. Der AWS Security Token Service muss in der AWS Region aktiv sein, in der der Pod ausgeführt wird. Darüber hinaus muss Ihre Anwendung über eine integrierte Redundanz für eine andere AWS Region verfügen, falls der Dienst in der AWS Region ausfällt. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [AWS STS in einer AWS Region verwalten](#).

- Einen vorhandenen -Cluster. Wenn Sie noch keinen haben, können Sie einen erstellen, indem Sie einen der Anleitungen unter verwenden. [Erste Schritte](#)
- Ein vorhandener IAM-OIDC-Anbieter für Ihren Cluster. Weitere Informationen finden Sie unter [the section called “IAM OIDC-Anbieter”](#).
- Ein vorhandenes Kubernetes-Servicekonto, das für die Verwendung mit der Funktion [Amazon-EKS-IAM für Servicekonten](#).

Die folgenden Beispiele verwenden alle das Kubernetes-Servicekonto `aws-node`, das vom [Amazon VPC CNI-Plugin](#) verwendet wird. Sie können das *example values* durch Ihre eigenen Dienstkonten, Pods, Namespaces und andere Ressourcen ersetzen.

1. Wählen Sie einen Pod aus, der ein Dienstkonto verwendet, für das Sie den Endpunkt ändern möchten. Ermitteln Sie, AWS in welcher Region der Pod ausgeführt wird. Ersetze es *aws-node-6mfgv* durch deinen Pod-Namen und *kube-system* durch den Namespace deines Pods.

```
kubectl describe pod aws-node-6mfgv -n kube-system |grep Node:
```

Eine Beispielausgabe sieht wie folgt aus.

```
ip-192-168-79-166.us-west-2/192.168.79.166
```

In der vorherigen Ausgabe läuft der Pod auf einem Knoten in der Region US-West-2 AWS .

2. Ermitteln Sie den Endpunkttyp, den das Dienstkonto des Pods verwendet.

```
kubectl describe pod aws-node-6mfgv -n kube-system |grep AWS_STS_REGIONAL_ENDPOINTS
```

Eine Beispielausgabe sieht wie folgt aus.

```
AWS_STS_REGIONAL_ENDPOINTS: regional
```

Wenn der aktuelle Endpunkt global ist, dann wird `global` in der Ausgabe zurückgegeben. Wenn keine Ausgabe zurückgegeben wird, wird der Standard-Endpunkttyp verwendet und wurde nicht überschrieben.

3. Wenn Ihre Cluster- oder Plattformversion dieselbe oder höher ist als die in der Tabelle aufgeführten, können Sie den von Ihrem Servicekonto verwendeten Endpunkttyp mit einem der folgenden Befehle vom Standardtyp in einen anderen Typ ändern. Ersetzen Sie *aws-node* mit dem Namen Ihres Servicekontos, *kube-system* mit dem Namespace Ihres vorhandenen Servicekontos.
- Wenn Ihr Standard- oder aktueller Endpunkttyp global ist und Sie ihn in regional ändern möchten:

```
kubectl annotate serviceaccount -n kube-system aws-node eks.amazonaws.com/sts-regional-endpoints=true
```

Wenn Sie [IAM-Rollen für Dienstkonten](#) verwenden, um vorsigniertes S3 URLs in Ihrer Anwendung zu generieren, die in den Containern von Pods ausgeführt wird, ähnelt das Format der URL für regionale Endpunkte dem folgenden Beispiel:

```
https://bucket.s3.us-west-2.amazonaws.com/path?...&X-Amz-Credential=your-access-key-id/date/us-west-2/s3/aws4_request&...
```

- Wenn Ihr Standard- oder aktueller Endpunkttyp regional ist und Sie ihn in global ändern möchten:

```
kubectl annotate serviceaccount -n kube-system aws-node eks.amazonaws.com/sts-regional-endpoints=false
```

Wenn Ihre Anwendung explizit Anfragen an globale AWS STS-Endpunkte stellt und Sie das Standardverhalten der Verwendung regionaler Endpunkte in Amazon EKS-Clustern nicht außer Kraft setzen, schlagen Anfragen mit einem Fehler fehl. Weitere Informationen finden

Sie unter [the section called “Pod-Container erhalten folgenden Fehler: An error occurred \(SignatureDoesNotMatch\) when calling the GetCallerIdentity operation: Credential should be scoped to a valid region”](#).

Wenn Sie [IAM-Rollen für Dienstkonten](#) verwenden, um vorsignierte S3 URLs in Ihrer Anwendung zu generieren, die in den Containern von Pods ausgeführt wird, ähnelt das Format der URL für globale Endpunkte dem folgenden Beispiel:

```
https://bucket.s3.amazonaws.com/path?...&X-Amz-Credential=your-access-key-id/date/us-west-2/s3/aws4_request&...
```

Wenn Ihre Automatisierung die vorsignierte URL in einem bestimmten Format erwartet, oder wenn Ihre Anwendung oder Downstream-Abhängigkeiten, die vorsigniert verwenden, Erwartungen an die AWS Zielregion URLs haben, nehmen Sie die erforderlichen Änderungen vor, um den entsprechenden STS-Endpunkt zu verwenden. AWS

4. Löschen Sie alle vorhandenen Pods, die dem Dienstkonto zugeordnet sind, und erstellen Sie sie neu, um die Umgebungsvariablen für die Anmeldeinformationen anzuwenden. Der mutierende Webhook wendet sie nicht auf Pods an, die bereits ausgeführt werden. Sie können *Podskube-system*, und *-l k8s-app=aws-node* durch die Informationen für die Pods ersetzen, für die Sie Ihre Anmerkung festgelegt haben.

```
kubectl delete Pods -n kube-system -l k8s-app=aws-node
```

5. Vergewissern Sie sich, dass alle Pods neu gestartet wurden.

```
kubectl get Pods -n kube-system -l k8s-app=aws-node
```

6. Sehen Sie sich die Umgebungsvariablen für einen der Pods an. Stellen Sie sicher, dass der AWS_STS_REGIONAL_ENDPOINTS-Wert der ist, den Sie im vorherigen Schritt festgelegt haben.

```
kubectl describe pod aws-node-kzbtr -n kube-system |grep AWS_STS_REGIONAL_ENDPOINTS
```

Eine Beispielausgabe sieht wie folgt aus.

```
AWS_STS_REGIONAL_ENDPOINTS=regional
```

Authentifizieren Sie sich bei einem anderen Konto mit IRSA

Sie können kontoübergreifende IAM-Berechtigungen konfigurieren, indem Sie entweder einen Identitätsanbieter aus dem Cluster eines anderen Kontos erstellen oder verkettete Operationen verwenden. `AssumeRole` In den folgenden Beispielen besitzt Konto A einen Amazon EKS-Cluster, der IAM-Rollen für Dienstkonten unterstützt. Pods, die auf diesem Cluster ausgeführt werden, müssen die IAM-Berechtigungen von Konto B annehmen.

Example Erstellen Sie einen Identitätsanbieter aus dem Cluster eines anderen Kontos

Example

In diesem Beispiel stellt Konto A dem Konto B die OpenID Connect (OIDC)-Aussteller-URL aus seinem Cluster bereit. Konto B folgt den Anweisungen unter [Erstellen Sie einen IAM-OIDC-Anbieter für Ihren Cluster](#) und [the section called "Weisen Sie eine IAM-Rolle zu"](#) verwendet die OIDC-Aussteller-URL aus dem Cluster von Konto A. Anschließend fügt ein Clusteradministrator dem Dienstkonto im Cluster von Konto A eine Anmerkung hinzu, um die Rolle von Konto B () zu verwenden. **444455556666**

```
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations:
    eks.amazonaws.com/role-arn: arn:aws: iam::444455556666:role/account-b-role
```

Example Verwenden von verketteten **AssumeRole**-Operationen

Example

In diesem Beispiel erstellt Konto B eine IAM-Richtlinie mit den Berechtigungen, die Pods im Cluster von Konto A zugewiesen werden können. Konto B (**444455556666**) ordnet diese Richtlinie einer IAM-Rolle mit einer Vertrauensstellung zu, die `AssumeRole` Berechtigungen für Konto A () gewährt. **111122223333**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws: iam::111122223333:root"
```

```

    },
    "Action": "sts:AssumeRole",
    "Condition": {}
  }
]
}

```

Konto A erstellt eine Rolle mit einer Vertrauensrichtlinie, die Anmeldeinformationen von dem Identitätsanbieter erhält, der mit der OIDC-Ausstelleradresse des Clusters erstellt wurde.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws: iam::111122223333:oidc-provider/oidc.eks.region-
code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
      },
      "Action": "sts:AssumeRoleWithWebIdentity"
    }
  ]
}

```

Konto A fügt dieser Rolle eine Richtlinie mit den folgenden Berechtigungen an, um die Rolle anzunehmen, die Konto B erstellt hat.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws: iam::444455556666:role/account-b-role"
    }
  ]
}

```

Der Anwendungscode für Pods, der die Rolle von Konto B übernimmt, verwendet zwei Profile: und. `account_b_role` `account_a_role` Das `account_b_role`-Profil verwendet das `account_a_role`-Profil als Quelle. Für die AWS CLI ähnelt die `~/.aws/config` Datei der folgenden.

```
[profile account_b_role]
source_profile = account_a_role
role_arn=arn:aws: iam::444455556666:role/account-b-role

[profile account_a_role]
web_identity_token_file = /var/run/secrets/eks.amazonaws.com/serviceaccount/token
role_arn=arn:aws: iam::111122223333:role/account-a-role
```

Informationen zur Angabe verketteter Profile für andere AWS SDKs finden Sie in der Dokumentation für das SDK, das Sie verwenden. Weitere Informationen finden Sie unter [Tools, auf AWS denen Sie aufbauen können](#).

Verwenden Sie IRSA mit dem SDK AWS

Verwenden von Anmeldeinformationen

Um die Anmeldeinformationen von IAM-Rollen für Dienstkonten (IRSA) zu verwenden, kann Ihr Code ein beliebiges AWS SDK verwenden, um einen Client für einen AWS Dienst mit einem SDK zu erstellen. Standardmäßig sucht das SDK in einer Kette von Speicherorten nach AWS Identity and Access Management-Anmeldeinformationen, die verwendet werden können. Die IAM-Rollen für Anmeldeinformationen für Dienstkonten werden verwendet, wenn Sie bei der Erstellung des Clients keinen Anmeldeinformationsanbieter angeben oder das SDK anderweitig initialisiert haben.

Das funktioniert, weil IAM-Rollen für Servicekonten als Schritt in der standardmäßigen Anmeldeinformationskette hinzugefügt wurden. Wenn Ihre Workloads derzeit Anmeldeinformationen verwenden, die sich an früherer Stelle in der Anmeldeinformationskette befinden, werden diese Anmeldeinformationen auch dann weiterhin verwendet, wenn Sie IAM-Rollen für Servicekonten für dieselbe Workload konfigurieren.

Das SDK tauscht mithilfe der Aktion automatisch das OIDC-Token des Dienstkontos gegen temporäre Anmeldeinformationen vom AWS Security Token Service aus. `AssumeRoleWithWebIdentity` Amazon EKS und diese SDK-Aktion rotieren weiterhin die temporären Anmeldeinformationen, indem sie erneuert werden, bevor sie ablaufen.

Wenn Sie [IAM-Rollen für Dienstkonten](#) verwenden, müssen die Container in Ihren Pods eine AWS SDK-Version verwenden, die die Übernahme einer IAM-Rolle über eine OpenID Connect-Webidentitäts-Tokendatei unterstützt. Stellen Sie sicher, dass Sie die folgenden Versionen oder höher für Ihr SDK verwenden: AWS

- Java (Version 2) – [2.10.11](#)

- Java — [1.12.782](#)
- AWS SDK for Go v1 — [1.23.13](#)
- AWS SDK for Go v2 — Unterstützung für alle Versionen
- Python (Boto3) — [1.9.220](#)
- Python (botocore) — [1.12.200](#)
- AWS CLI — [1.16.232](#)
- Knoten – [2.525.0](#) und [3.27.0](#)
- Ruby – [3.58.0](#)
- C++ – [1.7.174](#)
- .NET – [3.3.659.1](#) – Sie müssen auch `AWSSDK.SecurityToken` angeben.
- PHP – [3.110.7](#)

Viele beliebte Kubernetes-Add-Ons, wie der [Cluster Autoscaler](#), [Route Internet Traffic with Load AWS Balancer Controller](#) und das [Amazon VPC CNI-Plugin für Kubernetes, unterstützen IAM-Rollen für Dienstkonten](#).

[Um sicherzustellen, dass Sie ein unterstütztes SDK verwenden, folgen Sie beim Erstellen Ihrer Container den Installationsanweisungen für Ihr bevorzugtes SDK unter Tools to Build On. AWS](#)

Überlegungen

Java

Wenn Sie Java verwenden, müssen Sie das `sts` Modul in den Klassenpfad aufnehmen. Weitere Informationen finden Sie [WebIdentityTokenFileCredentialsProvider](#) in den Java SDK-Dokumenten.

Rufen Sie Signaturschlüssel ab, um OIDC-Token zu validieren

Kubernetes gibt für jedes Kubernetes-Servicekonto eine `ProjectedServiceAccountToken` aus. Dieses Token ist ein OIDC-Token, bei dem es sich außerdem um eine Art JSON-Webtoken (JWT) handelt. Amazon EKS hostet für jeden Cluster einen öffentlichen OIDC-Endpunkt, der die Signaturschlüssel für das Token enthält, sodass externe Systeme es validieren können.

Um einen `ProjectedServiceAccountToken` zu validieren, müssen Sie die öffentlichen OIDC-Signaturschlüssel abrufen, die auch als JSON Web Key Set (JWKS) bezeichnet werden. Verwenden Sie diese Schlüssel in Ihrer Anwendung, um das Token zu validieren. Sie können beispielsweise

die [Python-Bibliothek PyJWT](#) verwenden, um Token mit diesen Schlüsseln zu validieren. Weitere Informationen zu finden Sie unter `ProjectedServiceAccountToken`. [the section called “Hintergrundinformationen zu IAM, Kubernetes und OpenID Connect \(OIDC\)”](#)

Voraussetzungen

- Ein vorhandener AWS Identity and Access Management (IAM) OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Informationen zum Feststellen, ob Sie bereits über einen verfügen oder einen erstellen müssen, finden Sie unter [the section called “IAM OIDC-Anbieter”](#).
- AWS CLI — Ein Befehlszeilentool für die Arbeit mit AWS Services, einschließlich Amazon EKS. Weitere Informationen finden Sie unter [Installation](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Wir empfehlen, dass Sie die AWS CLI nach der Installation ebenfalls konfigurieren. Weitere Informationen finden Sie unter [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

Verfahren

1. Rufen Sie die OIDC-URL für Ihren Amazon EKS-Cluster mithilfe der AWS CLI ab.

```
$ aws eks describe-cluster --name my-cluster --query 'cluster.identity.oidc.issuer'
"https://oidc.eks.us-west-2.amazonaws.com/id/8EBDXXX00BAE"
```

2. Rufen Sie den öffentlichen Signaturschlüssel mit curl oder einem ähnlichen Tool ab. Das Ergebnis ist ein [JSON Web Key Set \(JWKS\)](#).

Important

Amazon EKS drosselt Anrufe an den OIDC-Endpunkt. Sie sollten den öffentlichen Signaturschlüssel zwischenspeichern. Respektieren Sie den in der Antwort enthaltenen `cache-control` Header.

Important

Amazon EKS rotiert den OIDC-Signaturschlüssel alle sieben Tage.

```
$ curl https://oidc.eks.us-west-2.amazonaws.com/id/8EBDXXX00BAE/keys
```



```
{"keys":  
[{"kty":"RSA","kid":"2284XXXX4a40","use":"sig","alg":"RS256","n":"wk1bXXXXMVfQ","e":"AQAB"}]}
```

Erfahren Sie, wie EKS Pod Identity Pods Zugriff auf AWS Dienste gewährt

Anwendungen in den Containern eines Pods können ein AWS SDK oder die AWS CLI verwenden, um API-Anfragen an AWS Dienste mithilfe von AWS Identity and Access Management (IAM) -Berechtigungen zu stellen. Anwendungen müssen ihre AWS API-Anfragen mit AWS Anmeldeinformationen signieren.

EKS Pod Identities bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie EC2 Amazon-Instance-Profile Anmeldeinformationen für EC2 Amazon-Instances bereitstellen. Anstatt Ihre AWS Anmeldeinformationen zu erstellen und an die Container zu verteilen oder die Rolle der EC2 Amazon-Instance zu verwenden, verknüpfen Sie eine IAM-Rolle mit einem Kubernetes-Dienstkonto und konfigurieren Ihre Pods so, dass sie das Dienstkonto verwenden.

Jede EKS-Pod-Identity-Zuordnung ordnet einem Servicekonto in einem Namespace im angegebenen Cluster eine Rolle zu. Wenn Sie dieselbe Anwendung in mehreren Clustern haben, können Sie in jedem Cluster identische Zuordnungen vornehmen, ohne die Vertrauensrichtlinie der Rolle zu ändern.

Wenn ein Pod ein Servicekonto mit einer Zuordnung verwendet, legt Amazon EKS Umgebungsvariablen in den Containern des Pods fest. Die Umgebungsvariablen konfigurieren die AWS SDKs, einschließlich der AWS CLI, für die Verwendung der EKS Pod Identity-Anmeldeinformationen.

Vorteile von EKS-Pod-Identitäten

EKS-Pod-Identitäten bieten die folgenden Vorteile:

- Geringste Rechte — Sie können IAM-Berechtigungen auf ein Dienstkonto beschränken, und nur Pods, die dieses Dienstkonto verwenden, haben Zugriff auf diese Berechtigungen. Mit diesem Feature entfällt auch die Notwendigkeit von Drittanbieterlösungen wie `kiam` oder `kube2iam`.
- Isolierung von Anmeldeinformationen — Wenn der Zugriff auf den [Amazon EC2 Instance Metadata Service \(IMDS\)](#) eingeschränkt ist, können die Container eines Pods nur Anmeldeinformationen für die IAM-Rolle abrufen, die dem Dienstkonto zugeordnet ist, das der Container verwendet. Ein Container hat niemals Zugriff auf Anmeldeinformationen, die von anderen Containern in anderen Pods verwendet werden. Wenn IMDS nicht eingeschränkt ist, haben die Container des Pods auch

Zugriff auf die [IAM-Rolle des Amazon EKS-Knotens](#), und die Container können möglicherweise auf Anmeldeinformationen von IAM-Rollen anderer Pods auf demselben Knoten zugreifen. Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

Note

Pods, `hostNetwork: true` die mit konfiguriert sind, haben immer IMDS-Zugriff, aber die AWS SDKs AND-CLI verwendet Pod Identity-Anmeldeinformationen, wenn sie aktiviert sind.

- Überprüfbarkeit — Zugriffs- und Ereignisprotokollierung sind über verfügbar AWS CloudTrail , um nachträgliche Prüfungen zu erleichtern.

Important

Container stellen keine Sicherheitsgrenze dar, und die Verwendung von Pod Identity ändert daran nichts. Pods, die demselben Knoten zugewiesen sind, teilen sich je nach Ihrer Pod-Konfiguration einen Kernel und möglicherweise weitere Ressourcen. Pods, die auf separaten Knoten laufen, werden zwar auf der Rechenebene isoliert, es gibt jedoch Knotenanwendungen, die über zusätzliche Berechtigungen in der Kubernetes-API verfügen, die über den Rahmen einer einzelnen Instanz hinausgehen. Einige Beispiele sind kubelet CSI-Speichertreiber oder Ihre eigenen Kubernetes-Anwendungen. kube-proxy

EKS Pod Identity ist eine einfachere Methode als [the section called “Referenzen bei IRSA”](#), da diese Methode keine IDC-Identitätsanbieter verwendet. EKS Pod Identity bietet die folgenden Verbesserungen:

- Unabhängiger Betrieb — In vielen Organisationen liegt die Verantwortung für die Erstellung von OIDC-Identitätsanbietern bei anderen Teams als für die Verwaltung der Kubernetes-Cluster. EKS Pod Identity hat eine klare Aufgabentrennung: Die gesamte Konfiguration der EKS-Pod-Identity-Zuordnungen erfolgt in Amazon EKS und die gesamte Konfiguration der IAM-Berechtigungen erfolgt in IAM.
- Wiederverwendbarkeit – EKS Pod Identity verwendet einen einzigen IAM-Prinzipal anstelle der separaten Prinzipale für jeden Cluster, den IAM-Rollen für Servicekonten verwenden. Ihr IAM-

Administrator fügt der Vertrauensrichtlinie jeder Rolle den folgenden Prinzipal hinzu, damit sie von EKS-Pod-Identitäten verwendet werden kann.

```
"Principal": {  
  "Service": "pods.eks.amazonaws.com"  
}
```

- Skalierbarkeit — Jeder Satz temporärer Anmeldeinformationen wird vom EKS-Authentifizierungsdienst in EKS Pod Identity übernommen und nicht von jedem AWS SDK, das Sie in jedem Pod ausführen. Anschließend gibt der Amazon EKS Pod Identity Agent, der auf jedem Knoten ausgeführt wird, die Anmeldeinformationen an den aus SDKs. Somit wird die Last für jeden Knoten auf einmal reduziert und nicht in jedem Pod dupliziert. Weitere Details zu diesem Prozess finden Sie unter [the section called “Funktionsweise”](#).

Weitere Informationen zum Vergleich der beiden Alternativen finden Sie unter [the section called “Workload-Zugriff auf AWS”](#).

Übersicht über die Einrichtung von EKS-Pod-Identitäten

Aktivieren Sie EKS-Pod-Identitäten, indem Sie die folgenden Verfahren ausführen:

1. [the section called “Richten Sie den Agenten ein”](#)— Sie führen dieses Verfahren nur einmal für jeden Cluster durch. Sie müssen diesen Schritt nicht abschließen, wenn der automatische EKS-Modus auf Ihrem Cluster aktiviert ist.
2. [the section called “Weisen Sie eine IAM-Rolle zu”](#)— Führen Sie dieses Verfahren für jeden eindeutigen Satz von Berechtigungen aus, über den eine Anwendung verfügen soll.
3. [the section called “Pod-Dienstkonto”](#)— Führen Sie dieses Verfahren für jeden Pod aus, der Zugriff auf AWS Dienste benötigt.
4. [the section called “Unterstützt SDKs”](#)— Vergewissern Sie sich, dass der Workload ein AWS SDK einer unterstützten Version verwendet und dass der Workload die standardmäßige Anmeldeinformationskette verwendet.

Einschränkungen

- Bis zu 5.000 EKS Pod Identity-Zuordnungen pro Cluster zur Zuordnung von IAM-Rollen zu Kubernetes-Dienstkonten werden unterstützt.

Überlegungen

- **IAM-Rollenzuordnung:** Jedes Kubernetes-Dienstkonto in einem Cluster kann mit einer IAM-Rolle aus demselben Konto wie der Cluster verknüpft werden. AWS Um die Rolle zu ändern, bearbeiten Sie die EKS Pod Identity-Zuordnung. Delegieren Sie für den kontoübergreifenden Zugriff den Zugriff auf die Rolle mithilfe von IAM-Rollen. Weitere Informationen finden Sie unter [AWS Kontenübergreifendes Delegieren des Zugriffs mithilfe von IAM-Rollen im IAM-Benutzerhandbuch](#).
- **EKS Pod Identity Agent:** Für die Verwendung von EKS Pod Identity ist der Pod Identity Agent erforderlich. Der Agent wird als Kubernetes DaemonSet auf Clusterknoten ausgeführt und stellt Anmeldeinformationen nur für Pods auf demselben Knoten bereit. Er verwendet die Adresse des KnotenshostNetwork, belegt den Port 80 und 2703 die Link-Local-Adresse (169.254.170.23 für IPv4, fd00:ec2::23 für IPv6). Wenn IPv6 in Ihrem Cluster deaktiviert ist, deaktivieren Sie es für den Pod Identity Agent. Weitere Informationen finden Sie unter [Deaktivieren IPv6 im EKS Pod Identity Agent](#).
- **Eventuelle Konsistenz:** Die EKS Pod Identity-Verknüpfungen sind letztendlich konsistent, was zu Verzögerungen von mehreren Sekunden nach API-Aufrufen führen kann. Vermeiden Sie es, Verknüpfungen in kritischen Codepfaden mit hoher Verfügbarkeit zu erstellen oder zu aktualisieren. Führen Sie diese Aktionen stattdessen in separaten, weniger häufigen Initialisierungs- oder Einrichtungsroutinen durch. Weitere Informationen finden Sie unter [Sicherheitsgruppen pro Pod](#) im EKS Best Practices Guide.
- **Überlegungen zu Proxys und Sicherheitsgruppen:** Fügen Sie bei Pods, die einen Proxy verwenden, den `no_proxy/NO_PROXY` Umgebungsvariablen `169.254.170.23 [fd00:ec2::23]` (IPv4/IPv6) und `()` hinzu, um fehlgeschlagene Anfragen an den EKS Pod Identity Agent zu verhindern. Wenn Sie Sicherheitsgruppen für Pods mit dem AWS VPC-CNI verwenden, setzen Sie das `ENABLE_POD_ENI` Flag auf „true“ und das `POD_SECURITY_GROUP_ENFORCING_MODE` Flag auf „standard“. Weitere Informationen finden Sie unter [Zuweisen von Sicherheitsgruppen](#) zu einzelnen Pods.

Cluster-Versionen von EKS Pod Identity

Um EKS Pod Identity verwenden zu können, muss der Cluster über eine Plattformversion verfügen, die mit der in der folgenden Tabelle aufgeführten Version identisch oder höher ist, oder über eine Kubernetes-Version, die höher als die in der Tabelle aufgeführten Versionen ist. Die vorgeschlagene Version des Amazon EKS Pod Identity Agent für eine Kubernetes-Version finden Sie unter [the section called “Überprüfen Sie die Kompatibilität”](#)

Kubernetes-Version	Plattformversion
Kubernetes-Versionen sind nicht aufgeführt	Alle Plattformversionen unterstützen
1.28	eks.4
1.27	eks.8
1.26	eks.9

Einschränkungen von EKS Pod Identity

EKS-Pod-Identitäten sind auf folgenden Plattformen verfügbar:

- Amazon-EKS-Cluster-Versionen, die im vorherigen Thema ([the section called “Cluster-Versionen von EKS Pod Identity”](#)) aufgeführt wurden.
- Worker-Knoten im Cluster, bei denen es sich um EC2 Linux-Amazon-Instances handelt.

EKS-Pod-Identitäten sind in folgenden Fällen nicht verfügbar:

- AWS Outposts.
- Amazon EKS Anywhere.
- Kubernetes-Cluster, die Sie auf Amazon erstellen und ausführen. EC2 Die EKS-Pod-Identity-Komponenten sind nur in Amazon EKS verfügbar.

Sie können EKS Pod Identities nicht verwenden mit:

- Pods, die überall außer EC2 Linux-Amazon-Instances laufen. Linux- und Windows-Pods, die auf AWS Fargate (Fargate) laufen, werden nicht unterstützt. Pods, die auf Windows EC2 Amazon-Instances ausgeführt werden, werden nicht unterstützt.

Verstehen Sie, wie EKS Pod Identity funktioniert

Amazon EKS Pod Identity-Zuordnungen bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie EC2 Amazon-Instance-Profile Anmeldeinformationen für EC2 Amazon-Instances bereitstellen.

Amazon EKS Pod Identity bietet Anmeldeinformationen für Ihre Workloads mit einer zusätzlichen EKS-Auth-API und einem Agent-Pod, der auf jedem Knoten ausgeführt wird.

In Ihren Add-Ons, wie Amazon EKS-Add-Ons und selbstverwalteten Controllern, Operatoren und anderen Add-Ons, muss der Autor seine Software aktualisieren, um die neueste Version AWS SDKs verwenden zu können. Die Liste der Kompatibilität zwischen EKS Pod Identity und den von Amazon EKS produzierten Add-ons finden Sie im vorherigen Abschnitt ([the section called “Einschränkungen von EKS Pod Identity”](#)).

Verwenden von EKS-Pod-Identitäten in Ihrem Code

In Ihrem Code können Sie die verwenden, AWS SDKs um auf AWS Dienste zuzugreifen. Sie schreiben Code, um einen Client für einen AWS Dienst mit einem SDK zu erstellen, und das SDK sucht standardmäßig in einer Kette von Speicherorten nach AWS Identity and Access Management-Anmeldeinformationen, die verwendet werden können. Nachdem gültige Anmeldeinformationen gefunden wurden, wird die Suche beendet. Weitere Informationen zu den verwendeten Standardspeicherorten finden Sie unter [Credential Provider Chain](#) im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.

EKS-Pod-Identitäten wurden dem Anbieter für Container-Anmeldeinformationen hinzugefügt, der in einem Schritt in der standardmäßigen Anmeldeinformationskette durchsucht wird. Wenn Ihre Workloads derzeit Anmeldeinformationen verwenden, die in der Kette der Anmeldeinformationen weiter vorn stehen, werden diese Anmeldeinformationen auch dann weiter verwendet, wenn Sie eine EKS-Pod-Identity-Zuordnung für dieselbe Workload konfigurieren. Auf diese Weise können Sie sicher von anderen Anmeldeinformationstypen migrieren, indem Sie die Zuordnung erstellen, bevor Sie die alten Anmeldeinformationen entfernen.

Der Anbieter für Container-Anmeldeinformationen stellt temporäre Anmeldeinformationen über einen Agent bereit, der auf jedem Knoten ausgeführt wird. In Amazon EKS ist dies der Amazon EKS Pod Identity Agent und bei Amazon Elastic Container Service ist es der `amazon-ecs-agent`. SDKs Sie verwenden Umgebungsvariablen, um den Agenten zu finden, zu dem eine Verbindung hergestellt werden soll.

Im Gegensatz dazu stellen IAM-Rollen für Dienstkonten ein Web-Identitätstoken bereit, das das AWS SDK mithilfe `AssumeRoleWithWebIdentity` von AWS Security Token Service austauschen muss.

So funktioniert EKS Pod Identity Agent mit einem Pod

1. Wenn Amazon EKS einen neuen Pod startet, der ein Dienstkonto mit einer EKS-Pod-Identity-Zuordnung verwendet, fügt der Cluster dem Pod-Manifest den folgenden Inhalt hinzu:

```
env:
- name: AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE
  value: "/var/run/secrets/pods.eks.amazonaws.com/serviceaccount/eks-pod-identity-token"
- name: AWS_CONTAINER_CREDENTIALS_FULL_URI
  value: "http://169.254.170.23/v1/credentials"
volumeMounts:
- mountPath: "/var/run/secrets/pods.eks.amazonaws.com/serviceaccount/"
  name: eks-pod-identity-token
volumes:
- name: eks-pod-identity-token
  projected:
    defaultMode: 420
    sources:
    - serviceAccountToken:
        audience: pods.eks.amazonaws.com
        expirationSeconds: 86400 # 24 hours
        path: eks-pod-identity-token
```

2. Kubernetes wählt aus, auf welchem Knoten der Pod ausgeführt werden soll. Anschließend verwendet der Amazon EKS Pod Identity Agent auf dem Knoten die [AssumeRoleForPodIdentity](#) Aktion, um temporäre Anmeldeinformationen von der EKS Auth API abzurufen.
3. Der EKS Pod Identity Agent stellt diese Anmeldeinformationen für die zur Verfügung AWS SDKs , die Sie in Ihren Containern ausführen.
4. Sie nutzen das SDK in Ihrer Anwendung, ohne einen Anmeldeinformationsanbieter für die Verwendung der standardmäßigen Anmeldeinformationskette anzugeben. Oder Sie geben den Anbieter für Container-Anmeldeinformationen an. Weitere Informationen zu den verwendeten Standardspeicherorten finden Sie in der [Credential-Provider-Kette](#) im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.
5. Das SDK verwendet die Umgebungsvariablen, um eine Verbindung zum EKS Pod Identity Agent herzustellen und die Anmeldeinformationen abzurufen.

Note

Wenn Ihre Workloads derzeit Anmeldeinformationen verwenden, die in der Kette der Anmeldeinformationen weiter vorn stehen, werden diese Anmeldeinformationen auch

dann weiter verwendet, wenn Sie eine EKS-Pod-Identity-Zuordnung für dieselbe Workload konfigurieren.

Richten Sie den Amazon EKS Pod Identity Agent ein

Amazon EKS Pod Identity-Zuordnungen bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie EC2 Amazon-Instance-Profile Anmeldeinformationen für EC2 Amazon-Instances bereitstellen.

Amazon EKS Pod Identity bietet Anmeldeinformationen für Ihre Workloads mit einer zusätzlichen EKS-Auth-API und einem Agent-Pod, der auf jedem Knoten ausgeführt wird.

Tip

Sie müssen den EKS Pod Identity Agent nicht auf EKS-Auto-Mode-Clustern installieren. Diese Funktion ist in den EKS Auto Mode integriert.

Überlegungen

- Standardmäßig überwacht der EKS Pod Identity Agent eine IPv4 IPv6 UND-Adresse für Pods, um Anmeldeinformationen anzufordern. Der Agent verwendet die Loopback-IP-Adresse (localhost) 169.254.170.23 für IPv4 und die Localhost-IP-Adresse für. [fd00:ec2::23] IPv6
- Wenn Sie IPv6 Adressen deaktivieren oder auf andere Weise IPv6 Localhost-IP-Adressen verhindern, kann der Agent nicht gestartet werden. Um den Agenten auf Knoten zu starten, die nicht verwendet werden können IPv6, folgen Sie den Schritten unter [the section called "Deaktivieren IPv6"](#) So deaktivieren Sie die IPv6 Konfiguration.

Erstellen des Amazon EKS Pod Identity Agent

Voraussetzungen für den Agent

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#). Die Clusterversion und die Plattformversion müssen mit den in den [EKS Pod Identity-Clusterversionen aufgeführten Versionen](#) identisch oder höher sein.
- Die Knotenrolle verfügt über Berechtigungen für den Agent, um die AssumeRoleForPodIdentity-Aktion in der EKS-Auth-API auszuführen. Sie können die [AWS](#)

[verwaltete Richtlinie verwenden: Amazon EKSWorker NodePolicy](#) oder eine benutzerdefinierte Richtlinie hinzufügen, die der folgenden ähnelt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource": "*"
    }
  ]
}
```

Diese Aktion kann durch Tags beschränkt werden, um einzuschränken, welche Rollen von Pods übernommen werden können, die den Agent verwenden.

- Die Knoten können auf Amazon ECR zugreifen und Images von Amazon ECR herunterladen. Das Container-Image für das Add-on befindet sich in den Registern, die unter [Amazon-Container-Image-Registrierungen für Amazon EKS-Add-Ons anzeigen](#) aufgeführt sind.

Beachten Sie, dass Sie den Speicherort des Images ändern und EKS-Add-Ons in den optionalen Konfigurationseinstellungen in der AWS Management Console und `--configuration-values` in der AWS CLI bereitstellen `imagePullSecrets` können.

- Die Knoten können die Amazon-EKS-Auth-API erreichen. Für private Cluster ist der `eks-auth` Endpunkt-IN AWS PrivateLink erforderlich.

Agent mit AWS Konsole einrichten

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster aus. Wählen Sie anschließend den Namen des Clusters aus, für den Sie das Add-on „EKS Pod Identity Agent“ konfigurieren möchten.
3. Wählen Sie die Registerkarte Add-ons.
4. Wählen Sie Weitere Add-Ons erhalten.
5. Wählen Sie das Kästchen oben rechts im Add-on-Bereich für EKS Pod Identity Agent aus und gehen Sie dann auf Bearbeiten.

6. Wählen Sie auf der Seite Konfigurieren ausgewählter Add-on-Einstellungen eine beliebige Version in der Dropdown-Liste Version aus.
7. (Optional) Erweitern Sie Optionale Konfigurationseinstellungen, um eine zusätzliche Konfiguration einzugeben. Sie können beispielsweise einen alternativen Speicherort für das Container-Image und ImagePullSecrets angeben. Das JSON-Schema mit den akzeptierten Schlüsseln wird im Konfigurationsschema des Add-ons angezeigt.

Geben Sie die Konfigurationsschlüssel und Werte in das Feld Konfigurationswerte ein

8. Wählen Sie Weiter.
9. Vergewissern Sie sich, dass die EKS-Pod-Identity-Pods auf Ihrem Cluster ausgeführt werden.

```
kubectl get pods -n kube-system | grep 'eks-pod-identity-agent'
```

Eine Beispielausgabe sieht wie folgt aus.

eks-pod-identity-agent-gmqp7	1/1	Running
1 (24h ago) 24h		
eks-pod-identity-agent-prnsh	1/1	Running
1 (24h ago) 24h		

Sie können jetzt EKS-Pod-Identity-Zuordnungen in Ihrem Cluster verwenden. Weitere Informationen finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).

Agent mit AWS CLI einrichten

1. Führen Sie den folgenden AWS CLI-Befehl aus. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks create-addon --cluster-name my-cluster --addon-name eks-pod-identity-agent --addon-version v1.0.0-eksbuild.1
```

Note

Der EKS Pod Identity Agent verwendet die vier `service-account-role-arn` IAM-Rollen nicht für Dienstkonten. Sie müssen dem EKS Pod Identity Agent Berechtigungen für die Knotenrolle gewähren.

2. Vergewissern Sie sich, dass die EKS-Pod-Identity-Pods auf Ihrem Cluster ausgeführt werden.

```
kubectl get pods -n kube-system | grep 'eks-pod-identity-agent'
```

Eine Beispielausgabe sieht wie folgt aus.

eks-pod-identity-agent-gmqp7	1/1	Running
1 (24h ago) 24h		
eks-pod-identity-agent-prnsh	1/1	Running
1 (24h ago) 24h		

Sie können jetzt EKS-Pod-Identity-Zuordnungen in Ihrem Cluster verwenden. Weitere Informationen finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).

Weisen Sie einem Kubernetes-Dienstkonto eine IAM-Rolle zu

In diesem Thema wird beschrieben, wie Sie ein Kubernetes-Dienstkonto so konfigurieren, dass es eine AWS Identity and Access Management (IAM) -Rolle mit EKS Pod Identity annimmt. Alle Pods, die für die Verwendung des Dienstkontos konfiguriert sind, können dann auf jeden AWS Dienst zugreifen, für den die Rolle Zugriffsberechtigungen besitzt.

Um eine EKS Pod Identity-Zuordnung zu erstellen, gibt es nur einen einzigen Schritt: Sie erstellen die Zuordnung in EKS über die AWS CLI AWS Management Console AWS SDKs, AWS CloudFormation und andere Tools. Es gibt keine Daten oder Metadaten zu den Verknüpfungen innerhalb des Clusters in irgendwelchen Kubernetes-Objekten, und Sie fügen den Dienstkonten keine Anmerkungen hinzu.

Voraussetzungen

- Einen vorhandenen -Cluster. Wenn Sie noch keinen haben, können Sie einen erstellen, indem Sie einer der Anleitungen unter folgen. [Erste Schritte](#)
- Der IAM-Prinzipal, der die Zuordnung erstellt, muss `iam:PassRole` haben.
- Die neueste Version der AWS CLI, die auf Ihrem Gerät installiert und konfiguriert ist, oder AWS CloudShell. Sie können Ihre aktuelle Version mit `aws --version | cut -d / -f2 | cut -d ' ' -f1` überprüfen. Paketmanager wie `yumapt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die in der installierte AWS CLI-Version AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen

zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).

- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called "Richten Sie kubectl und eksctl ein"](#).
- Eine vorhandene `kubectl config`-Datei, die Ihre Clusterkonfiguration enthält. Informationen zum Erstellen einer `kubectl config`-Datei finden Sie unter [the section called "Greifen Sie mit kubectl auf den Cluster zu"](#).

Erstellen Sie eine Pod Identity-Zuordnung (Konsole)AWS

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster aus. Wählen Sie anschließend den Namen des Clusters aus, für den Sie das Add-on „EKS Pod Identity Agent“ konfigurieren möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie in den Pod-Identity-Zuordnungen die Option Erstellen aus.
5. Wählen Sie als IAM-Rolle die IAM-Rolle mit den Berechtigungen aus, die die Workload haben soll.

 Note

Die Liste enthält nur Rollen mit der folgenden Vertrauensrichtlinie, die EKS Pod Identity ermöglicht, diese Rollen zu verwenden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEksAuthToAssumeRoleForPodIdentity",
      "Effect": "Allow",
      "Principal": {
        "Service": "pods.eks.amazonaws.com"
      },
      "Action": [
```

```
        "sts:AssumeRole",
        "sts:TagSession"
    ]
}
]
```

sts:AssumeRole— EKS Pod Identity verwendet `AssumeRole`, um die IAM-Rolle zu übernehmen, bevor die temporären Anmeldeinformationen an Ihre Pods weitergegeben werden.

sts:TagSession— EKS Pod Identity verwendet `TagSession`, um Sitzungs-Tags in die Anfragen an AWS STS aufzunehmen.

Sie können diese Tags in den Bedingungsschlüsseln in der Vertrauensrichtlinie verwenden, um einzuschränken, welche Dienstkonten, Namespaces und Cluster diese Rolle verwenden können.

Eine Liste der Amazon EKS-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für Amazon Elastic Kubernetes Service](#) in der Service-Autorisierungsreferenz. Um zu erfahren, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, lesen Sie von [Amazon Elastic Kubernetes Service definierte Aktionen](#).

6. Wählen Sie für den Kubernetes-Namespace den Kubernetes-Namespace aus, der das Dienstkonto und den Workload enthält. Optional können Sie einen Namespace nach Namen angeben, der im Cluster nicht existiert.
7. Wählen Sie für das Kubernetes-Dienstkonto das zu verwendende Kubernetes-Dienstkonto aus. Das Manifest für Ihren Kubernetes-Workload muss dieses Dienstkonto angeben. Optional können Sie ein Dienstkonto mit Namen angeben, das im Cluster nicht vorhanden ist.
8. (Optional) Wählen Sie für die Tags die Option `Tag` hinzufügen aus, um Metadaten in einem Schlüssel-Wert-Paar hinzuzufügen. Diese Tags werden auf die Zuordnung angewendet und können in IAM-Richtlinien verwendet werden.

Sie können diesen Schritt wiederholen, um mehrere Regionen hinzuzufügen.

9. Wählen Sie `Create` (Erstellen) aus.

Erstellen Sie eine Pod Identity-Zuordnung (AWS CLI)

1. Wenn Sie Ihrer IAM-Rolle eine vorhandene IAM-Richtlinie zuordnen möchten, fahren Sie mit dem nächsten Schritt fort.

Erstellen Sie eine IAM-Richtlinie. Sie können Ihre eigene Richtlinie erstellen oder eine AWS verwaltete Richtlinie kopieren, die bereits einige der benötigten Berechtigungen gewährt, und sie an Ihre spezifischen Anforderungen anpassen. Weitere Informationen finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

- a. Erstellen Sie eine Datei, die die Berechtigungen für die AWS Dienste enthält, auf die Ihre Pods zugreifen sollen. Eine Liste aller Aktionen für alle AWS Dienste finden Sie in der [Referenz zur Dienstautorisierung](#).

Sie können den folgenden Befehl ausführen, um eine Beispiel-Richtliniendatei zu erstellen, die schreibgeschützten Zugriff auf einen Amazon-S3-Bucket gewährt. Sie können optional Konfigurationsinformationen oder ein Bootstrap-Skript in diesem Bucket speichern, und die Container in Ihrem Pod können die Datei aus dem Bucket lesen und in Ihre Anwendung laden. Wenn Sie diese Beispielrichtlinie erstellen möchten, kopieren Sie den folgenden Inhalt auf Ihr Gerät. *my-pod-secrets-bucket* Ersetzen Sie es durch Ihren Bucket-Namen und führen Sie den Befehl aus.

```
cat >my-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::my-pod-secrets-bucket"
    }
  ]
}
EOF
```

- b. Erstellen Sie die IAM-Richtlinie.

```
aws iam create-policy --policy-name my-policy --policy-document file://my-policy.json
```

2. Erstellen Sie eine IAM-Rolle und verknüpfen Sie sie mit einem Kubernetes-Dienstkonto.

- a. Wenn Sie bereits ein Kubernetes-Dienstkonto haben, dem Sie eine IAM-Rolle zuweisen möchten, können Sie diesen Schritt überspringen.

Erstellen Sie ein Kubernetes-Servicekonto. Kopieren Sie den folgenden Inhalt auf Ihr Gerät.
my-service-account Ersetzen Sie es durch Ihren gewünschten Namen und gegebenenfalls *default* durch einen anderen Namespace. Wenn Sie eine Änderung vornehmen *default*, muss der Namespace bereits existieren.

```
cat >my-service-account.yaml <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
  name: my-service-account
  namespace: default
EOF
kubectl apply -f my-service-account.yaml
```

Führen Sie den folgenden Befehl aus.

```
kubectl apply -f my-service-account.yaml
```

- b. Führen Sie den folgenden Befehl aus, um eine Vertrauensrichtlinie für die IAM-Rolle zu erstellen.

```
cat >trust-relationship.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEksAuthToAssumeRoleForPodIdentity",
      "Effect": "Allow",
      "Principal": {
        "Service": "pods.eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
EOF
```

- c. Erstellen Sie die -Rolle. Ersetzen Sie *my-role* durch einen Namen für Ihre IAM-Rolle und *my-role-description* durch eine Beschreibung für Ihre Rolle.

```
aws iam create-role --role-name my-role --assume-role-policy-document file://trust-relationship.json --description "my-role-description"
```

- d. Hängen Sie eine IAM-Richtlinie an Ihre Rolle an. Ersetzen Sie *my-role* durch den Namen Ihrer IAM-Rolle und *my-policy* durch den Namen einer vorhandenen Richtlinie, die Sie erstellt haben.

```
aws iam attach-role-policy --role-name my-role --policy-arn=arn:aws:iam::111122223333:policy/my-policy
```

 Note

Im Gegensatz zu IAM-Rollen für Dienstkonten verwendet EKS Pod Identity keine Anmerkung zum Dienstkonto.

- e. Führen Sie den folgenden Befehl aus, um die Zuordnung zu erstellen. *my-cluster* Ersetzen Sie es durch den Namen des Clusters, *my-service-account* ersetzen Sie es durch Ihren gewünschten Namen und *default* gegebenenfalls durch einen anderen Namespace.

```
aws eks create-pod-identity-association --cluster-name my-cluster --role-arn arn:aws:iam::111122223333:role/my-role --namespace default --service-account my-service-account
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "association": {
    "clusterName": "my-cluster",
    "namespace": "default",
    "serviceAccount": "my-service-account",
    "roleArn": "arn:aws:iam::111122223333:role/my-role",
    "associationArn": "arn:aws:eks::111122223333:podidentityassociation/my-cluster/a-abcdefghijklmnop1",
    "associationId": "a-abcdefghijklmnop1",
    "tags": {},
    "createdAt": 1700862734.922,
    "modifiedAt": 1700862734.922
  }
}
```



```
}  
}
```

Note

Sie können einen Namespace und ein Dienstkonto nach Namen angeben, die im Cluster nicht vorhanden sind. Sie müssen den Namespace, das Servicekonto und die Workload erstellen, die das Servicekonto verwendet, damit die EKS-Pod-Identity-Zuordnung funktioniert.

Bestätigen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Vertrauensrichtlinie der IAM-Rolle korrekt konfiguriert ist.

```
aws iam get-role --role-name my-role --query Role.AssumeRolePolicyDocument
```

Eine Beispielausgabe sieht wie folgt aus.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Allow EKS Auth service to assume this role for Pod Identities",  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "pods.eks.amazonaws.com"  
      },  
      "Action": [  
        "sts:AssumeRole",  
        "sts:TagSession"  
      ]  
    }  
  ]  
}
```

2. Stellen Sie sicher, dass die Richtlinie, die Sie in einem vorherigen Schritt an Ihre Rolle angehängt haben, an die Rolle angehängt ist.

```
aws iam list-attached-role-policies --role-name my-role --query  
'AttachedPolicies[].PolicyArn' --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
arn:aws: iam::111122223333:policy/my-policy
```

3. Legen Sie eine Variable fest, um den Amazon-Ressourcennamen (ARN) der Richtlinie zu speichern, die Sie verwenden möchten. *my-policy* Ersetzen Sie es durch den Namen der Richtlinie, für die Sie die Berechtigungen bestätigen möchten.

```
export policy_arn=arn:aws: iam::111122223333:policy/my-policy
```

4. Zeigen Sie die Standardversion der Richtlinie an.

```
aws iam get-policy --policy-arn $policy_arn
```

Eine Beispielausgabe sieht wie folgt aus.

```
{  
  "Policy": {  
    "PolicyName": "my-policy",  
    "PolicyId": "EXAMPLEBIOWGLDEXAMPLE",  
    "Arn": "arn:aws: iam::111122223333:policy/my-policy",  
    "Path": "/",  
    "DefaultVersionId": "v1",  
    [...]  
  }  
}
```

5. Sehen Sie sich den Inhalt der Richtlinie an, um sicherzustellen, dass die Richtlinie alle Berechtigungen enthält, die Ihr Pod benötigt. Falls erforderlich, ersetzen Sie **1** den folgenden Befehl durch die Version, die in der vorherigen Ausgabe zurückgegeben wurde.

```
aws iam get-policy-version --policy-arn $policy_arn --version-id v1
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::my-pod-secrets-bucket"
  }
]
```

Wenn Sie die Beispielrichtlinie in einem vorherigen Schritt erstellt haben, ist Ihre Ausgabe dieselbe. Wenn Sie eine andere Richtlinie erstellt haben, ist der *example* Inhalt anders.

Nächste Schritte

[the section called “Pod-Dienstkonto”](#)

Zugreifen auf AWS Ressourcen mithilfe von EKS Pod Identity Target IAM-Rollen

Wenn Sie Anwendungen auf Amazon Elastic Kubernetes Service (Amazon EKS) ausführen, müssen Sie möglicherweise auf AWS Ressourcen zugreifen, die in denselben oder unterschiedlichen AWS Konten vorhanden sind. In dieser Anleitung erfahren Sie, wie Sie den Zugriff zwischen diesen Konten mithilfe von EKS Pod Identity einrichten, sodass Ihre Kubernetes-Pods auf andere Ressourcen zugreifen können. AWS

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Schritte abgeschlossen haben:

- [Den Amazon EKS Pod Identity Agent einrichten](#)
- [Erstellen Sie eine EKS Pod Identity-Rolle](#)

So funktioniert's

Mit Pod Identity können Anwendungen in Ihrem EKS-Cluster über einen Prozess, der als Rollenverkettung bezeichnet wird, kontenübergreifend auf AWS Ressourcen zugreifen. Wenn Sie eine Pod Identity-Zuordnung erstellen, können Sie zwei IAM-Rollen angeben — eine [EKS-Pod-Identity-Rolle](#) in demselben Konto wie Ihr EKS-Cluster und eine Ziel-IAM-Rolle aus dem Konto, das Ihre AWS Ressourcen enthält (wie S3-Buckets oder DynamoDB-Tabellen). Die [EKS-Pod-Identity-Rolle](#) muss sich aufgrund der [PassRoleIAM-Anforderungen im Konto Ihres EKS-Clusters](#)

[befinden, während sich die Ziel-IAM-Rolle](#) in jedem Konto befinden kann. AWS PassRole ermöglicht es einer AWS Entität, die Rollenübernahme an einen anderen Dienst zu delegieren. EKS Pod Identity verwendet PassRole, um eine Rolle mit einem Kubernetes-Dienstkonto zu verbinden. Dabei müssen sich sowohl die Rolle als auch die Identität, die sie übergibt, in demselben AWS Konto wie der EKS-Cluster befinden. Wenn Ihr Anwendungs-Pod auf AWS Ressourcen zugreifen muss, fordert er Anmeldeinformationen von Pod Identity an. Pod Identity führt dann automatisch nacheinander zwei Rollenannahmen durch: zuerst übernimmt sie die [EKS-Pod-Identity-Rolle](#) und verwendet dann diese Anmeldeinformationen, um die Ziel-IAM-Rolle anzunehmen. Durch diesen Vorgang erhält Ihr Pod temporäre Anmeldeinformationen mit den in der Zielrolle definierten Berechtigungen, sodass ein sicherer Zugriff auf Ressourcen in anderen AWS Konten möglich ist.

Überlegungen zum Zwischenspeichern

Aufgrund von Caching-Mechanismen werden Aktualisierungen einer IAM-Rolle in einer bestehenden Pod-Identity-Zuordnung möglicherweise nicht sofort in den Pods wirksam, die auf Ihrem EKS-Cluster ausgeführt werden. Der Pod Identity Agent speichert die IAM-Anmeldeinformationen auf der Grundlage der Konfiguration der Zuordnung zum Zeitpunkt des Abrufs der Anmeldeinformationen im Cache. Wenn die Zuordnung nur einen ARN für die [EKS-Pod-Identity-Rolle](#) und keine Ziel-IAM-Rolle enthält, sind die zwischengespeicherten Anmeldeinformationen 6 Stunden lang gültig. Wenn die Zuordnung sowohl den ARN der [EKS-Pod-Identity-Rolle](#) als auch eine Ziel-IAM-Rolle umfasst, sind die zwischengespeicherten Anmeldeinformationen 59 Minuten lang gültig. Durch das Ändern einer vorhandenen Zuordnung, z. B. das Aktualisieren des ARN der [EKS-Pod-Identity-Rolle](#) oder das Hinzufügen einer Ziel-IAM-Rolle, wird der vorhandene Cache nicht zurückgesetzt. Daher erkennt der Agent Aktualisierungen erst, wenn die zwischengespeicherten Anmeldeinformationen aktualisiert werden. Um Änderungen früher zu übernehmen, können Sie die vorhandenen Pods neu erstellen. Andernfalls müssen Sie warten, bis der Cache abläuft.

Schritt 1: Eine Ziel-IAM-Rolle erstellen und zuordnen

In diesem Schritt richten Sie eine sichere Vertrauenskette ein, indem Sie eine Ziel-IAM-Rolle erstellen und konfigurieren. Zur Veranschaulichung erstellen wir eine neue Target-IAM-Rolle, um eine Vertrauenskette zwischen zwei AWS Konten einzurichten: Die [EKS Pod Identity-Rolle](#) (z. B. eks-pod-identity-primary-role) im AWS Konto des EKS-Clusters erhält die Erlaubnis, die Target-IAM-Rolle (z. B. eks-pod-identity-aws-resources) in Ihrem Zielkonto zu übernehmen, wodurch der Zugriff auf AWS Ressourcen wie Amazon S3 S3-Buckets ermöglicht wird.

Erstellen Sie die Ziel-IAM-Rolle

1. Öffnen Sie die [Amazon IAM-Konsole](#).

2. Vergewissern Sie sich in der oberen Navigationsleiste, dass Sie bei dem Konto angemeldet sind, das die AWS Ressourcen (wie S3-Buckets oder DynamoDB-Tabellen) für Ihre Target IAM-Rolle enthält.
3. Wählen Sie im linken Navigationsbereich Roles aus.
4. Wählen Sie die Schaltfläche „Rolle erstellen“ und anschließend „AWS Konto“ unter „Vertrauenswürdiger Entitätstyp“.
5. Wählen Sie Anderes AWS Konto, geben Sie Ihre AWS Kontonummer ein (das Konto, für das Ihre [EKS Pod Identity-Rolle](#) existiert) und wählen Sie dann Weiter.
6. Fügen Sie die Berechtigungsrichtlinien hinzu, die Sie der Rolle zuordnen möchten (z. B. AmazonS3FullAccess), und wählen Sie dann Weiter.
7. Geben Sie einen Rollennamen ein, z. B. MyCustomIAMTargetRole, und wählen Sie dann Rolle erstellen aus.

Aktualisieren Sie die Vertrauensrichtlinie für die IAM-Zielrolle

1. Nachdem Sie die Rolle erstellt haben, kehren Sie zur Rollenliste zurück. Suchen Sie die neue Rolle, die Sie im vorherigen Schritt erstellt haben, und wählen Sie sie aus (z. B. MyCustomIAMTargetRole).
2. Wählen Sie den Tab Vertrauensbeziehungen.
3. Klicken Sie auf der rechten Seite auf Vertrauensrichtlinie bearbeiten.
4. Ersetzen Sie im Richtlinien-Editor den Standard-JSON durch Ihre Vertrauensrichtlinie. Ersetzen Sie die Platzhalterwerte für den Rollennamen und 111122223333 im ARN der IAM-Rolle durch die AWS Konto-ID, die Ihren EKS-Cluster hostet. Zum Beispiel:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/eks-pod-identity-primary-role"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
```

```

    "Principal": {
      "AWS": "arn:aws: iam::111122223333:role/eks-pod-identity-primary-role"
    },
    "Action": "sts:TagSession"
  }
]
}

```

Aktualisieren Sie die Berechtigungsrichtlinie für die EKS Pod Identity-Rolle

In diesem Schritt aktualisieren Sie die Berechtigungsrichtlinie der [EKS Pod Identity-Rolle](#), die Ihrem Amazon EKS-Cluster zugeordnet ist, indem Sie den Target IAM Role ARN als Ressource hinzufügen.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Clusters und dann den Namen Ihres EKS-Clusters aus.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie unter Pod Identity-Verknüpfungen Ihre [EKS Pod Identity-Rolle](#) aus.
5. Wählen Sie Berechtigungen, Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
6. Wählen Sie auf der rechten Seite JSON aus.
7. Ersetzen Sie im Richtlinien-Editor den Standard-JSON durch Ihre Berechtigungsrichtlinie. Ersetzen Sie den Platzhalterwert für den Rollennamen und 222233334444 im ARN der IAM-Rolle durch Ihre Ziel-IAM-Rolle. Zum Beispiel:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource": "arn:aws: iam::222233334444:role/eks-pod-identity-aws-
resources"
    }
  ]
}

```

Schritt 2: Ordnen Sie die Ziel-IAM-Rolle einem Kubernetes-Dienstkonto zu

In diesem Schritt erstellen Sie eine Zuordnung zwischen der Target-IAM-Rolle und dem Kubernetes-Dienstkonto in Ihrem EKS-Cluster.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster und dann den Namen des Clusters aus, dem Sie die Zuordnung hinzufügen möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie in den Pod-Identity-Zuordnungen die Option Erstellen aus.
5. Wählen Sie die [EKS Pod Identity-Rolle](#) in der IAM-Rolle aus, die Ihre Workloads annehmen sollen.
6. Wählen Sie in der Target-IAM-Rolle die Target-IAM-Rolle aus, die von der [EKS](#) Pod Identity-Rolle übernommen werden soll.
7. Geben Sie im Feld Kubernetes-Namespace den Namen des Namespaces ein, in dem Sie die Zuordnung erstellen möchten (z. B.). my-app-namespace Dies definiert, wo sich das Dienstkonto befindet.
8. Geben Sie im Feld Kubernetes-Dienstkonto den Namen des Dienstkontos ein (z. B. my-service-account), das die IAM-Anmeldeinformationen verwenden wird. Dadurch wird die IAM-Rolle mit dem Dienstkonto verknüpft.
9. Wählen Sie Erstellen aus, um die Zuordnung zu erstellen.

(Optional) Schritt 3: Fügen Sie einer IAM-Zielrolle externe Berechtigungen hinzu

Manchmal müssen Sie möglicherweise einer dritten Partei Zugriff auf Ihre AWS Ressourcen gewähren (Delegiertenzugriff). Sie entscheiden sich beispielsweise dafür, ein Drittanbieter namens Example Corp mit der Überwachung Ihres AWS Kontos und der Kostenoptimierung zu beauftragen. Um Ihre täglichen Ausgaben verfolgen zu können, muss Example Corp auf Ihre AWS Ressourcen zugreifen. In diesem Fall empfehlen wir, der Vertrauensrichtlinie Ihrer IAM-Zielrolle eine hinzuzufügen, ExternalId um mögliche Probleme mit [Confused Deputy](#) zu vermeiden.

Bearbeiten Sie die Vertrauensrichtlinie

1. Nachdem Sie die Rolle erstellt haben, kehren Sie zur Rollenliste zurück. Suchen Sie die neue Rolle, die Sie im vorherigen Schritt erstellt haben, und klicken Sie darauf (z. B. MyCustomIAMTargetRole).
2. Wählen Sie den Tab Vertrauensbeziehungen.

3. Klicken Sie auf der rechten Seite auf Vertrauensrichtlinie bearbeiten.
4. Ersetzen Sie im Richtlinien-Editor den Standard-JSON durch Ihre Vertrauensrichtlinie. Ersetzen Sie den ExternalId Platzhalterwert für `aws-region/other-account/cluster-name/namespace/service-account-name`, wobei „Region“ die AWS Region Ihres Clusters, „111122223333“ die andere AWS Konto-ID, „Clustername“ der EKS-Clustername, „Namespace“ der Kubernetes-Namespace und "" der Kubernetes-Dienstkontoname ist. service-account-name
Zum Beispiel:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws: iam::111122223333:role/eks-pod-identity-primary-role"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "region/111122223333/cluster-name/namespace/
service-account-name"
        }
      },
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws: iam::111122223333:role/eks-pod-identity-primary-role"
      },
      "Action": "sts:TagSession"
    }
  ]
}
```

Pods für den Zugriff auf AWS Dienste mit Dienstkonten konfigurieren

Wenn ein Pod auf AWS Dienste zugreifen muss, müssen Sie ihn für die Verwendung eines Kubernetes-Dienstkontos konfigurieren. Das Dienstkonto muss einer AWS Identity and Access Management (IAM) -Rolle zugeordnet sein, die über Berechtigungen für den Zugriff auf die AWS Dienste verfügt.

- Einen vorhandenen -Cluster. Falls Sie noch keinen haben, können Sie ihn mithilfe einer der Anleitungen unter erstellen. [Erste Schritte](#)
 - Ein vorhandenes Kubernetes-Dienstkonto und eine EKS Pod Identity-Zuordnung, die das Dienstkonto einer IAM-Rolle zuordnet. Der Rolle muss eine IAM-Richtlinie zugeordnet sein, die die Berechtigungen enthält, die Ihre Pods für die Nutzung von Diensten benötigen sollen. AWS Weitere Informationen zu Rollen, ihren Vorteilen sowie zu ihrer Erstellung und Konfiguration finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).
 - Die neueste Version der AWS CLI, die auf Ihrem Gerät installiert und konfiguriert ist, oder AWS CloudShell. Sie können Ihre aktuelle Version mit `aws --version | cut -d / -f2 | cut -d ' ' -f1` überprüfen. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit `aws configure`](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die in der installierte AWS CLI-Version AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
 - Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie `kubectl` und `eksctl` ein”](#).
 - Eine vorhandene `kubectl config`-Datei, die Ihre Clusterkonfiguration enthält. Informationen zum Erstellen einer `kubectl config`-Datei finden Sie unter [the section called “Greifen Sie mit `kubectl` auf den Cluster zu”](#).
1. Verwenden Sie den folgenden Befehl, um ein Bereitstellungsmanifest zu erstellen, mit dem Sie einen Pod bereitstellen können, um die Konfiguration zu bestätigen. Ersetzen Sie *example values* durch Ihre eigenen Werte.

```
cat >my-deployment.yaml <<EOF
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  selector:
    matchLabels:
```

```
    app: my-app
  template:
    metadata:
      labels:
        app: my-app
    spec:
      serviceAccountName: my-service-account
      containers:
      - name: my-app
        image: public.ecr.aws/nginx/nginx:X.XX
EOF
```

2. Stellen Sie das Manifest in Ihrem Cluster bereit.

```
kubectl apply -f my-deployment.yaml
```

3. Vergewissern Sie sich, dass die erforderlichen Umgebungsvariablen für Ihren Pod vorhanden sind.

- a. Sehen Sie sich die Pods an, die im vorherigen Schritt mit der Bereitstellung bereitgestellt wurden.

```
kubectl get pods | grep my-app
```

Eine Beispielausgabe sieht wie folgt aus.

```
my-app-6f4dfff6cb-76cv9    1/1    Running    0    3m28s
```

- b. Vergewissern Sie sich, dass der Pod über eine Tokendatei für ein Dienstkonto verfügt.

```
kubectl describe pod my-app-6f4dfff6cb-76cv9 | grep
AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE:
```

Eine Beispielausgabe sieht wie folgt aus.

```
AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE: /var/run/secrets/
pods.eks.amazonaws.com/serviceaccount/eks-pod-identity-token
```

4. Vergewissern Sie sich, dass Ihre Pods mithilfe der Berechtigungen, die Sie in der IAM-Richtlinie für Ihre Rolle zugewiesen haben, mit den AWS Diensten interagieren können.

 Note

Wenn ein Pod AWS Anmeldeinformationen von einer IAM-Rolle verwendet, die mit einem Dienstkonto verknüpft ist, verwendet die AWS CLI oder andere SDKs in den Containern für diesen Pod die Anmeldeinformationen, die von dieser Rolle bereitgestellt werden. Wenn Sie den Zugriff auf die Anmeldeinformationen, die für die [IAM-Rolle des Amazon EKS-Knotens](#) bereitgestellt werden, nicht einschränken, hat der Pod weiterhin Zugriff auf diese Anmeldeinformationen. Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

Wenn Ihre Pods nicht wie erwartet mit den Diensten interagieren können, führen Sie die folgenden Schritte durch, um sicherzustellen, dass alles ordnungsgemäß konfiguriert ist.

- a. Vergewissern Sie sich, dass Ihre Pods eine AWS SDK-Version verwenden, die die Übernahme einer IAM-Rolle über eine EKS Pod Identity-Zuordnung unterstützt. Weitere Informationen finden Sie unter [the section called "Unterstützt SDKs"](#).
- b. Stellen Sie sicher, dass die Bereitstellung das Servicekonto verwendet.

```
kubectl describe deployment my-app | grep "Service Account"
```

Eine Beispielausgabe sieht wie folgt aus.

```
Service Account:  my-service-account
```

Pods Zugriff auf AWS Ressourcen basierend auf Tags gewähren

Die attributebasierte Zugriffskontrolle (ABAC) gewährt Benutzern Rechte durch Richtlinien, die Attribute miteinander kombinieren. EKS Pod Identity fügt den temporären Anmeldeinformationen für jeden Pod Tags mit Attributen wie Clusternamen, Namespace und Dienstkontonamen hinzu. Diese Rollensitzungs-Tags ermöglichen es Administratoren, eine einzelne Rolle zu erstellen, die für alle Dienstkonten verwendet werden kann, indem sie den Zugriff auf AWS Ressourcen auf der Grundlage übereinstimmender Tags ermöglicht. Durch die zusätzliche Unterstützung für Rollensitzungs-Tags können Sie engere Sicherheitsgrenzen zwischen Clustern und Workloads innerhalb von Clustern durchsetzen und gleichzeitig dieselben IAM-Rollen und IAM-Richtlinien wiederverwenden.

Beispielrichtlinie mit Tags

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die `s3:GetObject` Berechtigungen gewährt, wenn das entsprechende Objekt mit dem EKS-Clusternamen gekennzeichnet ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/eks-cluster-name": "${aws:PrincipalTag/eks-cluster-name}"
        }
      }
    }
  ]
}
```

Aktivieren oder deaktivieren Sie Sitzungs-Tags

EKS Pod Identity fügt einen vordefinierten Satz von Sitzungs-Tags hinzu, wenn es die Rolle übernimmt. Diese Sitzungs-Tags ermöglichen es Administratoren, eine einzelne Rolle zu erstellen, die ressourcenübergreifend funktioniert, indem sie den Zugriff auf Ressourcen auf der Grundlage übereinstimmender Tags ermöglicht. AWS

Sitzungs-Tags aktivieren

Sitzungs-Tags werden mit EKS Pod Identity automatisch aktiviert — es sind keine Maßnahmen Ihrerseits erforderlich. Standardmäßig fügt EKS Pod Identity Ihrer Sitzung eine Reihe vordefinierter

Tags hinzu. Um in Richtlinien auf diese Tags zu verweisen, verwenden Sie die Syntax, `${aws:PrincipalTag/}` gefolgt vom Tag-Schlüssel. Beispiel, `${aws:PrincipalTag/kubernetes-namespace}`.

- `eks-cluster-arn`
- `eks-cluster-name`
- `kubernetes-namespace`
- `kubernetes-service-account`
- `kubernetes-pod-name`
- `kubernetes-pod-uid`

Deaktivieren Sie Sitzungs-Tags

AWS komprimiert Inline-Sitzungsrichtlinien, verwaltete Richtlinien ARNs und Sitzungs-Tags in ein gepacktes Binärformat, für das ein separates Limit gilt. Wenn Sie eine `PackedPolicyTooLarge` Fehlermeldung erhalten, die besagt, dass das gepackte Binärformat die Größenbeschränkung überschritten hat, können Sie versuchen, die Größe zu reduzieren, indem Sie die von EKS Pod Identity hinzugefügten Sitzungs-Tags deaktivieren. Gehen Sie folgendermaßen vor, um diese Sitzungs-Tags zu deaktivieren:

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster und dann den Namen des Clusters aus, den Sie ändern möchten.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie in den Pod-Identity-Zuordnungen die Zuordnungs-ID, die Sie ändern möchten, unter Zuordnungs-ID aus, und klicken Sie dann auf Bearbeiten.
5. Wählen Sie unter Sitzungs-Tags die Option Sitzungs-Tags deaktivieren aus.
6. Wählen Sie Änderungen speichern aus.

Kontoübergreifende Tags

Alle Sitzungs-Tags, die von EKS Pod Identity hinzugefügt werden, sind transitiv. Die Tag-Schlüssel und -Werte werden an alle `AssumeRole`-Aktionen weitergegeben, die Ihre Workloads verwenden, um Rollen auf ein anderes Konto zu wechseln. Sie können diese Tags in Richtlinien in anderen

Konten verwenden, um den Zugriff in kontoübergreifenden Szenarien einzuschränken. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Verketten von Rollen mit Sitzungs-Tags](#).

Benutzerdefinierte Tags

EKS Pod Identity kann der AssumeRole Aktion, die es ausführt, keine zusätzlichen benutzerdefinierten Tags hinzufügen. Tags, die Sie auf die IAM-Rolle anwenden, sind jedoch immer in demselben Format verfügbar: `${aws:PrincipalTag/}` gefolgt vom Schlüssel, zum Beispiel `${aws:PrincipalTag/MyCustomTag}`.

Note

Tags, die der Sitzung über die `sts:AssumeRole`-Anfrage hinzugefügt wurden, haben im Konfliktfall Vorrang. Sagen Sie zum Beispiel:

- Amazon EKS fügt der Sitzung einen Schlüssel `eks-cluster-name` und Mehrwert `my-cluster` hinzu, wenn EKS die Kundenrolle übernimmt und
- Sie fügen der IAM-Rolle ein `eks-cluster-name` Tag mit dem Wert `my-own-cluster` hinzu.

In diesem Fall hat Ersteres Vorrang und der Wert für das `eks-cluster-name` Tag lautet `my-cluster`.

Pod-Identität mit dem AWS SDK verwenden

Verwenden von EKS-Pod-Identity-Anmeldeinformationen

Um die Anmeldeinformationen einer EKS Pod Identity-Zuordnung zu verwenden, kann Ihr Code jedes AWS SDK verwenden, um einen Client für einen AWS Dienst mit einem SDK zu erstellen. Standardmäßig sucht das SDK in einer Kette von Speicherorten nach AWS Identity and Access Management-Anmeldeinformationen, die verwendet werden können. Die EKS Pod Identity-Anmeldeinformationen werden verwendet, wenn Sie bei der Erstellung des Clients keinen Anmeldeinformationsanbieter angeben oder das SDK anderweitig initialisiert haben.

Das funktioniert, weil EKS-Pod-Identitäten dem Anbieter für Container-Anmeldeinformationen hinzugefügt wurden, der in einem Schritt in der standardmäßigen Anmeldeinformationskette durchsucht wird. Wenn Ihre Workloads derzeit Anmeldeinformationen verwenden, die in der Kette

der Anmeldeinformationen weiter vorn stehen, werden diese Anmeldeinformationen auch dann weiter verwendet, wenn Sie eine EKS-Pod-Identity-Zuordnung für dieselbe Workload konfigurieren.

Weitere Informationen zur Funktionsweise von EKS-Pod-Identitäten finden Sie unter [the section called “Funktionsweise”](#).

Wenn Sie [Learn how EKS Pod Identity Pod Identity verwenden, um Pods Zugriff auf AWS Dienste zu gewähren](#), müssen die Container in Ihren Pods eine AWS SDK-Version verwenden, die die Übernahme einer IAM-Rolle vom EKS Pod Identity Agent unterstützt. Stellen Sie sicher, dass Sie die folgenden Versionen oder höher für Ihr AWS SDK verwenden:

- Java (Version 2) – [2.21.30](#)
- Java — [1.12.746](#)
- Go v1 – [v1.47.11](#)
- Go v2 – [release-2023-11-14](#)
- [Python \(Boto3\) — 1.34.41](#)
- [Python \(Botocore\) — 1.34.41](#)
- AWS CLI — [1,30,0](#)

AWS CLI — [2.15.0](#)

- JavaScript [v2 — 2.1550,0](#)
- JavaScript [v3 — v3.458.0](#)
- [Kotlin — v1.0.1](#)
- Ruby – [3.188.0](#)
- [Rust — Veröffentlichung 2024-03-13](#)
- C++ — [1.11.263](#)
- [.NET — 3.7.734.0](#)
- PowerShell — [4.1.502](#)
- PHP – [3.287.1](#)

Um sicherzustellen, dass Sie ein unterstütztes SDK verwenden, folgen Sie AWS beim Erstellen Ihrer Container den Installationsanweisungen für Ihr bevorzugtes SDK unter [Tools to Build On](#).

Eine Liste der Add-Ons, die EKS Pod Identity unterstützen, finden Sie unter [the section called “Referenz zur Support von Pod Identity”](#).

IPv6 Im EKS Pod Identity Agent deaktivieren

AWS Management Console

1. Fügen Sie zur Deaktivierung IPv6 im EKS Pod Identity Agent die folgende Konfiguration zu den optionalen Konfigurationseinstellungen des EKS Add-ons hinzu.
 - a. Öffnen Sie die [Amazon-EKS-Konsole](#).
 - b. Wählen Sie im linken Navigationsbereich Clusters (Cluster) aus. Wählen Sie anschließend den Namen des Clusters aus, für den Sie das Add-On konfigurieren möchten.
 - c. Wählen Sie die Registerkarte Add-ons.
 - d. Wählen Sie das Feld oben rechts im EKS Pod Identity Agent-Add-On-Feld aus und wählen Sie dann Bearbeiten.
 - e. Gehen Sie auf der Seite EKS Pod Identity Agent konfigurieren wie folgt vor:
 - i. Wählen Sie die Version aus, die Sie verwenden möchten. Wir empfehlen, dieselbe Version wie im vorherigen Schritt beizubehalten und die Version und Konfiguration in separaten Aktionen zu aktualisieren.
 - ii. Erweitern Sie Optionale Konfigurationseinstellungen.
 - iii. Geben Sie den JSON-Schlüssel "agent": und den JSON-Wert eines verschachtelten JSON-Objekts mit einem Schlüssel "additionalArgs": im Feld Konfigurationswerte ein. Der resultierende Text muss ein gültiges JSON-Objekt sein. Wenn dieser Schlüssel und dieser Wert die einzigen Daten im Textfeld sind, setzen Sie den Schlüssel und den Wert in geschweifte Klammern { }. Das folgende Beispiel zeigt, dass die Netzwerkrichtlinie aktiviert ist:
- ```
{
 "agent": {
 "additionalArgs": {
 "-b": "169.254.170.23"
 }
 }
}
```
- Diese Konfiguration legt fest, dass die IPv4 Adresse die einzige Adresse ist, die vom Agenten verwendet wird.
- f. Um die neue Konfiguration anzuwenden, indem die EKS Pod Identity Agent-Pods ersetzt werden, wählen Sie Änderungen speichern.



Amazon EKS wendet Änderungen an den EKS-Add-Ons mithilfe eines Rollouts des Kubernetes DaemonSet for EKS Pod Identity Agent an. Sie können den Status des Rollouts im Update-Verlauf des Add-ons in und mit verfolgen. AWS Management Console `kubectl rollout status daemonset/eks-pod-identity-agent --namespace kube-system`

`kubectl rollout` hat die folgenden Befehle:

```
$ kubectl rollout

history -- View rollout history
pause -- Mark the provided resource as paused
restart -- Restart a resource
resume -- Resume a paused resource
status -- Show the status of the rollout
undo -- Undo a previous rollout
```

Wenn der Rollout zu lange dauert, macht Amazon EKS den Rollout rückgängig und eine Meldung mit dem Typ `Addon-Update` und dem Status `Fehlgeschlagen` wird zum Update-Verlauf des Add-ons hinzugefügt. Um Probleme zu untersuchen, beginnen Sie mit dem Verlauf des Rollouts und führen Sie ihn `kubectl logs` auf einem EKS Pod Identity Agent-Pod aus, um die Protokolle von EKS Pod Identity Agent einzusehen.

2. Wenn der neue Eintrag im Update-Verlauf den Status `Erfolgreich` hat, ist der Rollout abgeschlossen und das Add-on verwendet die neue Konfiguration in allen EKS Pod Identity Agent-Pods.

## AWS CLI

1. Fügen Sie zur Deaktivierung IPv6 im EKS Pod Identity Agent die folgende Konfiguration zu den Konfigurationswerten des EKS Add-ons hinzu.

Führen Sie den folgenden AWS CLI-Befehl aus. Ersetzen Sie `my-cluster` durch den Namen Ihres Clusters und den IAM-Rollen-ARN durch die Rolle, die Sie verwenden.

```
aws eks update-addon --cluster-name my-cluster --addon-name eks-pod-identity-agent \
 --resolve-conflicts PRESERVE --configuration-values '{"agent":{"additionalArgs":
 { "-b": "169.254.170.23"}}}'
```

Diese Konfiguration legt fest, dass die IPv4 Adresse die einzige Adresse ist, die vom Agenten verwendet wird.

Amazon EKS wendet Änderungen an den EKS-Add-Ons mithilfe eines Rollouts des Kubernetes DaemonSet for EKS Pod Identity Agent an. Sie können den Status des Rollouts im Update-Verlauf des Add-ons in und mit verfolgen. AWS Management Console `kubectl rollout status daemonset/eks-pod-identity-agent --namespace kube-system`

`kubectl rollout` hat die folgenden Befehle:

```
kubectl rollout

history -- View rollout history
pause -- Mark the provided resource as paused
restart -- Restart a resource
resume -- Resume a paused resource
status -- Show the status of the rollout
undo -- Undo a previous rollout
```

Wenn der Rollout zu lange dauert, macht Amazon EKS den Rollout rückgängig und eine Meldung mit dem Typ Addon-Update und dem Status Fehlgeschlagen wird zum Update-Verlauf des Add-ons hinzugefügt. Um Probleme zu untersuchen, beginnen Sie mit dem Verlauf des Rollouts und führen Sie ihn `kubectl logs` auf einem EKS Pod Identity Agent-Pod aus, um die Protokolle von EKS Pod Identity Agent einzusehen.

Erstellen Sie eine IAM-Rolle mit der für EKS Pod Identity erforderlichen Vertrauensrichtlinie

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "AllowEksAuthToAssumeRoleForPodIdentity",
 "Effect": "Allow",
 "Principal": {
 "Service": "pods.eks.amazonaws.com"
 },
 "Action": [
 "sts:AssumeRole",
```

```
 "sts:TagSession"
]
}
]
```

## **sts:AssumeRole**

EKS Pod Identity nutzt AssumeRole, um die IAM-Rolle anzunehmen, bevor es die temporären Anmeldeinformationen an Ihre Pods übergibt.

## **sts:TagSession**

EKS Pod Identity verwendet TagSession, um Sitzungs-Tags in die Anfragen an STS aufzunehmen. AWS

Sie können diese Tags in den Bedingungsschlüsseln in der Vertrauensrichtlinie verwenden, um einzuschränken, welche Dienstkonten, Namespaces und Cluster diese Rolle verwenden können.

Eine Liste der Amazon EKS-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für Amazon Elastic Kubernetes Service](#) in der Service-Autorisierungsreferenz. Um zu erfahren, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, lesen Sie von [Amazon Elastic Kubernetes Service definierte Aktionen](#).

# Rechenressourcen mithilfe von Knoten verwalten

Ein Kubernetes-Knoten ist eine Maschine, auf der containerisierte Anwendungen ausgeführt werden. Jeder Knoten umfasst die folgenden Komponenten:

- [Container-Laufzeit](#) — Software, die für den Betrieb der Container verantwortlich ist.
- [kubelet](#) — Stellt sicher, dass Container fehlerfrei sind und innerhalb des zugehörigen Pods ausgeführt werden.
- [kube-proxy](#) — Verwaltet Netzwerkregeln, die die Kommunikation mit Ihren Pods ermöglichen.

Weitere Informationen finden Sie unter [Nodes](#) in der Kubernetes-Dokumentation.

Ihr Amazon EKS-Cluster kann Pods auf einer beliebigen Kombination von [verwalteten EKS-Automodus-Knoten](#), [selbstverwalteten Knoten](#), von [Amazon EKS verwalteten Knotengruppen](#), [AWS Fargate](#) und [Amazon EKS-Hybridknoten](#) planen. Weitere Informationen zu Knoten, die in Ihrem Cluster bereitgestellt werden, finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

## Note

Mit Ausnahme von Hybridknoten müssen sich die Knoten in derselben VPC befinden wie die Subnetze, die Sie bei der Erstellung des Clusters ausgewählt haben. Die Knoten müssen sich jedoch nicht in denselben Subnetzen befinden.

## Vergleichen Sie die Rechenoptionen

Die folgende Tabelle enthält mehrere Kriterien, die bei der Entscheidung ausgewertet werden müssen, welche Optionen Ihren Anforderungen am besten entsprechen. Selbstverwaltete Knoten sind eine weitere Option, die alle aufgeführten Kriterien unterstützen, aber sie erfordern viel mehr manuelle Wartung. Weitere Informationen finden Sie unter [the section called “Selbstverwaltete Knoten”](#).

**Note**

Bottlerocket weist einige spezifische Unterschiede zu den allgemeinen Informationen in dieser Tabelle auf. [Weitere Informationen finden Sie in der Bottlerocket-Dokumentation unter GitHub](#)

| Kriterien                                                           | EKS-verwaltete Knotengruppen                 | Automatischer EKS-Modus | Amazon EKS-Hybridknoten |
|---------------------------------------------------------------------|----------------------------------------------|-------------------------|-------------------------|
| Kann in <a href="#">AWS Outposts</a> eingesetzt werden              | Nein                                         | Nein                    | Nein                    |
| Kann auf eine <a href="#">AWS Lokale Zone</a> bereitgestellt werden | Ja                                           | Nein                    | Nein                    |
| Kann Container ausführen, die Windows benötigen                     | Ja                                           | Nein                    | Nein                    |
| Kann Container ausführen, die Linux benötigen                       | Ja                                           | Ja                      | Ja                      |
| Kann Workloads ausführen, die den Inferentia-Chip benötigen         | <a href="#">Ja</a> – nur Amazon-Linux-Knoten | Ja                      | Nein                    |
| Kann Workloads ausführen, die eine GPU benötigen                    | <a href="#">Ja</a> – nur Amazon-Linux-Knoten | Ja                      | Ja                      |
| Kann Workloads ausführen, die                                       | <a href="#">Ja</a>                           | Ja                      | Ja                      |

| Kriterien                                                                                   | EKS-verwaltete Knotengruppen | Automatischer EKS-Modus                                                | Amazon EKS-Hybridknoten                                                                                                                         |
|---------------------------------------------------------------------------------------------|------------------------------|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Arm-Prozessoren benötigen                                                                   |                              |                                                                        |                                                                                                                                                 |
| Kann ausgeführt werden AWS <a href="#">Bottlerocket</a>                                     | Ja                           | Ja                                                                     | Nein                                                                                                                                            |
| Pods teilen sich CPU-, Arbeitsspeicher-, Speicher- und Netzwerkressourcen mit anderen Pods. | Ja                           | Ja                                                                     | Ja                                                                                                                                              |
| EC2 Amazon-Instances müssen bereitgestellt und verwaltet werden                             | Ja                           | Nein — Erfahren Sie mehr über <a href="#">EC2 verwaltete Instances</a> | Ja — die physischen oder virtuellen Maschinen vor Ort werden von Ihnen mit den Tools Ihrer Wahl verwaltet.                                      |
| Muss das Betriebssystem von EC2 Amazon-Instances sichern, warten und patchen                | Ja                           | Nein                                                                   | Ja — das Betriebssystem, das auf Ihren physischen oder virtuellen Maschinen ausgeführt wird, wird von Ihnen mit den Tools Ihrer Wahl verwaltet. |

| Kriterien                                                                                                                      | EKS-verwaltete Knotengruppen                                                                                                                                     | Automatischer EKS-Modus                                                                  | Amazon EKS-Hybridknoten                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kann bei der Bereitstellung eines Knotens Bootstrap-Argumente angegeben, z. B. zusätzliche <a href="#">Kubelet-Argumente</a> . | Ja — Verwendung <code>eksctl</code> oder einer <a href="#">Startvorlage</a> mit einem benutzerdefinierten AMI.                                                   | Nein — <a href="#">Verwenden Sie <code>aNodeClass</code>, um Knoten zu konfigurieren</a> | Ja — Sie können Bootstrap-Argumente mit <code>nodeadm</code> anpassen. Siehe <a href="#">the section called “Hybridknoten <code>nodeadm</code>”</a> . |
| Kann Pods IP-Adressen aus einem anderen CIDR-Block als der dem Knoten zugewiesenen IP-Adresse zuweisen.                        | Ja – Verwenden einer Startvorlage mit einem benutzerdefinierten AMI. Weitere Informationen finden Sie unter <a href="#">the section called “Startvorlagen”</a> . | Nein                                                                                     | Ja — siehe <a href="#">the section called “CNI konfigurieren”</a> .                                                                                   |
| SSH im Knoten nicht möglich                                                                                                    | Ja                                                                                                                                                               | Nein — <a href="#">Erfahren Sie, wie Sie Probleme mit Knoten beheben</a>                 | Ja                                                                                                                                                    |
| Kann Ihr eigenes benutzerdefiniertes AMI auf Knoten bereitstellen                                                              | Ja – Verwenden eines <a href="#">Startvorlage</a>                                                                                                                | Nein                                                                                     | Ja                                                                                                                                                    |
| Kann Ihr eigenes benutzerdefiniertes CNI auf Knoten bereitstellen                                                              | Ja – Verwenden eines <a href="#">Startvorlage</a> mit einem benutzerdefinierten AMI                                                                              | Nein                                                                                     | Ja                                                                                                                                                    |

| Kriterien                                  | EKS-verwaltete Knotengruppen                                                                                                                                                                                                                                                                                                                                                                                                                            | Automatischer EKS-Modus | Amazon EKS-Hybridknoten                                                                                                                                                                                                |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Knoten-AMI muss selbst aktualisiert werden | <a href="#">Ja</a> — Wenn Sie ein für Amazon EKS optimiertes AMI bereitgestellt haben, werden Sie in der Amazon EKS-Konsole benachrichtigt, wenn Updates verfügbar sind. Sie können die Aktualisierung mit einem Klick in der Konsole durchführen. Wenn Sie ein benutzerdefiniertes AMI bereitgestellt haben, werden Sie in der Amazon EKS-Konsole nicht benachrichtigt, wenn Updates verfügbar sind. Sie müssen die Aktualisierung selbst durchführen. | Nein                    | Ja — das Betriebssystem, das auf Ihren physischen oder virtuellen Maschinen läuft, wird von Ihnen mit den Tools Ihrer Wahl verwaltet. Siehe <a href="#">the section called “Bereiten Sie das Betriebssystem vor”</a> . |



| Kriterien                                                    | EKS-verwaltete Knotengruppen                                                                                                                                                                                                                                                                                                                                                                                                                            | Automatischer EKS-Modus                                                                             | Amazon EKS-Hybridknoten                                                                                                                                                    |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Muss die Kubernetes-Version des Knotens selbst aktualisieren | <a href="#">Ja</a> — Wenn Sie ein für Amazon EKS optimiertes AMI bereitgestellt haben, werden Sie in der Amazon EKS-Konsole benachrichtigt, wenn Updates verfügbar sind. Sie können die Aktualisierung mit einem Klick in der Konsole durchführen. Wenn Sie ein benutzerdefiniertes AMI bereitgestellt haben, werden Sie in der Amazon EKS-Konsole nicht benachrichtigt, wenn Updates verfügbar sind. Sie müssen die Aktualisierung selbst durchführen. | Nein                                                                                                | Ja — Sie verwalten Hybrid-Knoten-Upgrades mit Tools Ihrer Wahl oder mit <code>nodeadm</code> . Siehe <a href="#">the section called “Aktualisieren Sie Hybridknoten”</a> . |
| Kann Amazon EBS-Speicher mit Pods verwenden                  | <a href="#">Ja</a>                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ja, als integrierte Funktion. Erfahren Sie, wie <a href="#">Sie eine Speicherklasse erstellen</a> . | Nein                                                                                                                                                                       |
| Kann Amazon EFS-Speicher mit Pods verwenden                  | <a href="#">Ja</a>                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ja                                                                                                  | Nein                                                                                                                                                                       |

| Kriterien                                                          | EKS-verwaltete Knotengruppen                               | Automatischer EKS-Modus                                    | Amazon EKS-Hybridknoten                                                                                     |
|--------------------------------------------------------------------|------------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Kann Amazon FSx für die Aufbewahrung von Lustre mit Pods verwenden | <a href="#">Ja</a>                                         | Ja                                                         | Nein                                                                                                        |
| Kann Network Load Balancer für Services verwenden                  | <a href="#">Ja</a>                                         | Ja                                                         | Ja — der Zieltyp <code>ip</code> muss verwendet werden.                                                     |
| Pods können in einem öffentlichen Subnetz ausgeführt werden        | Ja                                                         | Ja                                                         | Nein — Pods werden in einer lokalen Umgebung ausgeführt.                                                    |
| Kann einzelnen Pods verschiedene VPC-Sicherheitsgruppen zuweisen   | <a href="#">Ja</a> – Nur Linux-Knoten                      | Nein                                                       | Nein                                                                                                        |
| Kann Kubernetes ausführen DaemonSets                               | Ja                                                         | Ja                                                         | Ja                                                                                                          |
| Support HostPort und HostNetwork im Pod-Manifest                   | Ja                                                         | Ja                                                         | Ja                                                                                                          |
| AWS Verfügbarkeit in der Region                                    | <a href="#">Alle von Amazon EKS unterstützten Regionen</a> | <a href="#">Alle von Amazon EKS unterstützten Regionen</a> | <a href="#">Alle von Amazon EKS unterstützten Regionen</a> außer den Regionen AWS GovCloud (USA) und China. |

| Kriterien                                               | EKS-verwaltete Knotengruppen                                                                                                            | Automatischer EKS-Modus                                                                                                                                                                                                                                                                                                                                                                                           | Amazon EKS-Hybridknoten                                                                                             |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Kann Container auf Amazon EC2 Dedicated Hosts ausführen | Ja                                                                                                                                      | Nein                                                                                                                                                                                                                                                                                                                                                                                                              | Nein                                                                                                                |
| Preise                                                  | Kosten einer EC2 Amazon-Instance, die mehrere Pods ausführt. Weitere Informationen finden Sie unter <a href="#">EC2 Amazon-Preise</a> . | Wenn der automatische EKS-Modus in Ihrem Cluster aktiviert ist, zahlen Sie zusätzlich zu den EC2 Standard-Instance-Gebühren eine separate Gebühr für die Instances, die mit der Rechenfunktion des Auto-Modus gestartet werden. Der Betrag hängt vom gestarteten Instance-Typ und der AWS Region ab, in der sich Ihr Cluster befindet. Weitere Informationen finden Sie unter <a href="#">Amazon EKS-Preise</a> . | Kosten für vCPU-Hybridknoten pro Stunde. Weitere Informationen finden Sie unter <a href="#">Amazon EKS-Preise</a> . |

## Vereinfachen Sie den Knotenlebenszyklus mit verwalteten Knotengruppen

Von Amazon EKS verwaltete Knotengruppen automatisieren die Bereitstellung und das Lebenszyklusmanagement von Knoten ( EC2 Amazon-Instances) für Amazon EKS Kubernetes-Cluster.

Mit Amazon EKS-verwalteten Knotengruppen müssen Sie die EC2 Amazon-Instances, die Rechenkapazität für die Ausführung Ihrer Kubernetes-Anwendungen bereitstellen, nicht separat bereitstellen oder registrieren. Sie können Knoten für Ihren Cluster mit einem einzigen Vorgang erstellen, aktualisieren oder beenden. Knotenaktualisierungen und -beendigungen entleeren Knoten automatisch, um sicherzustellen, dass Ihre Anwendungen verfügbar bleiben.

Jeder verwaltete Knoten wird als Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe bereitgestellt, die von Amazon EKS für Sie verwaltet wird. Jede Ressource, einschließlich der Instances und Auto Scaling Scaling-Gruppen, wird in Ihrem AWS Konto ausgeführt. Jede Knotengruppe wird in mehreren Availability Zones ausgeführt, die Sie definieren.

Verwaltete Knotengruppen können optional auch die auto Knotenreparatur nutzen, mit der der Zustand der Knoten kontinuierlich überwacht wird. Es reagiert automatisch auf erkannte Probleme und ersetzt Knoten, wenn möglich. Dies trägt zur allgemeinen Verfügbarkeit des Clusters bei und erfordert nur minimale manuelle Eingriffe. Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).

Sie können mithilfe der Amazon EKS-Konsole, AWS CLI, eksctl AWS API oder Infrastruktur als Code-Tools eine verwaltete Knotengruppe zu neuen oder vorhandenen Clustern hinzufügen, einschließlich AWS CloudFormation. [Knoten, die als Teil einer verwalteten Knotengruppe gestartet werden, werden vom Kubernetes Cluster Autoscaler automatisch für die automatische Erkennung markiert](#). Sie können die Knotengruppe verwenden, um Kubernetes-Labels auf Knoten anzuwenden und sie jederzeit zu aktualisieren.

Für die Nutzung von Amazon EKS-verwalteten Knotengruppen fallen keine zusätzlichen Kosten an. Sie zahlen nur für die AWS Ressourcen, die Sie bereitstellen. Dazu gehören EC2 Amazon-Instances, Amazon EBS-Volumes, Amazon EKS-Cluster-Stunden und jede andere AWS Infrastruktur. Es fallen keine Mindestgebühren oder Vorauszahlungen an.

Weitere Informationen zu den ersten Schritten mit einem neuen Amazon-EKS-Cluster und einer verwalteten Knotengruppe finden Sie unter [the section called “Cluster erstellen \(Konsole und CLI\)”](#).

Informationen zum Hinzufügen einer verwalteten Knotengruppe zu einem bestehenden Cluster finden Sie unter [the section called “Erstellen”](#).

## Konzepte für verwaltete Knotengruppen

- Von Amazon EKS verwaltete Knotengruppen erstellen und verwalten EC2 Amazon-Instances für Sie.

- Jeder verwaltete Knoten wird als Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe bereitgestellt, die von Amazon EKS für Sie verwaltet wird. Darüber hinaus werden alle Ressourcen, einschließlich EC2 Amazon-Instances und Auto Scaling Scaling-Gruppen, in Ihrem AWS Konto ausgeführt.
- Die Auto-Scaling-Gruppe einer verwalteten Knotengruppe umfasst alle Subnetze, die Sie beim Erstellen der Gruppe angeben.
- Amazon EKS kennzeichnet verwaltete Knotengruppenressourcen, sodass sie für die Verwendung des Kubernetes [Cluster Autoscaler](#) konfiguriert sind.

 **Important**

Wenn Sie eine statusbehaftete Anwendung in mehreren Availability Zones ausführen, die von Amazon EBS-Volumes unterstützt wird und den Kubernetes [Cluster Autoscaler](#) verwendet, sollten Sie mehrere Knotengruppen konfigurieren, die jeweils auf eine einzelne Availability Zone beschränkt sind. Außerdem sollten Sie das `--balance-similar-node-groups`-Feature aktivieren.

- Sie können eine benutzerdefinierte Startvorlage für ein höheres Maß an Flexibilität und Anpassung bei der Bereitstellung verwalteter Knoten verwenden. Zum Beispiel können Sie zusätzliche `kubelet`-Argumente angeben und ein benutzerdefiniertes AMI verwenden. Weitere Informationen finden Sie unter [the section called “Startvorlagen”](#). Wenn Sie beim ersten Erstellen einer verwalteten Knotengruppe keine benutzerdefinierte Startvorlage verwenden, gibt es eine automatisch generierte Startvorlage. Ändern Sie diese automatisch generierte Vorlage nicht manuell, da sonst Fehler auftreten.
- Amazon EKS folgt dem Modell der gemeinsamen Verantwortung für CVEs und Sicherheitspatches auf verwalteten Knotengruppen. Wenn verwaltete Knoten ein für Amazon EKS optimiertes AMI ausführen, ist Amazon EKS für die Erstellung von Patch-Versionen des AMI verantwortlich, wenn Fehler oder Probleme gemeldet werden. Wir können eine Korrektur veröffentlichen. Sie sind jedoch dafür verantwortlich, diese gepatchten AMI-Versionen für Ihre verwalteten Knotengruppen bereitzustellen. Wenn verwaltete Knoten ein benutzerdefiniertes AMI ausführen, sind Sie dafür verantwortlich, gepatchte Versionen des AMI zu erstellen, wenn Fehler oder Probleme gemeldet werden, und dann das AMI bereitzustellen. Weitere Informationen finden Sie unter [the section called “Aktualisierung”](#).
- Von Amazon EKS verwaltete Knotengruppen können sowohl in öffentlichen als auch privaten Subnetzen gestartet werden. Wenn Sie eine verwaltete Knotengruppe am oder nach dem 22. April 2020 in einem öffentlichen Subnetz starten, muss `MapPublicIpOnLaunch` für das Subnetz

auf „Wahr“ gesetzt sein, damit die Instances einem Cluster hinzugefügt werden können. Wenn das öffentliche Subnetz am `eksctl` oder nach dem 26. März 2020 mithilfe der von [Amazon EKS bereitgestellten AWS CloudFormation Vorlagen](#) erstellt wurde, ist diese Einstellung bereits auf `true` gesetzt. Wenn die öffentlichen Subnetze vor dem 26. März 2020 erstellt wurden, müssen Sie die Einstellung manuell ändern. Weitere Informationen finden Sie unter [Ändern des Attributs für die öffentliche IPv4 Adressierung für Ihr Subnetz](#).

- Wenn Sie eine verwaltete Knotengruppe in privaten Subnetzen bereitstellen, müssen Sie sicherstellen, dass diese auf Amazon ECR zugreifen kann, um Container-Images abzurufen. Sie können dies tun, indem Sie ein NAT-Gateway mit der Routing-Tabelle des Subnetzes verbinden oder indem Sie die folgenden [AWS PrivateLink -VPC-Endpunkte](#) hinzufügen:
  - Amazon-ECR-API-Endpunktschnittstelle – `com.amazonaws.region-code.ecr.api`
  - API-Endpunktschnittstelle der Amazon-ECR-Docker-Registrierung – `com.amazonaws.region-code.ecr.dkr`
  - Amazon-S3-Gateway-Endpunkt – `com.amazonaws.region-code.s3`

Weitere häufig verwendete Services und Endpunkte finden Sie unter [the section called “Private Cluster”](#).

- Verwaltete Knotengruppen können nicht auf [AWS Outposts](#) oder in [AWS Wavelength](#) bereitgestellt werden. Verwaltete Knotengruppen können in [AWS Local Zones](#) erstellt werden. Weitere Informationen finden Sie unter [the section called “AWS Local Zones”](#).
- Sie können mehrere verwaltete Knotengruppen innerhalb eines einzelnen Clusters erstellen. Sie können beispielsweise eine Knotengruppe mit dem standardmäßigen Amazon EKS-optimierten Amazon Linux-AMI für einige Workloads und eine weitere mit der GPU-Variante für Workloads erstellen, die GPU-Unterstützung erfordern.
- Wenn Ihre verwaltete Knotengruppe auf einen Fehler bei der [Überprüfung des EC2 Amazon-Instance-Status](#) stößt, gibt Amazon EKS einen Fehlercode zurück, der Ihnen bei der Diagnose des Problems hilft. Weitere Informationen finden Sie unter [the section called “Fehlercodes bei verwalteten Knotengruppen”](#).
- Amazon EKS fügt Kubernetes-Labels zu verwalteten Knotengruppen-Instances hinzu. Diese von Amazon EKS bereitgestellten Labels sind mit dem Präfix `eks.amazonaws.com` versehen.
- Amazon EKS leert Knoten automatisch mit der Kubernetes-API während Beendigungs- oder Aktualisierungsvorgängen.
- Budgets für Pod-Unterbrechungen werden nicht eingehalten, wenn ein Knoten beendet `AZRebalance` oder die gewünschte Anzahl an Knoten reduziert wird. Mit diesen Aktionen wird versucht, Pods auf dem Knoten zu entfernen. Wenn es jedoch länger als 15 Minuten dauert, wird

der Knoten beendet, unabhängig davon, ob alle Pods auf dem Knoten beendet wurden. Um den Zeitraum bis zum Beenden des Knotens zu verlängern, fügen Sie der Auto-Scaling-Gruppe einen Lebenszyklus-Hook hinzu. Weitere Informationen finden [Sie unter Hinzufügen von Lifecycle-Hooks](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- Damit der Draining-Prozess nach Erhalt einer Benachrichtigung über eine Spot-Unterbrechung oder eine Kapazitätsumverteilung korrekt ausgeführt werden kann, muss `CapacityRebalance` auf `true` eingestellt sein.
- Bei der Aktualisierung verwalteter Knotengruppen werden die Budgets für Pod-Unterbrechungen berücksichtigt, die Sie für Ihre Pods festgelegt haben. Weitere Informationen finden Sie unter [the section called “Verhaltensdetails aktualisieren”](#).
- Für die Verwendung verwalteter Amazon-EKS-Knotengruppen fallen keine zusätzlichen Kosten an. Sie zahlen nur für die AWS Ressourcen, die Sie bereitstellen.
- Wenn Sie Amazon-EBS-Volumes für Ihre Knoten verschlüsseln möchten, können Sie die Knoten mithilfe einer Startvorlage bereitstellen. Um verwaltete Knoten mit verschlüsselten Amazon-EBS-Volumes ohne Verwendung einer Startvorlage bereitzustellen, verschlüsseln Sie alle neuen Amazon-EBS-Volumes, die in Ihrem Konto erstellt wurden. Weitere Informationen finden Sie unter [Standardverschlüsselung](#) im EC2 Amazon-Benutzerhandbuch.

## Kapazitätstypen für verwaltete Knotengruppen

Beim Erstellen einer verwalteten Knotengruppe können Sie entweder den Kapazitätstyp On-Demand oder Spot-Kapazität auswählen. Amazon EKS stellt eine verwaltete Knotengruppe mit einer Amazon EC2 Auto Scaling Scaling-Gruppe bereit, die entweder nur On-Demand-Instances oder nur Amazon EC2 Spot-Instances enthält. Sie können Pods für fehlertolerante Anwendungen für Spot-verwaltete Knotengruppen und fehlerintolerante Anwendungen für On-Demand-Knotengruppen innerhalb eines einzelnen Kubernetes-Clusters planen. Standardmäßig stellt eine verwaltete Knotengruppe EC2 On-Demand-Amazon-Instances bereit.

### On-Demand

Mit On-Demand-Instances zahlen Sie für Rechenkapazität bis zur zweiten Stunde ohne langfristige Verpflichtungen.

Standardmäßig: Wenn Sie keinen Capacity Type festlegen, wird die verwaltete Knotengruppe mit On-Demand-Instances bereitgestellt. Eine verwaltete Knotengruppe konfiguriert in Ihrem Namen eine Amazon EC2 Auto Scaling Scaling-Gruppe, wobei die folgenden Einstellungen angewendet werden:

- Die Allokationsstrategie zur Bereitstellung von On-Demand-Kapazität ist auf `prioritized` eingestellt. Verwaltete Knotengruppen verwenden die Reihenfolge der in der API übergebenen Instance-Typen, um zu bestimmen, welcher Instance-Typ bei der Erfüllung der On-Demand-Kapazität zuerst verwendet werden soll. Sie können beispielsweise drei Instance-Typen in der folgenden Reihenfolge angeben: `c5.large`, `c4.large`, und `c3.large`. Wenn Ihre On-Demand-Instances gestartet werden, erfüllt die verwaltete Knotengruppe On-Demand-Kapazität beginnend mit `c5.large`, dann `c4.large`, und dann `c3.large`. Weitere Informationen finden Sie unter [Amazon EC2 Auto Scaling Scaling-Gruppe](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Amazon EKS fügt allen Knoten in Ihrer verwalteten Knotengruppe die folgende Kubernetes-Bezeichnung hinzu, die den Kapazitätstyp angibt: `eks.amazonaws.com/capacityType: ON_DEMAND`. Sie können dieses Label verwenden, um statusbehaftete oder fehlerintolerante Anwendungen auf On-Demand-Knoten zu planen.

## Spot-Instances

Amazon EC2 Spot-Instances sind freie EC2 Amazon-Kapazitäten, die erhebliche Rabatte gegenüber den On-Demand-Preisen bieten. Amazon EC2 Spot-Instances können mit einer zweiminütigen Unterbrechungsbenachrichtigung unterbrochen werden, wenn die Kapazität wieder EC2 benötigt wird. Weitere Informationen finden Sie unter [Spot-Instances](#) im EC2 Amazon-Benutzerhandbuch. Sie können eine verwaltete Knotengruppe mit Amazon EC2 Spot-Instances konfigurieren, um die Kosten für die Rechenknoten zu optimieren, die in Ihrem Amazon EKS-Cluster ausgeführt werden.

Um Spot-Instances in einer verwalteten Knotengruppe zu verwenden, müssen Sie eine verwaltete Knotengruppe erstellen, indem Sie den Kapazitätstyp als `spot` einstellen. Eine verwaltete Knotengruppe konfiguriert in Ihrem Namen eine Amazon EC2 Auto Scaling Scaling-Gruppe, wobei die folgenden bewährten Spot-Methoden angewendet werden:

- Um sicherzustellen, dass Ihre Spot-Knoten in den optimalen Spot-Kapazitätspools bereitgestellt werden, ist die Zuweisungsstrategie auf eine der folgenden Optionen eingestellt:
  - `price-capacity-optimized(PCO)` — Beim Erstellen neuer Knotengruppen in einem Cluster mit Kubernetes-Version 1.28 oder höher ist die Zuweisungsstrategie auf `price-capacity-optimized` eingestellt. Die Zuweisungsstrategie wird jedoch nicht für Knotengruppen geändert, die bereits erstellt wurden, `capacity-optimized` bevor die verwalteten Knotengruppen von Amazon EKS mit der Unterstützung von PCO begannen.



- `capacity-optimized(CO)` — Beim Erstellen neuer Knotengruppen in einem Cluster mit Kubernetes-Version 1.27 oder niedriger ist die Zuweisungsstrategie auf eingestellt. `capacity-optimized`

Um die Anzahl der Spot-Kapazitätspools zu erhöhen, die für die Zuweisung von Kapazität verfügbar sind, konfigurieren Sie eine verwaltete Knotengruppe für die Verwendung mehrerer Instance-Typen.

- Amazon EC2 Spot Capacity Rebalancing ist aktiviert, sodass Amazon EKS Ihre Spot-Knoten problemlos entleeren und neu verteilen kann, um Anwendungsunterbrechungen zu minimieren, wenn ein Spot-Knoten einem erhöhten Unterbrechungsrisiko ausgesetzt ist. Weitere Informationen finden Sie unter [Amazon EC2 Auto Scaling Capacity Rebalancing](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Wenn ein Spot-Knoten eine Neuausgleichsempfehlung erhält, versucht Amazon EKS automatisch, einen neuen Ersatz-Spot-Knoten zu starten.
- Wenn ein Spot-Unterbrechungsnachweis in zwei Minuten eintrifft, bevor sich der Ersatz-Spot-Knoten in einem Ready, beginnt Amazon EKS mit dem Entleeren des Spot-Knotens, der die Neuausgleichsempfehlung erhalten hat. Amazon EKS entleert den Knoten nach bestem Wissen. Daher gibt es keine Garantie dafür, dass Amazon EKS wartet, bis der Ersatzknoten dem Cluster beitrifft, bevor der vorhandene Knoten entleert wird.
- Wenn ein Ersatz-Spot-Knoten gestartet wird und in dem Ready Zustand auf Kubernetes ist, sperrt Amazon EKS den Spot-Knoten, der die Neuausgleichs-Empfehlung erhalten hat, und entleert ihn. Durch das Sperren des Spot-Nodes wird sichergestellt, dass der Service Controller keine neuen Anfragen an diesen Spot-Knoten sendet. Es entfernt sie auch aus der Liste der gesunden, aktiven Spot-Knoten. Durch das Entleeren des Spot-Knotens wird sichergestellt, dass laufende Pods ordnungsgemäß entfernt werden.
- Amazon EKS fügt allen Knoten in Ihrer verwalteten Knotengruppe die folgende Kubernetes-Bezeichnung hinzu, die den Kapazitätstyp angibt: `eks.amazonaws.com/capacityType: SPOT`. Sie können dieses Label verwenden, um fehlertolerante Anwendungen auf Spot-Knoten zu planen.

Bei der Entscheidung, ob eine Knotengruppe mit On-Demand- oder Spot-Kapazität bereitgestellt werden soll, sollten Sie die folgenden Bedingungen berücksichtigen:

- Spot-Instances eignen sich gut für zustandslose, fehlertolerante, flexible Anwendungen. Dazu gehören Workloads für Batch- und Machine-Learning-Schulungen, Big Data ETLs wie Apache Spark, Anwendungen zur Verarbeitung von Warteschlangen und statusfreie API-Endpunkte. Da es sich bei Spot um freie EC2 Amazon-Kapazität handelt, die sich im Laufe der Zeit ändern kann,

empfehlen wir, Spot-Kapazität für unterbrechungstolerante Workloads zu verwenden. Insbesondere eignet sich Spot-Kapazität für Workloads, die Zeiten aushalten können, in denen die erforderliche Kapazität nicht verfügbar ist.

- Es wird empfohlen, On-Demand für Anwendungen zu verwenden, die fehlerintolerant sind. Dazu gehören Cluster-Verwaltungs-Tools wie Überwachungs- und Betriebstools, Bereitstellungen, die StatefulSets erfordern, und zustandsbehaftete Anwendungen wie Datenbanken.
- Um die Verfügbarkeit Ihrer Anwendungen bei der Verwendung von Spot-Instances zu maximieren, wird empfohlen, eine verwaltete Spot-Knotengruppe für die Verwendung mehrerer Instance-Typen zu konfigurieren. Es wird empfohlen, die folgenden Regeln anzuwenden, wenn mehrere Instance-Typen verwendet werden:
  - Wenn Sie innerhalb einer verwalteten Knotengruppe den [Cluster Autoscaler](#) verwenden, empfehlen wir, einen flexiblen Satz von Instanztypen mit derselben Menge an vCPU- und Speicherressourcen zu verwenden. Dies soll sicherstellen, dass die Knoten in Ihrem Cluster wie erwartet skalieren. Wenn Sie beispielsweise vier V CPUs - und acht GiB Arbeitsspeicher benötigen, verwenden Sie c3.xlarge, c4.xlarge, c5.xlarge, c5d.xlarge, c5a.xlarge, c5n.xlarge, oder andere ähnliche Instance-Typen.
  - Um die Anwendungsverfügbarkeit zu verbessern, empfehlen wir Ihnen, mehrere Spot-verwaltete Knotengruppen bereitzustellen. Dafür sollte jede Gruppe einen flexiblen Satz von Instance-Typen verwenden, die über die gleichen vCPU- und Speicherressourcen verfügen. Wenn Sie beispielsweise 4 V CPUs und 8 GiB Arbeitsspeicher benötigen, empfehlen wir Ihnen, eine verwaltete Knotengruppe mit c3.xlarge, c4.xlarge, c5.xlarge, c5d.xlarge, c5a.xlarge, c5n.xlarge, oder anderen ähnlichen Instanztypen und eine zweite verwaltete Knotengruppe mit m3.xlarge, m4.xlarge, m5.xlarge, m5d.xlarge, m5a.xlarge, m5n.xlarge oder anderen ähnlichen Instanztypen zu erstellen.
  - Wenn Sie Ihre Knotengruppe mit dem Spot-Kapazitätstyp bereitstellen, der eine benutzerdefinierte Startvorlage verwendet, verwenden Sie die API, um mehrere Instance-Typen zu übergeben. Übergeben Sie nicht einen einzelnen Instance-Typ durch die Startvorlage. Weitere Informationen zum Bereitstellen einer Knotengruppe mithilfe einer Startvorlage finden Sie unter [the section called “Startvorlagen”](#) aus.

## Erstellen Sie eine verwaltete Knotengruppe für Ihren Cluster

Dieses Thema beschreibt, wie Sie von Amazon EKS verwaltete Knotengruppen von Knoten starten können, die sich bei Ihrem Amazon-EKS-Cluster registrieren. Nachdem die Knoten dem Cluster beigetreten sind, können Sie Kubernetes-Anwendungen darin bereitstellen.

Wenn Sie zum ersten Mal eine von Amazon EKS verwaltete Knotengruppe starten, empfehlen wir Ihnen, stattdessen einer unserer Anleitungen unter zu folgen [Erste Schritte](#). Diese Anleitungen bieten exemplarische Vorgehensweisen für die Erstellung eines Amazon EKS-Clusters mit Knoten.

 Important

- Amazon EKS-Knoten sind EC2 Standard-Amazon-Instances. Ihnen wird auf der Grundlage der normalen EC2 Amazon-Preise in Rechnung gestellt. Weitere Informationen finden Sie unter [EC2 Amazon-Preise](#).
  - Sie können keine verwalteten Knoten in einer AWS Region erstellen, in der AWS Outposts oder AWS Wavelength aktiviert sind. Sie können Selbstverwaltetes-Knoten. Weitere Informationen finden Sie unter [the section called “Amazon Linux”](#), [the section called “Windows”](#) und [the section called “Bottlerocket”](#). Sie können auch eine selbstverwaltete Amazon-Linux-Knotengruppe auf einem Outpost erstellen. Weitere Informationen finden Sie unter [the section called “Knoten”](#).
  - Wenn Sie keine [AMI-ID für die bootstrap.sh Datei angeben](#), die in Amazon EKS-optimiertem Linux oder Bottlerocket enthalten ist, erzwingen verwaltete Knotengruppen eine maximale Anzahl auf den Wert von. maxPods Für Instances mit weniger als 30 V ist CPUs die maximale Anzahl. 110 Bei Instanzen mit mehr als 30 V CPUs springt die maximale Anzahl auf 250. Diese Zahlen basieren auf den [Skalierbarkeitsschwellenwerten von Kubernetes](#) und den empfohlenen Einstellungen, die von internen Tests des Amazon EKS-Skalierbarkeitsteams durchgeführt wurden. Weitere Informationen finden Sie im Blogbeitrag [Amazon VPC CNI plugin increases pods per node limits](#) (VPC-CNI-Plugin von Amazon erhöht Grenzwerte für Pods pro Knoten).
- 
- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [the section called “Erstellen eines -Clusters”](#).
  - Eine vorhandene IAM-Rolle, die von den Knoten verwendet werden soll. Informationen zum Erstellen finden Sie unter [the section called “Knoten-IAM-Rolle”](#). Wenn diese Rolle keine der Richtlinien für das VPC-CNI hat, ist die folgende separate Rolle für die VPC-CNI-Pods erforderlich.
  - (Optional, aber empfohlen) Das Amazon VPC CNI-Plug-In für Kubernetes ist mit einer eigenen IAM-Rolle konfiguriert, der die erforderliche IAM-Richtlinie zugeordnet ist. Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).

- Vertrautheit mit den unter [Wählen Sie einen optimalen EC2 Amazon-Node-Instance-Typ](#) aufgeführten Überlegungen. Je nachdem, welchen Instance-Typ Sie wählen, kann es zusätzliche Voraussetzungen für Ihren Cluster und Ihre VPC geben.
- Um eine von Windows verwaltete Knotengruppe hinzuzufügen, müssen Sie zunächst die Windows-Unterstützung für Ihren Cluster aktivieren. Weitere Informationen finden Sie unter [the section called “Aktivieren Sie die Windows-Unterstützung”](#).

Sie können eine verwaltete Knotengruppe mit einer der folgenden Optionen erstellen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

## eksctl

Erstellen Sie eine verwaltete Knotengruppe mit eksctl

Für diesen Vorgang ist eksctl Version 0.210.0 oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Eine Installations- und Upgrade-Anleitung für eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).

1. (Optional) Wenn die von AmazonEKS\_CNI\_Policy verwaltete IAM-Richtlinie mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Servicekonto zuordnen. aws-node Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).
2. Erstellen Sie eine verwaltete Knotengruppe mit oder ohne Verwendung einer benutzerdefinierten Startvorlage. Das manuelle Angeben einer Startvorlage ermöglicht eine bessere Anpassung einer Knotengruppe. Zum Beispiel kann es die Bereitstellung eines benutzerdefinierten AMI oder die Bereitstellung von Argumenten für das bootstrap.sh-Skript in einem für Amazon EKS optimierten AMI ermöglichen. Geben Sie den folgenden Befehl ein, um eine vollständige Liste aller verfügbaren Optionen und Standardwerte anzuzeigen.

```
eksctl create nodegroup --help
```

Ersetzen Sie im folgenden Befehl *my-cluster* durch den Namen Ihres Clusters und ersetzen Sie *my-mng* durch den Namen Ihrer Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.

 **Important**

Wenn Sie beim ersten Erstellen einer verwalteten Knotengruppe keine benutzerdefinierte Startvorlage verwenden, verwenden Sie zu einem späteren Zeitpunkt keine Vorlage für die Knotengruppe. Wenn Sie keine benutzerdefinierte Startvorlage angegeben haben, generiert das System automatisch eine Startvorlage, deren manuelle Änderung nicht empfohlen wird. Das manuelle Ändern dieser automatisch generierten Startvorlage kann zu Fehlern führen.

## Ohne Startvorlage

`eksctl` erstellt eine standardmäßige EC2 Amazon-Startvorlage in Ihrem Konto und stellt die Knotengruppe mithilfe einer Startvorlage bereit, die auf der Grundlage der von Ihnen angegebenen Optionen erstellt wird. Bevor Sie einen Wert für `--node-type` festlegen, siehe [the section called “EC2 Amazon-Instance-Typen”](#).

Ersetzen Sie *ami-family* durch ein zulässiges Schlüsselwort. Weitere Informationen finden Sie unter [Einrichtung der Knoten-AMI-Familie](#) in der `eksctl`-Dokumentation. *my-key* Ersetzen Sie es durch den Namen Ihres EC2 Amazon-Schlüsselpaars oder öffentlichen Schlüssels. Dieser Schlüssel wird für den SSH-Zugriff zu Ihren Knoten verwendet, nachdem diese gestartet wurden.

 **Note**

Für Windows aktiviert dieser Befehl SSH nicht. Stattdessen wird Ihr EC2 Amazon-Schlüsselpaar mit der Instance verknüpft und Sie können per RDP auf die Instance zugreifen.

Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Informationen zu Linux finden Sie unter [EC2 Amazon-Schlüsselpaare und Linux-Instances](#) im EC2 Amazon-Benutzerhandbuch. Informationen zu Windows finden Sie unter [EC2 Amazon-Schlüsselpaare und Windows-Instances](#) im EC2 Amazon-Benutzerhandbuch.

Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:

- Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
- Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

Wenn Sie den Pod-Zugriff auf IMDS blockieren möchten, fügen Sie die `--disable-pod-imds` Option zum folgenden Befehl hinzu.

```
eksctl create nodegroup \
 --cluster my-cluster \
 --region region-code \
 --name my-mng \
 --node-ami-family ami-family \
 --node-type m5.large \
 --nodes 3 \
 --nodes-min 2 \
 --nodes-max 4 \
 --ssh-access \
 --ssh-public-key my-key
```

Ihre Instances können Pods optional eine deutlich höhere Anzahl von IP-Adressen zuweisen, Pods aus einem anderen CIDR-Block als dem der Instance IP-Adressen zuweisen und in einem Cluster ohne Internetzugang bereitgestellt werden. Weitere Informationen dazu finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#), [the section called “Benutzerdefinierte Netzwerke”](#) und [the section called “Private Cluster”](#) für weitere Optionen, die dem vorherigen Befehl hinzugefügt werden.

Managed Node Groups berechnet und wendet je nach Instanztyp einen einzigen Wert für die maximale Anzahl von Pods an, die auf jedem Knoten Ihrer Knotengruppe ausgeführt werden können. Wenn Sie eine Knotengruppe mit unterschiedlichen Instanztypen erstellen, wird der kleinste Wert, der für alle Instanztypen berechnet wird, als maximale Anzahl von Pods verwendet, die auf jedem Instanztyp in der Knotengruppe ausgeführt werden können. Managed Node Groups berechnet den Wert anhand des Skripts, auf das in der von [Amazon EKS empfohlenen maximalen Pods für jeden EC2 Amazon-Instance-Typ](#) verwiesen wird.

Mit einer Startvorlage

Die Startvorlage muss bereits vorhanden sein und die unter [Grundlagen der Konfiguration der Startvorlage](#) angegebenen Anforderungen erfüllen. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:

- Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
- Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

Wenn Sie den Pod-Zugriff auf IMDS blockieren möchten, geben Sie die erforderlichen Einstellungen in der Startvorlage an.

- a. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie die *example values* und führen Sie dann den geänderten Befehl aus, um die `eks-nodegroup.yaml`-Datei zu erstellen. Mehrere Einstellungen, die Sie bei der Bereitstellung ohne Startvorlage angeben, werden in die Startvorlage verschoben. Wenn Sie keine `angabenversion` angeben, wird die Standardversion der Vorlage verwendet.

```
cat >eks-nodegroup.yaml <<EOF
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
 name: my-cluster
 region: region-code
managedNodeGroups:
- name: my-mng
 launchTemplate:
 id: lt-id
 version: "1"
EOF
```

Eine vollständige Liste der `eksctl` Konfigurationsdateieinstellungen finden Sie unter [Konfigurationsdateischema](#) in der `eksctl` Dokumentation. Ihre Instances können Pods optional eine deutlich höhere Anzahl von IP-Adressen zuweisen, Pods aus einem anderen CIDR-Block als dem der Instance IP-Adressen zuweisen und in einem Cluster ohne ausgehenden Internetzugang bereitgestellt werden. Weitere Informationen finden Sie unter [the section called "Erhöhen Sie die](#)

[IP-Adressen](#)“the section called [“Benutzerdefinierte Netzwerke”](#), und [the section called “Private Cluster”](#) für zusätzliche Optionen, die Sie der Konfigurationsdatei hinzufügen können.

Wenn Sie in Ihrer Startvorlage keine AMI-ID angegeben haben, berechnet Managed Node Groups einen einzigen Wert für die maximale Anzahl von Pods, die auf jedem Knoten Ihrer Knotengruppe ausgeführt werden können, und wendet diesen an, basierend auf dem Instance-Typ. Wenn Sie eine Knotengruppe mit unterschiedlichen Instance-Typen erstellen, wird der kleinste Wert, der für alle Instance-Typen berechnet wird, als maximale Anzahl von Pods verwendet, die auf jedem Instance-Typ in der Knotengruppe ausgeführt werden können. Managed Node Groups berechnet den Wert anhand des Skripts, auf das in der von [Amazon EKS empfohlenen maximalen Pods für jeden EC2 Amazon-Instance-Typ](#) verwiesen wird.

Wenn Sie in Ihrer Startvorlage eine AMI-ID angegeben haben, geben Sie die maximale Anzahl von Pods an, die auf jedem Knoten Ihrer Knotengruppe ausgeführt werden können, wenn Sie ein [benutzerdefiniertes Netzwerk](#) verwenden oder [die Anzahl der Ihrer Instance zugewiesenen IP-Adressen erhöhen](#) möchten. Weitere Informationen finden Sie unter [the section called “Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen”](#).

b. Stellen Sie die Knotengruppe mit dem folgenden Befehl bereit.

```
eksctl create nodegroup --config-file eks-nodegroup.yaml
```

## AWS Management Console

Erstellen Sie eine verwaltete Knotengruppe mit dem AWS Management Console

1. Warten Sie, bis der Status des Clusters als ACTIVE angezeigt wird. Sie können keine verwaltete Knotengruppe für einen Cluster erstellen, der dies noch nicht getan hatACTIVE.
2. Öffnen Sie die [Amazon-EKS-Konsole](#).
3. Wählen Sie den Namen des Clusters aus, in dem Sie eine verwaltete Knotengruppe erstellen möchten.
4. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
5. Wählen Sie Add Node Group (Knotengruppe hinzufügen) aus.
6. Geben Sie auf der Seite Configure node group (Knotengruppe konfigurieren) die Parameter entsprechend aus, und wählen Sie dann Next (Weiter).



- **Name** – Geben Sie einen eindeutigen Namen für die verwaltete Knotengruppe ein. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.
- **Node IAM role (Knoten-IAM-Rolle)** – Wählen Sie die Knoten-Instance-Rolle aus, die mit Ihrer Knotengruppe verwendet werden soll. Weitere Informationen finden Sie unter [the section called “Knoten-IAM-Rolle”](#).

 **Important**

- Sie können nicht dieselbe Rolle verwenden, die zum Erstellen von Clustern verwendet wird.
  - Wir empfehlen, eine Rolle zu verwenden, die derzeit von keiner selbstverwalteten Knotengruppe verwendet wird. Andernfalls planen Sie die Verwendung mit einer neuen selbstverwalteten Knotengruppe. Weitere Informationen finden Sie unter [the section called “Löschen”](#).
- 
- **Startvorlage verwenden** – (Optional) Wählen Sie aus, ob Sie eine bestehende Startvorlage verwenden möchten. Wählen Sie einen Namen für die Startvorlage aus. Wählen Sie dann eine Launch template version (Startvorlagenversion) aus. Wenn Sie keine Version auswählen, verwendet Amazon EKS die Standardversion der Vorlage. Startvorlagen ermöglichen eine umfassendere Anpassung Ihrer Knotengruppe, sodass Sie beispielsweise ein benutzerdefiniertes AMI bereitstellen, Pods eine deutlich höhere Anzahl von IP-Adressen zuweisen, Pods IP-Adressen aus einem anderen CIDR-Block als dem der Instance zuweisen und Knoten in einem Cluster ohne ausgehenden Internetzugang bereitstellen können. Weitere Informationen finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#), [the section called “Benutzerdefinierte Netzwerke”](#) und [the section called “Private Cluster”](#).

Die Startvorlage muss die Anforderungen unter [Anpassen verwalteter Knoten mit Startvorlagen](#) erfüllen. Wenn Sie keine eigene Startvorlage verwenden, erstellt die Amazon EKS-API eine standardmäßige EC2 Amazon-Startvorlage in Ihrem Konto und stellt die Knotengruppe mithilfe der Standard-Startvorlage bereit.

Wenn Sie [IAM-Rollen für Dienstkonten](#) implementieren, jedem Pod, der Zugriff auf AWS Dienste benötigt, die erforderlichen Berechtigungen direkt zuweisen und keine Pods in Ihrem Cluster aus anderen Gründen Zugriff auf IMDS benötigen, z. B. zum Abrufen der aktuellen AWS Region, können Sie den Zugriff auf IMDS auch für Pods deaktivieren, die kein Host-Netzwerk in einer

Startvorlage verwenden. Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

- Kubernetes labels – (Optional) Sie können Kubernetes-Labels auf die Knoten in Ihrer verwalteten Knotengruppe anwenden.
  - Kubernetes-Taints — (Optional) Sie können wählen, ob Sie Kubernetes-Taints auf die Knoten in Ihrer verwalteten Knotengruppe anwenden möchten. Die verfügbaren Optionen im Menü Effect (Effekt) sind **NoSchedule** , **NoExecute** und **PreferNoSchedule** . Weitere Informationen finden Sie unter [the section called “Verfälschen Sie GPU-Knoten”](#).
  - Tags – (Optional) Sie können wählen, ob Sie Ihre mit Amazon EKS verwaltete Knotengruppe taggen möchten. Diese Tags werden nicht auf andere Ressourcen in der Knotengruppe übertragen, z. B. auf Auto Scaling Scaling-Gruppen oder -Instances. Weitere Informationen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#).
7. Geben Sie auf der Seite Set compute configuration (Datenverarbeitung-Konfiguration einrichten) die Parameter entsprechend ein, und wählen Sie dann Next (Weiter).

- AMI-Typ — Wählen Sie einen AMI-Typ aus. Wenn Sie Arm-Instances bereitstellen, sollten Sie AMIs vor der Bereitstellung unbedingt die Überlegungen unter [Amazon EKS-optimiertes Arm Amazon Linux](#) lesen.

Wenn Sie auf der vorherigen Seite eine Startvorlage und in der Startvorlage ein AMI angegeben haben, können Sie keinen Wert auswählen. Der Wert aus der Vorlage wird angezeigt. Das in der Vorlage angegebene AMI muss die Anforderungen [unter Spezifizieren eines AMI](#) erfüllen.

- Capacity type (Kapazitätstyp) — Wählen Sie einen Kapazitätstyp aus. Weitere Informationen zur Auswahl eines Kapazitätstyps finden Sie unter [the section called “Kapazitätstypen für verwaltete Knotengruppen”](#). Sie können innerhalb derselben Knotengruppe nicht verschiedene Kapazitätstypen mischen. Wenn Sie beide Kapazitätstypen verwenden möchten, erstellen Sie separate Knotengruppen mit jeweils eigenen Kapazitäts- und Instance-Typen. Informationen [the section called “Reservieren Sie GPUs für MNG”](#) zur Bereitstellung und Skalierung von GPU-beschleunigten Worker-Knoten finden Sie unter.
- Instance-Typen- Standardmäßig wird ein oder mehrere Instance-Typen angegeben. Um einen Standard-Instance-Typ zu entfernen, wählen Sie X auf der rechten Seite des Instance-Typs. Wählen Sie den Instance-Typ aus, der in der verwalteten Knotengruppe verwendet werden soll. Weitere Informationen finden Sie unter [the section called “ EC2 Amazon-Instance-Typen”](#).

Die Konsole zeigt eine Reihe von häufig verwendeten Instance-Typen an. Wenn Sie eine verwaltete Knotengruppe mit einem Instanztyp erstellen müssen, der nicht angezeigt wird, verwenden Sie die AWS CLI oder ein SDK AWS CloudFormation, um die

Knotengruppe zu erstellen. Wenn Sie auf der vorherigen Seite eine Startvorlage angegeben haben, können Sie keinen Wert auswählen, da der Instanztyp in der Startvorlage angegeben werden muss. Der Wert aus der Startvorlage wird angezeigt. Wenn Sie die OptionSpot-InstancesfürCapacity type (Kapazitätstyp)Wir empfehlen Ihnen, mehrere Instance-Typen anzugeben, um die Verfügbarkeit zu verbessern.

- Festplattengröße — Geben Sie die Festplattengröße (in GiB) ein, die für das Root-Volume Ihres Knotens verwendet werden soll.

Wenn Sie auf der vorherigen Seite eine Startvorlage angegeben haben, können Sie keinen Wert auswählen, da er in der Startvorlage angegeben werden muss.

- Desired size (Gewünschte Größe) – Geben Sie die aktuelle Anzahl von Knoten an, die die verwaltete Knotengruppe beim Start beibehalten soll.

 Note

Amazon EKS skaliert Ihre Knotengruppe nicht automatisch nach innen oder außen. Sie können den Kubernetes Cluster Autoscaler jedoch so konfigurieren, dass er dies für Sie erledigt. [Weitere Informationen finden Sie unter Cluster Autoscaler on. AWS](#)

- Minimum size (Mindestgröße) – Geben Sie die Mindestanzahl von Knoten an, auf die die verwaltete Knotengruppe skaliert werden kann.
- Maximum size (Maximale Größe) – Geben Sie die maximale Anzahl von Knoten an, auf die die verwaltete Knotengruppe skaliert werden kann.
- Konfiguration der Knotengruppe aktualisieren— (Optional) Sie können die Anzahl oder den Prozentsatz der Knoten auswählen, die parallel aktualisiert werden sollen. Diese Knoten werden während der Aktualisierung nicht verfügbar sein. FürMaximal nicht verfügbarWählen Sie eine der folgenden Optionen und geben Sie einenValue:
  - Zahl – Wählen Sie die Anzahl der Knoten in Ihrer Knotengruppe, die parallel aktualisiert werden können, und geben Sie diese an.
  - Prozentsatz – Wählen und geben Sie den Prozentsatz der Knoten in der Knotengruppe an, die parallel aktualisiert werden können. Dies ist nützlich, wenn Sie eine große Anzahl von Knoten in Ihrer Knotengruppe haben.
- Konfiguration der auto Knotenreparatur — (Optional) Wenn Sie das Kontrollkästchen auto Knotenreparatur aktivieren aktivieren aktivieren, ersetzt Amazon EKS die Knoten automatisch, wenn Probleme erkannt werden. Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).

8. Füllen Sie auf der Seite Specify Details (Details angeben) die Parameter entsprechend aus, und klicken Sie dann auf Next.

- Subnets (Subnetze) – Wählen Sie die Subnetze aus, in die die verwalteten Knoten gestartet werden sollen.

 Important

Wenn Sie eine statusbehaftete Anwendung in mehreren Availability Zones ausführen, die von Amazon EBS-Volumes unterstützt wird und den Kubernetes [Cluster Autoscaler](#) verwendet, sollten Sie mehrere Knotengruppen konfigurieren, die jeweils auf eine einzelne Availability Zone beschränkt sind. Außerdem sollten Sie das `--balance-similar-node-groups`-Feature aktivieren.

 Important

- Wenn Sie ein öffentliches Subnetz wählen und in Ihrem Cluster nur der öffentliche API-Server-Endpunkt aktiviert ist, muss das Subnetz `MapPublicIPOnLaunch` auf `true` eingestellt sein, damit die Instances erfolgreich einem Cluster zugeordnet werden können. Wenn das Subnetz am `eksctl` oder nach dem 26. März 2020 mithilfe der von [Amazon EKS bereitgestellten AWS CloudFormation Vorlagen](#) erstellt wurde, ist diese Einstellung bereits auf `true` gesetzt. Wenn die Subnetze mit `eksctl` oder den AWS CloudFormation Vorlagen vor dem 26. März 2020 erstellt wurden, müssen Sie die Einstellung manuell ändern. Weitere Informationen finden Sie unter [Ändern des Attributs für die öffentliche IPv4 Adressierung für Ihr Subnetz](#).
- Wenn Sie eine Startvorlage verwenden und mehrere Netzwerkschnittstellen angeben, weist Amazon EC2 nicht automatisch eine öffentliche IPv4 Adresse zu, auch wenn sie auf `true` eingestellt `MapPublicIpOnLaunch` ist. Damit Knoten in diesem Szenario dem Cluster beitreten können, müssen Sie entweder den privaten API-Serverendpunkt des Clusters aktivieren oder Knoten in einem privaten Subnetz mit ausgehendem Internetzugang starten, der über eine alternative Methode, z. B. ein NAT-Gateway, bereitgestellt wird. Weitere Informationen finden Sie unter [EC2 Amazon-Instance-IP-Adressierung](#) im EC2 Amazon-Benutzerhandbuch.

- Konfigurieren des SSH-Zugriffs auf Knoten (Optional). Mit der Aktivierung von SSH können Sie eine Verbindung zu Ihren Instances herstellen und Diagnoseinformationen erfassen,

wenn Probleme auftreten. Wir empfehlen dringend, den Fernzugriff zu aktivieren, sobald Sie eine Knotengruppe erstellen. Sie können den Fernzugriff nicht mehr aktivieren, nachdem die Knotengruppe erstellt wurde.

Wenn Sie sich für die Verwendung einer Startvorlage entschieden haben, wird diese Option nicht angezeigt. Um den Remotezugriff auf Ihre Knoten zu aktivieren, geben Sie in der Startvorlage ein Schlüsselpaar an und stellen Sie sicher, dass die richtige Schnittstelle für die Knoten in den Sicherheitsgruppen geöffnet ist, die Sie in der Startvorlage angeben. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Sicherheitsgruppen”](#).

 Note

Für Windows aktiviert dieser Befehl SSH nicht. Stattdessen wird Ihr EC2 Amazon-Schlüsselpaar mit der Instance verknüpft und Sie können per RDP auf die Instance zugreifen.

- Wählen Sie für das SSH-Schlüsselpaar (optional) einen Amazon EC2 SSH-Schlüssel aus, den Sie verwenden möchten. Informationen zu Linux finden Sie unter [EC2 Amazon-Schlüsselpaare und Linux-Instances](#) im EC2 Amazon-Benutzerhandbuch. Informationen zu Windows finden Sie unter [EC2 Amazon-Schlüsselpaare und Windows-Instances](#) im EC2 Amazon-Benutzerhandbuch. Wenn Sie sich für die Verwendung einer Startvorlage entschieden haben, können Sie keine auswählen. Wenn ein Amazon EC2 SSH-Schlüssel für Knotengruppen bereitgestellt wird, die Bottlerocket verwenden AMLs, ist der administrative Container ebenfalls aktiviert. Weitere Informationen finden Sie unter [Administrator-Container](#) auf GitHub.
  - Für Zulassen des SSH-Remote-Zugriffs von, wenn Sie den Zugriff auf bestimmte Instances beschränken möchten, wählen Sie die Sicherheitsgruppen aus, die diesen Instances zugeordnet sind. Wenn Sie keine bestimmten Sicherheitsgruppen auswählen, ist der SSH-Zugriff von überall im Internet aus erlaubt (). 0.0.0.0/0
9. Überprüfen Sie auf der Seite Review and create (Überprüfen und Erstellen) die Konfiguration der verwalteten Knoten, und wählen Sie Create (Erstellen).

Wenn Knoten dem Cluster nicht beitreten können, finden Sie weitere Informationen [the section called “Knoten können nicht mit dem Cluster verknüpft werden”](#) im Kapitel Fehlerbehebung.

10. Sehen Sie sich den Status Ihrer Knoten an und warten Sie, bis diese in den Ready-Status eintreten.

```
kubectl get nodes --watch
```

11.(Nur GPU-Knoten) Wenn Sie einen GPU-Instance-Typ und ein für Amazon EKS optimiertes beschleunigtes AMI ausgewählt haben, müssen Sie das [NVIDIA-Geräte-Plug-In für Kubernetes](#) als DaemonSet auf Ihrem Cluster anwenden. Ersetzen Sie es `vX.X.X` durch die gewünschte [s-device-pluginNVIDIA/K8-Version](#), bevor Sie den folgenden Befehl ausführen.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/deployments/static/nvidia-device-plugin.yml
```

## Installieren Sie Kubernetes-Add-Ons

Da Sie nun über einen funktionierenden Amazon EKS-Cluster mit Knoten verfügen, können Sie mit der Installation von Kubernetes-Add-Ons und der Bereitstellung von Anwendungen in Ihrem Cluster beginnen. Die folgenden Dokumentationsthemen helfen Ihnen bei der Erweiterung der Funktionalität Ihres Clusters.

- Der [IAM-Principal](#), der den Cluster erstellt hat, ist der einzige Principal, der Aufrufe an den Kubernetes-API-Server mit oder dem tätigen kann. `kubectl` AWS Management Console Wenn Sie möchten, dass andere IAM-Prinzipale Zugriff auf Ihren Cluster haben, müssen Sie sie hinzufügen. Weitere Informationen erhalten Sie unter [the section called “Kubernetes-API-Zugriff”](#) und [the section called “Erforderliche Berechtigungen”](#).
- Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:
  - Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
  - Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

- Konfigurieren Sie den Kubernetes [Cluster Autoscaler](#) so, dass die Anzahl der Knoten in Ihren Knotengruppen automatisch angepasst wird.
- Stellen Sie eine [Beispielanwendung](#) für Ihr Cluster bereit.
- [Organisieren und überwachen Sie Cluster-Ressourcen](#) mit wichtigen Tools für die Verwaltung Ihres Clusters.

## Aktualisieren Sie eine verwaltete Knotengruppe für Ihren Cluster

Wenn Sie ein Update für verwaltete Knotengruppen initiieren, aktualisiert Amazon EKS Ihre Knoten automatisch für Sie und führt dabei die unter [Grundlegendes zu jeder Phase der Knotenaktualisierungen](#) aufgeführten Schritte durch. Wenn Sie ein für Amazon EKS optimiertes AMI verwenden, wendet Amazon EKS als Teil der neuesten AMI-Release-Version automatisch die neuesten Sicherheitspatches und Betriebssystemupdates auf Ihre Knoten an.

Es gibt mehrere Szenarien, in denen es nützlich ist, die Version oder Konfiguration Ihrer Amazon EKS-verwalteten Knotengruppe zu aktualisieren:

- Sie haben die Kubernetes-Version für Ihren Amazon-EKS-Cluster aktualisiert und möchten Ihre Arbeitsknoten so aktualisieren, dass sie dieselbe Kubernetes-Version verwenden.
- Eine neue AMI-Version ist für Ihre verwaltete Knotengruppe verfügbar. Weitere Informationen zu AMI-Versionen finden Sie unter diesen Abschnitten:
  - [the section called “Versionsinformationen abrufen”](#)
  - [the section called “Bottlerocket”](#)
  - [the section called “Versionsinformationen abrufen”](#)
- Sie möchten die minimale, maximale oder gewünschte Anzahl der Instances in Ihrer verwalteten Knotengruppe anpassen.
- Sie möchten Kubernetes-Labels hinzufügen oder aus den Instances in Ihrer verwalteten Knotengruppe entfernen.
- Sie möchten Ihrer verwalteten Knotengruppe AWS Tags hinzufügen oder daraus entfernen.
- Sie müssen eine neue Version einer Startvorlage mit Konfigurationsänderungen bereitstellen, z. B. ein aktualisiertes benutzerdefiniertes AMI.
- Sie haben Version 1.9.0 oder höher des Amazon VPC CNI-Add-ons bereitgestellt, das Add-on für die Präfix-Delegierung aktiviert und möchten, dass neue AWS Nitro System-Instances in einer Knotengruppe eine deutlich höhere Anzahl von Pods unterstützen. Weitere Informationen finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#).
- Sie haben die IP-Präfix-Delegierung für Windows-Knoten aktiviert und möchten, dass neue AWS Nitro System-Instances in einer Knotengruppe eine deutlich höhere Anzahl von Pods unterstützen. Weitere Informationen finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#).

Wenn es eine neuere AMI-Release-Version für die Kubernetes-Version Ihrer verwalteten Knotengruppe gibt, können Sie die Version Ihrer Knotengruppe aktualisieren, um die neuere AMI-



Version zu verwenden. Ebenso können Sie, wenn auf Ihrem Cluster eine Kubernetes-Version ausgeführt wird, die neuer als Ihre Knotengruppe ist, die Knotengruppe so aktualisieren, dass sie die neueste AMI-Release-Version verwendet, die der Kubernetes-Version Ihres Clusters entspricht.

Wenn ein Knoten in einer verwalteten Knotengruppe aufgrund eines Skalierungsvorgangs oder einer Aktualisierung beendet wird, werden die Pods in diesem Knoten zuerst entleert. Weitere Informationen finden Sie unter [the section called “Verhaltensdetails aktualisieren”](#).

## Aktualisieren einer Knotengruppenversion

Sie können eine Knotengruppenversion mit einer der folgenden Optionen aktualisieren:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

Die Version, auf die Sie aktualisieren, darf nicht höher sein als die Version der Steuerungsebene.

## eksctl

Aktualisieren Sie eine verwaltete Knotengruppe mit **eksctl**

Aktualisieren Sie eine verwaltete Knotengruppe mit dem folgenden Befehl auf die neueste AMI-Version derselben Kubernetes-Version, die derzeit auf den Knoten bereitgestellt wird. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
eksctl upgrade nodegroup \
 --name=node-group-name \
 --cluster=my-cluster \
 --region=region-code
```

### Note

Wenn Sie eine Knotengruppe, die mit einer Startvorlage bereitgestellt wurde, auf eine neue Version der Startvorlage aktualisieren, fügen Sie den vorherigen `--launch-template-version` *version-number* Befehl hinzu. Die Startvorlage muss die unter [Anpassen verwalteter Knoten mit Startvorlagen](#) beschriebenen Anforderungen erfüllen. Wenn die Startvorlage ein benutzerdefiniertes AMI enthält, muss das AMI die Anforderungen [unter Spezifizieren eines AMI](#) erfüllen. Wenn Sie Ihre Knotengruppe auf eine neuere Version



Ihrer Startvorlage aktualisieren, wird jeder Knoten wiederverwendet, damit er der neuen Konfiguration der angegebenen Startvorlagenversion entspricht.

Sie können eine Knotengruppe, die ohne Startvorlage bereitgestellt wurde, nicht direkt auf eine neue Version der Startvorlage aktualisieren. Stattdessen müssen Sie mithilfe der Startvorlage eine neue Knotengruppe bereitstellen, um die Knotengruppe auf eine neue Version der Startvorlage zu aktualisieren.

Sie können eine Knotengruppe auf dieselbe Version wie die Kubernetes-Version der Steuerungsebene aktualisieren. Wenn Sie beispielsweise einen Cluster haben, auf dem Kubernetes ausgeführt wird, können Sie Knoten 1.33, auf denen Kubernetes derzeit ausgeführt wird, mit dem folgenden Befehl 1.32 auf Version aktualisieren. 1.33

```
eksctl upgrade nodegroup \
 --name=node-group-name \
 --cluster=my-cluster \
 --region=region-code \
 --kubernetes-version=1.33
```

## AWS Management Console

Aktualisieren Sie eine verwaltete Knotengruppe mit dem AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Cluster aus, der die zu aktualisierende Knotengruppe enthält.
3. Wenn mindestens eine Knotengruppe über ein verfügbares Update verfügt, wird oben auf der Seite ein Feld angezeigt, in dem Sie über das verfügbare Update informiert werden. Wenn Sie die Registerkarte Compute auswählen, wird in der Spalte AMI-Release-Version in der Tabelle Knotengruppen für die Knotengruppe, für die ein Update verfügbar ist, die Option Jetzt aktualisieren angezeigt. Um die Knotengruppe zu aktualisieren, wählen Sie Update now (Jetzt aktualisieren).

Für Knotengruppen, die mit einem benutzerdefinierten AMI bereitgestellt wurden, wird keine Benachrichtigung angezeigt. Wenn Ihre Knoten mit einem benutzerdefinierten AMI bereitgestellt werden, führen Sie die folgenden Schritte aus, um ein neues aktualisiertes benutzerdefiniertes AMI bereitzustellen.

- a. Erstellen Sie eine neue Version Ihres AMI.

- b. Erstellen Sie eine neue Version der Startvorlage mit der neuen AMI-ID.
  - c. Aktualisieren Sie die Knoten auf die neue Version der Startvorlage.
4. Aktivieren oder deaktivieren Sie im Dialogfeld Update node group version (Knotengruppenversion aktualisieren) die folgenden Optionen:
- Update node group version (Knotengruppenversion aktualisieren) – Diese Option ist nicht verfügbar, wenn Sie ein benutzerdefiniertes AMI bereitgestellt haben oder Ihr Amazon EKS-optimiertes AMI derzeit über die neueste Version für Ihren Cluster verfügt.
  - Change launch template version (Startvorlagenversion ändern) – Diese Option ist nicht verfügbar, wenn die Knotengruppe ohne eine benutzerdefinierte Startvorlage bereitgestellt wird. Sie können die Version der Startvorlage nur für eine Knotengruppe aktualisieren, die mit einer benutzerdefinierten Startvorlage bereitgestellt wurde. Wählen Sie die Launch template version (Startvorlagenversion) aus, auf die Sie die Knotengruppe aktualisieren möchten. Wenn Ihre Knotengruppe mit einem benutzerdefinierten AMI konfiguriert ist, muss die ausgewählte Version auch ein AMI angeben. Wenn Sie ein Upgrade auf eine neuere Version Ihrer Startvorlage durchführen, wird jeder Knoten wiederverwertet, damit er der neuen Konfiguration der angegebenen Startvorlagenversion entspricht.
5. Wählen Sie für Update strategy (Aktualisierungsstrategie) eine der folgenden Optionen aus:
- Fortlaufendes Update — Diese Option berücksichtigt die Budgets für Pod-Unterbrechungen in Ihrem Cluster. Updates schlagen fehl, wenn es ein Budgetproblem bei einer Pod-Unterbrechung gibt, das dazu führt, dass Amazon EKS die Pods, die auf dieser Knotengruppe ausgeführt werden, nicht ordnungsgemäß entladen kann.
  - Aktualisierung erzwingen — Diese Option berücksichtigt nicht die Budgets für Pod-Unterbrechungen. Updates erfolgen unabhängig von Budgetproblemen bei Pod-Unterbrechungen, indem ein Neustart des Knotens erzwungen wird.
6. Wählen Sie Aktualisieren.

## Bearbeiten einer Knotengruppenkonfiguration

Sie können einige Konfigurationen einer verwalteten Knotengruppe ändern.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Cluster aus, der die zu bearbeitende Knotengruppe enthält.
3. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
4. Wählen Sie die zu bearbeitende Knotengruppe aus und wählen Sie dann Edit (Bearbeiten).

5. (Optional) Gehen Sie auf der Seite Edit node group (Knotengruppe bearbeiten) wie folgt vor:
- Bearbeiten Sie die Node group scaling configuration (Skalierungskonfiguration der Knotengruppe).
    - Desired size (Gewünschte Größe) – Geben Sie die aktuelle Anzahl von Knoten an, die die verwaltete Knotengruppe beibehalten soll.
    - Minimum size (Mindestgröße) – Geben Sie die Mindestanzahl von Knoten an, auf die die verwaltete Knotengruppe skaliert werden kann.
    - Maximum size (Maximale Größe) – Geben Sie die maximale Anzahl von Knoten an, auf die die verwaltete Knotengruppe skaliert werden kann. Die maximale Anzahl von Knoten, die in einer Knotengruppe unterstützt werden, finden Sie unter [the section called “Servicekontingente”](#).
  - (Optional) Fügen Sie den Knoten in Ihrer Knotengruppe Kubernetes-Labels hinzu oder entfernen Sie sie. Die hier gezeigten Labels sind nur die Labels, die Sie mit Amazon EKS angewendet haben. Möglicherweise sind auf Ihren Knoten andere Labels vorhanden, die hier nicht angezeigt werden.
  - (Optional) Fügen Sie den Knoten in Ihrer Knotengruppe Kubernetes-Taints hinzu oder entfernen Sie sie. Hinzugefügte Färbungen können die Wirkung von **NoSchedule** , **NoExecute** , oder **PreferNoSchedule** haben. Weitere Informationen finden Sie unter [the section called “Verfälschen Sie GPU-Knoten”](#).
  - (Optional) Fügen Sie Tags zu Ihrer Knotengruppenressource hinzu oder entfernen Sie sie. Diese Markierungen werden nur auf die Amazon-EKS-Knotengruppe angewendet. Sie werden nicht auf andere Ressourcen wie Subnetze oder EC2 Amazon-Instances in der Knotengruppe übertragen.
  - (Optional) Bearbeiten Sie Konfiguration der Knotengruppe aktualisieren. Wählen Sie entweder Zahl oder Prozentanteil aus.
    - Zahl – Wählen und geben Sie die Anzahl der Knoten in Ihrer Knotengruppe an, die parallel aktualisiert werden können. Diese Knoten sind während der Aktualisierung nicht verfügbar.
    - Prozentsatz – Wählen und geben Sie den Prozentsatz der Knoten in der Knotengruppe an, die parallel aktualisiert werden können. Diese Knoten sind während der Aktualisierung nicht verfügbar. Dies ist nützlich, wenn Sie viele Knoten in Ihrer Knotengruppe haben.
  - Wenn Sie mit der Bearbeitung fertig sind, wählen Sie Änderungen speichern.

### Important

Wenn Sie die Konfiguration der Knotengruppe aktualisieren, werden bei der Änderung der [NodegroupScalingConfig](#) nicht die Budgets für Pod-Unterbrechungen berücksichtigt (PDBs). Im Gegensatz zum Prozess zum [Aktualisieren von Knotengruppen](#) (bei dem PDBs während der Upgrade-Phase Knoten geleert und respektiert werden) führt die Aktualisierung der Skalierungskonfiguration dazu, dass Knoten sofort durch einen Auto Scaling Scale-Down-Aufruf (ASG) beendet werden. Dies geschieht ohne weitere Überlegungen PDBs, unabhängig von der Zielgröße, auf die Sie herunterskalieren. Das heißt, wenn Sie die Anzahl einer `desiredSize` von Amazon EKS verwalteten Knotengruppe reduzieren, werden Pods entfernt, sobald die Knoten beendet werden, ohne dass sie berücksichtigt werden. PDBs

## Verstehen Sie jede Phase der Knotenaktualisierungen

Die Upgrade-Strategie für verwaltete Amazon-EKS-Worker-Knoten umfasst vier verschiedene Phasen, die in den folgenden Abschnitten beschrieben werden.

### Einrichtungsphase

Die Einrichtungsphase umfasst folgende Schritte:

1. Es erstellt eine neue EC2 Amazon-Startvorlagenversion für die Auto Scaling Scaling-Gruppe, die Ihrer Knotengruppe zugeordnet ist. Die neue Version der Startvorlage verwendet das Ziel-AMI oder die vom Kunden bereitgestellte Startvorlagenversion für die Aktualisierung.
2. Es aktualisiert die Auto Scaling Group, sodass sie die neueste Version der Startvorlage verwendet.
3. Es bestimmt die maximale Anzahl der parallel zu aktualisierenden Knoten mithilfe der `updateConfig`-Eigenschaft für die Knotengruppe. Der maximal nicht verfügbare Wert hat ein Kontingent von 100 Knoten. Der Standardwert beträgt einen Knoten. Weitere Informationen finden Sie in der Eigenschaft [updateConfig](#) in der Amazon EKS API-Referenz.

### Aufskalierungsphase

Beim Upgrade der Knoten in einer verwalteten Knotengruppe werden die aktualisierten Knoten in derselben Availability Zone gestartet wie diejenigen, die aktualisiert werden. Um diese Platzierung zu garantieren, verwenden wir EC2 das Availability Zone Rebalancing von Amazon. Weitere Informationen finden Sie unter [Availability Zone Rebalancing](#) im Amazon EC2 Auto Scaling Scaling-

Benutzerhandbuch. Um diese Anforderung zu erfüllen, ist es möglich, dass wir bis zu zwei Instances pro Availability Zone in Ihrer verwalteten Knotengruppe starten.

Die Aufskalierungsphase umfasst folgende Schritte:

1. Es erhöht die maximale Größe und die gewünschte Größe der Auto Scaling Scaling-Gruppe um den jeweils größeren der folgenden Werte:

- Bis zu doppelt so viele Availability Zones, in denen die Auto Scaling Group bereitgestellt wird.
- Die maximale Nichtverfügbarkeit der Aktualisierung.

Wenn Ihre Knotengruppe beispielsweise über fünf Availability Zones und `maxUnavailable` als eine verfügt, kann der Upgrade-Prozess maximal zehn Knoten starten. Wenn jedoch 20 (oder etwas höher als 10) `maxUnavailable` ist, würde der Prozess 20 neue Knoten starten.

2. Nach dem Skalieren der Auto-Scaling-Gruppe wird überprüft, ob die Knoten, die die neueste Konfiguration verwenden, in der Knotengruppe vorhanden sind. Dieser Schritt ist nur erfolgreich, wenn er diese Kriterien erfüllt:

- Mindestens ein neuer Knoten wird in jeder Availability Zone gestartet, in der der Knoten existiert.
- Jeder neue Knoten sollte im Ready-Zustand sein.
- Neue Knoten sollten Amazon-EKS-Labels angewandt haben.

Dies sind die von Amazon EKS auf die Worker-Knoten in einer regulären Knotengruppe angewandten Labels:

- `eks.amazonaws.com/nodegroup-image=$amiName`
- `eks.amazonaws.com/nodegroup=$nodeGroupName`

Dies sind die von Amazon EKS angewendeten Labels auf den Worker-Knoten in einer benutzerdefinierten Startvorlage oder AMI-Knotengruppe:

- `eks.amazonaws.com/nodegroup-image=$amiName`
- `eks.amazonaws.com/nodegroup=$nodeGroupName`
- `eks.amazonaws.com/sourceLaunchTemplateId=$launchTemplateId`
- `eks.amazonaws.com/sourceLaunchTemplateVersion=$launchTemplateVersion`

3. Es markiert Knoten als nicht planbar, um die Planung neuer Pods zu vermeiden. Es kennzeichnet Knoten auch mit `node.kubernetes.io/exclude-from-external-load-balancers=true`, um die alten Knoten aus den Load Balancern zu entfernen, bevor die Knoten beendet werden.

Die folgenden sind bekannte Gründe, die zu einem `NodeCreationFailure`-Fehler in dieser Phase führen:

### Unzureichende Kapazität in der Availability Zone

Es besteht die Möglichkeit, dass die Availability Zone nicht über die Kapazität der angeforderten Instance-Typen verfügt. Es wird empfohlen, bei der Erstellung einer verwalteten Knotengruppe mehrere Instanztypen zu konfigurieren.

### EC2 Instanzlimits in Ihrem Konto

Möglicherweise müssen Sie die Anzahl der EC2 Amazon-Instances erhöhen, die Ihr Konto mithilfe von Service Quotas gleichzeitig ausführen kann. Weitere Informationen finden Sie unter [EC2 Service Quotas](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.

### Benutzerdefinierte Benutzerdaten

Anwenderbezogene Benutzerdaten können manchmal den Bootstrap-Prozess stören. Dieses Szenario kann dazu führen, dass `kubelet` nicht auf dem Knoten startet oder Knoten nicht die erwarteten Amazon-EKS-Labels auf ihnen erhalten. Weitere Informationen finden Sie unter [the section called "Angeben eines AMI"](#).

Alle Änderungen, die dazu führen, dass ein Knoten fehlerhaft ist oder nicht bereit ist

Knotenfestplattendruck, Speicherdruck und ähnliche Bedingungen können dazu führen, dass ein Knoten nicht in den Ready-Zustand wechselt.

Jeder Knoten ist innerhalb von 15 Minuten startbereit

Wenn ein Knoten länger als 15 Minuten benötigt, um zu booten und dem Cluster beizutreten, führt dies zu einem Timeout für das Upgrade. Dies ist die Gesamtlaufzeit für das Bootstrapping eines neuen Knotens, gemessen vom Zeitpunkt, zu dem ein neuer Knoten benötigt wird, bis zu dem Zeitpunkt, zu dem er dem Cluster beitrifft. Beim Upgrade einer verwalteten Knotengruppe startet der Zeitzähler, sobald die Größe der Auto Scaling Scaling-Gruppe zunimmt.

## Aktualisierungs-Phase

Die Upgrade-Phase verhält sich je nach Aktualisierungsstrategie auf zwei verschiedene Arten. Es gibt zwei Aktualisierungsstrategien: Standard - und Minimalaktualisierungsstrategien.

In den meisten Szenarien empfehlen wir die Standardstrategie. Sie erstellt neue Knoten, bevor die alten beendet werden, sodass die verfügbare Kapazität während der Upgrade-Phase erhalten bleibt.

Die Minimalstrategie ist in Szenarien nützlich, in denen Sie auf Ressourcen oder Kosten beschränkt sind, z. B. bei Hardwarebeschleunigern wie GPUs. Dabei werden die alten Knoten beendet, bevor die neuen erstellt werden, sodass die Gesamtkapazität nie über die konfigurierte Menge hinausgeht.

Die Standard-Aktualisierungsstrategie umfasst die folgenden Schritte:

1. Es erhöht die Anzahl der Knoten (gewünschte Anzahl) in der Auto Scaling Scaling-Gruppe, wodurch die Knotengruppe zusätzliche Knoten erstellt.
2. Es wählt nach dem Zufallsprinzip einen Knoten aus, der aktualisiert werden muss, bis zum Maximum der für die Knotengruppe nicht verfügbar ist.
3. Es entleert die Pods aus dem Knoten. Wenn die Pods den Knoten nicht innerhalb von 15 Minuten verlassen und kein Force-Flag angezeigt wird, schlägt die Upgrade-Phase mit einem `PodEvictionFailure` Fehler fehl. In diesem Szenario können Sie das Force-Flag mit der `update-nodegroup-version` Aufforderung zum Löschen der Pods anwenden.
4. Es sperrt den Knoten ab, nachdem jeder Pod geräumt wurde, und wartet 60 Sekunden. Dies geschieht, damit der Service Controller keine neuen Anfragen an diesen Knoten sendet und diesen Knoten aus seiner Liste der aktiven Knoten entfernt.
5. Es sendet eine Beendigungsanforderung an die Auto-Scaling-Gruppe für den abgesperrten Knoten.
6. Es wiederholt die vorherigen Aktualisierungsschritte, bis keine Knoten in der Knotengruppe mehr vorhanden sind, die mit der früheren Version der Startvorlage bereitgestellt wurden.

Die Minimalaktualisierungsstrategie umfasst die folgenden Schritte:

1. Sie sperrt zu Beginn alle Knoten der Knotengruppe ab, sodass der Service Controller keine neuen Anfragen an diese Knoten sendet.
2. Es wählt nach dem Zufallsprinzip einen Knoten aus, der aktualisiert werden muss, bis zum Maximum der für die Knotengruppe nicht verfügbar ist.
3. Er entleert die Pods von den ausgewählten Knoten. Wenn die Pods den Knoten nicht innerhalb von 15 Minuten verlassen und kein Force-Flag angezeigt wird, schlägt die Upgrade-Phase mit einem `PodEvictionFailure` Fehler fehl. In diesem Szenario können Sie das Force-Flag mit der `update-nodegroup-version` Aufforderung zum Löschen der Pods anwenden.
4. Nachdem jeder Pod entfernt wurde und 60 Sekunden gewartet hat, sendet er eine Kündigungsanfrage an die Auto Scaling Group für die ausgewählten Knoten. Die Auto Scaling Group erstellt neue Knoten (entspricht der Anzahl der ausgewählten Knoten), um die fehlende Kapazität zu ersetzen.

5. Es wiederholt die vorherigen Aktualisierungsschritte, bis keine Knoten in der Knotengruppe mehr vorhanden sind, die mit der früheren Version der Startvorlage bereitgestellt wurden.

## PodEvictionFailureFehler während der Upgrade-Phase

Die folgenden sind bekannte Gründe, die zu einem PodEvictionFailure-Fehler in dieser Phase führen:

### Aggressives PDB

Aggressive PDB ist auf dem Pod definiert, oder es gibt mehrere, die auf denselben Pod PDBs verweisen.

### Einsatz, der alle Makel toleriert

Sobald jeder Pod entfernt wurde, wird davon ausgegangen, dass der Knoten leer ist, da der Knoten in den vorherigen Schritten [beschädigt wurde](#). Wenn das Deployment jedoch jeden Makel toleriert, ist es wahrscheinlicher, dass der Knoten nicht leer ist, was dazu führt, dass der Pod nicht entfernt werden kann.

## Abskalierungsphase

Die Abskalierungsphase verringert die maximale Größe der Auto-Scaling-Gruppe und die gewünschte Größe um eins, um zu den Werten zurückzukehren, bevor die Aktualisierung gestartet wurde.

Wenn der Upgrade-Workflow feststellt, dass der Cluster-Autoscaler die Knotengruppe während der Herunterskalierungsphase des Workflows skaliert, wird er sofort beendet, ohne die Knotengruppe wieder auf ihre ursprüngliche Größe zu bringen.

## Passen Sie verwaltete Knoten mit Startvorlagen an

Für die höchste Anpassungsstufe können Sie verwaltete Knoten mithilfe Ihrer eigenen Startvorlage bereitstellen. Die Verwendung einer Startvorlage ermöglicht Funktionen wie die folgenden:

- Geben Sie bei der Bereitstellung eines Knotens Bootstrap-Argumente an, z. B. zusätzliche [Kubelet-Argumente](#).
- Weisen Sie Pods IP-Adressen zu, die aus einem anderen CIDR-Block stammen als der IP-Adresse, die dem Knoten zugewiesen wurde.
- Bereitstellen Ihres eigenen benutzerdefinierten AMI auf Knoten



- Bereitstellen Ihres eigenen benutzerdefinierten CNI auf Knoten

Wenn Sie beim ersten Erstellen einer verwalteten Knotengruppe Ihre eigene Startvorlage angeben, haben Sie auch später mehr Flexibilität. Wenn Sie eine verwaltete Knotengruppe mit Ihrer eigenen Startvorlage bereitstellen, können Sie sie schrittweise mit einer anderen Version derselben Startvorlage aktualisieren. Wenn Sie Ihre Knotengruppe auf eine andere Version Ihrer Startvorlage aktualisieren, werden alle Knoten in der Gruppe wiederverwertet, damit sie der neuen Konfiguration der angegebenen Startvorlagenversion entsprechen.

Verwaltete Knotengruppen werden immer mit einer Startvorlage bereitgestellt, die mit der Amazon EC2 Auto Scaling Scaling-Gruppe verwendet werden kann. Wenn Sie keine Startvorlage angeben, erstellt die Amazon EKS-API automatisch eine mit Standardwerten in Ihrem Konto. Wir empfehlen jedoch nicht, automatisch generierte Startvorlagen zu ändern. Darüber hinaus können bestehende Knotengruppen, die keine benutzerdefinierte Startvorlage verwenden, nicht direkt aktualisiert werden. Stattdessen müssen Sie eine neue Knotengruppe mit einer benutzerdefinierten Startvorlage erstellen.

## Grundlagen der Konfiguration der Vorlage starten

Sie können eine Amazon EC2 Auto Scaling Scaling-Startvorlage mit der AWS Management Console, AWS CLI oder einem AWS SDK erstellen. Weitere Informationen finden Sie unter [Erstellen einer Startvorlage für eine Auto Scaling Scaling-Gruppe](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. Einige der Einstellungen in einer Startvorlage ähneln den Einstellungen, die für die Konfiguration verwalteter Knoten verwendet werden. Beim Bereitstellen oder Aktualisieren einer Knotengruppe mit einer Startvorlage müssen einige Einstellungen entweder in der Knotengruppenkonfiguration oder in der Startvorlage angegeben werden. Geben Sie nicht an beiden Stellen eine Einstellung an. Wenn eine Einstellung dort vorhanden ist, wo sie nicht sein sollte, schlagen Operationen wie das Erstellen oder Aktualisieren einer Knotengruppe fehl.

In der folgenden Tabelle werden die Einstellungen aufgelistet, die in einer Startvorlage nicht zulässig sind. Es listet auch ähnliche Einstellungen auf, falls verfügbar, die in der Konfiguration der verwalteten Knotengruppe erforderlich sind. Die aufgelisteten Einstellungen sind die Einstellungen, die in der Konsole angezeigt werden. Sie haben möglicherweise ähnliche, aber unterschiedliche Namen in der AWS CLI und im SDK.

| Startvorlage - Verboten                                                    | Amazon-EKS-Knotengruppenkonfiguration                                                |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Subnetz in Netzwerkschnittstellen (Hinzufügen einer Netzwerkschnittstelle) | Subnets (Subnetze) unter Node group network configuration (Netzwerkkonfiguration der |

|                                                                                                                                                                                                       |                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Startvorlage - Verboten                                                                                                                                                                               | Amazon-EKS-Knotengruppenkonfiguration                                                                                                                        |
|                                                                                                                                                                                                       | Knotengruppe) auf der Seite Specify networking (Netzwerk angeben)                                                                                            |
| IAM-Instance-Profil in Erweiterte Details                                                                                                                                                             | Node IAM role (Knoten-IAM-Rolle) unter Node group configuration (Knotengruppenkonfiguration) auf der Seite Configure Node group (Knotengruppe konfigurieren) |
| Verhalten beim Herunterfahren und Stop – Ruhezustand Verhalten in Erweiterte Details. Standard beibehalten Nicht in die Startvorlageinstellung in der Startvorlage für beide Einstellungen aufnehmen. | Keine Entsprechung Amazon EKS muss den Instance-Lebenszyklus steuern, nicht die Auto-Scaling-Gruppe.                                                         |

In der folgenden Tabelle sind die unzulässigen Einstellungen in einer Konfiguration einer verwalteten Knotengruppe aufgeführt. Sie listet auch ähnliche Einstellungen auf, falls vorhanden, die in einer Startvorlage erforderlich sind. Die aufgelisteten Einstellungen sind die Einstellungen, die in der Konsole angezeigt werden. Sie haben möglicherweise ähnliche Namen in der AWS CLI und im SDK.

| Konfiguration der Amazon-EKS-Knotengruppe — Verboten                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Startvorlage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>(Nur wenn Sie ein benutzerdefiniertes AMI in einer Startvorlage angegeben haben) AMI type (AMI-Typ) unter Node Group compute configuration (Computing-Konfiguration der Knotengruppe) auf der Seite Set compute and scaling configuration (Computing- und Skalierungskonfiguration festlegen) – Die Konsole zeigt Specified in launch template (In Startvorlage angegeben) und die angegebene AMI-ID an.</p> <p>Wenn Anwendungs- und Betriebssystem-Images (Amazon Machine Image) in der Startvorlage</p> | <p>Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) unter Inhalt der Startvorlage – Sie müssen eine ID angeben, wenn Sie eine der folgenden Anforderungen haben:</p> <ul style="list-style-type: none"> <li>• Verwenden eines benutzerdefinierten AMI<br/>Wenn Sie ein AMI angeben, das die unter <a href="#">AMI angeben</a> aufgeführten Anforderungen nicht erfüllt, schlägt die Bereitstellung der Knotengruppe fehl.</li> </ul> |

| Konfiguration der Amazon-EKS-Knotengruppe<br>— Verboten                                                                                                                                                                                                                                                   | Startvorlage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>age nicht angegeben wurden, können Sie in der Knotengruppenkonfiguration ein AMI auswählen.</p>                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• Sie möchten Benutzerdaten bereitstellen, um Argumente für die Datei bereitzustellen, die in einem für Amazon EKS optimierten AMI enthalten ist. Sie können es Ihren Instances ermöglichen, Pods eine deutlich höhere Anzahl von IP-Adressen zuzuweisen, Pods aus einem anderen CIDR-Block als dem der Instance IP-Adressen zuzuweisen oder einen privaten Cluster ohne ausgehenden Internetzugang bereitzustellen. Weitere Informationen finden Sie unter den folgenden Themen: <ul style="list-style-type: none"> <li>• <a href="#">Weisen Sie Amazon EKS-Knoten mehr IP-Adressen mit Präfixen zu</a></li> <li>• <a href="#">Stellen Sie Pods in alternativen Subnetzen mit benutzerdefiniertem Netzwerk bereit</a></li> <li>• <a href="#">Stellen Sie private Cluster mit eingeschränktem Internetzugang bereit</a></li> <li>• <a href="#">Ein AMI angeben</a></li> </ul> </li> </ul> |
| <p>Datenträgergröße unter Node Group compute configuration (Computing-Konfiguration der Knotengruppe) auf der Seite Set compute and scaling configuration – Die Konsole zeigt Specified in launch template (In Startvorlage angegeben) an.</p>                                                            | <p>Größe unter Speicher (Volumes) (Hinzufügen eines neuen Volumes) enthalten. Sie müssen dies in der Startvorlage angeben.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>SSH key pair (SSH-Schlüsselpaar) unter Node group configuration (Knotengruppenkonfiguration) auf der Seite Specify Networking (Netzwerk angeben) – Die Konsole zeigt den in der Startvorlage angegebenen Schlüssel an oder Not specified in launch template (Nicht in der Startvorlage angegeben).</p> | <p>Schlüsselpaarname in Schlüsselpaar (Login).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Konfiguration der Amazon-EKS-Knotengruppe<br>— Verboten                                                               | Startvorlage                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bei Verwendung einer Startvorlage können Sie keine Quellsicherheitsgruppen angeben, denen Remotezugriff gewährt wird. | Sicherheitsgruppen unter Netzwerkeinstellungen für die Instance oder Sicherheitsgruppen unter Netzwerkschnittstellen (Netzwerkschnittstelle hinzufügen), aber nicht beides. Weitere Informationen finden Sie unter <a href="#">the section called “Benutzerdefinierte Sicherheitsgruppen”</a> . |

### Note

- Wenn Sie eine Knotengruppe mithilfe einer Startvorlage bereitstellen, geben Sie in einer Startvorlage unter Inhalt der Startvorlage null oder einen Instance-Typ an. Alternativ können Sie 0 bis 20 Instance-Typen für Instance-Typen auf der Seite Einstellen von Compute- und Skalierungskonfiguration in der Konsole angeben. Oder Sie können dies mit anderen Tools tun, die die Amazon EKS API verwenden. Wenn Sie einen Instance-Typ in einer Startvorlage angeben und diese Startvorlage für die Bereitstellung Ihrer Knotengruppe verwenden, können Sie in der Konsole oder mit anderen Tools, die die Amazon EKS-API verwenden, keine Instance-Typen angeben. Wenn Sie in einer Startvorlage, in der Konsole oder mit anderen Tools, die die Amazon EKS-API verwenden, keinen Instance-Typ angeben, wird der `t3.medium` Instance-Typ verwendet. Wenn Ihre Knotengruppe den Spot-Kapazitätstyp verwendet, empfehlen wir, mehrere Instance-Typen über die Konsole anzugeben. Weitere Informationen finden Sie unter [the section called “Kapazitätstypen für verwaltete Knotengruppen”](#).
- Wenn Container, die Sie für die Knotengruppe bereitstellen, den Instance-Metadaten-Service Version 2 verwenden, stellen Sie sicher, dass Sie die Hop-Limits für Metadaten auf 2 in Ihrer Startvorlage festsetzen. Weitere Informationen finden Sie unter [Instance-Metadaten und Benutzerdaten](#) im EC2 Amazon-Benutzerhandbuch. Wenn Sie eine verwaltete Knotengruppe bereitstellen, ohne eine benutzerdefinierte Startvorlage zu verwenden, wird dieser Wert automatisch für die Knotengruppe in der Standardstartvorlage festgelegt.

- Startvorlagen unterstützen die `InstanceRequirements` Funktion, die eine flexible Auswahl des Instance-Typs ermöglicht, nicht.

## EC2 Amazon-Instances taggen

Sie können den `TagSpecification` Parameter einer Startvorlage verwenden, um anzugeben, welche Tags auf EC2 Amazon-Instances in Ihrer Knotengruppe angewendet werden sollen. Die IAM-Entität, die das `CreateNodegroup` oder aufruft, `UpdateNodegroupVersion` APIs muss über Berechtigungen für `ec2:RunInstances` und `ec2:CreateTags`, und die Tags müssen der Startvorlage hinzugefügt werden.

## Benutzerdefinierte Sicherheitsgruppen

Sie können eine Startvorlage verwenden, um benutzerdefinierte EC2 [Amazon-Sicherheitsgruppen](#) anzugeben, die auf Instances in Ihrer Knotengruppe angewendet werden sollen. Dies kann entweder im Parameter für Sicherheitsgruppen auf Instance-Ebene oder als Teil der Konfigurationsparameter der Netzwerkschnittstelle sein. Sie können jedoch keine Startvorlage erstellen, die sowohl Sicherheitsgruppen auf Instance-Ebene als auch auf Netzwerkschnittstellenebene festlegt. Beachten Sie die folgenden Bedingungen, die für die Verwendung benutzerdefinierter Sicherheitsgruppen mit verwalteten Knotengruppen gelten:

- Bei Verwendung von erlaubt Amazon EKS nur Startvorlagen mit einer einzigen Netzwerkschnittstellenspezifikation. AWS Management Console
- Standardmäßig wendet Amazon EKS die [Cluster-Sicherheitsgruppe](#) zu den Instances in Ihrer Knotengruppe hinzu, um die Kommunikation zwischen Knoten und der Steuerungsebene zu erleichtern. Wenn Sie benutzerdefinierte Sicherheitsgruppen in der Startvorlage mit einer der oben genannten Optionen angeben, fügt Amazon EKS die Cluster-Sicherheitsgruppe nicht hinzu. Sie müssen daher sicherstellen, dass die eingehenden und ausgehenden Regeln Ihrer Sicherheitsgruppen die Kommunikation mit dem Endpunkt Ihres Clusters ermöglichen. Wenn Ihre Sicherheitsgruppenregeln falsch sind, können die Worker-Knoten dem Cluster nicht beitreten. Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter [the section called "Anforderungen an Sicherheitsgruppen"](#).
- Wenn Sie SSH-Zugriff auf die Instances in Ihrer Knotengruppe benötigen, müssen Sie eine Sicherheitsgruppe einschließen, die diesen Zugriff zulässt.

## EC2 Amazon-Benutzerdaten

Die Einführungsvorlage enthält einen Abschnitt für benutzerdefinierte Benutzerdaten. In diesem Abschnitt können Sie die Konfigurationseinstellungen für Ihre Knotengruppe angeben, ohne manuell individuelle benutzerdefinierte Einstellungen erstellen zu müssen AMIs. Weitere Informationen zu den für Bottlerocket verfügbaren Einstellungen finden Sie unter [Benutzerdaten verwenden](#) am. GitHub

Sie können EC2 Amazon-Benutzerdaten in Ihrer Startvorlage angeben, die Sie `ccloud-init` beim Starten Ihrer Instances verwenden. Weitere Informationen dazu finden Sie in der [cloud-init-Dokumentation](#). Ihre Benutzerdaten können verwendet werden, um allgemeine Konfigurationsvorgänge durchzuführen. Dieser Filter umfasst die folgenden Optionen:

- [Einschließen von Benutzern oder Gruppen](#)
- [Installieren von Paketen](#)

EC2 Amazon-Benutzerdaten in Startvorlagen, die mit verwalteten Knotengruppen verwendet werden, müssen im [mehrteiligen MIME-Archivformat](#) für Amazon Linux AMIs und im TOML-Format für Bottlerocket vorliegen. AMIs Dies liegt daran, dass Ihre Benutzerdaten mit Amazon-EKS-Benutzerdaten zusammengeführt werden, die für Knoten erforderlich sind, um dem Cluster beizutreten. Geben Sie in Ihren Benutzerdaten keine Befehle an, die gestartet oder geändert werden. `kubelet` Dies wird als Teil der von Amazon EKS zusammengeführten Benutzerdaten durchgeführt. Bestimmte `kubelet`-Parameter, z. B. das Festlegen von Beschriftungen auf Knoten, können direkt über die API für verwaltete Knotengruppen konfiguriert werden.

### Note

Weitere Hinweise zur erweiterten `kubelet`-Anpassung, einschließlich des manuellen Startens oder Übergebens benutzerdefinierter Konfigurationsparameter, finden Sie unter [the section called “Angeben eines AMI”](#). Wenn eine benutzerdefinierte AMI-ID in einer Startvorlage angegeben ist, führt Amazon EKS keine Benutzerdaten zusammen.

Die folgenden Details enthalten weitere Informationen zum Abschnitt Benutzerdaten.

### Amazon Linux 2-Benutzerdaten

Sie können mehrere Benutzerdatenblöcke in einer einzelnen mehrteiligen MIME-Datei kombinieren. So können Sie beispielsweise einen Cloud-Boothook, der den Docker-Daemon

konfiguriert, mit einem Benutzerdaten-Shell-Skript kombinieren, das ein benutzerdefiniertes Paket installiert. Eine mehrteilige MIME-Datei umfasst folgende Komponenten:

- Deklaration von Inhaltstyp und Teilgrenze – Content-Type: `multipart/mixed; boundary="==MYBOUNDARY=="`
- Deklaration der MIME-Version – MIME-Version: `1.0`
- Ein oder mehrere Benutzerdatenblöcke mit folgenden Komponenten:
  - Eröffnungsgrenze, die den Beginn eines Benutzerdatenblocks signalisiert – `--==MYBOUNDARY==`
  - Die Inhaltstypdeklaration für den Block: Content-Type: `text/cloud-config; charset="us-ascii"`. Weitere Informationen zu Inhaltstypen finden Sie in der [Cloud-Init-Dokumentation](#).
  - Der Inhalt der Benutzerdaten (z. B. eine Liste von Shell-Befehlen oder `cloud-init`-Direktiven).
  - Abschlussgrenze, die das Ende der mehrteiligen MIME-Datei signalisiert: `--==MYBOUNDARY==--`

Im Folgenden finden Sie ein Beispiel für eine mehrteilige MIME-Datei, die Sie verwenden können, um Ihre eigene zu erstellen.

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="==MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
echo "Running custom user data script"

--==MYBOUNDARY==--
```

## Amazon Linux 2023 Benutzerdaten

Amazon Linux 2023 (AL2023) führt einen neuen Knoteninitialisierungsprozess `enodeadm`, der ein YAML-Konfigurationsschema verwendet. Wenn Sie selbstverwaltete Knotengruppen oder ein AMI mit einer Startvorlage verwenden, müssen Sie jetzt beim Erstellen einer neuen Knotengruppe explizit zusätzliche Cluster-Metadaten angeben. Ein [Beispiel](#) für die mindestens erforderlichen Parameter lautet wie folgt, wobei `apiServerEndpointcertificateAuthority`, und `Service` jetzt erforderlich `cidr` sind:

```

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: my-cluster
 apiServerEndpoint: https://example.com
 certificateAuthority: Y2VydG1maWNhdGVBdXRob3JpdHk=
 cidr: 10.100.0.0/16

```

In der Regel legen Sie diese Konfiguration in Ihren Benutzerdaten fest, entweder unverändert oder eingebettet in ein mehrteiliges MIME-Dokument:

```

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="BOUNDARY"

--BOUNDARY
Content-Type: application/node.eks.aws

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig spec: [...]

--BOUNDARY--

```

AL2In wurden die Metadaten dieser Parameter aus dem Amazon DescribeCluster EKS-API-Aufruf ermittelt. Mit AL2 023 hat sich dieses Verhalten geändert, da durch den zusätzlichen API-Aufruf die Gefahr einer Drosselung bei der Skalierung großer Knoten besteht. Diese Änderung hat keine Auswirkungen auf Sie, wenn Sie verwaltete Knotengruppen ohne Startvorlage verwenden oder wenn Sie Karpenter verwenden. Weitere Informationen zu `certificateAuthority` und `Service cidr` finden Sie [DescribeCluster](#) in der Amazon EKS API-Referenz.

Hier ist ein vollständiges Beispiel für AL2 023-Benutzerdaten, das ein Shell-Skript für die Anpassung des Knotens (wie die Installation von Paketen oder das Pre-Caching von Container-Images) mit der erforderlichen Konfiguration kombiniert. `nodeadm` Dieses Beispiel zeigt allgemeine Anpassungen, darunter:

- \* Installation zusätzlicher Systempakete
- \* Zwischenspeichern von Container-Images vor dem Zwischenspeichern, um die Startzeit des Pods zu verkürzen
- \* Einrichtung der HTTP-Proxykonfiguration
- \* Konfiguration von Flags für die Knotenbeschriftung

`kubelet`



```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
set -o errexit
set -o pipefail
set -o nounset

Install additional packages
yum install -y htop jq iptables-services

Pre-cache commonly used container images
nohup docker pull public.ecr.aws/eks-distro/kubernetes/pause:3.2 &

Configure HTTP proxy if needed
cat > /etc/profile.d/http-proxy.sh << 'EOF'
export HTTP_PROXY="http://proxy.example.com:3128"
export HTTPS_PROXY="http://proxy.example.com:3128"
export NO_PROXY="localhost,127.0.0.1,169.254.169.254,.internal"
EOF

--BOUNDARY
Content-Type: application/node.eks.aws

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: my-cluster
 apiServerEndpoint: https://example.com
 certificateAuthority: Y2VydGlmaWNhdGVBdXRob3JpdHk=
 cidr: 10.100.0.0/16
 kubelet:
 config:
 clusterDNS:
 - 10.100.0.10
 flags:
 - --node-labels=app=my-app,environment=production

--BOUNDARY--
```

## Bottlerocket-Benutzerdaten

Bottlerocket strukturiert Benutzerdaten im TOML-Format. Sie können Benutzerdaten angeben, die mit den von Amazon EKS bereitgestellten Benutzerdaten zusammengeführt werden sollen. Zum Beispiel können Sie zusätzliche kubelet-Einstellungen bereitstellen.

```
[settings.kubernetes.system-reserved]
cpu = "10m"
memory = "100Mi"
ephemeral-storage = "1Gi"
```

Weitere Informationen zu unterstützten Einstellungen finden Sie in der [Bottlerocket-Dokumentation](#). Sie können Knotenbezeichnungen und [Taints](#) in Ihren Benutzerdaten konfigurieren. Es wird jedoch empfohlen, diese stattdessen in Ihrer Knotengruppe zu konfigurieren. Amazon EKS wendet diese Konfigurationen an, wenn Sie dies tun.

Wenn Benutzerdaten zusammengeführt werden, bleibt die Formatierung nicht erhalten, der Inhalt bleibt jedoch derselbe. Die Konfiguration, die Sie in Ihren Benutzerdaten angeben, überschreibt alle Einstellungen, die von Amazon EKS konfiguriert wurden. Wenn Sie also `settings.kubernetes.max-pods` oder festlegen `settings.kubernetes.cluster-dns-ip`, werden diese Werte in Ihren Benutzerdaten auf die Knoten angewendet.

Amazon EKS unterstützt nicht alle gültigen TOML. Im Folgenden finden Sie eine Liste bekannter nicht unterstützter Formate:

- Zitate in Anführungszeichen: `'quoted "value"' = "value"`
- Anführungszeichen mit Escapezeichen in Werten: `str = "I'm a string. \"You can quote me\""`
- Gemischte Gleitkommazahlen und ganze Zahlen: `numbers = [ 0.1, 0.2, 0.5, 1, 2, 5 ]`
- Gemischte Typen in Arrays: `contributors = [ "foo@example.com", { name = "Baz", email = "baz@example.com" } ]`
- Kopfzeilen in Klammern mit Anführungszeichen: `[foo."bar.baz"]`

## Windows-Benutzerdaten

Windows-Benutzerdaten verwenden PowerShell Befehle. Beim Erstellen einer verwalteten Knotengruppe werden Ihre benutzerdefinierten Benutzerdaten mit den von Amazon EKS

verwalteten Benutzerdaten kombiniert. Ihre PowerShell Befehle stehen an erster Stelle, gefolgt von den Befehlen für verwaltete Benutzerdaten, alles innerhalb eines `<powershell></powershell>` Tags.

#### Important

Beim Erstellen von Windows-Knotengruppen aktualisiert Amazon EKS die `aws-authConfigMap`, damit Linux-basierte Knoten dem Cluster beitreten können. Der Service konfiguriert die Berechtigungen für Windows AMIs nicht automatisch. Wenn Sie Windows-Knoten verwenden, müssen Sie den Zugriff entweder über die Access Entry API oder durch `aws-auth ConfigMap` direkte Aktualisierung der API verwalten. Weitere Informationen finden Sie unter [the section called “Aktivieren Sie die Windows-Unterstützung”](#).

#### Note

Wenn in der Startvorlage keine AMI-ID angegeben ist, verwenden Sie nicht das Windows Amazon EKS Bootstrap-Skript in Benutzerdaten, um Amazon EKS zu konfigurieren.

Beispielbenutzerdaten lauten wie folgt.

```
<powershell>
Write-Host "Running custom user data script"
</powershell>
```

## Angeben eines AMI

Wenn Sie eine der folgenden Anforderungen haben, geben Sie eine AMI-ID in der ImageId-Startvorlage. Wählen Sie die Anforderung, die Sie für zusätzliche Informationen haben.

Geben Sie Benutzerdaten an, um Argumente an die **bootstrap.sh** Datei zu übergeben, die in einem Amazon EKS-optimierten Linux/Bottlerocket-AMI enthalten ist

Bootstrapping ist ein Begriff, der verwendet wird, um das Hinzufügen von Befehlen zu beschreiben, die beim Start einer Instance ausgeführt werden können. [Bootstrapping ermöglicht beispielsweise die](#)

Verwendung zusätzlicher Kubelet-Argumente. Sie können Argumente mithilfe von `eksctl` an das `bootstrap.sh`-Skript übergeben, ohne eine Startvorlage anzugeben. Oder Sie können dies tun, indem Sie die Informationen im Abschnitt Benutzerdaten einer Startvorlage angeben.

### eksctl ohne Angabe einer Startvorlage

Erstellen Sie eine Datei mit dem Namen *my-nodegroup.yaml* und dem folgenden Inhalt. Ersetzen Sie jede *example value* durch Ihre eigenen Werte. Die Argumente `--apiserver-endpoint`, `--b64-cluster-ca` und `--dns-cluster-ip` sind optional. Wenn sie definiert werden, verhindert dies jedoch, dass das `bootstrap.sh`-Skript einen `describeCluster`-Aufruf durchführt. Dies ist nützlich in privaten Cluster-Setups oder Clustern, in denen Sie häufig Knoten ein- und auswärts skalieren. Weitere Informationen zum `bootstrap.sh` Skript finden Sie in der Datei [bootstrap.sh](#) unter GitHub.

- Das einzige erforderliche Argument ist der Clustername (*my-cluster*).
- Informationen zum Abrufen einer optimierten AMI-ID für `ami-1234567890abcdef0` finden Sie in den folgenden Abschnitten:
  - [Rufen Sie das empfohlene Amazon Linux AMI ab IDs](#)
  - [Empfohlenes Bottlerocket-AMI abrufen IDs](#)
  - [Rufen Sie das empfohlene Microsoft Windows AMI ab IDs](#)
- Um die *certificate-authority* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus.

```
aws eks describe-cluster --query "cluster.certificateAuthority.data" --output text
--name my-cluster --region region-code
```

- Um den *api-server-endpoint* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus.

```
aws eks describe-cluster --query "cluster.endpoint" --output text --name my-
cluster --region region-code
```

- Der Wert für `--dns-cluster-ip` ist Ihr Service CIDR mit .10am Ende. Um das *service-cidr* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus. Wenn der zurückgegebene Wert beispielsweise `ipv4 10.100.0.0/16` ist, ist Ihr Wert *10.100.0.10*.

```
aws eks describe-cluster --query "cluster.kubernetesNetworkConfig.serviceIpv4Cidr"
--output text --name my-cluster --region region-code
```

- Dieses Beispiel umfasst ein kubelet-Argument, mit dem ein benutzerdefinierter max-pods-Wert anhand des bootstrap.sh-Skripts festgelegt wird, das im Amazon-EKS-optimierten AMI enthalten ist. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Hilfe zur Auswahl von *my-max-pods-value* finden Sie unter [the section called “Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen”](#).

```

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: my-cluster
 region: region-code

managedNodeGroups:
- name: my-nodegroup
 ami: ami-1234567890abcdef0
 instanceType: m5.large
 privateNetworking: true
 disableIMDSv1: true
 labels: { x86-a12-specified-mng }
 overrideBootstrapCommand: |
 #!/bin/bash
 /etc/eks/bootstrap.sh my-cluster \
 --b64-cluster-ca certificate-authority \
 --apiserver-endpoint api-server-endpoint \
 --dns-cluster-ip service-cidr.10 \
 --kubelet-extra-args '--max-pods=my-max-pods-value' \
 --use-max-pods false
```

Informationen zu allen verfügbaren eksctl-config-Dateioptionen finden Sie im [Config file schema](#) (Config-Datei-Schema) in der eksctl-Dokumentation. Das eksctl-Dienstprogramm erstellt eine Startvorlage für Sie und füllt die Benutzerdaten mit den Daten aus, die Sie in der config-Datei angeben.

Erstellen Sie eine Knoten-Gruppe mit dem folgenden Befehl.

```
eksctl create nodegroup --config-file=my-nodegroup.yaml
```

## Benutzerdaten in einer Startvorlage

Geben Sie die folgenden Informationen im Abschnitt Benutzerdaten Ihrer Startvorlage an. Ersetzen Sie jede *example value* durch Ihre eigenen Werte. Die Argumente `--apiserver-endpoint`, `--b64-cluster-ca` und `--dns-cluster-ip` sind optional. Wenn sie definiert werden, verhindert dies jedoch, dass das `bootstrap.sh`-Skript einen `describeCluster`-Aufruf durchführt. Dies ist nützlich in privaten Cluster-Setups oder Clustern, in denen Sie häufig Knoten ein- und auswärts skalieren. Weitere Informationen zum `bootstrap.sh` Skript finden Sie in der Datei [bootstrap.sh](#) unter GitHub.

- Das einzige erforderliche Argument ist der Clustername (*my-cluster*).
- Um die *certificate-authority* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus.

```
aws eks describe-cluster --query "cluster.certificateAuthority.data" --output text
--name my-cluster --region region-code
```

- Um den *api-server-endpoint* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus.

```
aws eks describe-cluster --query "cluster.endpoint" --output text --name my-
cluster --region region-code
```

- Der Wert für `--dns-cluster-ip` ist Ihr Service CIDR mit .10am Ende. Um das *service-cidr* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus. Wenn der zurückgegebene Wert beispielsweise `ipv4 10.100.0.0/16` ist, ist Ihr Wert *10.100.0.10*.

```
aws eks describe-cluster --query "cluster.kubernetesNetworkConfig.serviceIpv4Cidr"
--output text --name my-cluster --region region-code
```

- Dieses Beispiel umfasst ein `kubelet`-Argument, mit dem ein benutzerdefinierter `max-pods`-Wert anhand des `bootstrap.sh`-Skripts festgelegt wird, das im Amazon-EKS-optimierten AMI enthalten ist. Hilfe zur Auswahl von *my-max-pods-value* finden Sie unter [the section called "Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen"](#).

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="MYBOUNDARY=="

--==MYBOUNDARY==
```

```
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
set -ex
/etc/eks/bootstrap.sh my-cluster \
 --b64-cluster-ca certificate-authority \
 --apiserver-endpoint api-server-endpoint \
 --dns-cluster-ip service-cidr.10 \
 --kubenet-extra-args '--max-pods=my-max-pods-value' \
 --use-max-pods false

--==MYBOUNDARY==--
```

Geben Sie Benutzerdaten an, um Argumente an die **Start-EKSBootstrap.ps1** Datei zu übergeben, die in einem für Amazon EKS optimierten Windows-AMI enthalten ist

Bootstrapping ist ein Begriff, der verwendet wird, um das Hinzufügen von Befehlen zu beschreiben, die beim Start einer Instance ausgeführt werden können. Sie können Argumente mithilfe von `eksctl` an das `Start-EKSBootstrap.ps1`-Skript übergeben, ohne eine Startvorlage anzugeben. Oder Sie können dies tun, indem Sie die Informationen im Abschnitt Benutzerdaten einer Startvorlage angeben.

Wenn Sie eine benutzerdefinierte Windows AMI-ID angeben möchten, sollten Sie die folgenden Überlegungen berücksichtigen:

- Sie müssen eine Startvorlage verwenden und die erforderlichen Bootstrap-Befehle im Abschnitt Benutzerdaten angeben. Um Ihre gewünschte Windows-ID abzurufen, können Sie die Tabelle unter [Knoten mit optimiertem Windows erstellen](#) verwenden AMIs.
- Es gibt verschiedene Grenzwerte und Bedingungen. Sie müssen beispielsweise `eks:kube-proxy-windows` zu Ihrer AWS IAM Authenticator-Konfigurationsübersicht etwas hinzufügen. Weitere Informationen finden Sie unter [the section called "Grenzen und Bedingungen bei der Angabe einer AMI-ID"](#).

Geben Sie die folgenden Informationen im Abschnitt Benutzerdaten Ihrer Startvorlage an. Ersetzen Sie jede *example value* durch Ihre eigenen Werte. Die Argumente `-APIServerEndpoint`, `-Base64ClusterCA` und `-DNSClusterIP` sind optional. Wenn sie definiert werden, verhindert dies jedoch, dass das `Start-EKSBootstrap.ps1`-Skript einen `describeCluster`-Aufruf durchführt.

- Das einzige erforderliche Argument ist der Clustername (*my-cluster*).

- Um die *certificate-authority* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus.

```
aws eks describe-cluster --query "cluster.certificateAuthority.data" --output text --name my-cluster --region region-code
```

- Um den *api-server-endpoint* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus.

```
aws eks describe-cluster --query "cluster.endpoint" --output text --name my-cluster --region region-code
```

- Der Wert für `--dns-cluster-ip` ist Ihr Service CIDR mit .10 am Ende. Um das *service-cidr* für Ihren Cluster zu überprüfen, führen Sie den folgenden Befehl aus. Wenn der zurückgegebene Wert beispielsweise `ipv4 10.100.0.0/16` ist, ist Ihr Wert *10.100.0.10*.

```
aws eks describe-cluster --query "cluster.kubernetesNetworkConfig.serviceIpv4Cidr" --output text --name my-cluster --region region-code
```

- Weitere Argumente finden Sie unter [the section called "Bootstrap-Skript-Konfigurationsparameter"](#).

#### Note

Wenn Sie den benutzerdefinierten Dienst CIDR verwenden, müssen Sie ihn mithilfe des Parameters angeben. `-ServiceCIDR` Andernfalls schlägt die DNS-Auflösung für Pods im Cluster fehl.

```
<powershell>
[string]$EKSBootstrapScriptFile = "$env:ProgramFiles\Amazon\EKS\Start-EKSBootstrap.ps1"
& $EKSBootstrapScriptFile -EKSClusterName my-cluster `
 -Base64ClusterCA certificate-authority `
 -APIServerEndpoint api-server-endpoint `
 -DNSClusterIP service-cidr.10
</powershell>
```



Führen Sie ein benutzerdefiniertes AMI aufgrund bestimmter Sicherheits-, Compliance- oder interner Richtlinienanforderungen aus

Weitere Informationen finden Sie unter [Amazon Machine Images \(AMI\)](#) im EC2 Amazon-Benutzerhandbuch. Die Amazon EKS AMI-Build-Spezifikation enthält Ressourcen und Konfigurationsskripts für die Erstellung eines benutzerdefinierten Amazon EKS-AMI auf Basis von Amazon Linux. Weitere Informationen finden Sie unter [Amazon-EKS-AMI-Build-Spezifikation](#) auf GitHub. Informationen zum Erstellen benutzerdefinierter AMIs Installationen mit anderen Betriebssystemen finden Sie unter [Amazon EKS Sample Custom AMIs](#) unter GitHub.

Sie können keine dynamischen Parameterreferenzen für AMI IDs in Startvorlagen verwenden, die mit verwalteten Knotengruppen verwendet werden.

 **Important**

Bei der Angabe eines AMI führt Amazon EKS keine Benutzerdaten zusammen. Vielmehr sind Sie dafür verantwortlich, die erforderlichen bootstrap Befehle für Knoten bereitzustellen, die dem Cluster beitreten sollen. Wenn Ihre Knoten dem Cluster nicht beitreten können, wird Amazon EKS CreateNodegroup und UpdateNodegroupVersion-Aktionen ebenfalls fehlschlagen.

## Grenzen und Bedingungen bei der Angabe einer AMI-ID

Im Folgenden sind die Grenzen und Bedingungen aufgeführt, die mit der Angabe einer AMI-ID mit verwalteten Knotengruppen verbunden sind:

- Sie müssen eine neue Knotengruppe erstellen, um zwischen der Angabe einer AMI-ID in einer Startvorlage und der Nicht-Angabe einer AMI-ID zu wechseln.
- Sie werden in der Konsole nicht benachrichtigt, wenn eine neuere AMI-Version verfügbar ist. Um Ihre Knotengruppe auf eine neuere AMI-Version zu aktualisieren, müssen Sie eine neue Version Ihrer Startvorlage mit einer aktualisierten AMI-ID erstellen. Dann müssen Sie die Knotengruppe mit der neuen Version der Startvorlage aktualisieren.
- Die folgenden Felder können in der API nicht festgelegt werden, wenn Sie eine AMI-ID angeben:
  - `amiType`
  - `releaseVersion`
  - `version`

- Alle in der API festgelegten taints werden asynchron angewendet, wenn Sie eine AMI-ID angeben. Um Taints anzuwenden, bevor ein Knoten mit dem Cluster verbunden wird, müssen Sie die Taints über das Befehlszeilen-Flag `--register-with-taints` an kubelet in Ihren Benutzerdaten weitergeben. Weitere Informationen finden Sie unter [kubelet](#) in der Kubernetes-Dokumentation.
- Wenn Sie eine benutzerdefinierte AMI-ID für von Windows verwaltete Knotengruppen angeben, fügen Sie `eks:kube-proxy-windows` diese Ihrer AWS IAM Authenticator-Konfigurationsübersicht hinzu. Dies ist erforderlich, damit DNS ordnungsgemäß funktioniert.
  - a. Öffnen Sie die AWS IAM Authenticator-Konfigurationsübersicht zur Bearbeitung.

```
kubectl edit -n kube-system cm aws-auth
```

- b. Fügen Sie diesen Eintrag der groups Liste unter jedem rolearn Windows-Knoten hinzu. Ihre Konfigurationsübersicht sollte ähnlich wie [aws-auth-cm-windows.yaml](#) aussehen.

```
- eks:kube-proxy-windows
```

- c. Speichern Sie die Datei und beenden Sie den Text-Editor.

## Löschen Sie eine verwaltete Knotengruppe aus Ihrem Cluster

In diesem Thema wird beschrieben, wie Sie eine verwaltete Amazon-EKS-Knotengruppe löschen. Wenn Sie eine verwaltete Knotengruppe löschen, legt Amazon EKS zunächst die minimale, maximale und gewünschte Größe Ihrer Auto-Scaling-Gruppe auf Null fest. Dies bewirkt dann, dass Ihre Knotengruppe abskaliert wird.

Bevor jede Instance beendet wird, sendet Amazon EKS ein Signal, um die Pods von diesem Knoten zu entleeren. Wenn die Pods nach einigen Minuten nicht leer sind, lässt Amazon EKS Auto Scaling die Beendigung der Instance fortsetzen. Nachdem jede Instance beendet wurde, wird die Auto-Scaling-Gruppe gelöscht.

### Important

Wenn Sie eine verwaltete Knotengruppe löschen, die eine Knoten-IAM-Rolle verwendet, die von keiner anderen verwalteten Knotengruppe im Cluster verwendet wird, wird die Rolle aus der `aws-auth` ConfigMap entfernt. Wenn eine der selbstverwalteten Knotengruppen im Cluster dieselbe Knoten-IAM-Rolle verwendet, werden die selbstverwalteten Knoten in den `NotReady`-Status verschoben. Darüber hinaus wird auch der Clusterbetrieb gestört.

Um eine Zuordnung für die Rolle hinzuzufügen, die Sie nur für die selbstverwalteten Knotengruppen verwenden, überprüfen Sie [the section called “Zugangseinträge erstellen”](#), ob die Plattformversion Ihres Clusters mindestens die Mindestversion ist, die im Abschnitt Voraussetzungen unter Gewähren Sie [IAM-Benutzern Zugriff auf Kubernetes mit EKS-Zugriffseinträgen gewähren](#) aufgeführt ist. Wenn Ihre Plattformversion älter ist als die erforderliche Mindestversion für Zugriffseinträge, können Sie den Eintrag wieder zu der hinzufügen. `aws-auth ConfigMap` Weitere Informationen erhalten Sie durch Eingabe von `eksctl create iamidentitymapping --help` im Terminal.

Sie können eine verwaltete Knotengruppe löschen mit:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)
- [the section called “AWS CLI”](#)

## eksctl

Löschen Sie eine verwaltete Knotengruppe mit **eksctl**

Geben Sie den folgenden Befehl ein. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
eksctl delete nodegroup \
 --cluster my-cluster \
 --name my-mng \
 --region region-code
```

Weitere Optionen finden Sie unter [Löschen und Löschen von Knotengruppen](#) in der eksctl-Dokumentation.

## AWS Management Console

Löschen Sie eine verwaltete Knotengruppe mit AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie auf der Seite Clusters den Cluster aus, der die zu löschende Knotengruppe enthält.
3. Wählen Sie auf der ausgewählten Cluster-Seite die Registerkarte Datenverarbeitung aus.

4. Wählen Sie im Abschnitt Node groups (Knotengruppen) die zu löschende Knotengruppe aus. Wählen Sie dann Löschen aus.
5. Geben Sie im Bestätigungsdialogfeld Knotengruppe löschen den Namen der Knotengruppe ein. Wählen Sie dann Löschen aus.

## AWS CLI

Löschen Sie eine verwaltete Knotengruppe mit AWS CLI

1. Geben Sie den folgenden Befehl ein. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
aws eks delete-nodegroup \
 --cluster-name my-cluster \
 --nodegroup-name my-mng \
 --region region-code
```

2. Verwenden Sie die Pfeiltasten auf Ihrer Tastatur, um durch die Antwortausgabe zu blättern. Drücken Sie die q Taste, wenn Sie fertig sind.

Weitere Optionen finden Sie unter dem [delete-nodegroup](#) Befehl in der AWS CLI-Befehlsreferenz.

## Verwalten Sie Knoten selbst mit selbstverwalteten Knoten

Ein Cluster enthält einen oder mehrere EC2 Amazon-Knoten, für die Pods geplant sind. Amazon EKS-Knoten werden in Ihrem AWS Konto ausgeführt und stellen über den Cluster-API-Serverendpunkt eine Verbindung zur Steuerungsebene Ihres Clusters her. Sie werden Ihnen auf der Grundlage der EC2 Amazon-Preise in Rechnung gestellt. Weitere Informationen finden Sie unter [EC2 Amazon-Preise](#).

Ein Cluster kann mehrere Knotengruppen enthalten. Jede Knotengruppe enthält einen oder mehrere Knoten, die in einer [Amazon EC2 Auto Scaling Scaling-Gruppe](#) bereitgestellt werden. [Der Instance-Typ der Knoten innerhalb der Gruppe kann variieren, z. B. wenn die attributbasierte Instance-Typauswahl mit Karpenter verwendet wird.](#) Alle Instances in einer Knotengruppe müssen die [Amazon-EKS-Knoten-IAM-Rolle](#) verwenden.

Amazon EKS bietet spezielle Amazon Machine Images (AMIs), die als Amazon EKS-optimiert bezeichnet werden AMIs. Sie AMIs sind für die Verwendung mit Amazon EKS konfiguriert. Zu ihren Komponenten gehören `containerd` und der AWS IAM Authenticator. Sie enthalten AMIs außerdem ein spezielles [Bootstrap-Skript](#), das es ermöglicht, die Steuerungsebene Ihres Clusters automatisch zu erkennen und eine Verbindung zu ihr herzustellen.

Wenn Sie den Zugriff auf den öffentlichen Endpunkt Ihres Clusters mithilfe von CIDR-Blöcken einschränken, empfehlen wir, dass Sie auch den privaten Endpunktzugriff aktivieren. Auf diese Weise können Knoten mit dem Cluster kommunizieren. Wenn der private Endpunkt nicht aktiviert ist, müssen die CIDR-Blöcke, die Sie für den öffentlichen Zugriff angeben, die Ausgangsquellen aus Ihrer VPC enthalten. Weitere Informationen finden Sie unter [the section called "Cluster-Endpunktzugriff"](#).

Informationen zum Hinzufügen selbstverwalteter Knoten zu Ihrem Amazon-EKS-Cluster finden Sie in den folgenden Themen. Wenn Sie selbstverwaltete Knoten manuell starten, fügen Sie jedem Knoten das folgende Tag hinzu und stellen Sie dabei sicher, dass es zu Ihrem `<cluster-name>` Cluster passt. Weitere Informationen dazu finden Sie unter [Hinzufügen und Löschen von Markierungen für einzelne Ressourcen](#). Wenn Sie die Schritte in der Anleitung ausführen, wird die erforderliche Markierung für Sie zum Knoten hinzugefügt.

| Schlüssel                                               | Value (Wert)       |
|---------------------------------------------------------|--------------------|
| <code>kubernetes.io/cluster/&lt;cluster-name&gt;</code> | <code>owned</code> |

 **Important**

Tags im Amazon EC2 Instance Metadata Service (IMDS) sind nicht mit EKS-Knoten kompatibel. Wenn Instance-Metadaten-Tags aktiviert sind, wird die Verwendung von Schrägstrichen (‘/’) in Tag-Werten verhindert. Diese Einschränkung kann zu Fehlern beim Starten von Instances führen, insbesondere bei der Verwendung von Knotenverwaltungstools wie Karpenter oder Cluster Autoscaler, da diese Dienste für die korrekte Funktionalität auf Tags angewiesen sind, die Schrägstriche enthalten.

Weitere Informationen zu Worker-Knoten aus einer allgemeinen Kubernetes-Perspektive finden Sie unter [Nodes](#) in der Kubernetes-Dokumentation.

## Themen

- [Erstellen Sie selbstverwaltete Amazon Linux-Knoten](#)
- [Erstellen Sie selbstverwaltete Bottlerocket-Knoten](#)
- [Erstellen Sie selbstverwaltete Microsoft Windows-Knoten](#)
- [Erstellen Sie selbstverwaltete Ubuntu-Linux-Knoten](#)
- [Aktualisieren Sie selbstverwaltete Knoten für Ihren Cluster](#)

## Erstellen Sie selbstverwaltete Amazon Linux-Knoten

Dieses Thema beschreibt Hinweise zum Starten von Auto-Scaling-Gruppen von Linux-Knoten, die mit Ihrem Amazon-EKS-Cluster registriert sind. Nachdem die Knoten dem Cluster beigetreten sind, können Sie Kubernetes-Anwendungen darin bereitstellen. Sie können auch selbstverwaltete Amazon Linux-Knoten mit `eksctl` oder dem AWS Management Console starten. Informationen dazu, wie Sie Knoten auf AWS Outposts starten müssen, finden Sie unter [the section called “Knoten”](#).

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [the section called “Erstellen eines -Clusters”](#). Wenn Sie Subnetze in der AWS Region haben, in der Sie AWS Outposts, AWS Wavelength oder AWS Local Zones aktiviert haben, dürfen diese Subnetze bei der Erstellung Ihres Clusters nicht weitergegeben worden sein.
- Eine vorhandene IAM-Rolle, die von den Knoten verwendet werden soll. Informationen zum Erstellen finden Sie unter [the section called “Knoten-IAM-Rolle”](#). Wenn diese Rolle keine der Richtlinien für das VPC-CNI hat, ist die folgende separate Rolle für die VPC-CNI-Pods erforderlich.
- (Optional, aber empfohlen) Das Amazon VPC CNI-Plug-In für Kubernetes ist mit einer eigenen IAM-Rolle konfiguriert, der die erforderliche IAM-Richtlinie zugeordnet ist. Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).
- Vertrautheit mit den unter [Wählen Sie einen optimalen EC2 Amazon-Node-Instance-Typ](#) aufgeführten Überlegungen. Je nachdem, welchen Instance-Typ Sie wählen, kann es zusätzliche Voraussetzungen für Ihren Cluster und Ihre VPC geben.

Sie können selbstverwaltete Linux-Knoten mit einer der folgenden Methoden starten:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

## eksctl

Starten Sie selbstverwaltete Linux-Knoten mit **eksctl**

1. Installieren Sie die Version 0.210.0 oder höher des auf Ihrem Gerät installierten `eksctl` Befehlszeilentools oder AWS CloudShell. Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).
2. (Optional) Wenn die von `AmazonEKS_CNI_Policy` verwaltete IAM-Richtlinie mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Servicekonto zuordnen. `aws-node` Weitere Informationen finden Sie unter [the section called "Für IRSA konfigurieren"](#).
3. Der folgende Befehl erstellt eine Knotengruppe in einem bestehenden Cluster. Ersetzen Sie *al-nodes* durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Ersetzen Sie den Rest der *example value* durch Ihre eigenen Werte. Die Knoten werden standardmäßig mit derselben Kubernetes-Version wie die Steuerungsebene erstellt.

Bevor Sie einen Wert für `--node-type` auswählen, lesen [Sie den Artikel Wählen Sie einen optimalen EC2 Amazon-Node-Instance-Typ](#).

*my-key* Ersetzen Sie es durch den Namen Ihres EC2 Amazon-Schlüsselpaars oder öffentlichen Schlüssels. Dieser Schlüssel wird für den SSH-Zugriff zu Ihren Knoten verwendet, nachdem diese gestartet wurden. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch.

Erstellen Sie Ihre Knoten-Gruppe mit dem folgenden Befehl.

### Important

Wenn Sie eine Knotengruppe in AWS Outposts-, Wavelength- oder Local Zone-Subnetzen bereitstellen möchten, gibt es zusätzliche Überlegungen:

- Die Subnetze dürfen beim Erstellen des Clusters nicht übergeben worden sein.

- Sie müssen die Knotengruppe mit einer Konfigurationsdatei erstellen, die die Subnetze und [volumeType](#): gp2 angibt. Weitere Informationen dazu finden Sie unter [Verwenden von Config-Dateien](#) und im [Config-Datei-Schema](#) in der eksctl-Dokumentation.

```
eksctl create nodegroup \
 --cluster my-cluster \
 --name al-nodes \
 --node-type t3.medium \
 --nodes 3 \
 --nodes-min 1 \
 --nodes-max 4 \
 --ssh-access \
 --managed=false \
 --ssh-public-key my-key
```

Zum Bereitstellen einer Knotengruppe, die:

- kann Pods eine deutlich höhere Anzahl von IP-Adressen zuweisen als in der Standardkonfiguration, siehe [the section called “Erhöhen Sie die IP-Adressen”](#)
- kann Pods IPv4 Adressen aus einem anderen CIDR-Block als dem der Instanz zuweisen, siehe [the section called “Benutzerdefinierte Netzwerke”](#).
- kann Pods und Diensten IPv6 Adressen zuweisen, siehe [the section called “IPv6”](#).
- Sie haben keinen ausgehenden Internetzugang, siehe [the section called “Private Cluster”](#).

Geben Sie den folgenden Befehl ein, um eine vollständige Liste aller verfügbaren Optionen und Standardwerte anzuzeigen.

```
eksctl create nodegroup --help
```

Wenn Knoten dem Cluster nicht beitreten können, finden Sie weitere Informationen [the section called “Knoten können nicht mit dem Cluster verknüpft werden”](#) im Kapitel Fehlerbehebung.

Eine Beispielausgabe sieht wie folgt aus. Mehrere Zeilen werden ausgegeben, während die Knoten erstellt werden. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```



4. (Optional) [???](#) Stellen Sie eine Beispielanwendung bereit, um Ihren Cluster und Ihre Linux-Worker-Knoten zu testen.
5. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:
  - Sie planen, all Ihren Kubernetes-Dienstknoten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
  - Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

## AWS Management Console

Schritt 1: Starten Sie selbstverwaltete Linux-Knoten mit AWS Management Console

1. Laden Sie die neueste Version der AWS CloudFormation Vorlage herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/amazon-eks-nodegroup.yaml
```

2. Warten Sie, bis der Status des Clusters als ACTIVE angezeigt wird. Wenn Sie Ihre Knoten starten, bevor der Cluster aktiv ist, werden die Knoten nicht mit dem Cluster registriert und Sie müssen sie neu starten.
3. Öffnen Sie die [AWS CloudFormation -Konsole](#).
4. Wählen Sie Create stack (Stack erstellen) und dann With new resources (standard) (Mit neuen Ressourcen [Standard]) aus.
5. Wählen Sie für Specify template (Vorlage festlegen) Upload a template file (Vorlagendatei hochladen) aus und wählen Sie dann Choose file (Datei wählen).
6. Wählen Sie die heruntergeladene amazon-eks-nodegroup.yaml-Datei aus.
7. Klicken Sie auf Weiter.
8. Geben Sie auf der Seite Specify stack details (Stack-Details angeben) die folgenden Parameter ein und klicken Sie dann auf Next (Weiter):
  - Stack-Name: Wählen Sie einen Stack-Namen für Ihren AWS CloudFormation Stack. Sie können ihn beispielsweise *my-cluster-nodes* nennen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er

muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.

- **ClusterName:** Geben Sie den Namen ein, den Sie bei der Erstellung Ihres Amazon EKS-Clusters verwendet haben. Dieser Name muss dem Clusternamen entsprechen, sonst können Ihre Knoten dem Cluster nicht beitreten.
- **ClusterControlPlaneSecurityGroup:** Wählen Sie den SecurityGroupsWert aus der AWS CloudFormation Ausgabe aus, die Sie bei der Erstellung Ihrer [VPC](#) generiert haben.

Die folgenden Schritte zeigen einen Vorgang zum Abrufen der entsprechenden Gruppe.

- a. Öffnen Sie die [Amazon-EKS-Konsole](#).
  - b. Wählen Sie den Namen des Clusters.
  - c. Wählen Sie die Registerkarte Network (Network) aus.
  - d. Verwenden Sie den Wert Zusätzliche Sicherheitsgruppen als Referenz, wenn Sie aus der ClusterControlPlaneSecurityGroupDropdownliste auswählen.
- **NodeGroupName:** Geben Sie einen Namen für Ihre Knotengruppe ein. Dieser Name kann später verwendet werden, um die Auto Scaling-Knotengruppe zu identifizieren, die für Ihre Knoten erstellt wurde. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.
  - **NodeAutoScalingGroupMinSize:** Geben Sie die Mindestanzahl von Knoten ein, auf die Ihre Auto Scaling Scaling-Gruppe für Knoten skalieren kann.
  - **NodeAutoScalingGroupDesiredCapacity:** Geben Sie die gewünschte Anzahl von Knoten ein, auf die bei der Erstellung Ihres Stacks skaliert werden soll.
  - **NodeAutoScalingGroupMaxSize:** Geben Sie die maximale Anzahl von Knoten ein, auf die Ihre Auto Scaling Scaling-Gruppe für Knoten skalieren kann.
  - **NodeInstanceType:** Wählen Sie einen Instance-Typ für Ihre Knoten. Weitere Informationen finden Sie unter [the section called “ EC2 Amazon-Instance-Typen”](#).
  - **NodeImageIdSSMParam:** Vorab mit dem Amazon EC2 Systems Manager Manager-Parameter eines kürzlich für Amazon EKS optimierten AMI für eine variable Kubernetes-Version gefüllt. Um eine andere Kubernetes-Nebenversion zu verwenden, die von Amazon EKS unterstützt wird, ersetzen Sie **1.XX** durch eine andere [unterstützte Version](#). Wir empfehlen, dieselbe Kubernetes-Version wie Ihr Cluster anzugeben.

Sie können es auch *amazon-linux-2* durch einen anderen AMI-Typ ersetzen. Weitere Informationen finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).

 Note

Die Amazon EKS-Knoten AMIs basieren auf Amazon Linux. Sie können Sicherheits- oder Datenschutzereignisse für Amazon Linux 2 im [Amazon Linux-Sicherheitszentrum](#) verfolgen oder den zugehörigen [RSS-Feed](#) abonnieren. Sicherheits- oder Datenschutzereignisse enthalten eine Übersicht über das Problem, welche Pakete betroffen sind und wie Sie Ihre Instances aktualisieren, um das Problem zu beheben.

- **NodeImageId:** (Optional) Wenn Sie Ihr eigenes benutzerdefiniertes AMI (anstelle eines für Amazon EKS optimierten AMI) verwenden, geben Sie eine Knoten-AMI-ID für Ihre AWS Region ein. Wenn Sie hier einen Wert angeben, überschreibt dieser alle Werte im `NodeImageIdSSMParamField`.
- **NodeVolumeSize:** Geben Sie eine Root-Volume-Größe für Ihre Knoten in GiB an.
- **NodeVolumeType:** Geben Sie einen Root-Volume-Typ für Ihre Knoten an.
- **KeyName:** Geben Sie den Namen eines Amazon EC2 SSH-Schlüsselpaars ein, mit dem Sie nach dem Start über SSH eine Verbindung zu Ihren Knoten herstellen können. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch.

 Note

Wenn Sie hier kein key pair angeben, schlägt die AWS CloudFormation Stack-Erstellung fehl.

- **BootstrapArguments:** Geben Sie alle optionalen Argumente an, die an das Node-Bootstrap-Skript übergeben werden sollen, z. B. zusätzliche `kubelet` Argumente. Weitere Informationen finden Sie in den [Bootstrap-Skript-Nutzungsinformationen](#) auf GitHub.

Zum Bereitstellen einer Knotengruppe, die:

- kann Pods eine deutlich höhere Anzahl von IP-Adressen zuweisen als in der Standardkonfiguration, siehe [the section called “Erhöhen Sie die IP-Adressen”](#).

- kann Pods IPv4 Adressen aus einem anderen CIDR-Block als dem der Instanz zuweisen, siehe [the section called “Benutzerdefinierte Netzwerke”](#).
- kann Pods und Diensten IPv6 Adressen zuweisen, siehe [the section called “IPv6”](#).
- Sie haben keinen ausgehenden Internetzugang, siehe [the section called “Private Cluster”](#).
- Deaktivieren IMDSv1: Standardmäßig unterstützt jeder Knoten den Instanz-Metadatendienst Version 1 (IMDSv1) und IMDSv2. Sie können deaktivieren IMDSv1. Um zu verhindern, dass future Knoten und Pods in der Knotengruppe verwendet werden MDSv1, setzen Sie Disable IMDSv1 auf true. Weitere Informationen finden Sie unter [Konfiguration des Instance-Metadatenservice](#). Weitere Informationen zum Einschränken des Zugriffs darauf auf Ihre Knoten finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).
- VpcId: Geben Sie die ID für die [VPC](#) ein, die Sie erstellt haben.
- Subnetze: Wählen Sie die Subnetze aus, die Sie für Ihre VPC erstellt haben. Wenn Sie Ihre VPC mit den Schritten erstellt haben, die unter [Amazon VPC für Ihren Amazon EKS-Cluster erstellen](#) beschrieben sind, geben Sie nur die privaten Subnetze innerhalb der VPC an, in denen Ihre Knoten gestartet werden sollen. Sie können sehen, welche Subnetze privat sind, indem Sie den jeweiligen Subnetzlink in der Registerkarte Networking (Netzwerk) Ihres Clusters öffnen.

 **Important**

- Wenn es sich bei einem oder einigen der Subnetze um öffentliche Subnetze handelt, muss die Einstellung für die automatische Zuweisung öffentlicher IP-Adressen aktiviert sein. Wenn die Einstellung für das öffentliche Subnetz nicht aktiviert ist, wird allen Knoten, die Sie in diesem öffentlichen Subnetz bereitstellen, keine öffentliche IP-Adresse zugewiesen und sie können nicht mit dem Cluster oder anderen Diensten kommunizieren. AWS Wenn das Subnetz vor dem 26. März 2020 mithilfe einer der [Amazon AWS CloudFormation EKS-VPC-Vorlagen](#) oder mithilfe eksctl von bereitgestellt wurde, ist die automatische Zuweisung öffentlicher IP-Adressen für öffentliche Subnetze deaktiviert. Informationen zum Aktivieren der Zuweisung öffentlicher IP-Adressen für ein Subnetz finden Sie unter [Ändern des Attributs für die öffentliche IPv4 Adressierung](#) für Ihr Subnetz. Wenn der Knoten in einem privaten Subnetz bereitgestellt wird, kann er über ein NAT-Gateway mit dem Cluster und anderen AWS Diensten kommunizieren.

- Wenn die Subnetze keinen Internetzugang haben, stellen Sie sicher, dass Sie die Überlegungen und zusätzlichen Schritte unter [Bereitstellen von privaten Clustern mit eingeschränktem Internetzugang](#) kennen.
- Wenn Sie AWS Outposts-, Wavelength- oder Local Zone-Subnetze auswählen, dürfen die Subnetze bei der Erstellung des Clusters nicht übergeben worden sein.

9. Treffen Sie die gewünschte Auswahl auf der Seite Configure stack options (Stackoptionen konfigurieren) und wählen Sie dann Next (Weiter) aus.
10. Aktivieren Sie das Kontrollkästchen links neben Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden. , und wählen Sie dann Stapel erstellen aus.
11. Wenn Ihr Stack fertig erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgaben).
12. Notieren Sie das NodeInstanceRole für die Knotengruppe, die erstellt wurde. Sie benötigen diese, wenn Sie Ihre Amazon-EKS--Arbeitsknoten konfigurieren.

Schritt 2: Ermöglichen Sie den Knoten, Ihrem Cluster beizutreten

 Note

Wenn Sie Knoten innerhalb einer privaten VPC ohne ausgehenden Internetzugang gestartet haben, müssen Sie ihnen ermöglichen, Ihrem Cluster innerhalb der VPC beizutreten.

1. Überprüfen Sie, ob Sie bereits über eine aws-auth ConfigMap verfügen.

```
kubectl describe configmap -n kube-system aws-auth
```

2. Wenn eine aws-auth ConfigMap angezeigt wird, aktualisieren Sie sie nach Bedarf.
  - a. Öffnen Sie ConfigMap zum Bearbeiten.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Fügen Sie nach Bedarf einen neuen mapRoles-Eintrag hinzu. Setzen Sie den roleARN Wert auf den NodeInstanceRoleWert, den Sie im vorherigen Verfahren aufgezeichnet haben.

```
[...]
data:
```

```
mapRoles: |
 - rolearn: <ARN of instance role (not instance profile)>
 username: system:node:{{EC2PrivateDNSName}}
 groups:
 - system:bootstrappers
 - system:nodes
[...]
```

c. Speichern Sie die Datei und beenden Sie den Text-Editor.

3. Wenn die Fehlermeldung `Error from server (NotFound): configmaps "aws-auth" not found` angezeigt wird, wenden Sie die standardmäßige ConfigMap an.

a. Laden Sie die Konfigurationszuordnung herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/
aws-auth-cm.yaml
```

b. Stellen Sie in der `aws-auth-cm.yaml` Datei den `rolearn` Wert auf den `NodeInstanceRole` Wert ein, den Sie im vorherigen Verfahren aufgezeichnet haben. Hierzu können Sie einen Texteditor verwenden oder `my-node-instance-role` ersetzen und den folgenden Befehl ausführen:

```
sed -i.bak -e 's|<ARN of instance role (not instance profile)>|my-node-instance-
role|' aws-auth-cm.yaml
```

c. Wenden Sie die Konfiguration an. Die Ausführung dieses Befehls kann einige Minuten dauern.

```
kubectl apply -f aws-auth-cm.yaml
```

4. Sehen Sie sich den Status Ihrer Knoten an und warten Sie, bis diese in den Ready-Status eintreten.

```
kubectl get nodes --watch
```

Geben Sie `Ctrl+C` ein, um zu einer Shell-Eingabeaufforderung zurückzukehren.

 Note

Wenn Sie Autorisierungs- oder Ressourcenfehler erhalten, finden Sie weitere Informationen unter [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#) im Thema zur Fehlerbehebung.

Wenn Knoten dem Cluster nicht beitreten können, finden Sie weitere Informationen [the section called “Knoten können nicht mit dem Cluster verknüpft werden”](#) im Kapitel Fehlerbehebung.

5. (Nur GPU-Knoten) Wenn Sie einen GPU-Instance-Typ und das für Amazon EKS optimierte beschleunigte AMI ausgewählt haben, müssen Sie das [NVIDIA-Geräte-Plug-In für Kubernetes](#) als a DaemonSet auf Ihrem Cluster anwenden. Ersetzen Sie es `vX.X.X` durch die gewünschte [s-device-pluginNVIDIA/K8-Version](#), bevor Sie den folgenden Befehl ausführen.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/
deployments/static/nvidia-device-plugin.yml
```

### Schritt 3: Zusätzliche Aktionen

1. (Optional) [???](#) Stellen Sie eine Beispielanwendung bereit, um Ihren Cluster und Ihre Linux-Worker-Knoten zu testen.
2. (Optional) Wenn die von AmazonEKS\_CNI\_Policy verwaltete IAM-Richtlinie (wenn Sie einen IPv4 Cluster haben) oder die *AmazonEKS\_CNI\_IPv6\_PoLicy* (die Sie [selbst erstellt](#) haben, wenn Sie einen IPv6 Cluster haben) mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Servicekonto zuordnen. `aws-node` Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).
3. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:
  - Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
  - Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

# Erstellen Sie selbstverwaltete Bottlerocket-Knoten

## Note

Verwaltete Knotengruppen bieten möglicherweise einige Vorteile für Ihren Anwendungsfall. Weitere Informationen finden Sie unter [the section called “Verwaltete Knotengruppen”](#).

In diesem Thema wird beschrieben, wie Sie Auto Scaling Scaling-Gruppen von [Bottlerocket-Knoten](#) starten, die sich bei Ihrem Amazon EKS-Cluster registrieren. Bottlerocket ist ein Linux-basiertes Open-Source-Betriebssystem, mit dem Sie Container auf virtuellen AWS Maschinen oder Bare-Metal-Hosts ausführen können. Nachdem die Knoten dem Cluster beigetreten sind, können Sie Kubernetes-Anwendungen darin bereitstellen. Weitere Informationen zu Bottlerocket finden Sie in der Dokumentation unter [Using a Bottlerocket AMI with Amazon EKS](#) on GitHub and [Custom](#) AMI support. `eksctl`

[Informationen zu direkten Upgrades finden Sie unter Bottlerocket Update Operator unter](#). GitHub

## Important

- Amazon EKS-Knoten sind EC2 Standard-Amazon-Instances, und sie werden Ihnen auf der Grundlage der normalen EC2 Amazon-Instance-Preise in Rechnung gestellt. Weitere Informationen finden Sie unter [EC2 Amazon-Preise](#).
- Sie können Bottlerocket-Knoten in erweiterten Amazon EKS-Clustern auf AWS Outposts starten, aber Sie können sie nicht in lokalen Clustern auf Outposts starten. AWS Weitere Informationen finden Sie unter [Amazon EKS auf AWS Outposts](#).
- Sie können die Bereitstellung auf EC2 Amazon-Instances mit x86 oder ARM-Prozessoren durchführen. Sie können die Bereitstellung jedoch nicht auf Instances durchführen, die über Inferentia-Chips verfügen.
- Bottlerocket ist kompatibel mit AWS CloudFormation Es gibt jedoch keine offizielle CloudFormation Vorlage, die kopiert werden kann, um Bottlerocket-Knoten für Amazon EKS bereitzustellen.
- Bottlerocket-Images werden nicht mit einem SSH-Server oder einer Shell geliefert. Sie können out-of-band Zugriffsmethoden verwenden, um die SSH-Aktivierung des Admin-Containers zu ermöglichen und einige Bootstrapping-Konfigurationsschritte mit



Benutzerdaten zu durchlaufen. Weitere Informationen finden Sie in diesen Abschnitten im [bottlerocket README.md](#) auf GitHub:

- [Exploration](#) (Erkundung)
- [Administrator-Container](#)
- [Kubernetes-Einstellungen](#)

Für diesen Vorgang ist `eksctl` Version `0.210.0` oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Anweisungen zur Installation oder zum Upgrade `eksctl` finden Sie in der `eksctl` Dokumentation unter [Installation](#). Hinweis: Dieses Verfahren funktioniert nur für Cluster, die mit erstellt wurden.

`eksctl`

1. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Ersetzen Sie *ng-bottlerocket* durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Um die Bereitstellung auf Arm-Instances durchzuführen, ersetzen Sie *m5.large* durch einen Arm-Instance-Typ. *my-ec2-keypair-name* Ersetzen Sie es durch den Namen eines Amazon EC2 SSH-Schlüsselpaars, mit dem Sie nach dem Start über SSH eine Verbindung zu Ihren Knoten herstellen können. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch. Ersetzen Sie *example values* durch Ihre eigenen Werte. Sobald Sie die Ersetzungen vorgenommen haben, führen Sie den modifizierten Befehl aus, um die `bottlerocket.yaml` Datei zu erstellen.

Wenn Sie einen Arm EC2 Amazon-Instance-Typ angeben, lesen Sie AMIs vor der Bereitstellung die Überlegungen in [Amazon EKS-optimiertem Arm Amazon Linux](#) durch. Anweisungen zur Bereitstellung mit einem benutzerdefinierten AMI finden Sie in der Dokumentation unter [Building Bottlerocket](#) on GitHub und [Custom AMI support](#). `eksctl` Um eine verwaltete Knotengruppe

bereitzustellen, stellen Sie ein benutzerdefiniertes AMI mithilfe einer Startvorlage bereit. Weitere Informationen finden Sie unter [the section called “Startvorlagen”](#).

 **Important**

Um eine Knotengruppe in AWS Outposts-, AWS Wavelength- oder AWS Local Zone-Subnetzen bereitzustellen, übergeben Sie beim Erstellen des Clusters keine AWS Outposts-, AWS Wavelength- oder AWS Local Zone-Subnetze. Sie müssen die Subnetze im folgenden Beispiel angeben. Weitere Informationen finden Sie unter [Verwenden von Config-Dateien](#) und im [Config-Datei-Schema](#) in der eksctl-Dokumentation. Ersetzen Sie es *region-code* durch die AWS Region, in der sich Ihr Cluster befindet.

```
cat >bottlerocket.yaml <<EOF

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: my-cluster
 region: region-code
 version: '1.33'

iam:
 withOIDC: true

nodeGroups:
- name: ng-bottlerocket
 instanceType: m5.large
 desiredCapacity: 3
 amiFamily: Bottlerocket
 ami: auto-ssm
 iam:
 attachPolicyARNs:
 - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
 - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
 - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
 - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
 ssh:
 allow: true
 publicKeyName: my-ec2-keypair-name
```

EOF

2. Stellen Sie den Treiber mit dem folgenden Befehl bereit.

```
eksctl create nodegroup --config-file=bottlerocket.yaml
```

Eine Beispielausgabe sieht wie folgt aus.

Mehrere Zeilen werden ausgegeben, während die Knoten erstellt werden. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) Erstellen eines Kubernetes [Persistenter](#) auf einem Bottlerocket-Knoten mit dem [Amazon-EBS-CSI-Plugin](#). Der standardmäßige Amazon EBS-Treiber basiert auf Dateisystem-Tools, die nicht in Bottlerocket enthalten sind. Weitere Informationen zur Erstellung einer Speicherklasse mit dem Treiber finden Sie unter [the section called "Amazon EBS"](#).
4. (Optional) Standardmäßig setzt kube-proxy den Kernelparameter `nf_conntrack_max` auf einen Standardwert, der sich von dem unterscheiden kann, was Bottlerocket ursprünglich beim Booten festgelegt hat. Um die [Standardeinstellung](#) von Bottlerocket beizubehalten, bearbeiten Sie die Konfiguration mit dem folgenden Befehl. kube-proxy

```
kubectyl edit -n kube-system daemonset kube-proxy
```

Fügen Sie `--conntrack-max-per-core` und `--conntrack-min` zu den kube-proxy-Argumenten im folgenden Beispiel hinzu. Eine Einstellung von 0 impliziert keine Änderung.

```
containers:
- command:
 - kube-proxy
 - --v=2
 - --config=/var/lib/kube-proxy-config/config
 - --conntrack-max-per-core=0
 - --conntrack-min=0
```

5. (Optional) Bereitstellen einer [Beispielanwendung](#), um Ihre Bottlerocket-Knoten zu testen.
6. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:

- Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
- Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

## Erstellen Sie selbstverwaltete Microsoft Windows-Knoten

Dieses Thema beschreibt Hinweise zum Starten von Auto-Scaling-Gruppen von -Windows-Knoten, die mit Ihrem Amazon-EKS-Cluster registriert sind. Nachdem die Knoten dem Cluster beigetreten sind, können Sie Kubernetes-Anwendungen darin bereitstellen.

### Important

- Amazon EKS-Knoten sind EC2 Standard-Arbeitsspeicher-Instanzen, und sie werden Ihnen auf der Grundlage der normalen EC2 Amazon-Instanz-Preise in Rechnung gestellt. Weitere Informationen finden Sie unter [EC2 Amazon-Preise](#).
- Sie können Windows-Knoten in erweiterten Amazon EKS-Clustern auf AWS Outposts starten, aber Sie können sie nicht in lokalen Clustern auf AWS Outposts starten. Weitere Informationen finden Sie unter [Amazon EKS auf AWS Outposts](#).

Aktivieren Sie den Windows-Support für Ihren Cluster. Es wird empfohlen, wichtige Überlegungen zu berücksichtigen, bevor Sie eine Windows-Knotengruppe starten. Weitere Informationen finden Sie unter [the section called “Aktivieren Sie die Windows-Unterstützung”](#).

Sie können selbstverwaltete Windows-Knoten mit einer der folgenden Optionen starten:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

## eksctl

Starten Sie selbstverwaltete Windows-Knoten mit **eksctl**

Bei diesem Verfahren wird davon ausgegangen, dass Sie `eksctl` installiert haben und dass Ihre `eksctl`-Version mindestens `0.210.0` ist. Sie können Ihre Version mit dem folgenden Befehl überprüfen.

```
eksctl version
```

Eine Installations- und Upgrade-Anleitung für `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).

 Note

Dieses Verfahren funktioniert nur für Cluster, die mit `eksctl` erstellt wurden.

1. (Optional) Wenn die von `AmazonEKS_CNI_Policy` verwaltete IAM-Richtlinie (wenn Sie einen IPv4 Cluster haben) oder die *`AmazonEKS_CNI_IPv6_Policy`* (die Sie [selbst erstellt](#) haben, wenn Sie einen IPv6 Cluster haben) mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Servicekonto zuordnen. `aws-node` Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).
2. Bei diesem Verfahren wird davon ausgegangen, dass Sie einen bestehenden Cluster haben. Wenn Sie noch keinen Amazon EKS-Cluster und keine Amazon Linux-Knotengruppe haben, zu der Sie eine Windows-Knotengruppe hinzufügen können, empfehlen wir Ihnen, die folgenden Schritte zu befolgen [the section called “Cluster erstellen \(eksctl\)”](#). Dieses Handbuch bietet eine vollständige Anleitung zur Erstellung eines Amazon EKS-Clusters mit Amazon Linux-Knoten.

Erstellen Sie Ihre Knoten-Gruppe mit dem folgenden Befehl. *`region-code`* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. Ersetzen Sie *`my-cluster`* mit Ihrem Clusternamen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Ersetzen Sie *`ng-windows`* durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Sie können es durch *`2019`* ersetzen *`2022`*, um Windows Server 2022 zu verwenden. Ersetzen Sie den Rest der *`example values`* durch Ihre eigenen Werte.

 Important

Um eine Knotengruppe in AWS Outposts-, AWS Wavelength- oder AWS Local Zone-Subnetzen bereitzustellen, übergeben Sie die Subnetze AWS Outposts, Wavelength oder Local Zone nicht, wenn Sie den Cluster erstellen. Erstellen Sie die Knotengruppe mit einer Konfigurationsdatei, in der Sie die Subnetze AWS Outposts, Wavelength oder Local Zone angeben. Weitere Informationen finden Sie unter [Verwenden von Config-Dateien](#) und im [Config-Datei-Schema](#) in der eksctl-Dokumentation.

```
eksctl create nodegroup \
 --region region-code \
 --cluster my-cluster \
 --name ng-windows \
 --node-type t2.large \
 --nodes 3 \
 --nodes-min 1 \
 --nodes-max 4 \
 --managed=false \
 --node-ami-family WindowsServer2019FullContainer
```

 Note

- Wenn Arbeitsknoten dem Cluster nicht beitreten können, finden Sie weitere Informationen unter [the section called “Knoten können nicht mit dem Cluster verknüpft werden”](#) im Handbuch zur Fehlerbehebung.
- Geben Sie den folgenden Befehl ein, um die verfügbaren Optionen für eksctl-Befehle anzuzeigen.

```
eksctl command -help
```

Eine Beispielausgabe sieht wie folgt aus. Mehrere Zeilen werden ausgegeben, während die Knoten erstellt werden. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) [???](#) Stellen Sie eine Beispielanwendung bereit, um Ihren Cluster und Ihre Windows-Worker-Knoten zu testen.
4. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:
  - Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
  - Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

## AWS Management Console

### Voraussetzungen

- Ein bestehender Amazon-EKS-Cluster und eine Linux-Knotengruppe. Wenn Sie nicht über diese Ressourcen verfügen, empfehlen wir Ihnen, sie mithilfe einer unserer Anleitungen unter zu erstellen. [Erste Schritte](#) In diesen Anleitungen wird beschrieben, wie Sie einen Amazon EKS-Cluster mit Linux-Knoten erstellen.
- Eine vorhandene VPC und eine Sicherheitsgruppe, die die Voraussetzungen für einen Amazon-EKS-Cluster erfüllen. Weitere Informationen erhalten Sie unter [the section called “VPC- und Subnetz-Anforderungen”](#) und [the section called “Anforderungen an Sicherheitsgruppen”](#). Die Anleitungen zur [Erste Schritte](#) Erstellung einer VPC, die die Anforderungen erfüllt. Alternativ können Sie auch auf [Create an Amazon VPC for your Amazon EKS Cluster klicken, um einen Cluster](#) manuell zu erstellen.
- Ein vorhandener Amazon-EKS-Cluster, der eine VPC und eine Sicherheitsgruppe verwendet, die die Voraussetzungen eines Amazon-EKS-Clusters erfüllt. Weitere Informationen finden Sie unter [the section called “Erstellen eines -Clusters”](#). Wenn Sie Subnetze in der AWS Region haben, in der Sie AWS Outposts, AWS Wavelength oder AWS Local Zones aktiviert haben, dürfen diese Subnetze bei der Erstellung des Clusters nicht weitergegeben worden sein.

Schritt 1: Starten Sie selbstverwaltete Windows-Knoten mit AWS Management Console

1. Warten Sie, bis der Status des Clusters als ACTIVE angezeigt wird. Wenn Sie Ihre Knoten starten, bevor der Cluster aktiv ist, werden die Knoten nicht mit dem Cluster registriert und Sie müssen sie neu starten.
2. Öffnen Sie die [AWS CloudFormation -Konsole](#).
3. Wählen Sie Stack erstellen aus.
4. Wählen Sie unter Vorlage angeben die Option Amazon-S3-URL aus.
5. Kopieren Sie die folgende URL und fügen Sie sie in die Amazon S3 URL (Amazon-S3-URL) ein.

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2023-02-09/amazon-eks-windows-nodegroup.yaml
```

6. Wählen Sie zweimal Next (Weiter) aus.
7. Füllen Sie auf der Seite Quick create stack (Stack schnell erstellen) die folgenden Parameter entsprechend aus:
  - Stack-Name: Wählen Sie einen Stack-Namen für Ihren AWS CloudFormation Stack. Sie können ihn beispielsweise `my-cluster-nodes` nennen.
  - ClusterName: Geben Sie den Namen ein, den Sie bei der Erstellung Ihres Amazon EKS-Clusters verwendet haben.

 Important

Dieser Name muss genau mit dem Namen übereinstimmen, den Sie in [Schritt 1: Amazon EKS-Cluster erstellen](#) verwendet haben. Andernfalls können Ihre Knoten dem Cluster nicht beitreten.

- ClusterControlPlaneSecurityGroup: Wählen Sie die Sicherheitsgruppe aus der AWS CloudFormation Ausgabe aus, die Sie bei der Erstellung Ihrer [VPC](#) generiert haben. Die folgenden Schritte zeigen eine Methode zum Abrufen der entsprechenden Gruppe.
  - a. Öffnen Sie die [Amazon-EKS-Konsole](#).
  - b. Wählen Sie den Namen des Clusters.
  - c. Wählen Sie die Registerkarte Network (Network) aus.
  - d. Verwenden Sie den Wert Zusätzliche Sicherheitsgruppen als Referenz, wenn Sie aus der ClusterControlPlaneSecurityGroupDropdownliste auswählen.
- NodeGroupName: Geben Sie einen Namen für Ihre Knotengruppe ein. Dieser Name kann später verwendet werden, um die Auto Scaling-Knotengruppe zu identifizieren, die für Ihre



Knoten erstellt wurde. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.

- **NodeAutoScalingGroupMinSize:** Geben Sie die Mindestanzahl von Knoten ein, auf die Ihre Auto Scaling Group für Knoten skalieren kann.
- **NodeAutoScalingGroupDesiredCapacity:** Geben Sie die gewünschte Anzahl von Knoten ein, auf die bei der Erstellung Ihres Stacks skaliert werden soll.
- **NodeAutoScalingGroupMaxSize:** Geben Sie die maximale Anzahl von Knoten ein, auf die Ihre Auto Scaling Group für Knoten skalieren kann.
- **NodeInstanceType:** Wählen Sie einen Instance-Typ für Ihre Knoten. Weitere Informationen finden Sie unter [the section called “EC2 Amazon-Instance-Typen”](#).

 Note

[Die unterstützten Instance-Typen für die neueste Version des Amazon VPC CNI-Plug-ins für Kubernetes sind in `vpc\_ip\_resource\_limit.go` on aufgeführt.](#) GitHub

Möglicherweise müssen Sie Ihre CNI-Version aktualisieren, um die neuesten unterstützten Instance-Typen zu nutzen. Weitere Informationen finden Sie unter [the section called “Amazon VPC CNI”](#).

- **NodeImageIdSSMParam:** Vorab mit dem Amazon EC2 Systems Manager Manager-Parameter der aktuell empfohlenen Amazon EKS-optimierten Windows Core-AMI-ID gefüllt. Um die Vollversion von Windows zu verwenden, ersetzen Sie **Core** durch **Full**.
- **NodeImageId:** (Optional) Wenn Sie Ihr eigenes benutzerdefiniertes AMI (anstelle eines für Amazon EKS optimierten AMI) verwenden, geben Sie eine Knoten-AMI-ID für Ihre AWS Region ein. Wenn Sie einen Wert für dieses Feld angeben, überschreibt dieser alle Werte in dem **NodeImageIdSSMParamFeld**.
- **NodeVolumeSize:** Geben Sie eine Root-Volume-Größe für Ihre Knoten in GiB an.
- **KeyName:** Geben Sie den Namen eines Amazon EC2 SSH-Schlüsselpaars ein, mit dem Sie nach dem Start über SSH eine Verbindung zu Ihren Knoten herstellen können. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch.

 Note

Wenn Sie hier kein key pair angeben, kann der AWS CloudFormation Stack nicht erstellt werden.

- **BootstrapArguments:** Geben Sie alle optionalen Argumente an, die an das Node-Bootstrap-Skript übergeben werden sollen, z. B. zusätzliche `kubelet` Argumente mit `KubeletExtraArgs`.
- **Deaktivieren IMDSv1:** Standardmäßig unterstützt jeder Knoten den Instanz-Metadatendienst Version 1 (IMDSv1) und IMDSv2. Sie können deaktivieren IMDSv1. Um zu verhindern, dass future Knoten und Pods in der Knotengruppe verwendet werden MDSv1, setzen Sie `Disable IMDSv1` auf `true`. Weitere Informationen finden Sie unter [Konfiguration des Instance-Metadatenservice](#).
- **VpcId:** Wählen Sie die ID für die [VPC](#) aus, die Sie erstellt haben.
- **NodeSecurityGroups:** Wählen Sie die Sicherheitsgruppe aus, die für Ihre Linux-Knotengruppe erstellt wurde, als Sie Ihre [VPC](#) erstellt haben. Wenn Ihren Linux-Knoten mehr als eine Sicherheitsgruppe angehängt ist, geben Sie alle an. Dies z. B., wenn die Linux-Knotengruppe mit `eksctl` erstellt wurde.
- **Subnets (Subnetze):** Wählen Sie die Subnetze aus, die Sie erstellt haben. Wenn Sie Ihre VPC mit den Schritten unter [Amazon VPC für Ihren Amazon EKS-Cluster erstellen](#) erstellt haben, geben Sie nur die privaten Subnetze innerhalb der VPC an, in denen Ihre Knoten gestartet werden sollen.

 Important

- Wenn es sich bei einem oder einigen der Subnetze um öffentliche Subnetze handelt, muss die Einstellung für die automatische Zuweisung öffentlicher IP-Adressen aktiviert sein. Wenn die Einstellung für das öffentliche Subnetz nicht aktiviert ist, wird allen Knoten, die Sie in diesem öffentlichen Subnetz bereitstellen, keine öffentliche IP-Adresse zugewiesen und sie können nicht mit dem Cluster oder anderen Diensten kommunizieren. AWS Wenn das Subnetz vor dem 26. März 2020 mithilfe einer der [Amazon AWS CloudFormation EKS-VPC-Vorlagen](#) oder mithilfe `eksctl` von bereitgestellt wurde, ist die automatische Zuweisung öffentlicher IP-Adressen für öffentliche Subnetze deaktiviert. Informationen dazu, wie Sie die Zuweisung öffentlicher IP-Adressen für ein Subnetz aktivieren, finden Sie unter [Ändern des](#)

[Attributs für die öffentliche IPv4 Adressierung](#) für Ihr Subnetz. Wenn der Knoten in einem privaten Subnetz bereitgestellt wird, kann er über ein NAT-Gateway mit dem Cluster und anderen AWS Diensten kommunizieren.

- Wenn die Subnetze keinen Internetzugang haben, stellen Sie sicher, dass Sie die Überlegungen und zusätzlichen Schritte unter [Bereitstellen von privaten Clustern mit eingeschränktem Internetzugang](#) kennen.
- Wenn Sie AWS Outposts-, Wavelength- oder Local Zone-Subnetze auswählen, dürfen die Subnetze bei der Erstellung des Clusters nicht übergeben worden sein.

8. Bestätigen Sie, dass der Stack IAM-Ressourcen erstellen kann, und wählen Sie dann Create stack (Stack erstellen) aus.
9. Wenn Ihr Stack fertig erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgaben).
10. Notieren Sie das NodeInstanceRole für die Knotengruppe, die erstellt wurde. Sie benötigen diese, wenn Sie Ihre Amazon-EKS-Windows-Knoten konfigurieren.

Schritt 2: Ermöglichen Sie den Knoten, Ihrem Cluster beizutreten

1. Überprüfen Sie, ob Sie bereits über eine aws-auth ConfigMap verfügen.

```
kubectl describe configmap -n kube-system aws-auth
```

2. Wenn eine aws-auth ConfigMap angezeigt wird, aktualisieren Sie sie nach Bedarf.

- a. Öffnen Sie ConfigMap zum Bearbeiten.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Fügen Sie nach Bedarf neue mapRoles-Einträge hinzu. Stellen Sie die roleARN Werte auf die NodeInstanceRole Werte ein, die Sie in den vorherigen Verfahren aufgezeichnet haben.

```
[...]
data:
 mapRoles: |
- roleARN: <ARN of linux instance role (not instance profile)>
 username: system:node:{{EC2PrivateDNSName}}
 groups:
 - system:bootstrappers
 - system:nodes
```

```
- rolearn: <ARN of windows instance role (not instance profile)>
 username: system:node:{{EC2PrivateDNSName}}
 groups:
 - system:bootstrappers
 - system:nodes
 - eks:kube-proxy-windows
[...]
```

c. Speichern Sie die Datei und beenden Sie den Text-Editor.

3. Wenn die Fehlermeldung `Error from server (NotFound): configmaps "aws-auth" not found` angezeigt wird, wenden Sie die standardmäßige ConfigMap an.

a. Laden Sie die Konfigurationszuordnung herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/
aws-auth-cm-windows.yaml
```

b. Stellen Sie in der `aws-auth-cm-windows.yaml` Datei die `rolearn` Werte auf die entsprechenden `NodeInstanceRole` Werte ein, die Sie in den vorherigen Verfahren aufgezeichnet haben. Hierzu können Sie einen Texteditor verwenden oder die *example values* ersetzen und den folgenden Befehl ausführen:

```
sed -i.bak -e 's|<ARN of linux instance role (not instance profile)>|my-node-
linux-instance-role|' \
 -e 's|<ARN of windows instance role (not instance profile)>|my-node-windows-
instance-role|' aws-auth-cm-windows.yaml
```

#### Important

- Ändern Sie keine anderen Zeilen in dieser Datei.
- Verwenden Sie nicht dieselbe IAM-Rolle für Windows- und Linux-Knoten.

c. Wenden Sie die Konfiguration an. Die Ausführung dieses Befehls kann einige Minuten dauern.

```
kubectl apply -f aws-auth-cm-windows.yaml
```

4. Sehen Sie sich den Status Ihrer Knoten an und warten Sie, bis diese in den Ready-Status eintreten.

```
kubectl get nodes --watch
```

Geben Sie `Ctrl+C` ein, um zu einer Shell-Eingabeaufforderung zurückzukehren.

 Note

Wenn Sie Autorisierungs- oder Ressourcenfehler erhalten, finden Sie weitere Informationen unter [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#) im Thema zur Fehlerbehebung.

Wenn Knoten dem Cluster nicht beitreten können, finden Sie weitere Informationen [the section called “Knoten können nicht mit dem Cluster verknüpft werden”](#) im Kapitel Fehlerbehebung.

### Schritt 3: Zusätzliche Aktionen

1. (Optional) [???](#) Stellen Sie eine Beispielanwendung bereit, um Ihren Cluster und Ihre Windows-Worker-Knoten zu testen.
2. (Optional) Wenn die von `AmazonEKS_CNI_Policy` verwaltete IAM-Richtlinie (wenn Sie einen IPv4 Cluster haben) oder die *AmazonEKS\_CNI\_IPv6\_Policy* (die Sie [selbst erstellt](#) haben, wenn Sie einen IPv6 Cluster haben) mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Servicekonto zuordnen. `aws-node` Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).
3. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:
  - Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
  - Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

# Erstellen Sie selbstverwaltete Ubuntu-Linux-Knoten

## Note

Verwaltete Knotengruppen bieten möglicherweise einige Vorteile für Ihren Anwendungsfall. Weitere Informationen finden Sie unter [the section called “Verwaltete Knotengruppen”](#).

In diesem Thema wird beschrieben, wie Sie Auto Scaling Scaling-Gruppen von [Ubuntu auf Amazon Elastic Kubernetes Service \(EKS\)](#) oder [Ubuntu Pro auf Amazon Elastic Kubernetes Service \(EKS\)](#) - Knoten starten, die sich bei Ihrem Amazon EKS-Cluster registrieren. Ubuntu und Ubuntu Pro für EKS basieren auf dem offiziellen Ubuntu Minimal LTS, enthalten den benutzerdefinierten AWS Kernel, der gemeinsam mit EKS entwickelt wurde AWS, und wurden speziell für EKS entwickelt. Ubuntu Pro bietet zusätzlichen Sicherheitsschutz, indem es erweiterte EKS-Supportzeiten, Kernel-Livepatch, FIPS-Konformität und die Möglichkeit, eine unbegrenzte Anzahl von Pro-Containern auszuführen, unterstützt.

Nachdem die Knoten dem Cluster beigetreten sind, können Sie containerisierte Anwendungen für sie bereitstellen. Weitere Informationen finden Sie in der Dokumentation für [Ubuntu on AWS](#) und [Custom AMI Support](#) in der eksctl Dokumentation.

## Important

- Amazon EKS-Knoten sind EC2 Standard-Amazon-Instances, und sie werden Ihnen auf der Grundlage der normalen EC2 Amazon-Instance-Preise in Rechnung gestellt. Weitere Informationen finden Sie unter [EC2 Amazon-Preise](#).
- Sie können Ubuntu-Knoten in erweiterten Amazon EKS-Clustern auf AWS Outposts starten, aber Sie können sie nicht in lokalen Clustern auf AWS Outposts starten. Weitere Informationen finden Sie unter [Amazon EKS auf AWS Outposts](#).
- Sie können die Bereitstellung auf EC2 Amazon-Instances mit x86 oder ARM-Prozessoren durchführen. Instances mit Inferentia-Chips müssen jedoch möglicherweise zuerst das [Neuron](#) SDK installieren.

Für diesen Vorgang ist eksctl Version 0.210.0 oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Anweisungen zur Installation oder zum Upgrade `eksctl` finden Sie in der `eksctl` Dokumentation unter [Installation](#). Hinweis: Dieses Verfahren funktioniert nur für Cluster, die mit `eksctl` erstellt wurden.

1. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphabetischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Ersetzen Sie `ng-ubuntu` durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Um die Bereitstellung auf Arm-Instances durchzuführen, ersetzen Sie `m5.large` durch einen Arm-Instance-Typ. `my-ec2-keypair-name` Ersetzen Sie es durch den Namen eines Amazon EC2 SSH-Schlüsselpaars, mit dem Sie nach dem Start über SSH eine Verbindung zu Ihren Knoten herstellen können. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch. Ersetzen Sie *example values* durch Ihre eigenen Werte. Sobald Sie die Ersetzungen vorgenommen haben, führen Sie den modifizierten Befehl aus, um die `ubuntu.yaml` Datei zu erstellen.

#### Important

Um eine Knotengruppe in AWS Outposts-, AWS Wavelength- oder AWS Local Zone-Subnetzen bereitzustellen, übergeben Sie beim Erstellen des Clusters keine AWS Outposts-, AWS Wavelength- oder AWS Local Zone-Subnetze. Sie müssen die Subnetze im folgenden Beispiel angeben. Weitere Informationen finden Sie unter [Verwenden von Config-Dateien](#) und im [Config-Datei-Schema](#) in der `eksctl`-Dokumentation. Ersetzen Sie es *region-code* durch die AWS Region, in der sich Ihr Cluster befindet.

```
cat >ubuntu.yaml <<EOF

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
```

```
name: my-cluster
region: region-code
version: '1.33'

iam:
 withOIDC: true

nodeGroups:
 - name: ng-ubuntu
 instanceType: m5.large
 desiredCapacity: 3
 amiFamily: Ubuntu2204
 iam:
 attachPolicyARNs:
 - arn:aws:iam::aws:policy/AmazonEKSEKSWorkerNodePolicy
 - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
 - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
 - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
 ssh:
 allow: true
 publicKeyName: my-ec2-keypair-name

EOF
```

Um eine Ubuntu Pro-Knotengruppe zu erstellen, ändern Sie den `amiFamily` Wert einfach in `UbuntuPro2204`.

2. Stellen Sie den Treiber mit dem folgenden Befehl bereit.

```
eksctl create nodegroup --config-file=ubuntu.yaml
```

Eine Beispielausgabe sieht wie folgt aus.

Mehrere Zeilen werden ausgegeben, während die Knoten erstellt werden. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) Stellen Sie eine [Beispielanwendung](#) bereit, um Ihre Ubuntu-Knoten zu testen.
4. Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:



- Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
- Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

## Aktualisieren Sie selbstverwaltete Knoten für Ihren Cluster

Wenn eine neue Amazon-EKS-optimierte AMI veröffentlicht wird, ziehen Sie in Betracht, die Knoten in Ihrer selbstverwalteten Knoten-Gruppe durch die neue AMI zu ersetzen. Ebenso gilt, dass Sie bei einer Aktualisierung der Kubernetes-Version für Ihren Amazon-EKS-Cluster auch die Worker-Knoten aktualisieren, um Knoten mit derselben Kubernetes-Version zu verwenden.

### Important

In diesem Thema werden Worker-Knotenaktualisierungen für selbstverwaltete Knotengruppen behandelt. Wenn Sie [verwaltete Knotengruppen](#) verwenden, finden Sie weitere Informationen unter [the section called “Aktualisierung”](#).

Es gibt zwei grundlegende Möglichkeiten, selbstverwaltete Knotengruppen in Ihren Clustern zu aktualisieren, um ein neues AMI zu verwenden:

### [Migrieren Sie Anwendungen auf eine neue Knotengruppe](#)

Erstellen Sie eine neue Knotengruppe und migrieren Sie Ihre Pods zu dieser Gruppe. Die Migration zu einer neuen Knotengruppe ist eleganter als die einfache Aktualisierung der AMI-ID in einem vorhandenen AWS CloudFormation Stack. Das liegt daran, dass der Migrationsprozess die alte Knotengruppe als [unbrauchbar](#) macht `NoSchedule` und die Knoten leer werden, sobald ein neuer Stack bereit ist, die bestehende Pod-Arbeitslast zu akzeptieren.

### [Aktualisieren Sie einen Knotenstapel AWS CloudFormation](#)

Aktualisieren Sie den AWS CloudFormation Stack für eine bestehende Knotengruppe, um das neue AMI zu verwenden. Diese Methode wird nicht für Knotengruppen unterstützt, die mit `wurdeneksctl` erstellt wurden.

## Anwendungen auf eine neue Knotengruppe migrieren

Dieses Thema beschreibt Hinweise zum Erstellen einer neuen Knoten-Gruppe, zum ordnungsgemäßen Migrieren Ihrer vorhandenen Anwendungen zur neuen Gruppe und zum Entfernen der alten Knoten-Gruppe aus Ihrem Cluster. Sie können zu einer neuen Knotengruppe migrieren, indem Sie `eksctl` oder AWS Management Console benutzen.

- [the section called “eksctl”](#)
- [the section called “AWS Management Console und AWS CLI”](#)

### eksctl

Migrieren Sie Ihre Anwendungen auf eine neue Knotengruppe mit **eksctl**

Weitere Informationen zur Verwendung von `eksctl` für die Migration finden Sie in der Dokumentation unter [Unmanaged Nodegroups](#). `eksctl`

Für diesen Vorgang ist `eksctl` Version 0.210.0 oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Eine Installations- und Upgrade-Anleitung für `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).

#### Note

Dieses Verfahren funktioniert nur für Cluster, die mit `eksctl` erstellt wurden.

1. Rufen Sie den Namen Ihrer vorhandenen Knotengruppen ab und ersetzen Sie *my-cluster* durch Ihren Clusternamen.

```
eksctl get nodegroups --cluster=my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

| CLUSTER          | NODEGROUP     | CREATED  | MIN SIZE | MAX SIZE |
|------------------|---------------|----------|----------|----------|
| DESIRED CAPACITY | INSTANCE TYPE | IMAGE ID |          |          |

|         |                |                       |   |   |   |
|---------|----------------|-----------------------|---|---|---|
| default | standard-nodes | 2019-05-01T22:26:58Z  | 1 | 4 | 3 |
|         | t3.medium      | ami-05a71d034119ffc12 |   |   |   |

2. Starten Sie eine neue Knotengruppe mit `eksctl` mit dem folgenden Befehl. Ersetzen Sie im Befehl jedes *example value* durch Ihre eigenen Werte. Die Versionsnummer darf nicht neuer sein als die Kubernetes-Version für Ihre Steuerungsebene. Außerdem dürfen nicht mehr als zwei Nebenversionen vor der Kubernetes-Version für Ihre Kontrollebene liegen. Es wird empfohlen, dieselbe Version wie die Steuerebene zu verwenden.

Wir empfehlen, den Pod-Zugriff auf IMDS zu blockieren, wenn die folgenden Bedingungen zutreffen:

- Sie planen, all Ihren Kubernetes-Dienstkonten IAM-Rollen zuzuweisen, sodass Pods nur über die Mindestberechtigungen verfügen, die sie benötigen.
- Keine Pods im Cluster benötigen aus anderen Gründen Zugriff auf den Amazon EC2 Instance Metadata Service (IMDS), z. B. zum Abrufen der aktuellen AWS Region.

Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

Um den Pod-Zugriff auf IMDS zu blockieren, fügen Sie dem folgenden Befehl die `--disable-pod-imds` Option hinzu.

#### Note

Weitere verfügbare Flags und deren Beschreibungen finden Sie unter <https://eksctl.io/>.

```
eksctl create nodegroup \
 --cluster my-cluster \
 --version 1.33 \
 --name standard-nodes-new \
 --node-type t3.medium \
 --nodes 3 \
 --nodes-min 1 \
 --nodes-max 4 \
 --managed=false
```

3. Wenn der vorherige Befehl abgeschlossen ist, bestätigen Sie mit folgendem Befehl, dass alle Ihre Worker-Knoten den Ready-Status erreicht haben:

```
kubectl get nodes
```

4. Löschen Sie die ursprüngliche Knotengruppe mit dem folgenden Befehl. Ersetzen Sie im Befehl alle *example value* mit Ihren Cluster- und Knotengruppennamen:

```
eksctl delete nodegroup --cluster my-cluster --name standard-nodes-old
```

## AWS Management Console und AWS CLI

Migrieren Sie Ihre Anwendungen mit der AWS Management Console und AWS CLI auf eine neue Knotengruppe

1. Starten Sie eine neue Knotengruppe, indem Sie die unter [Selbstverwalteten Amazon Linux-Knoten erstellen](#) beschriebenen Schritte ausführen.
2. Wenn Ihr Stack fertig erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgaben).
3. Notieren Sie sich das NodeInstanceRole für die Knotengruppe, die erstellt wurde. Sie benötigen diese Informationen zum Hinzufügen der neuen Amazon EKS-Knoten zu Ihrem Cluster.

### Note

Wenn Sie der IAM-Rolle Ihrer alten Knotengruppen zusätzliche IAM-Richtlinien angefügt haben, dann sollten Sie die gleichen Richtlinien auch der IAM-Rolle Ihrer neuen Knotengruppe zuweisen, um diese Funktionalität für die neue Gruppe zu erhalten. Dies gilt für Sie, wenn Sie beispielsweise Berechtigungen für den Kubernetes [Cluster Autoscaler](#) hinzugefügt haben.

4. Aktualisieren Sie die Sicherheitsgruppen für beide Worker-Knoten-Gruppen, sodass sie miteinander kommunizieren können. Weitere Informationen finden Sie unter [the section called "Anforderungen an Sicherheitsgruppen"](#).
  - a. Notieren Sie die Sicherheitsgruppe IDs für beide Knotengruppen. Dies wird als NodeSecurityGroupWert in den AWS CloudFormation Stack-Ausgaben angezeigt.

Sie können die folgenden AWS CLI-Befehle verwenden, um die Sicherheitsgruppe IDs aus den Stack-Namen abzurufen. In diesen Befehlen `oldNodes` steht der AWS CloudFormation

Stack-Name für Ihren älteren Knoten-Stack und newNodes der Name des Stacks, zu dem Sie migrieren. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
oldNodes="old_node_CFN_stack_name"
newNodes="new_node_CFN_stack_name"

oldSecGroup=$(aws cloudformation describe-stack-resources --stack-name $oldNodes \
--query 'StackResources[?
ResourceType=='AWS::EC2::SecurityGroup`].PhysicalResourceId' \
--output text)
newSecGroup=$(aws cloudformation describe-stack-resources --stack-name $newNodes \
--query 'StackResources[?
ResourceType=='AWS::EC2::SecurityGroup`].PhysicalResourceId' \
--output text)
```

- b. Fügen Sie Regeln für eingehenden Datenverkehr für jede Worker-Knoten-Sicherheitsgruppe hinzu, sodass sie voneinander Datenverkehr annehmen können.

Die folgenden AWS CLI-Befehle fügen jeder Sicherheitsgruppe Regeln für eingehenden Datenverkehr hinzu, die den gesamten Datenverkehr auf allen Protokollen der anderen Sicherheitsgruppe zulassen. Diese Konfiguration ermöglicht es Pods in jeder Knotengruppe, miteinander zu kommunizieren, während Sie Ihren Workload in die neue Gruppe migrieren.

```
aws ec2 authorize-security-group-ingress --group-id $oldSecGroup \
--source-group $newSecGroup --protocol -1
aws ec2 authorize-security-group-ingress --group-id $newSecGroup \
--source-group $oldSecGroup --protocol -1
```

5. Bearbeiten Sie die aws-auth-configmap, um die neue Worker-Knoten-Instance-Rolle in RBAC zuzuordnen.

```
kubectl edit configmap -n kube-system aws-auth
```

Fügen Sie einen neuen mapRoles-Eintrag für die neue Worker-Knoten-Gruppe hinzu.

```
apiVersion: v1
data:
 mapRoles: |
 - rolearn: ARN of instance role (not instance profile)
 username: system:node:{{EC2PrivateDNSName}}
 groups:
```

```

- system:bootstrappers
- system:nodes>
- rolearn: arn:aws: iam::111122223333:role/nodes-1-16-NodeInstanceRole-
U11V27W93CX5
 username: system:node:{{EC2PrivateDNSName}}
 groups:
 - system:bootstrappers
 - system:nodes

```

Ersetzen Sie das *ARN of instance role (not instance profile)* Snippet durch den [NodeInstanceRoleWert](#), den Sie in einem vorherigen Schritt aufgezeichnet haben. Speichern und schließen Sie dann die Datei, um die aktualisierte configmap anzuwenden.

6. Achten Sie auf den Status Ihrer Knoten und warten Sie, bis Ihre neuen Worker-Knoten Ihrem Cluster beigetreten sind und den Status Ready angenommen haben.

```
kubectl get nodes --watch
```

7. (Optional) Wenn Sie den [Kubernetes Cluster Autoscaler](#) verwenden, skalieren Sie die Bereitstellung auf Null (0) Replikate, um widersprüchliche Skalierungsaktionen zu vermeiden.

```
kubectl scale deployments/cluster-autoscaler --replicas=0 -n kube-system
```

8. Verwenden Sie den folgenden Befehl, um jeden der Knoten, die Sie mit `NoSchedule` entfernen möchten, mit einem Taint zu versehen. Dadurch wird verhindert, dass neue Pods auf den Knoten, die Sie ersetzen, geplant oder verschoben werden. Weitere Informationen finden Sie unter [Taints and Tolerations](#) in der Kubernetes-Dokumentation.

```
kubectl taint nodes node_name key=value:NoSchedule
```

Wenn Sie Ihre Knoten auf eine neue Kubernetes-Version aktualisieren, können Sie alle Knoten einer bestimmten Kubernetes-Version (in diesem Fall) mit dem folgenden Codeausschnitt identifizieren und manipulieren. 1.31 Die Versionsnummer darf nicht nach der Kubernetes-Version Ihrer Steuerungsebene liegen. Sie darf auch nicht mehr als zwei Nebenversionen vor der Kubernetes-Version Ihrer Kontrollebene sein. Es wird empfohlen, dieselbe Version wie die Steuerebene zu verwenden.

```

K8S_VERSION=1.31
nodes=$(kubectl get nodes -o jsonpath="{.items[?(@.status.nodeInfo.kubeletVersion==
\"v$K8S_VERSION\")].metadata.name}")

```

```
for node in ${nodes[@]}
do
 echo "Tainting $node"
 kubectl taint nodes $node key=value:NoSchedule
done
```

## 9. Ermitteln Sie den DNS-Anbieter Ihres Clusters.

```
kubectl get deployments -l k8s-app=kube-dns -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus. Dieser Cluster verwendet CoreDNS für die DNS-Auflösung, aber Ihr Cluster kann kube-dns stattdessen zurückkehren):

| NAME    | DESIRED | CURRENT | UP-TO-DATE | AVAILABLE | AGE |
|---------|---------|---------|------------|-----------|-----|
| coredns | 1       | 1       | 1          | 1         | 31m |

10. Wenn Ihre aktuelle Bereitstellung weniger als zwei Replikate ausführt, skalieren die Bereitstellung auf zwei Replikate. Ersetzen Sie kubedns durch *coredns*, falls Ihre vorherige Befehlsausgabe dies stattdessen zurückgegeben hat.

```
kubectl scale deployments/coredns --replicas=2 -n kube-system
```

11. Lassen Sie die einzelnen Knoten, die Sie aus Ihrem Cluster entfernen möchten, mit dem folgenden Befehl sperren:

```
kubectl drain node_name --ignore-daemonsets --delete-local-data
```

Wenn Sie Ihre Knoten auf eine neue Kubernetes-Version aktualisieren, identifizieren und entleeren Sie alle Knoten einer bestimmten Kubernetes-Version (in diesem Fall *1.31*) mit dem folgenden Codeausschnitt.

```
K8S_VERSION=1.31
nodes=$(kubectl get nodes -o jsonpath="{.items[?(@.status.nodeInfo.kubeletVersion==\"v$K8S_VERSION\")].metadata.name}")
for node in ${nodes[@]}
do
 echo "Draining $node"
 kubectl drain $node --ignore-daemonsets --delete-local-data
done
```

12 Nachdem die alten Knoten entladen wurden, widerrufen Sie die Regeln für eingehenden Datenverkehr für Sicherheitsgruppen, die Sie zuvor autorisiert haben. Löschen Sie anschließend den Stack, um die Instanzen zu beenden AWS CloudFormation .

 Note

Wenn Sie Ihrer alten Knotengruppen-IAM-Rolle zusätzliche IAM-Richtlinien hinzugefügt haben, z. B. das Hinzufügen von Berechtigungen für den [Kubernetes Cluster Autoscaler](#), trennen Sie diese zusätzlichen Richtlinien von der Rolle, bevor Sie Ihren Stack löschen können. AWS CloudFormation

- a. Heben Sie die Regeln für eingehenden Datenverkehr auf, die Sie zuvor für die Knoten-Sicherheitsgruppen erstellt haben. In diesen Befehlen `oldNodes` steht der AWS CloudFormation Stack-Name für Ihren älteren Knoten-Stack und `newNodes` der Name des Stacks, zu dem Sie migrieren.

```
oldNodes="old_node_CFN_stack_name"
newNodes="new_node_CFN_stack_name"

oldSecGroup=$(aws cloudformation describe-stack-resources --stack-name $oldNodes \
--query 'StackResources[?
ResourceType=='AWS::EC2::SecurityGroup'].PhysicalResourceId' \
--output text)
newSecGroup=$(aws cloudformation describe-stack-resources --stack-name $newNodes \
--query 'StackResources[?
ResourceType=='AWS::EC2::SecurityGroup'].PhysicalResourceId' \
--output text)
aws ec2 revoke-security-group-ingress --group-id $oldSecGroup \
--source-group $newSecGroup --protocol -1
aws ec2 revoke-security-group-ingress --group-id $newSecGroup \
--source-group $oldSecGroup --protocol -1
```

- b. Öffnen Sie die [AWS CloudFormation -Konsole](#).
- c. Wählen Sie Ihren alten Worker-Knoten-Stack aus.
- d. Wählen Sie Löschen aus.
- e. Wählen Sie im Bestätigungsdiaologfeld Stack löschen Stack löschen aus.

13 Bearbeiten Sie die `aws-auth-configmap`, um die alten Worker-Knoten-Instance-Rolle aus RBAC zu entfernen.



```
kubectl edit configmap -n kube-system aws-auth
```

Löschen Sie den mapRoles-Eintrag für die alte Worker-Knoten-Gruppe.

```
apiVersion: v1
data:
 mapRoles: |
 - rolearn: arn:aws:iam::111122223333:role/nodes-1-16-NodeInstanceRole-
W70725MZQFF8
 username: system:node:{{EC2PrivateDNSName}}
 groups:
 - system:bootstrappers
 - system:nodes
 - rolearn: arn:aws:iam::111122223333:role/nodes-1-15-NodeInstanceRole-
U11V27W93CX5
 username: system:node:{{EC2PrivateDNSName}}
 groups:
 - system:bootstrappers
 - system:nodes>
```

Speichern und schließen Sie die Datei, um die aktualisierte configmap anzuwenden.

14.(Optional) Wenn Sie den Kubernetes-[Cluster Autoscaler](#) verwenden, skalieren Sie die Bereitstellung wieder auf ein Replikat.

#### Note

Außerdem müssen Sie Ihre neue Auto-Scaling-Gruppe (z. B. `k8s.io/cluster-autoscaler/enabled`, `k8s.io/cluster-autoscaler/my-cluster`) mit einem Tag versehen und den Befehl für die Cluster-Autoscaler-Bereitstellung so aktualisieren, dass er auf die neu getaggte Auto-Scaling-Gruppe verweist. Weitere Informationen finden Sie unter [Cluster Autoscaler on](#). AWS

```
kubectl scale deployments/cluster-autoscaler --replicas=1 -n kube-system
```

15.(Optional) Stellen Sie sicher, dass Sie die neueste Version des [Amazon VPC CNI-Plug-ins für](#) Kubernetes verwenden. Möglicherweise müssen Sie Ihre CNI-Version aktualisieren, um die

neuesten unterstützten Instance-Typen zu nutzen. Weitere Informationen finden Sie unter [the section called “Amazon VPC CNI”](#).

16. Wenn Ihr Cluster die DNS-Auflösung kube-dns verwendet (siehe [\[migrate-determine-dns-step\]](#)), skalieren Sie die kube-dns Bereitstellung auf ein Replikat.

```
kubectl scale deployments/kube-dns --replicas=1 -n kube-system
```

## Einen AWS CloudFormation Knotenstapel aktualisieren

In diesem Thema wird beschrieben, wie Sie einen vorhandenen AWS CloudFormation selbstverwalteten Knotenstapel mit einem neuen AMI aktualisieren können. Sie können diese Anleitung verwenden, um Ihre Knoten nach einer Cluster-Aktualisierung auf eine neue Version von Kubernetes zu aktualisieren. Andernfalls können Sie auf das neueste von Amazon EKS optimierte AMI für eine vorhandene Kubernetes-Version aktualisieren.

### Important

In diesem Thema werden Worker-Knotenaktualisierungen für selbstverwaltete Knotengruppen behandelt. Informationen zur Verwendung von [Simplify Node Lifecycle mit verwalteten Knotengruppen](#) finden Sie unter [the section called “Aktualisierung”](#).

Die neueste Amazon AWS CloudFormation EKS-Standardknotenvorlage ist so konfiguriert, dass eine Instance mit dem neuen AMI in Ihrem Cluster gestartet wird, bevor nacheinander eine alte entfernt wird. Diese Konfiguration stellt sicher, dass Sie während des fortlaufenden Updates immer die von Ihrer Auto Scaling Scaling-Gruppe gewünschte Anzahl an aktiven Instances in Ihrem Cluster haben.

### Note

Diese Methode wird nicht für Knotengruppen unterstützt, die mit `eksctl` erstellt wurden. Wenn Sie Ihr Cluster oder Ihre Worker-Knoten-Gruppe mit `eksctl` erstellt haben, finden Sie Informationen unter [the section called “Migration”](#).

1. Bestimmen Sie den DNS-Anbieter Ihres Clusters.

```
kubectl get deployments -l k8s-app=kube-dns -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus. Dieser Cluster verwendet CoreDNS für die DNS-Auflösung, aber Ihr Cluster kehrt möglicherweise stattdessen zurück kube-dns. Ihre Ausgabe kann je nach der Version, die Sie verwenden `kubectl`, anders aussehen.

| NAME    | DESIRED | CURRENT | UP-TO-DATE | AVAILABLE | AGE |
|---------|---------|---------|------------|-----------|-----|
| coredns | 1       | 1       | 1          | 1         | 31m |

2. Wenn Ihre aktuelle Bereitstellung weniger als zwei Replikate ausführt, skalieren die Bereitstellung auf zwei Replikate. Ersetzen Sie `kube-dns` durch `coredns`, falls Ihre vorherige Befehlsausgabe dies stattdessen zurückgegeben hat.

```
kubectl scale deployments/coredns --replicas=2 -n kube-system
```

3. (Optional) Wenn Sie den Kubernetes [Cluster Autoscaler](#) verwenden, skalieren Sie die Bereitstellung auf Null (0) Replikate, um widersprüchliche Skalierungsaktionen zu vermeiden.

```
kubectl scale deployments/cluster-autoscaler --replicas=0 -n kube-system
```

4. Ermitteln Sie den Instanztyp und die gewünschte Anzahl der Instanzen Ihrer aktuellen Knotengruppe. Sie geben diese Werte später ein, wenn Sie die AWS CloudFormation Vorlage für die Gruppe aktualisieren.
  - a. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
  - b. Wählen Sie im linken Navigationsbereich Launch Configurations (Startkonfigurationen) aus und beachten Sie den Instance-Typ für die Startkonfiguration der vorhandenen Knoten.
  - c. Wählen Sie im linken Navigationsbereich Auto Scaling Groups (Auto-Scaling-Gruppen) aus und beachten Sie die Desired (gewünschte) Instance-Anzahl für die Auto-Scaling-Gruppe der vorhandenen Knoten.
5. Öffnen Sie die [AWS CloudFormation -Konsole](#).
6. Wählen Sie Ihren Workerknoten-Gruppen-Stack aus und klicken Sie dann auf Update (Aktualisieren).
7. Wählen Sie Replace current template (Aktuelle Vorlage ersetzen) und dann Amazon S3 URL (Amazon S3-URL) aus.
8. Fügen Sie für Amazon S3 S3-URL die folgende URL in den Textbereich ein, um sicherzustellen, dass Sie die neueste Version der AWS CloudFormation Node-Vorlage verwenden. Klicken Sie dann auf Next (Weiter):

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/amazon-eks-
nodegroup.yaml
```

9. Geben Sie auf der Seite Specify stack details (Stack-Details angeben) die folgenden Parameter ein und wählen Sie Next (Weiter) aus:

- **NodeAutoScalingGroupDesiredCapacity**— Geben Sie die gewünschte Anzahl von Instanzen ein, die Sie in einem [vorherigen Schritt](#) aufgezeichnet haben. Oder geben Sie die neue gewünschte Anzahl von Knoten ein, auf die bei der Aktualisierung Ihres Stacks skaliert werden soll.
- **NodeAutoScalingGroupMaxSize**— Geben Sie die maximale Anzahl von Knoten ein, auf die Ihre Node-Auto-Scaling-Gruppe skalieren kann. Dieser Wert muss mindestens einen Knoten größer sein als Ihre gewünschte Kapazität. Auf diese Weise können Sie eine fortlaufende Aktualisierung Ihrer Knoten durchführen, ohne die Knotenanzahl während der Aktualisierung zu reduzieren.
- **NodeInstanceType**— Wählen Sie den Instance-Typ, den Sie in einem [vorherigen Schritt](#) aufgezeichnet haben. Wählen Sie alternativ einen anderen Instance-Typ für Ihre Knoten aus. Bevor Sie einen anderen Instance-Typ auswählen, lesen [Sie den Artikel Wählen Sie einen optimalen EC2 Amazon-Node-Instance-Typ](#). Jeder EC2 Amazon-Instance-Typ unterstützt eine maximale Anzahl von elastischen Netzwerkschnittstellen (Netzwerkschnittstelle) und jede Netzwerkschnittstelle unterstützt eine maximale Anzahl von IP-Adressen. Da jedem Worker-Knoten und Pod eine eigene IP-Adresse zugewiesen wird, ist es wichtig, einen Instance-Typ zu wählen, der die maximale Anzahl von Pods unterstützt, die Sie auf jedem EC2 Amazon-Knoten ausführen möchten. Eine Liste der Netzwerkschnittstellen und IP-Adressen, die von Instance-Typen unterstützt werden, finden Sie unter [IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ](#). Beispielsweise unterstützt der `m5.large` Instance-Typ maximal 30 IP-Adressen für den Worker-Knoten und die Pods.

 **Note**

Die unterstützten Instance-Typen für die neueste Version des [Amazon VPC CNI-Plugins für Kubernetes](#) sind in [vpc\\_ip\\_resource\\_limit.go](#) auf GitHub aufgeführt. Möglicherweise müssen Sie Ihre Version des Amazon VPC CNI-Plug-ins für Kubernetes aktualisieren, um die neuesten unterstützten Instance-Typen verwenden zu können. Weitere Informationen finden Sie unter [the section called “Amazon VPC CNI”](#).

 **Important**

Einige Instance-Typen sind möglicherweise nicht in allen Regionen verfügbar. AWS

- **NodeImageIdSSMParam**— Der Amazon EC2 Systems Manager Manager-Parameter der AMI-ID, auf die Sie aktualisieren möchten. Der folgende Wert verwendet die neueste für Amazon EKS optimierte AMI-Version für Kubernetes. 1.33

```
/aws/service/eks/optimized-ami/1.33/amazon-linux-2/recommended/image_id
```

Sie können es **1.33** durch eine [unterstützte Kubernetes-Version ersetzen, die identisch](#) ist. Oder er sollte bis zu einer Version älter sein als die Kubernetes-Version, die auf Ihrer Steuerebene läuft. Es wird empfohlen, die Knoten auf der gleichen Version wie die Steuerungsebene zu halten. Sie können es auch **amazon-linux-2** durch einen anderen AMI-Typ ersetzen. Weitere Informationen finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).

 **Note**

Mithilfe des Amazon EC2 Systems Manager Manager-Parameters können Sie Ihre Knoten in future aktualisieren, ohne eine AMI-ID suchen und angeben zu müssen. Wenn Ihr AWS CloudFormation Stack diesen Wert verwendet, startet jedes Stack-Update immer das neueste empfohlene Amazon EKS-optimierte AMI für Ihre angegebene Kubernetes-Version. Dies ist auch dann der Fall, wenn Sie keine Werte in der Vorlage ändern.

- **NodeImageId**— Um Ihr eigenes benutzerdefiniertes AMI zu verwenden, geben Sie die ID ein, die das AMI verwenden soll.

 **Important**

Dieser Wert überschreibt jeden Wert, der für **NodeImageIdSSMParam** angegeben wurde. Wenn Sie den **NodeImageIdSSMParam** Wert verwenden möchten, stellen Sie sicher, dass der Wert für **NodeImageId** leer ist.

- Deaktivieren IMDSv1 — Standardmäßig unterstützt jeder Knoten den Instanz-Metadatendienst Version 1 (IMDSv1) und IMDSv2. Sie können ihn jedoch deaktivieren IMDSv1. Wählen Sie `true` aus, wenn Sie nicht möchten, dass Knoten oder Pods, die in der Knotengruppe geplant sind, verwendet IMDSv1 werden. Weitere Informationen finden Sie unter [Konfiguration des Instance-Metadatenservice](#). Wenn Sie IAM-Rollen für Dienstkonten implementiert haben, weisen Sie allen Pods, die Zugriff auf AWS Dienste benötigen, die erforderlichen Berechtigungen direkt zu. Auf diese Weise benötigen keine Pods in Ihrem Cluster Zugriff auf IMDS aus anderen Gründen, z. B. zum Abrufen der aktuellen Region. AWS Anschließend können Sie den Zugriff auf auch IMDSv2 für Pods deaktivieren, die kein Host-Netzwerk verwenden. Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

10.(Optional) Markieren Sie auf der Seite Options (Optionen) Ihre Stack-Ressourcen. Wählen Sie Weiter aus.

11.Überprüfen Sie Ihre Angaben auf der Seite Review (Überprüfen), bestätigen Sie, dass der Stack IAM-Ressourcen erstellen kann, und klicken Sie dann auf Update stack (Stack aktualisieren).

 Note

Die Aktualisierung jedes Knotens im Cluster dauert mehrere Minuten. Warten Sie, bis die Aktualisierung aller Knoten abgeschlossen ist, bevor Sie die nächsten Schritte durchführen.

12.Wenn es der DNS-Anbieter Ihres Clusters ist `kube-dns`, skalieren Sie die `kube-dns` Bereitstellung auf ein Replikat.

```
kubectl scale deployments/kube-dns --replicas=1 -n kube-system
```

13.(Optional) Wenn Sie den Kubernetes-[Cluster Autoscaler](#) verwenden, skalieren Sie die Bereitstellung zurück auf die gewünschte Zahl von Replikaten.

```
kubectl scale deployments/cluster-autoscaler --replicas=1 -n kube-system
```

14.(Optional) Stellen Sie sicher, dass Sie die neueste Version des [Amazon VPC CNI-Plug-ins für Kubernetes](#) verwenden. Möglicherweise müssen Sie Ihre Version des Amazon VPC CNI-Plug-ins für Kubernetes aktualisieren, um die neuesten unterstützten Instance-Typen verwenden zu können. Weitere Informationen finden Sie unter [the section called "Amazon VPC CNI"](#).

# Vereinfachen Sie das Rechenmanagement mit AWS Fargate

In diesem Thema wird die Verwendung von Amazon EKS zur Ausführung von Kubernetes-Pods auf AWS Fargate erörtert. Fargate ist eine Technologie, die bedarfsgerechte On-Demand-Rechenkapazität für [Container](#) bereitstellt. Mit Fargate müssen Sie Gruppen von virtuellen Maschinen nicht selbst bereitstellen, konfigurieren oder skalieren, um Container auszuführen. Sie müssen auch keine Servertypen auswählen, entscheiden, wann Sie Ihre Knotengruppen skalieren möchten, oder die Clusterpackung optimieren.

[Mit Fargate-Profilen können Sie steuern, welche Pods auf Fargate gestartet werden und wie sie ausgeführt werden.](#) Fargate-Profile werden als Teil Ihres Amazon-EKS-Clusters definiert. Amazon EKS integriert Kubernetes mit Fargate mithilfe von Controllern, die mithilfe des von Kubernetes bereitgestellten AWS , erweiterbaren Upstream-Modells erstellt wurden. Diese Controller werden als Teil der von Amazon EKS verwalteten Kubernetes-Steuerebene ausgeführt und sind für die Planung nativer Kubernetes-Pods auf Fargate verantwortlich. Die Fargate-Controller enthalten einen neuen Scheduler, der neben dem Standard-Kubernetes-Scheduler und zusätzlich zu mehreren mutierenden und validierenden Zugangscontrollern ausgeführt wird. Wenn Sie einen Pod starten, der die Kriterien für die Ausführung auf Fargate erfüllt, erkennen, aktualisieren und planen die Fargate-Controller, die im Cluster ausgeführt werden, den Pod auf Fargate ein.

In diesem Thema werden die verschiedenen Komponenten von Pods beschrieben, die auf Fargate ausgeführt werden, und es werden besondere Überlegungen zur Verwendung von Fargate mit Amazon EKS beschrieben.

## AWS Überlegungen zu Fargate

Hier sind einige Dinge, die Sie bei der Verwendung von Fargate auf Amazon EKS beachten sollten.

- Jeder Pod, der auf Fargate läuft, hat seine eigene Rechengrenze. Sie teilen sich den zugrunde liegenden Kernel, die CPU-Ressourcen, die Speicherressourcen oder die elastic network interface nicht mit einem anderen Pod.
- Network Load Balancers und Application Load Balancers (ALBs) können mit Fargate nur mit IP-Zielen verwendet werden. Weitere Informationen erhalten Sie unter [the section called “Erstellen eines Network Load Balancers”](#) und [the section called “Application Load Balancing”](#).
- Fargate-exponierte Services werden nur im IP-Modus des Zieltyps und nicht im Knoten-IP-Modus ausgeführt. Die empfohlene Möglichkeit, die Konnektivität von einem Service zu überprüfen, der auf einem verwalteten Knoten ausgeführt wird, und einem Service, der auf Fargate ausgeführt wird, besteht darin, eine Verbindung über den Servicennamen herzustellen.

- Pods müssen zu dem Zeitpunkt, zu dem sie auf Fargate laufen sollen, einem Fargate-Profil entsprechen. Pods, die keinem Fargate-Profil entsprechen, bleiben möglicherweise hängen als `Pending`. Wenn ein passendes Fargate-Profil vorhanden ist, können Sie ausstehende Pods, die Sie erstellt haben, löschen, um sie auf Fargate zu verschieben.
- Daemonsets werden auf Fargate nicht unterstützt. Wenn Ihre Anwendung einen Daemon benötigt, konfigurieren Sie diesen Daemon neu, sodass er als Sidecar-Container in Ihren Pods ausgeführt wird.
- Privilegierte Container werden auf Fargate nicht unterstützt.
- Pods, die auf Fargate laufen, können `HostPort` oder nicht `HostNetwork` im Pod-Manifest angeben.
- Das Standard `nofile` - und `nproc` Soft-Limit ist 1024 und das Hard-Limit ist 65535 für Fargate Pods.
- GPUs sind derzeit nicht auf Fargate verfügbar.
- Pods, die auf Fargate ausgeführt werden, werden nur in privaten Subnetzen unterstützt (mit NAT-Gateway-Zugriff auf AWS Dienste, aber nicht mit direkter Route zu einem Internet Gateway). Daher muss die VPC Ihres Clusters über private Subnetze verfügen. Weitere Informationen zu Clustern ohne ausgehenden Internetzugang finden Sie unter [the section called “Private Cluster”](#).
- Sie können die Option [Pod-Ressourcen anpassen mit Vertical Pod Autoscaler](#) verwenden, um die anfängliche korrekte CPU- und Speichergröße für Ihre Fargate-Pods festzulegen, und dann die [Skalierungs-Pod-Bereitstellungen mit Horizontalem Pod-Autoscaler verwenden, um diese Pods](#) zu skalieren. Wenn Sie möchten, dass der Vertical Pod Autoscaler Pods mit größeren CPU- und Speicherkombinationen automatisch erneut auf Fargate bereitstellt, stellen Sie den Modus für den Vertical Pod Autoscaler entweder Auto auf oder ein, um die korrekte Funktionalität sicherzustellen. Recreate Weitere Informationen finden Sie in der [Vertical Pod Autoscaler](#)-Dokumentation auf GitHub.
- DNS-Auflösung und DNS-Hostnamen müssen für Ihre VPC aktiviert sein. Weitere Informationen finden Sie unter [Anzeigen und Aktualisieren der DNS-Unterstützung für Ihre VPC](#).
- Amazon EKS Fargate bietet zusätzliche Funktionen defense-in-depth für Kubernetes-Anwendungen, indem jeder Pod innerhalb einer virtuellen Maschine (VM) isoliert wird. Diese VM-Grenze verhindert den Zugriff auf hostbasierte Ressourcen, die von anderen Pods im Falle eines Container-Escapes verwendet werden. Dies ist eine übliche Methode, um containerisierte Anwendungen anzugreifen und Zugriff auf Ressourcen außerhalb des Containers zu erhalten.

Die Verwendung von Amazon EKS ändert nichts an Ihren Verantwortlichkeiten im Rahmen des [Modells der gemeinsamen Verantwortung](#). Sie sollten die Konfiguration von Cluster-Sicherheits-



und Governance-Kontrollen sorgfältig prüfen. Der sicherste Weg, eine Anwendung zu isolieren, besteht immer darin, sie in einem separaten Cluster auszuführen.

- Fargate-Profile unterstützen die Angabe von Subnetzen aus sekundären VPC-CIDR-Blöcken. Möglicherweise möchten Sie einen sekundären CIDR-Block angeben. Dies liegt daran, dass in einem Subnetz nur eine begrenzte Anzahl von IP-Adressen verfügbar ist. Aus diesem Grund gibt es auch eine begrenzte Anzahl von Pods, die im Cluster erstellt werden können. Durch die Verwendung verschiedener Subnetze für Pods können Sie die Anzahl der verfügbaren IP-Adressen erhöhen. Weitere Informationen finden Sie unter [Hinzufügen von IPv4 CIDR-Blöcken zu einer VPC](#).
- Der Amazon EC2 Instance Metadata Service (IMDS) ist nicht für Pods verfügbar, die auf Fargate-Knoten bereitgestellt werden. Wenn Sie Pods haben, die in Fargate bereitgestellt sind und IAM-Anmeldeinformationen benötigen, weisen Sie sie Ihren Pods mithilfe von [IAM-Rollen für Dienstkonten](#) zu. Wenn Ihre Pods Zugriff auf andere Informationen benötigen, die über IMDS verfügbar sind, müssen Sie diese Informationen in Ihrer Pod-Spezifikation fest codieren. Dazu gehört die AWS Region oder Availability Zone, in der ein Pod bereitgestellt wird.
- Du kannst Fargate-Pods nicht in AWS Outposts, AWS Wellenlängenzonen oder AWS Local Zones einsetzen.
- Amazon EKS muss Fargate Pods regelmäßig patchen, um sie zu schützen. Wir versuchen, die Updates so durchzuführen, dass die Auswirkungen reduziert werden, aber manchmal müssen Pods gelöscht werden, wenn sie nicht erfolgreich entfernt wurden. Es gibt einige Maßnahmen, die Sie durchführen können, um Unterbrechungen zu minimieren. Weitere Informationen finden Sie unter [the section called “Betriebssystem-Patch-Ereignisse”](#).
- Das [Amazon-VPC-CNI-Plugin für Amazon EKS](#) ist standardmäßig auf Fargate-Knoten installiert. Sie können keine [alternativen CNI-Plug-ins für Amazon EKS-Cluster](#) mit Fargate-Knoten verwenden.
- Ein Pod, der auf Fargate läuft, mountet automatisch ein Amazon EFS-Dateisystem, ohne dass manuelle Schritte zur Treiberinstallation erforderlich sind. Sie können kein dynamisches persistentes Volume Provisioning mit Fargate-Knoten verwenden, aber Sie können statische Bereitstellung verwenden.
- Amazon EKS unterstützt Fargate Spot nicht.
- Sie können Amazon EBS-Volumes nicht auf Fargate Pods mounten.
- Sie können den Amazon EBS CSI-Controller auf Fargate-Knoten ausführen, aber der Amazon EBS CSI-Knoten DaemonSet kann nur auf Amazon-Instances ausgeführt werden. EC2
- Nachdem ein [Kubernetes-Job](#) markiert wurde Completed oder Failed, existieren die Pods, die der Job erstellt, normalerweise weiter. Dieses Verhalten ermöglicht es Ihnen, Ihre Logs und

Ergebnisse einzusehen, aber mit Fargate werden Ihnen Kosten entstehen, wenn Sie den Job danach nicht bereinigen.

Um die zugehörigen Pods automatisch zu löschen, nachdem ein Job abgeschlossen wurde oder fehlschlägt, können Sie mithilfe des time-to-live (TTL-) Controllers einen Zeitraum angeben. Das folgende Beispiel zeigt die Angabe `.spec.ttlSecondsAfterFinished` in Ihrem Job-Manifest.

```
apiVersion: batch/v1
kind: Job
metadata:
 name: busybox
spec:
 template:
 spec:
 containers:
 - name: busybox
 image: busybox
 command: ["/bin/sh", "-c", "sleep 10"]
 restartPolicy: Never
 ttlSecondsAfterFinished: 60 # <-- TTL controller
```

## Fargate-Vergleichstabelle

| Kriterien                                                           | AWS Fargate |
|---------------------------------------------------------------------|-------------|
| Kann in <a href="#">AWS Outposts</a> eingesetzt werden              | Nein        |
| Kann auf eine <a href="#">AWS Lokale Zone</a> bereitgestellt werden | Nein        |
| Kann Container ausführen, die Windows benötigen                     | Nein        |
| Kann Container ausführen, die Linux benötigen                       | Ja          |
| Kann Workloads ausführen, die den Inferentia-Chip benötigen         | Nein        |

| Kriterien                                                                                                                          | AWS Fargate                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Kann Workloads ausführen, die eine GPU benötigen                                                                                   | Nein                                                                                                                                          |
| Kann Workloads ausführen, die Arm-Prozessoren benötigen                                                                            | Nein                                                                                                                                          |
| Kann ausgeführt werden AWS <a href="#">Bottlerocket</a>                                                                            | Nein                                                                                                                                          |
| Pods teilen sich eine Kernel-Laufzeitumgebung mit anderen Pods                                                                     | Nein — Jeder Pod hat einen eigenen Kernel                                                                                                     |
| Pods teilen sich CPU-, Arbeitsspeicher-, Speicher- und Netzwerkressourcen mit anderen Pods.                                        | Nein — Jeder Pod verfügt über eigene Ressourcen und kann unabhängig voneinander dimensioniert werden, um die Ressourcennutzung zu maximieren. |
| Pods können mehr Hardware und Speicher verwenden als in den Pod-Spezifikationen angegeben                                          | Nein — Der Pod kann jedoch mit einer größeren vCPU- und Speicherkonfiguration erneut bereitgestellt werden.                                   |
| EC2 Amazon-Instances müssen bereitgestellt und verwaltet werden                                                                    | Nein                                                                                                                                          |
| Muss das Betriebssystem von EC2 Amazon-Instances sichern, warten und patchen                                                       | Nein                                                                                                                                          |
| Kann bei der Bereitstellung eines Knotens Bootstrap-Argumente bereitstellen, z. B. zusätzliche <a href="#">Kubelet-Argumente</a> . | Nein                                                                                                                                          |
| Kann Pods IP-Adressen aus einem anderen CIDR-Block als der dem Knoten zugewiesenen IP-Adresse zuweisen.                            | Nein                                                                                                                                          |
| SSH im Knoten nicht möglich                                                                                                        | Nein — Es gibt kein Node-Host-Betriebssystem, mit dem SSH verbunden werden kann.                                                              |

| Kriterien                                                          | AWS Fargate                                                                |
|--------------------------------------------------------------------|----------------------------------------------------------------------------|
| Kann Ihr eigenes benutzerdefiniertes AMI auf Knoten bereitstellen  | Nein                                                                       |
| Kann Ihr eigenes benutzerdefiniertes CNI auf Knoten bereitstellen  | Nein                                                                       |
| Knoten-AMI muss selbst aktualisiert werden                         | Nein                                                                       |
| Muss die Kubernetes-Version des Knotens selbst aktualisieren       | Nein — Sie verwalten keine Knoten.                                         |
| Kann Amazon EBS-Speicher mit Pods verwenden                        | Nein                                                                       |
| Kann Amazon EFS-Speicher mit Pods verwenden                        | <a href="#">Ja</a>                                                         |
| Kann Amazon FSx für die Aufbewahrung von Lustre mit Pods verwenden | Nein                                                                       |
| Kann Network Load Balancer für Services verwenden                  | Ja, wenn Sie den <a href="#">Netzwerk-Loadbalancer erstellen</a> verwenden |
| Pods können in einem öffentlichen Subnetz ausgeführt werden        | Nein                                                                       |
| Kann einzelnen Pods verschiedene VPC-Sicherheitsgruppen zuweisen   | Ja                                                                         |
| Kann Kubernetes ausführen DaemonSets                               | Nein                                                                       |
| Support HostPort und HostNetwork im Pod-Manifest                   | Nein                                                                       |
| AWS Verfügbarkeit in der Region                                    | <a href="#">Einige von Amazon EKS unterstützte Regionen</a>                |
| Kann Container auf Amazon EC2 Dedicated Hosts ausführen            | Nein                                                                       |

| Kriterien | AWS Fargate                                                                                                                                                                                 |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preise    | Kosten für eine individuelle Fargate-Speicher- und CPU-Konfiguration. Jeder Pod hat seine eigenen Kosten. Weitere Informationen dazu finden Sie unter <a href="#">AWS -Fargate-Preise</a> . |

## Beginnen Sie mit AWS Fargate für Ihren Cluster

In diesem Thema werden die ersten Schritte zum Ausführen von Pods auf AWS Fargate mit Ihrem Amazon EKS-Cluster beschrieben.

Wenn Sie den Zugriff auf den öffentlichen Endpunkt Ihres Clusters mithilfe von CIDR-Blöcken einschränken, empfehlen wir, dass Sie auch den privaten Endpunktzugriff aktivieren. Auf diese Weise können Fargate Pods mit dem Cluster kommunizieren. Wenn der private Endpunkt nicht aktiviert ist, müssen die CIDR-Blöcke, die Sie für den öffentlichen Zugriff angeben, die Ausgangsquellen aus Ihrer VPC enthalten. Weitere Informationen finden Sie unter [the section called “Cluster-Endpunktzugriff”](#).

### Voraussetzung

Einen vorhandenen -Cluster. Wenn Sie noch keinen Amazon EKS-Cluster haben, finden Sie weitere Informationen unter [Erste Schritte](#).

## Schritt 1: Stellen Sie sicher, dass bestehende Knoten mit Fargate Pods kommunizieren können

Wenn Sie mit einem neuen Cluster ohne Knoten oder mit einem Cluster mit nur verwalteten Knotengruppen (siehe [the section called “Verwaltete Knotengruppen”](#)) arbeiten, können Sie zu [the section called “Schritt 2: Erstellen Sie eine Fargate Pod-Ausführungsrolle”](#) wechseln.

Gehen Sie davon aus, dass Sie mit einem vorhandenen Cluster arbeiten, dem bereits Knoten zugeordnet sind. Stellen Sie sicher, dass Pods auf diesen Knoten ungehindert mit den Pods kommunizieren können, die auf Fargate laufen. Pods, die auf Fargate ausgeführt werden, werden automatisch so konfiguriert, dass sie die Cluster-Sicherheitsgruppe für den Cluster verwenden, dem sie zugeordnet sind. Stellen Sie sicher, dass alle vorhandenen Knoten in Ihrem Cluster Datenverkehr an die Cluster-Sicherheitsgruppe senden und von dieser empfangen können. Verwaltete Knotengruppen werden automatisch so konfiguriert, dass sie auch die Cluster-

Sicherheitsgruppe verwenden, sodass Sie sie nicht ändern oder auf ihre Kompatibilität überprüfen müssen (siehe [the section called “Verwaltete Knotengruppen”](#)).

Für bestehende Knotengruppen, die mit `eksctl` oder den von Amazon EKS verwalteten AWS CloudFormation Vorlagen erstellt wurden, können Sie die Cluster-Sicherheitsgruppe manuell zu den Knoten hinzufügen. Alternativ können Sie die Auto-Scaling-Gruppstartvorlage für die Knotengruppe ändern, um die Cluster-Sicherheitsgruppe an die Instances anzuhängen. Weitere Informationen finden Sie unter [Ändern der Sicherheitsgruppen einer Instance](#) im Amazon VPC-Benutzerhandbuch.

Sie können im Abschnitt Netzwerk für den Cluster AWS Management Console nach einer Sicherheitsgruppe für Ihren Cluster suchen. Oder Sie können dies mit dem folgenden AWS CLI-Befehl tun. Wenn Sie diesen Befehl verwenden, ersetzen Sie `<my-cluster>` durch den Namen Ihres Clusters.

```
aws eks describe-cluster --name <my-cluster> --query
cluster.resourcesVpcConfig.clusterSecurityGroupId
```

## Schritt 2: Erstellen Sie eine Fargate Pod-Ausführungsrolle

Wenn Ihr Cluster Pods auf AWS Fargate erstellt, müssen die Komponenten, die auf der Fargate-Infrastruktur ausgeführt werden, in AWS APIs Ihrem Namen Aufrufe tätigen. Die Amazon EKS Pod-Ausführungsrolle stellt die IAM-Berechtigungen dafür bereit. Informationen zum Erstellen einer AWS Fargate-Pod-Ausführungsrolle finden Sie unter [the section called “IAM-Rolle zur Pod-Ausführung”](#).

### Note

Wenn Sie Ihren Cluster `eksctl` mit dieser `--fargate` Option erstellt haben, verfügt Ihr Cluster bereits über eine Pod-Ausführungsrolle, die Sie in der IAM-Konsole mit dem Muster finden. `eksctl-my-cluster-FargatePodExecutionRole-ABCDEFGHIJKL` Ebenso wird, wenn Sie `eksctl` Ihre Fargate-Profil erstellen, Ihre Pod-Ausführungsrolle `eksctl` erstellt, sofern noch keine erstellt wurde.

## Schritt 3: Erstellen Sie ein Fargate-Profil für Ihren Cluster

Bevor Sie Pods planen können, die auf Fargate in Ihrem Cluster ausgeführt werden, müssen Sie ein Fargate-Profil definieren, das festlegt, welche Pods Fargate verwenden, wenn sie gestartet werden. Weitere Informationen finden Sie unter [the section called “Definieren Sie Profile”](#).

 Note

Wenn Sie Ihren Cluster `eksctl` mithilfe der `--fargate` Option erstellt haben, wurde bereits ein Fargate-Profil für Ihren Cluster mit Selektoren für alle Pods in den Namespaces `kube-system` und `default` erstellt. Gehen Sie wie folgt vor, um Fargate-Profile für alle anderen Namespaces zu erstellen, die Sie mit Fargate verwenden möchten.

Sie können ein Fargate-Profil mit einem der folgenden Tools erstellen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

## eksctl

Für diesen Vorgang ist `eksctl` Version `0.210.0` oder höher erforderlich. Sie können Ihre -Version mit dem folgenden Befehl überprüfen:

```
eksctl version
```

Eine Installations- und Upgrade-Anleitung für `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).

Um ein Fargate-Profil zu erstellen mit **eksctl**

Erstellen Sie Ihr Fargate-Profil mit dem folgenden `eksctl`-Befehl und ersetzen Sie jede `<example value>` durch Ihre eigenen Werte. Sie müssen einen Namespace angeben. Die `--labels` Option ist jedoch nicht erforderlich.

```
eksctl create fargateprofile \
 --cluster <my-cluster> \
 --name <my-fargate-profile> \
 --namespace <my-kubernetes-namespace> \
 --labels <key=value>
```

Sie können bestimmte Platzhalter für `<my-kubernetes-namespace>`- und `<key=value>`-Labels verwenden. Weitere Informationen finden Sie unter [the section called “Fargate-Profil-Platzhalter”](#).

## AWS Management Console

Um ein Fargate-Profil zu erstellen mit AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Cluster aus, für den Sie ein Fargate-Profil erstellen möchten.
3. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
4. Wählen Sie unter Fargate-Profile die Option Fargate-Profil hinzufügen aus.
5. Auf der Seite Konfigurieren des Fargate Profils führen Sie folgende Schritte aus:
  - a. Geben Sie unter Name einen Namen für Ihr Fargate-Profil ein. Der Name muss eindeutig sein.
  - b. Wählen Sie für die Pod-Ausführungsrolle die Pod-Ausführungsrolle aus, die Sie mit Ihrem Fargate-Profil verwenden möchten. Es werden nur IAM-Rollen mit dem `eks-fargate-pods.amazonaws.com`-Service-Prinzipal angezeigt. Wenn keine Rollen aufgeführt sind, müssen Sie eine erstellen. Weitere Informationen finden Sie unter [the section called "IAM-Rolle zur Pod-Ausführung"](#).
  - c. Ändern Sie die ausgewählten Subnetze nach Bedarf.

### Note

Für Pods, die auf Fargate laufen, werden nur private Subnetze unterstützt.

- d. Für Tags können Sie Ihr Fargate-Profil wahlweise markieren. Diese Tags werden nicht auf andere Ressourcen übertragen, die dem Profil zugeordnet sind, z. B. Pods.
  - e. Wählen Sie Weiter aus.
6. Gehen Sie auf der Auswahlseite „Pod konfigurieren“ wie folgt vor:
- a. Geben Sie für Namespace einen Namespace ein, der mit Pods übereinstimmt.
    - Sie können bestimmte Namespaces für den Abgleich verwenden, z. B. `kube-system` oder `default`.
    - Sie können bestimmte Platzhalter verwenden (z. B. `prod-*`), um mehrere Namespaces abzugleichen (z. B. `prod-deployment` und `prod-test`). Weitere Informationen finden Sie unter [the section called "Fargate-Profil-Platzhalter"](#).
  - b. (Optional) Fügen Sie dem Selektor Kubernetes-Markierungen hinzu. Fügen Sie sie ausdrücklich dem Namen hinzu, dem die Pods im angegebenen Namespace entsprechen müssen.



- Sie können das Label `infrastructure: fargate` zum Selektor hinzufügen, sodass nur Pods im angegebenen Namespace, die auch das `infrastructure: fargate` Kubernetes-Label haben, mit dem Selektor übereinstimmen.
- Sie können bestimmte Platzhalter verwenden (z. B. `key?: value?`), um mehrere Namespaces abzugleichen (z. B. `keya: valuea` und `keyb: valueb`). Weitere Informationen finden Sie unter [the section called “Fargate-Profil-Platzhalter”](#).

c. Wählen Sie Weiter aus.

7. Überprüfen Sie auf der Seite Überprüfen und erstellen die Informationen für Ihr -Profil und wählen Sie Erstellen aus.

## Schritt 4: CoreDNS aktualisieren

Standardmäßig ist CoreDNS so konfiguriert, dass es auf der EC2 Amazon-Infrastruktur auf Amazon EKS-Clustern ausgeführt wird. Wenn Sie Ihre Pods nur auf Fargate in Ihrem Cluster ausführen möchten, führen Sie die folgenden Schritte aus.

### Note

Wenn Sie einen Cluster mit `eksctl` unter Verwendung von `--fargate`-Option erstellt haben, können Sie zu [the section called “Nächste Schritte”](#) springen.

1. Erstellen Sie mit dem folgenden Befehl ein Fargate-Profil für CoreDNS. `<my-cluster>` Ersetzen Sie es durch Ihren Clusternamen, `<111122223333>` durch Ihre Konto-ID, `<AmazonEKSFargatePodExecutionRole>` durch den Namen Ihrer Pod-Ausführungsrolle und `<0000000000000000a>`, `<0000000000000000b>`, und `<0000000000000000c>` durch die IDs Ihrer privaten Subnetze. Wenn Sie keine Pod-Ausführungsrolle haben, müssen Sie zuerst eine erstellen (siehe [the section called “Schritt 2: Erstellen Sie eine Fargate Pod-Ausführungsrolle”](#)).

### Important

Der Rollen-ARN darf keinen anderen [Pfad](#) als enthalten/. Wenn der Name Ihrer Rolle also beispielsweise `development/apps/AmazonEKSFargatePodExecutionRole` lautet, müssen Sie ihn beim Angeben des ARN für die Rolle in `AmazonEKSFargatePodExecutionRole` ändern. Das

Format des Rollen-ARN muss `arn:aws: iam::<111122223333>:role/<AmazonEKSFargatePodExecutionRole>` sein.

```
aws eks create-fargate-profile \
 --fargate-profile-name coredns \
 --cluster-name <my-cluster> \
 --pod-execution-role-arn arn:aws: iam::<111122223333>:role/
<AmazonEKSFargatePodExecutionRole> \
 --selectors namespace=kube-system,labels={k8s-app=kube-dns} \
 --subnets subnet-<0000000000000000a> subnet-<0000000000000000b> subnet-
<0000000000000000c>
```

2. Löst einen Rollout der coredns Bereitstellung aus.

```
kubectl rollout restart -n kube-system deployment coredns
```

## Nächste Schritte

- Mit dem folgenden Workflow können Sie mit der Migration Ihrer vorhandenen Anwendungen zum Ausführen in Fargate beginnen.
  - a. [the section called “Erstellen eines Fargate-Profiles”](#) das dem Kubernetes-Namespace und den Kubernetes-Labels Ihrer Anwendung entspricht.
  - b. Löschen Sie alle vorhandenen Pods und erstellen Sie sie neu, sodass sie auf Fargate geplant sind. Ändern Sie die `<namespace>` und `<deployment-type>`, um Ihre spezifischen Pods zu aktualisieren.

```
kubectl rollout restart -n <namespace> deployment <deployment-type>
```

- Stellen Sie das bereit[the section called “Application Load Balancing”](#), um Ingress-Objekte für Ihre Pods zuzulassen, die auf Fargate ausgeführt werden.
- Sie können den verwenden[the section called “Vertical Pod Autoscaler”](#), um die anfängliche korrekte CPU- und Speichergröße für Ihre Fargate-Pods festzulegen und dann diese Pods [the section called “Horizontal Pod Autoscaler”](#) zu skalieren. Wenn Sie möchten, dass der Vertical Pod Autoscaler Pods mit höheren CPU- und Speicherkombinationen automatisch erneut auf Fargate bereitstellt, stellen Sie den Modus des Vertical Pod Autoscalers entweder auf oder ein. Auto

Recreate Dies dient der Gewährleistung einer korrekten Funktion. Weitere Informationen finden Sie in der [Vertical Pod Autoscaler](#)-Dokumentation auf GitHub.

- Sie können den [AWS Distro für OpenTelemetry](#)(ADOT)-Kollektor zur Anwendungsüberwachung durch Befolgen [dieser Anweisungen](#) einrichten.

## Definieren Sie, welche Pods AWS Fargate beim Start verwenden

Bevor Sie Pods auf Fargate in Ihrem Cluster planen, müssen Sie mindestens ein Fargate-Profil definieren, das angibt, welche Pods Fargate beim Start verwenden.

Als Administrator können Sie ein Fargate-Profil verwenden, um zu deklarieren, welche Pods auf Fargate ausgeführt werden. Sie können dies über die Selektoren des Profils tun. Sie können bis zu fünf Selektoren zu jedem Profil hinzufügen. Jeder Selektor muss einen Namespace enthalten. Der Selector kann auch Labels enthalten. Das Label-Feld besteht aus mehreren optionalen Schlüssel-Wert-Paaren. Pods, die den Selektoren entsprechen, werden auf Fargate geplant. Pods werden mit einem Namespace und den Labels abgeglichen, die im Selektor angegeben sind. Wenn ein Namespace-Selektor ohne Labels definiert ist, versucht Amazon EKS, mithilfe des Profils alle Pods, die in diesem Namespace ausgeführt werden, auf Fargate einzuplanen. Wenn ein to-be-scheduled Pod mit einem der Selektoren im Fargate-Profil übereinstimmt, ist dieser Pod auf Fargate geplant.

Wenn ein Pod mit mehreren Fargate-Profilen übereinstimmt, können Sie angeben, welches Profil ein Pod verwendet, indem Sie der Pod-Spezifikation das folgende Kubernetes-Label hinzufügen: `eks.amazonaws.com/fargate-profile: my-fargate-profile` Der Pod muss mit einem Selektor in diesem Profil übereinstimmen, damit er für Fargate geplant werden kann. Kubernetes-Affinitäts-/Anti-Affinitätsregeln gelten nicht und sind für Amazon EKS Fargate Pods auch nicht erforderlich.

Wenn Sie ein Fargate-Profil erstellen, müssen Sie eine Pod-Ausführungsrolle angeben. Diese Ausführungsrolle ist für die Amazon-EKS-Komponenten vorgesehen, die auf der Fargate-Infrastruktur mit dem Profil ausgeführt werden. Sie wird zur Autorisierung zur Kubernetes [Role Based Access Control](#) (RBAC) des Clusters hinzugefügt. Auf diese Weise kann sich `kubelet`, das in der Fargate-Infrastruktur ausgeführt wird, bei Ihrem Amazon-EKS-Cluster registrieren und als Knoten in Ihrem Cluster angezeigt werden. Die Pod-Ausführungsrolle bietet auch IAM-Berechtigungen für die Fargate-Infrastruktur, um Lesezugriff auf Amazon ECR-Image-Repositorys zu ermöglichen. Weitere Informationen finden Sie unter [the section called "IAM-Rolle zur Pod-Ausführung"](#).

Fargate-Profile können nicht geändert werden. Sie können jedoch ein neues aktuelles Profil erstellen, um ein vorhandenes Profil zu ersetzen, und dann das Original löschen.

 Note

Alle Pods, die ein Fargate-Profil verwenden, werden gestoppt und in den Status „Ausstehend“ versetzt, wenn das Profil gelöscht wird.

Wenn Fargate-Profile in einem Cluster den Status DELETING haben, müssen Sie warten, bis dieses Fargate-Profil gelöscht wurde, bevor Sie andere Profile in diesem Cluster erstellen können.

 Note

Fargate unterstützt [topologySpreadConstraints](#) Kubernetes derzeit nicht.

Amazon EKS und Fargate verteilen Pods auf jedes der Subnetze, die im Fargate-Profil definiert sind. Es kann jedoch zu einer ungleichmäßigen Verteilung kommen. Wenn Sie eine gleichmäßige Verteilung benötigen, verwenden Sie zwei Fargate-Profile. Eine gleichmäßige Verteilung ist wichtig in Szenarien, in denen Sie zwei Replikate bereitstellen möchten und keine Ausfallzeiten wünschen. Wir empfehlen, dass jedes Profil nur ein Subnetz hat.

## Fargate-Profilkomponenten

Die folgenden Komponenten sind in einem Fargate-Profil enthalten.

### Pod-Ausführungsrolle

Wenn Ihr Cluster Pods auf AWS Fargate erstellt, müssen die, `kubelet` die auf der Fargate-Infrastruktur ausgeführt werden, in AWS APIs Ihrem Namen Anrufe tätigen. Beispielsweise muss er Aufrufe tätigen, um Container-Images aus Amazon ECR zu ziehen. Die Amazon EKS Pod-Ausführungsrolle stellt die IAM-Berechtigungen dafür bereit.

Wenn Sie ein Fargate-Profil erstellen, müssen Sie eine Pod-Ausführungsrolle angeben, die mit Ihren Pods verwendet werden soll. Diese Rolle wird zur Autorisierung der [rollenbasierten Zugriffskontrolle \(RBAC\)](#) von Kubernetes des Clusters hinzugefügt. Auf diese Weise kann sich `kubelet` das, was auf der Fargate-Infrastruktur läuft, bei Ihrem Amazon EKS-Cluster registrieren und in Ihrem Cluster als Knoten erscheinen. Weitere Informationen finden Sie unter [the section called "IAM-Rolle zur Pod-Ausführung"](#).

## Subnets

Die IDs Subnetze, in denen Pods gestartet werden sollen, verwenden dieses Profil. Derzeit werden Pods, die auf Fargate ausgeführt werden, keine öffentlichen IP-Adressen zugewiesen. Daher werden für diesen Parameter nur private Subnetze ohne direkte Route zu einem Internet-Gateway akzeptiert.

## Selektoren

Die Selektoren, die den Pods zugeordnet werden müssen, um dieses Fargate-Profil zu verwenden. Sie können bis zu fünf Selektoren in einem Fargate-Profil angeben. Die Selektoren bestehen aus folgenden Komponenten:

- **Namespace** – Sie müssen einen Namespace für einen Selektor angeben. Der Selektor entspricht nur Pods, die in diesem Namespace erstellt wurden. Sie können jedoch mehrere Selektoren erstellen, um mehrere Namespaces zu adressieren.
- **Bezeichnungen** – Sie können optional Kubernetes-Bezeichnungen angeben, mit denen der Selektor übereinstimmen muss. Der Selektor entspricht nur Pods, die alle im Selektor angegebenen Labels haben.

## Fargate-Profil-Platzhalter

Zusätzlich zu den von Kubernetes zugelassenen Zeichen dürfen Sie \* und ? in den Auswahlkriterien für Namespaces, Label Schlüssel und Labelwerte verwenden:

- \* steht für kein, ein oder mehrere Zeichen. Zum Beispiel kann `prod*` `prod` und `prod-metrics` darstellen.
- ? steht für ein einzelnes Zeichen (z. B. kann `value?` `valuea` darstellen). Es kann jedoch nicht `value` und `value-a` darstellen, weil ? nur genau ein Zeichen darstellen kann.

Diese Platzhalterzeichen können an jeder Position und in Kombination verwendet werden (z. B. `prod*`, `*dev` und `frontend*?`). Andere Platzhalter und Formen des Mustervergleichs, wie reguläre Ausdrücke, werden nicht unterstützt.

Wenn es in der Pod-Spezifikation mehrere übereinstimmende Profile für den Namespace und die Labels gibt, wählt Fargate das Profil anhand der alphanumerischen Sortierung nach dem Profilnamen aus. Wenn beispielsweise sowohl Profil A (mit dem Namen `beta-workload`) als auch Profil B (mit dem Namen `prod-workload`) übereinstimmende Selektoren für die zu startenden Pods haben,

wählt Fargate Profil A (beta-workload) für die Pods aus. Die Pods haben Beschriftungen mit dem Profil A auf den Pods (z. B. `eks.amazonaws.com/fargate-profile=beta-workload`).

Wenn Sie bestehende Fargate-Pods auf neue Profile migrieren möchten, die Platzhalter verwenden, gibt es zwei Möglichkeiten:

- Erstellen Sie ein neues Profil mit passenden Selektoren und löschen Sie dann die alten Profile. Mit alten Profilen gekennzeichnete Pods werden in neue übereinstimmende Profile verschoben.
- Wenn Sie Workloads migrieren möchten, sich aber nicht sicher sind, welche Fargate-Labels sich auf jedem Fargate-Pod befinden, können Sie die folgende Methode verwenden. Erstellen Sie ein neues Profil mit einem Namen, das zuerst alphanumerisch unter den Profilen auf demselben Cluster sortiert. Recyceln Sie anschließend die Fargate-Pods, die auf neue Profile migriert werden müssen.

## Erstellen eines Fargate-Profiles

In diesem Abschnitt wird beschrieben, wie Sie ein Fargate-Profil erstellen. Sie müssen außerdem eine Pod-Ausführungsrolle erstellt haben, die Sie für Ihr Fargate-Profil verwenden können. Weitere Informationen finden Sie unter [the section called “IAM-Rolle zur Pod-Ausführung”](#). Pods, die auf Fargate laufen, werden nur in privaten Subnetzen mit [NAT-Gateway-Zugriff](#) auf AWS Dienste unterstützt, nicht jedoch in einer direkten Route zu einem Internet Gateway. Aus diesem Grund muss die VPC Ihres Clusters über private Subnetze verfügen.

Sie können ein Profil mit den folgenden Angaben erstellen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

## eksctl

Um ein Fargate-Profil zu erstellen mit **eksctl**

Erstellen Sie Ihr Fargate-Profil mit dem folgenden `eksctl` Befehl und ersetzen Sie dabei jeden Beispielwert durch Ihre eigenen Werte. Sie müssen einen Namespace angeben. Die `--labels` Option ist jedoch nicht erforderlich.

```
eksctl create fargateprofile \
 --cluster my-cluster \
 --profile-name beta-workload
```

```
--name my-fargate-profile \
--namespace my-kubernetes-namespace \
--labels key=value
```

Sie können bestimmte Platzhalter für my-kubernetes-namespace- und key=value-Labels verwenden. Weitere Informationen finden Sie unter [the section called “Fargate-Profil-Platzhalter”](#).

## AWS Management Console

Um ein Fargate-Profil zu erstellen mit AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Cluster aus, für den Sie ein Fargate-Profil erstellen möchten.
3. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
4. Wählen Sie unter Fargate-Profile die Option Fargate-Profil hinzufügen aus.
5. Auf der Seite Konfigurieren des Fargate Profils führen Sie folgende Schritte aus:
  - a. Geben Sie unter Name einen eindeutigen Namen für Ihr Fargate-Profil ein, wie z. B. my-profile.
  - b. Wählen Sie für die Pod-Ausführungsrolle die Pod-Ausführungsrolle aus, die Sie mit Ihrem Fargate-Profil verwenden möchten. Es werden nur IAM-Rollen mit dem eks-fargate-pods.amazonaws.com-Service-Prinzipal angezeigt. Wenn keine Rollen aufgeführt sind, müssen Sie eine erstellen. Weitere Informationen finden Sie unter [the section called “IAM-Rolle zur Pod-Ausführung”](#).
  - c. Ändern Sie die ausgewählten Subnetze nach Bedarf.

### Note

Für Pods, die auf Fargate laufen, werden nur private Subnetze unterstützt.

- d. Für Tags können Sie Ihr Fargate-Profil wahlweise markieren. Diese Tags werden nicht auf andere Ressourcen übertragen, die mit dem Profil verknüpft sind, wie z. B. Pods.
  - e. Wählen Sie Weiter.
6. Gehen Sie auf der Auswahlseite „Pod konfigurieren“ wie folgt vor:
    - a. Geben Sie für Namespace einen Namespace ein, der mit Pods übereinstimmt.
      - Sie können bestimmte Namespaces für den Abgleich verwenden, z. B. kube-system oder default.

- Sie können bestimmte Platzhalter verwenden (z. B. prod- \*), um mehrere Namespaces abzugleichen (z. B. prod-deployment und prod-test). Weitere Informationen finden Sie unter [the section called “Fargate-Profil-Platzhalter”](#).
- b. (Optional) Fügen Sie dem Selektor Kubernetes-Markierungen hinzu. Fügen Sie sie insbesondere dem Namen hinzu, dem die Pods im angegebenen Namespace entsprechen müssen.
- Sie können das Label dem Selektor hinzufügen `infrastructure: fargate`, sodass nur Pods im angegebenen Namespace, die auch das `infrastructure: fargate` Kubernetes-Label haben, mit dem Selektor übereinstimmen.
  - Sie können bestimmte Platzhalter verwenden (z. B. key?: value?), um mehrere Namespaces abzugleichen (z. B. keya: valuea und keyb: valueb). Weitere Informationen finden Sie unter [the section called “Fargate-Profil-Platzhalter”](#).
- c. Wählen Sie Weiter.
7. Überprüfen Sie auf der Seite Überprüfen und erstellen die Informationen für Ihr -Profil und wählen Sie Erstellen aus.

## Ein Fargate-Profil löschen

In diesem Thema wird beschrieben, wie Sie ein Fargate-Profil löschen. Wenn Sie ein Fargate-Profil löschen, werden alle Pods gelöscht, die mit dem Profil für Fargate geplant waren. Wenn diese Pods mit einem anderen Fargate-Profil übereinstimmen, sind sie auf Fargate mit diesem Profil geplant. Wenn sie keinen Fargate-Profilen mehr entsprechen, sind sie nicht für Fargate geplant und bleiben möglicherweise weiterhin ausstehend.

Nur ein Fargate-Profil in einem Cluster kann sich jeweils im DELETING-Status befinden. Warten Sie, bis das Löschen eines Fargate-Profiles abgeschlossen ist, bevor Sie andere Profile in diesem Cluster löschen können.

Sie können ein Profil mit einem der folgenden Tools löschen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)
- [the section called “AWS CLI”](#)



## eksctl

Löschen Sie ein Fargate-Profil mit **eksctl**

Verwenden Sie den folgenden Befehl, um ein Profil aus einem Cluster zu löschen. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
eksctl delete fargateprofile --name my-profile --cluster my-cluster
```

## AWS Management Console

Löschen Sie ein Fargate-Profil mit AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus. Wählen Sie in der Clusterliste den Cluster aus, in dem Sie das Fargate-Profil löschen möchten.
3. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
4. Wählen Sie das zu löschende Fargate-Profil und dann Delete (Löschen) aus.
5. Geben Sie auf der Seite Delete Fargate profile (Fargate-Profil löschen) den Namen des Profils ein und wählen Sie dann Delete (Löschen) aus.

## AWS CLI

Löschen Sie ein Fargate-Profil mit CLI AWS

Verwenden Sie den folgenden Befehl, um ein Profil aus einem Cluster zu löschen. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
aws eks delete-fargate-profile --fargate-profile-name my-profile --cluster-name my-cluster
```

## Die Konfigurationsdetails des Fargate Pod verstehen

In diesem Abschnitt werden einige der einzigartigen Pod-Konfigurationsdetails für die Ausführung von Kubernetes-Pods auf AWS Fargate beschrieben.

## CPU und Arbeitsspeicher des Pods

Mit Kubernetes können Sie Anfragen, eine vCPU-Mindestmenge und Speicherressourcen definieren, die jedem Container in einem Pod zugewiesen werden. Pods werden von Kubernetes geplant, um sicherzustellen, dass mindestens die angeforderten Ressourcen für jeden Pod auf der Rechenressource verfügbar sind. Weitere Informationen finden Sie unter [Managing Compute Resources for Containers](#) in der Kubernetes-Dokumentation.

### Note

Da Amazon EKS Fargate nur einen Pod pro Knoten ausführt, tritt das Szenario, Pods zu entfernen, wenn weniger Ressourcen zur Verfügung stehen, nicht auf. Alle Amazon EKS Fargate Pods werden mit garantierter Priorität ausgeführt, sodass die angeforderte CPU und der angeforderte Arbeitsspeicher dem Limit für alle Container entsprechen müssen. Weitere Informationen finden Sie unter [Konfigurieren von Dienstqualität für Pods](#) in der Kubernetes-Dokumentation.

Wenn Pods auf Fargate geplant sind, bestimmen die vCPU- und Speicherreservierungen innerhalb der Pod-Spezifikation, wie viel CPU und Arbeitsspeicher für den Pod bereitgestellt werden müssen.

- Die maximale Anforderung von Init-Containern wird verwendet, um die vCPU- und Speicheranforderungen für die Init-Anforderung zu bestimmen.
- Anforderungen für alle lang laufenden Container werden addiert, um die Anforderungen an die vCPU und den Arbeitsspeicher für lange laufende Anforderungen zu bestimmen.
- Der größere der beiden vorherigen Werte wird für die vCPU- und Speicheranforderung ausgewählt, die für Ihren Pod verwendet werden sollen.
- Fargate erhöht die Speicherreservierung jedes Pods um 256 MB für die erforderlichen Kubernetes-Komponenten (kubelet, kube-proxy, und) containerd

Fargate rundet auf die folgende Rechenkonfiguration ab, die der Summe der vCPU- und Speicheranforderungen am ehesten entspricht, um sicherzustellen, dass Pods immer über die Ressourcen verfügen, die sie zum Ausführen benötigen.

Wenn Sie keine Kombination aus vCPU und Arbeitsspeicher angeben, wird die kleinste verfügbare Kombination verwendet (0,25 vCPU und 0,5 GB Arbeitsspeicher).

Die folgende Tabelle zeigt die vCPU- und Speicherkombinationen, die für Pods verfügbar sind, die auf Fargate ausgeführt werden.

| vCPU-Wert | Speicherwert                                |
|-----------|---------------------------------------------|
| 0,25 vCPU | 0,5 GB, 1 GB, 2 GB                          |
| 0,5 vCPU  | 1 GB, 2 GB, 3 GB, 4 GB                      |
| 1 vCPU    | 2 GB, 3 GB, 4 GB, 5 GB, 6 GB, 7 GB, 8 GB    |
| 2 vCPU    | Zwischen 4 GB und 16 GB in 1-GB-Schritten   |
| 4 vCPU    | Zwischen 8 GB und 30 GB in 1-GB-Schritten   |
| 8 vCPU    | Zwischen 16 GB und 60 GB in 4-GB-Schritten  |
| 16 vCPU   | Zwischen 32 GB und 120 GB in 8-GB-Schritten |

Der zusätzliche Speicher, der für die Kubernetes-Komponenten reserviert ist, kann dazu führen, dass eine Fargate-Aufgabe mit mehr v CPUs als angefordert bereitgestellt wird. Bei einer Anforderung für 1 vCPU und 8 GB Arbeitsspeicher werden beispielsweise 256 MB zur Speichieranforderung hinzugefügt, und es wird eine Fargate-Aufgabe mit 2 V CPUs und 9 GB Arbeitsspeicher bereitgestellt, da keine Aufgabe mit 1 vCPU und 9 GB Arbeitsspeicher verfügbar ist.

Es besteht keine Korrelation zwischen der Größe des Pods, der auf Fargate läuft, und der von Kubernetes gemeldeten Knotengröße mit `kubectl get nodes`. Die gemeldete Knotengröße ist oft größer als die Kapazität des Pods. Sie können die Pod-Kapazität mit dem folgenden Befehl überprüfen. Ersetze es *default* durch den Namespace deines Pods und *pod-name* durch den Namen deines Pods.

```
kubectl describe pod --namespace default pod-name
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
annotations:
 CapacityProvisioned: 0.25vCPU 0.5GB
[...]
```

Die CapacityProvisioned Anmerkung stellt die erzwungene Pod-Kapazität dar und bestimmt die Kosten für den Betrieb Ihres Pods auf Fargate. Preisinformationen für die Computing-Konfigurationen finden Sie unter [AWS -Fargate-Preise](#).

## Fargate-Speicher

Ein Pod, der auf Fargate läuft, mountet automatisch ein Amazon EFS-Dateisystem, ohne dass manuelle Schritte zur Treiberinstallation erforderlich sind. Sie können kein dynamisches persistentes Volume Provisioning mit Fargate-Knoten verwenden, aber Sie können statische Bereitstellung verwenden. Weitere Informationen finden Sie unter [Amazon EFS CSI Driver](#) on GitHub.

Bei der Bereitstellung erhält jeder Pod, der auf Fargate läuft, standardmäßig 20 GiB kurzlebigen Speicher. Dieser Speichertyp wird gelöscht, wenn ein Pod beendet wird. Bei neuen Pods, die auf Fargate eingeführt werden, ist die Verschlüsselung des kurzlebigen Speichervolumens standardmäßig aktiviert. Der kurzlebige Pod-Speicher ist mit einem AES-256-Verschlüsselungsalgorithmus verschlüsselt, der von Fargate verwaltete Schlüssel verwendet AWS .

### Note

Der nutzbare Standardspeicher für Amazon EKS-Pods, die auf Fargate ausgeführt werden, beträgt weniger als 20 GiB. Dies liegt daran, dass ein Teil des Speicherplatzes von den kubelet und anderen Kubernetes-Modulen belegt wird, die in den Pod geladen werden.

Sie können die Gesamtmenge des flüchtigen Speichers bis zu einem Maximum von 175 GB erhöhen. Um die Größe mit Kubernetes zu konfigurieren, geben Sie die ephemeral-storage Ressourcenanforderungen für jeden Container in einem Pod an. Wenn Kubernetes Pods plant, wird sichergestellt, dass die Summe der Ressourcenanfragen für jeden Pod geringer ist als die Kapazität der Fargate-Aufgabe. Weitere Informationen finden Sie unter [Ressourcenmanagement für Pods und Container](#) in der Kubernetes-Dokumentation.

Amazon EKS Fargate stellt mehr kurzlebigen Speicher bereit, als für die Systemnutzung angefordert wurde. Eine Anforderung von 100 GB stellt beispielsweise eine Fargate-Aufgabe mit 115 GB flüchtigem Speicher bereit.

## Aktionen für AWS Fargate OS-Patching-Ereignisse festlegen

Amazon EKS patcht das Betriebssystem für AWS Fargate-Knoten regelmäßig, um deren Sicherheit zu gewährleisten. Im Rahmen des Patching-Prozesses werden die Knoten recycelt, um

Betriebssystem-Patches zu installieren. Updates werden so durchgeführt, dass sie Ihre Services möglichst wenig beeinflussen. Wenn Pods jedoch nicht erfolgreich entfernt werden, müssen sie manchmal gelöscht werden. Die folgenden Maßnahmen können Ihnen helfen, potenzielle Unterbrechungen zu minimieren:

- Legen Sie entsprechende Budgets für Pod-Unterbrechungen (PDBs) fest, um die Anzahl der Pods zu kontrollieren, die gleichzeitig ausgefallen sind.
- Erstellen Sie EventBridge Amazon-Regeln, um fehlgeschlagene Räumungen zu behandeln, bevor die Pods gelöscht werden.
- Starten Sie Ihre betroffenen Pods vor dem Räumungsdatum, das in der Benachrichtigung, die Sie erhalten, angegeben ist, manuell neu.
- Erstellen Sie unter AWS Benutzerbenachrichtigungen eine Benachrichtigungskonfiguration.

Amazon EKS arbeitet eng mit der Kubernetes-Community zusammen, um Bugfixes und Sicherheitspatches so schnell wie möglich verfügbar zu machen. Alle Fargate Pods beginnen mit der neuesten Kubernetes-Patch-Version, die bei Amazon EKS für die Kubernetes-Version Ihres Clusters erhältlich ist. Wenn Sie einen Pod mit einer älteren Patch-Version haben, recycelt Amazon EKS ihn möglicherweise, um ihn auf die neueste Version zu aktualisieren. Dadurch wird sichergestellt, dass Ihre Pods mit den neuesten Sicherheitsupdates ausgestattet sind. Auf diese Weise werden Sie bei einem kritischen CVE-Problem ([Common Vulnerabilities and Exposures](#)) auf dem Laufenden gehalten, um Sicherheitsrisiken zu reduzieren.

Wenn das AWS Fargate-Betriebssystem aktualisiert wird, sendet Ihnen Amazon EKS eine Benachrichtigung, die Ihre betroffenen Ressourcen und das Datum der bevorstehenden Pod-Räumung enthält. Wenn das angegebene Räumungsdatum ungünstig ist, haben Sie die Möglichkeit, Ihre betroffenen Pods vor dem in der Benachrichtigung angegebenen Räumungsdatum manuell neu zu starten. Alle Pods, die vor dem Zeitpunkt, zu dem du die Benachrichtigung erhältst, erstellt wurden, unterliegen der Räumung. Weitere Anweisungen zum manuellen Neustart Ihrer Pods finden Sie in der [Kubernetes-Dokumentation](#).

Um die Anzahl der Pods zu begrenzen, die beim Recycling von Pods gleichzeitig ausgefallen sind, können Sie Budgets für die Unterbrechung von Pods festlegen (PDBs). Sie können diese verwenden PDBs , um die Mindestverfügbarkeit auf der Grundlage der Anforderungen Ihrer einzelnen Anwendungen zu definieren und gleichzeitig Aktualisierungen zuzulassen. Die Mindestverfügbarkeit Ihrer PDB muss unter 100% liegen. Weitere Informationen finden Sie in der Kubernetes-Dokumentation [unter Angabe eines Unterbrechungsbudgets für Ihre Anwendung](#).

Amazon EKS verwendet die [Eviction-API](#), um den Pod sicher zu entleeren und dabei die Einstellungen zu berücksichtigen PDBs, die Sie für die Anwendung festgelegt haben. Pods werden von der Availability Zone bereinigt, um Auswirkungen zu minimieren. Wenn die Räumung erfolgreich ist, erhält der neue Pod den neuesten Patch und es sind keine weiteren Maßnahmen erforderlich.

Wenn die Räumung eines Pods fehlschlägt, sendet Amazon EKS ein Ereignis mit Details zu den Pods, bei denen die Räumung fehlgeschlagen ist, an Ihr Konto. Sie können vor der geplanten Beendigungszeit auf die Nachricht reagieren. Die spezifische Zeit variiert je nach Dringlichkeit des Patches. Wenn es soweit ist, versucht Amazon EKS erneut, die Pods zu vertreiben. Dieses Mal wird bei einer fehlgeschlagenen Bereinigung jedoch kein neues Ereignis gesendet. Schlägt die Räumung erneut fehl, werden Ihre vorhandenen Pods regelmäßig gelöscht, sodass die neuen Pods über den neuesten Patch verfügen können.

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das ausgelöst wurde, wenn die Pod-Entfernung fehlschlägt. Es enthält Details zum Cluster, zum Pod-Namen, zum Pod-Namespace, zum Fargate-Profil und zur geplanten Kündigungszeit.

```
{
 "version": "0",
 "id": "12345678-90ab-cdef-0123-4567890abcde",
 "detail-type": "EKS Fargate Pod Scheduled Termination",
 "source": "aws.eks",
 "account": "111122223333",
 "time": "2021-06-27T12:52:44Z",
 "region": "region-code",
 "resources": [
 "default/my-database-deployment"
],
 "detail": {
 "clusterName": "my-cluster",
 "fargateProfileName": "my-fargate-profile",
 "podName": "my-pod-name",
 "podNamespace": "default",
 "evictErrorMessage": "Cannot evict pod as it would violate the pod's disruption budget",
 "scheduledTerminationTime": "2021-06-30T12:52:44.832Z[UTC]"
 }
}
```

Wenn einem Pod mehrere PDBs zugeordnet sind, kann dies außerdem dazu führen, dass die Räumung fehlschlägt. In diesem Fall gibt das Ereignis die folgende Fehlernachricht zurück.

```
"evictErrorMessage": "This pod has multiple PodDisruptionBudget, which the eviction subresource does not support",
```

Basierend auf diesem Ereignis können Sie eine gewünschte Aktion erstellen. Sie können beispielsweise Ihr Budget für die Unterbrechung Ihres Pods (PDB) anpassen, um zu kontrollieren, wie die Pods geräumt werden. Nehmen wir genauer an, dass Sie mit einer PDB beginnen, die den Zielprozentsatz der verfügbaren Pods festlegt. Bevor Ihre Pods während eines Upgrades zwangsweise beendet werden, können Sie die PDB auf einen anderen Prozentsatz an Pods anpassen. Um dieses Ereignis zu erhalten, müssen Sie eine EventBridge Amazon-Regel für das AWS Konto und die AWS Region erstellen, zu der der Cluster gehört. Die Regel muss das folgende benutzerdefinierte Muster verwenden. Weitere Informationen finden Sie im [EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren](#).

```
{
 "source": ["aws.eks"],
 "detail-type": ["EKS Fargate Pod Scheduled Termination"]
}
```

Es kann ein geeignetes Ziel zur Erfassung durch das Ereignis festgelegt werden. Eine vollständige Liste der verfügbaren Ziele finden Sie unter [EventBridge Amazon-Ziele](#) im EventBridge Amazon-Benutzerhandbuch. Sie können auch eine Benachrichtigungskonfiguration unter AWS Benutzerbenachrichtigungen erstellen. Wenn Sie AWS Management Console zum Erstellen der Benachrichtigung verwenden, wählen Sie unter Event Rules Elastic Kubernetes Service (EKS) als AWS Servicename und EKS Fargate Pod Scheduled Termination als Ereignistyp aus. Weitere Informationen finden Sie unter [Erste Schritte mit AWS Benutzerbenachrichtigungen](#) im Benutzerhandbuch für AWS Benutzerbenachrichtigungen.

Häufig gestellte Fragen zu [EKS Pod-Räumungen finden Sie unter FAQs: Räumungsmitteilung für Fargate](#) Pod in AWS re:POST.

## Erfassen Sie die App- und Nutzungsmetriken von AWS Fargate

Sie können Systemmetriken und CloudWatch Nutzungsmetriken für AWS Fargate sammeln.

### Anwendungsmetriken

Für Anwendungen, die auf Amazon EKS und AWS Fargate ausgeführt werden, können Sie die AWS Distribution for OpenTelemetry (ADOT) verwenden. ADOT ermöglicht es Ihnen, Systemmetriken zu sammeln und sie an Container Insights-Dashboards zu CloudWatch senden. Informationen

zu den ersten Schritten mit ADOT für Anwendungen, die auf Fargate ausgeführt werden, finden Sie unter [Using CloudWatch Container Insights with AWS Distro for OpenTelemetry](#) in der ADOT-Dokumentation.

## Nutzungsmetriken

Sie können CloudWatch Nutzungsmetriken verwenden, um einen Überblick über die Ressourcennutzung Ihres Kontos zu erhalten. Verwenden Sie diese Kennzahlen, um Ihre aktuelle Servicenutzung in CloudWatch Diagrammen und Dashboards zu visualisieren.

AWS Die Nutzungsmetriken von Fargate entsprechen den AWS Servicekontingenten. Sie können Alarme konfigurieren, mit denen Sie benachrichtigt werden, wenn sich Ihre Nutzung einem Servicekontingent nähert. Weitere Hinweise zu Servicekontingenten für Fargate finden Sie unter [the section called “Servicekontingente”](#).

AWS Fargate veröffentlicht die folgenden Metriken im `AWS/Usage` Namespace.

| Metrik        | Beschreibung                                                                                                                                                           |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ResourceCount | Die Gesamtanzahl der angegebenen Ressourcen, die in Ihrem Konto ausgeführt werden. Die Ressource wird durch die Dimensionen definiert, die der Metrik zugeordnet sind. |

Die folgenden Dimensionen werden verwendet, um die von AWS Fargate veröffentlichten Nutzungsmetriken zu verfeinern.

| Dimension | Beschreibung                                                                                                                        |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------|
| Service   | Der Name des AWS Dienstes, der die Ressource enthält. Für AWS Fargate-Nutzungsmetriken ist Fargate der Wert für diese Dimension.    |
| Type      | Der Typ der Entität, die gemeldet wird. Derzeit ist der einzig gültige Wert für AWS Fargate-Nutzungsmetriken. <code>Resource</code> |



| Dimension | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource  | <p>Der Typ der Ressource, die ausgeführt wird.</p> <p>Derzeit gibt AWS Fargate Informationen zu Ihrer Fargate On-Demand-Nutzung zurück. Der Ressourcenwert für Fargate On-Demand-Nutzung ist OnDemand.</p> <p>[HINWEIS] ====</p> <p>Die Nutzung von Fargate On-Demand kombiniert Amazon EKS-Pods, die Fargate verwenden, Amazon ECS-Aufgaben, die den Fargate-Starttyp verwenden, und Amazon ECS-Aufgaben, die den FARGATE Kapazität sanbieter verwenden.</p> <p>=====</p> |
| Class     | <p>Die Klasse der nachverfolgten Ressource. Derzeit verwendet AWS Fargate die Klassendimension nicht.</p>                                                                                                                                                                                                                                                                                                                                                                  |

Einen CloudWatch Alarm zur Überwachung der Fargate-Ressourcennutzungsmetriken erstellen

AWS Fargate stellt CloudWatch Nutzungsmetriken bereit, die den AWS Servicekontingenten für die Nutzung von Fargate On-Demand-Ressourcen entsprechen. In der Service-Quotas-Konsole können Sie Ihre Nutzung in einem Diagramm visualisieren. Sie können auch Alarmer konfigurieren, die Sie warnen, wenn sich Ihre Nutzung einem Service Quotas nähert. Weitere Informationen finden Sie unter [the section called “Erfassen Sie Messwerte”](#).

Gehen Sie wie folgt vor, um einen CloudWatch Alarm auf der Grundlage der Fargate-Kennzahlen zur Ressourcennutzung zu erstellen.

1. Öffnen Sie die Service Quotas-Konsole unter <https://console.aws.amazon.com/servicequotas/>.
2. Wählen Sie im linken Navigationsbereich AWS Dienste aus.
3. Suchen Sie in der AWS Serviceliste nach AWS Fargate und wählen Sie es aus.

4. Wählen Sie in der Liste Service quotas (Servicekontingente) das Fargate-Nutzungskontingent aus, für das Sie einen Alarm erstellen möchten.
5. Wählen Sie im Bereich CloudWatch Amazon-Alarme die Option Erstellen aus.
6. Wählen Sie bei Alarmschwellenwert den Prozentsatz des angewendeten Kontingentwerts aus, den Sie als Alarmwert festlegen möchten.
7. Geben Sie bei Alarmname einen Namen für den Alarm ein und wählen Sie dann Erstellen aus.

## Starten Sie die AWS Fargate-Protokollierung für Ihren Cluster

Amazon EKS auf Fargate bietet einen integrierten Log-Router basierend auf Fluent Bit. Das bedeutet, dass Sie einen Fluent Bit-Container nicht explizit als Sidecar ausführen, sondern Amazon ihn für Sie ausführt. Alles, was Sie tun müssen, ist den Log-Router zu konfigurieren. Die Konfiguration erfolgt über ein dediziertes ConfigMap, das die folgenden Kriterien erfüllen muss:

- Benannte `aws-logging`
- Erstellt in einem dedizierten Namespace namens `aws-observability`
- Darf 5300 Zeichen nicht überschreiten.

Sobald Sie das erstellt haben ConfigMap, erkennt Amazon EKS on Fargate es automatisch und konfiguriert den Protokollrouter damit. Fargate verwendet eine Version von AWS for Fluent Bit, einer Upstream-konformen Distribution von Fluent Bit, die von verwaltet wird. AWS Weitere Informationen finden Sie unter [Fluent AWS Bit](#) on. GitHub

Mit dem Protokollrouter können Sie die gesamte Bandbreite der Dienste AWS für Protokollanalysen und -speicherung nutzen. Sie können Protokolle von Fargate direkt zu Amazon CloudWatch, Amazon OpenSearch Service streamen. Sie können Protokolle auch über Amazon Data [Firehose](#) an Ziele wie [Amazon S3](#), [Amazon Kinesis Data Streams](#) und Partnertools streamen.

- Ein vorhandenes Fargate-Profil, das einen vorhandenen Kubernetes-Namespace angibt, in dem Sie Fargate Pods bereitstellen. Weitere Informationen finden Sie unter [the section called “Schritt 3: Erstellen Sie ein Fargate-Profil für Ihren Cluster”](#).
- Eine bestehende Fargate Pod-Ausführungsrolle. Weitere Informationen finden Sie unter [the section called “Schritt 2: Erstellen Sie eine Fargate Pod-Ausführungsrolle”](#).

## Router-Konfiguration protokollieren

### Important

Damit Protokolle erfolgreich veröffentlicht werden können, muss von der VPC, in der sich Ihr Cluster befindet, Netzwerkzugriff auf das Protokollziel bestehen. Dies betrifft hauptsächlich Benutzer, die Ausgangsregeln für ihre VPC anpassen. Ein Anwendungsbeispiel finden Sie unter [Using CloudWatch Logs with Interface VPC Endpoints](#) im Amazon CloudWatch Logs-Benutzerhandbuch. CloudWatch

Ersetzen Sie in den folgenden Schritten jede *example value* durch Ihre eigenen Werte.

1. Erstellen Sie einen dedizierten Kubernetes-Namespace namens `aws-observability`.
  - a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `aws-observability-namespace.yaml` auf Ihrem Computer. Der Wert für `name` muss `aws-observability` sein und das Label `aws-observability: enabled` ist erforderlich.

```
kind: Namespace
apiVersion: v1
metadata:
 name: aws-observability
 labels:
 aws-observability: enabled
```

- b. Erstellen Sie den Namespace.

```
kubectl apply -f aws-observability-namespace.yaml
```

2. Erstellen Sie ein ConfigMap mit einem Fluent Conf-Datenwert, um Container-Logs an ein Ziel zu versenden. Fluent Conf ist Fluent Bit, eine schnelle und einfache Protokollprozessor-Konfigurationssprache, die verwendet wird, um Container-Logs an ein Log-Ziel Ihrer Wahl weiterzuleiten. Weitere Informationen finden Sie unter [Konfigurationsdatei](#) in der Fluent-Bit-Dokumentation.

### Important

In einer typischen Fluent Conf sind die Hauptabschnitte `Service`, `Input`, `Filter` und `Output` enthalten. Der Fargate-Protokoll-Router akzeptiert jedoch nur:

- Die Abschnitte `Filter` und `Output`.
- Ein `Parser`-Abschnitt.

Wenn Sie andere Abschnitte angeben, werden diese abgelehnt.

Der Fargate-Protokollrouter verwaltet die Abschnitte `Service` und `Input`. Es hat den folgenden `Input` Abschnitt, der nicht geändert werden kann und in Ihrem nicht benötigt wird. `ConfigMap` Sie können daraus jedoch Erkenntnisse gewinnen, z. B. die Speicherpuffergrenze und das für Protokolle angewendete Tag.

```
[INPUT]
 Name tail
 Buffer_Max_Size 66KB
 DB /var/log/flb_kube.db
 Mem_Buf_Limit 45MB
 Path /var/log/containers/*.log
 Read_From_Head On
 Refresh_Interval 10
 Rotate_Wait 30
 Skip_Long_Lines On
 Tag kube.*
```

Berücksichtigen Sie beim Erstellen des `ConfigMap`, die folgenden Regeln, die Fargate verwendet, um Felder zu validieren:

- `[FILTER]`, `[OUTPUT]`, und `[PARSER]` sollen unter jedem entsprechenden Schlüssel angegeben werden. `[FILTER]` muss beispielsweise unter `filters.conf` liegen. Sie können ein oder mehrere `[FILTER]` in der `filters.conf` haben. Die Abschnitte `[OUTPUT]` und `[PARSER]` sollten sich auch unter den entsprechenden Schlüssel befinden. Durch die Angabe mehrerer `[OUTPUT]`-Abschnitte können Sie Ihre Protokolle gleichzeitig an verschiedene Ziele weiterleiten.
- Fargate validiert die erforderlichen Schlüssel für jeden Abschnitt. `Name` und `match` sind für jedes `[FILTER]` und `[OUTPUT]` erforderlich. `Name` und `format` werden jeweils für jeden `[PARSER]` benötigt. Bei den Schlüssel wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Umgebungsvariablen wie `${ENV_VAR}` sind in der nicht erlaubt `ConfigMap`.
- Die Einrückung muss für die Direktive oder das Schlüssel-Wert-Paar innerhalb von `filters.conf`, `output.conf` und `parsers.conf` gleich sein. Schlüssel-Wert-Paare müssen stärker eingerückt werden als Direktiven.

- Fargate validiert gegen die folgenden unterstützten Filter: `grep`, `parser`, `record_modifier`, `rewrite_tag`, `throttle`, `nest`, `modify`, und `kubernetes`.
- Fargate validiert mit der folgenden unterstützten Ausgabe: `es`, `firehose`, `kinesis_firehose`, `cloudwatch`, `cloudwatch_logs`, und `kinesis`.
- Um die Protokollierung zu aktivieren, muss mindestens ein unterstütztes Output Plugin in der ConfigMap bereitgestellt werden. Filter und Parser sind nicht erforderlich, um die Protokollierung zu aktivieren.

Sie können Fluent Bit auch auf Amazon EC2 mit der gewünschten Konfiguration ausführen, um Probleme zu beheben, die sich aus der Validierung ergeben. Erstellen Sie Ihr ConfigMap mit einem der folgenden Beispiele.

#### Important

Die Amazon EKS Fargate-Protokollierung unterstützt keine dynamische Konfiguration von a. ConfigMap Alle Änderungen an a ConfigMap werden nur auf neue Pods angewendet. Änderungen werden nicht auf bestehende Pods angewendet.

Erstellen Sie anhand des Beispiels ein ConfigMap für Ihr gewünschtes Protokollziel.

#### Note

Sie können auch Amazon Kinesis Data Streams als Protokollziel verwenden. Stellen Sie bei der Nutzung von Kinesis Data Streams sicher, dass der Pod-Ausführungsrolle die Berechtigung `kinesis:PutRecords` erteilt wurde. Weitere Informationen finden Sie unter Amazon Kinesis Data Streams [Streams-Berechtigungen](#) im Fluent Bit: Offizielles Handbuch.

## Example

### CloudWatch

Sie haben zwei Ausgabeoptionen, wenn Sie Folgendes verwenden: CloudWatch

- [Ein Ausgabe-Plug-In in C geschrieben](#)
- [Ein in Golang geschriebenes Ausgabe-Plug-In](#)

Das folgende Beispiel zeigt Ihnen, wie Sie das `cloudwatch_logs` Plugin verwenden, um Logs an zu senden CloudWatch.

- a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `aws-logging-cloudwatch-configmap.yaml`. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. Die Parameter unter `[OUTPUT]` sind erforderlich.

```
kind: ConfigMap
apiVersion: v1
metadata:
 name: aws-logging
 namespace: aws-observability
data:
 flb_log_cw: "false" # Set to true to ship Fluent Bit process logs to
 CloudWatch.
 filters.conf: |
 [FILTER]
 Name parser
 Match *
 Key_name log
 Parser crio
 [FILTER]
 Name kubernetes
 Match kube.*
 Merge_Log On
 Keep_Log Off
 Buffer_Size 0
 Kube_Meta_Cache_TTL 300s
 output.conf: |
 [OUTPUT]
 Name cloudwatch_logs
 Match kube.*
 region region-code
 log_group_name my-logs
 log_stream_prefix from-fluent-bit-
 log_retention_days 60
 auto_create_group true
 parsers.conf: |
 [PARSER]
 Name crio
 Format Regex
 Regex ^(?<time>[^\]+) (?<stream>stdout|stderr) (?<logtag>P|F) (?
<log>.*)$
```

```
Time_Key time
Time_Format %Y-%m-%dT%H:%M:%S.%L%z
```

- b. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f aws-logging-cloudwatch-configmap.yaml
```

## Amazon OpenSearch Service

Wenn Sie Logs an Amazon OpenSearch Service senden möchten, können Sie [es output verwenden](#). Dabei handelt es sich um ein in C geschriebenes Plugin. Das folgende Beispiel zeigt Ihnen, wie Sie das Plugin verwenden, um Logs an zu senden OpenSearch.

- a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `aws-logging-opensearch-configmap.yaml`. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

```
kind: ConfigMap
apiVersion: v1
metadata:
 name: aws-logging
 namespace: aws-observability
data:
 output.conf: |
 [OUTPUT]
 Name es
 Match *
 Host search-example-gjxdcilagiprbqlqn42jsty66y.region-
code.es.amazonaws.com
 Port 443
 Index example
 Type example_type
 AWS_Auth On
 AWS_Region region-code
 tls On
```

- b. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f aws-logging-opensearch-configmap.yaml
```

## Firehose

Sie haben zwei Ausgabeoptionen, wenn Sie Logs an Firehose senden:

- [kinesis\\_firehose](#) — Ein in C geschriebenes Ausgabe-Plugin.
- [firehose](#) — Ein in Golang geschriebenes Ausgabe-Plugin.

Das folgende Beispiel zeigt Ihnen, wie Sie das `kinesis_firehose` Plugin verwenden, um Logs an Firehose zu senden.

- a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `aws-logging-firehose-configmap.yaml`. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet.

```
kind: ConfigMap
apiVersion: v1
metadata:
 name: aws-logging
 namespace: aws-observability
data:
 output.conf: |
 [OUTPUT]
 Name kinesis_firehose
 Match *
 region region-code
 delivery_stream my-stream-firehose
```

- b. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f aws-logging-firehose-configmap.yaml
```

3. Richten Sie Berechtigungen für die Fargate Pod-Ausführungsrolle ein, um Protokolle an Ihr Ziel zu senden.

- a. Laden Sie die IAM-Richtlinie für Ihr Ziel auf Ihren Computer herunter.

Example

CloudWatch

Laden Sie die CloudWatch IAM-Richtlinie auf Ihren Computer herunter. Sie können [die Richtlinie auch unter GitHub einsehen](#).

```
curl -O https://raw.githubusercontent.com/aws-samples/amazon-eks-fluent-logging-examples/mainline/examples/fargate/cloudwatchlogs/permissions.json
```



## Amazon OpenSearch Service

Laden Sie die OpenSearch IAM-Richtlinie auf Ihren Computer herunter. Sie können [die Richtlinie auch unter GitHub einsehen](#).

```
curl -O https://raw.githubusercontent.com/aws-samples/amazon-eks-fluent-logging-examples/mainline/examples/fargate/amazon-elasticsearch/permissions.json
```

Stellen Sie sicher, dass die Zugriffskontrolle OpenSearch von Dashboards richtig konfiguriert ist. Den `all_access` role OpenSearch In-Dashboards müssen die Fargate-Pod-Ausführungsrolle und die IAM-Rolle zugeordnet sein. Das gleiche Mapping muss für die `security_manager`-Rolle durchgeführt werden. Sie können die vorherigen Zuordnungen hinzufügen, indem Sie `Menu`, dann `Security`, dann `Roles` und dann die entsprechenden Rollen auswählen. Weitere Informationen finden Sie unter [Wie behebe ich Fehler bei CloudWatch Protokollen, sodass sie an meine Amazon ES-Domain gestreamt werden?](#).

## Firehose

Laden Sie die Firehose IAM-Richtlinie auf Ihren Computer herunter. Sie können die [Richtlinie auch unter einsehen](#). GitHub

```
curl -O https://raw.githubusercontent.com/aws-samples/amazon-eks-fluent-logging-examples/mainline/examples/fargate/kinesis-firehose/permissions.json
```

- b. Erstellen Sie eine IAM-Richtlinie aus der Richtliniendatei, die Sie heruntergeladen haben.

```
aws iam create-policy --policy-name eks-fargate-logging-policy --policy-document file://permissions.json
```

- c. Hängen Sie die IAM-Richtlinie an die Pod-Ausführungsrolle an, die für Ihr Fargate-Profil angegeben ist, mit dem folgenden Befehl. Ersetzen Sie `111122223333` durch Ihre Konto-ID. `AmazonEKSFargatePodExecutionRole` Ersetzen Sie sie durch Ihre Pod-Ausführungsrolle (weitere Informationen finden Sie unter [the section called "Schritt 2: Erstellen Sie eine Fargate Pod-Ausführungsrolle"](#)).

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::111122223333:policy/eks-fargate-logging-policy \
 --role-name AmazonEKSFargatePodExecutionRole
```

## Support von Kubernetes-Filtern

Mit dem Fluent-Bit-Kubernetes-Filter können Sie Kubernetes-Metadaten zu Ihren Protokolldateien hinzufügen. Weitere Informationen über den Filter finden Sie unter [Kubernetes](#) in der Fluent-Bit-Dokumentation. Sie können einen Filter unter Verwendung des Endpunkts des API-Servers anwenden.

```
filters.conf: |
 [FILTER]
 Name kubernetes
 Match kube.*
 Merge_Log On
 Buffer_Size 0
 Kube_Meta_Cache_TTL 300s
```

### Important

- Kube\_URL, Kube\_CA\_File, Kube\_Token\_Command, und Kube\_Token\_File sind Konfigurationsparameter im Servicebesitz und dürfen nicht angegeben werden. Amazon-EKS-Fargate füllt diese Werte aus.
- Kube\_Meta\_Cache\_TTL ist die Zeit, in der Fluent Bit wartet, bis es mit dem API-Server für die neuesten Metadaten kommuniziert. Wenn Kube\_Meta\_Cache\_TTL nicht angegeben, hängt Amazon EKS Fargate einen Standardwert von 30 Minuten an, um die Last auf dem API-Server zu verringern.

## Um Fluent Bit-Prozessprotokolle an Ihr Konto zu senden

Sie können Fluent Bit-Prozessprotokolle optional wie folgt ConfigMap an CloudWatch Amazon senden. Für den Versand von Fluent Bit-Prozessprotokollen an fallen zusätzliche CloudWatch Kosten für die Aufnahme und Lagerung der Protokolle an. Ersetzen Sie es *region-code* durch die AWS Region, in der sich Ihr Cluster befindet.

```
kind: ConfigMap
apiVersion: v1
```

```

metadata:
 name: aws-logging
 namespace: aws-observability
 labels:
data:
 # Configuration files: server, input, filters and output
 # =====
 flb_log_cw: "true" # Ships Fluent Bit process logs to CloudWatch.

output.conf: |
 [OUTPUT]
 Name cloudwatch
 Match kube.*
 region region-code
 log_group_name fluent-bit-cloudwatch
 log_stream_prefix from-fluent-bit-
 auto_create_group true

```

Die Protokolle befinden sich CloudWatch in derselben AWS Region wie der Cluster. Der Name der Protokollgruppe lautet *my-cluster*-fluent-bit-logs und der Name des Fluent-Bit-Logstreams lautet fluent-bit-*podname-pod-namespace* .

#### Note

- Die Prozessprotokolle werden nur ausgeliefert, wenn der Fluent-Bit-Prozess erfolgreich gestartet wird. Wenn beim Starten von Fluent Bit ein Fehler auftritt, werden die Prozessprotokolle verpasst. Sie können Prozessprotokolle nur an senden CloudWatch.
- Um Versandprozessprotokolle auf Ihr Konto zu debuggen, können Sie die vorherigen ConfigMap anwenden, um die Prozessprotokolle zu erhalten. Dass Fluent Bit nicht gestartet werden kann, liegt normalerweise daran, dass Ihr ConfigMap beim Starten nicht von Fluent Bit analysiert oder akzeptiert wird.

Um den Versand von Fluent Bit-Prozessprotokollen zu beenden

Für den Versand von Fluent Bit-Prozessprotokollen an fallen CloudWatch zusätzliche Kosten für die Protokollaufnahme und Speicherung an. Gehen Sie wie folgt vor, um Prozessprotokolle in einem vorhandenen ConfigMap-Setup auszuschließen.

1. Suchen Sie die CloudWatch Protokollgruppe, die automatisch für die Fluent Bit-Prozessprotokolle Ihres Amazon EKS-Clusters erstellt wurde, nachdem Sie die Fargate-Protokollierung aktiviert haben. Es folgt dem Format *my-cluster-fluent-bit-logs*.
2. Löschen Sie die vorhandenen CloudWatch Protokollstreams, die für die Prozessprotokolle jedes Pods in der CloudWatch Protokollgruppe erstellt wurden.
3. Bearbeiten Sie die ConfigMap und stellen Sie `flb_log_cw: "false"` ein.
4. Starten Sie alle vorhandenen Pods im Cluster neu.

## Testanwendung

1. Stellen Sie einen Beispiel-Pod bereit.
  - a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `sample-app.yaml` auf Ihrem Computer.

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: sample-app
 namespace: same-namespace-as-your-fargate-profile
spec:
 replicas: 3
 selector:
 matchLabels:
 app: nginx
 template:
 metadata:
 labels:
 app: nginx
 spec:
 containers:
 - name: nginx
 image: nginx:latest
 ports:
 - name: http
 containerPort: 80
```

- b. Wenden Sie das Manifest auf den Cluster an.

```
kubectl apply -f sample-app.yaml
```

2. Zeigen Sie die NGINX-Protokolle mit den Zielen an, die Sie im ConfigMap.

## Größenüberlegungen

Wir empfehlen Ihnen, für den Protokoll-Router bis zu 50 MB Speicher einzuplanen. Wenn Sie erwarten, dass Ihre Anwendung Protokolle mit sehr hohem Durchsatz generiert, sollten Sie bis zu 100 MB einplanen.

## Fehlerbehebung

Um zu überprüfen, ob die Protokollierungsfunktion aus irgendeinem Grund aktiviert oder deaktiviert ist, z. B. weil sie ungültig ist ConfigMap, und warum sie ungültig ist, überprüfen Sie Ihre Pod-Ereignisse mit `kubectl describe pod pod-name`. Die Ausgabe kann Pod-Ereignisse enthalten, die verdeutlichen, ob die Protokollierung aktiviert ist oder nicht, wie die folgende Beispielausgabe.

```
[...]
Annotations: CapacityProvisioned: 0.25vCPU 0.5GB
 Logging: LoggingDisabled: LOGGING_CONFIGMAP_NOT_FOUND

[...]
Events:
 Type Reason Age From
 Message
 ---- -
Warning LoggingDisabled <unknown> fargate-scheduler
 Disabled logging because aws-logging configmap was not found. configmap
 "aws-logging" not found
```

Die Pod-Ereignisse sind kurzlebig und haben einen bestimmten Zeitraum, der von den Einstellungen abhängt. Du kannst die Anmerkungen eines Pods auch mithilfe von anzeigen. `kubectl describe pod pod-name` In der Pod-Anmerkung finden Sie Informationen darüber, ob die Protokollierungsfunktion aktiviert oder deaktiviert ist, und den Grund dafür.

## Wählen Sie einen optimalen EC2 Amazon-Node-Instance-Typ

Amazon EC2 bietet eine große Auswahl an Instance-Typen für Worker-Knoten. Jeder Instance-Typ bietet andere Merkmale in Bezug auf Datenverarbeitung, Arbeitsspeicher, Speicher und Netzwerkfunktionen. Jede Instance wird abhängig von diesen Eigenschaften auch in Instance-Familien eingeordnet. Eine Liste finden Sie unter [Verfügbare Instance-Typen](#) im EC2 Amazon-

Benutzerhandbuch. Amazon EKS veröffentlicht mehrere Varianten von Amazon EC2 AMIs, um den Support zu ermöglichen. Berücksichtigen Sie die folgenden Kriterien, um sicherzustellen, dass der ausgewählte Instance-Typ mit Amazon EKS kompatibel ist.

- Alle Amazon EKS unterstützen die mac Familie derzeit AMIs nicht.
- Arm und Amazon EKS ohne Beschleunigung unterstützen die p Familieng3, g4inf, und AMIs nicht.
- Accelerated Amazon EKS unterstützt die t Familien ac,hpc,m, und AMIs nicht.
- Für ARM-basierte Instances unterstützt Amazon Linux 2023 (AL2023) nur Instance-Typen, die Graviton2-Prozessoren oder neuere Prozessoren verwenden. AL2023 unterstützt keine Instances. A1

Berücksichtigen Sie bei der Auswahl zwischen Instance-Typen, die von Amazon EKS unterstützt werden, die folgenden Funktionen jedes Typs.

#### Anzahl der Instanzen in einer Knotengruppe

Im Allgemeinen sind weniger, größere Instanzen besser, insbesondere wenn Sie viele Daemonsets haben. Jede Instance erfordert API-Aufrufe an den API-Server. Je mehr Instances Sie haben, desto mehr Last auf dem API-Server.

#### Betriebssystem

Überprüfen Sie die unterstützten Instance-Typen für [Linux](#), [Windows](#) und [Bottlerocket](#). Lesen Sie vor dem Erstellen von Windows-Instanzen den Artikel [Windows-Knoten auf EKS-Clustern bereitstellen](#).

#### Hardwarearchitektur

Benötigen Sie x86 oder Arm? Bevor Sie Arm-Instances bereitstellen, sollten Sie sich das für [Amazon EKS optimierte Arm Amazon Linux ansehen AMIs](#). Benötigen Sie Instances, die auf dem Nitro System ([Linux](#) oder [Windows](#)) basieren oder über [beschleunigte](#) Funktionen verfügen? Wenn Sie beschleunigte Funktionen benötigen, können Sie Linux nur mit Amazon EKS verwenden.

#### Maximale Anzahl von Pods

Da jedem Pod eine eigene IP-Adresse zugewiesen wird, bestimmt die Anzahl der von einem Instance-Typ unterstützten IP-Adressen die Anzahl der Pods, die auf der Instance ausgeführt werden können. Informationen zur manuellen Bestimmung, wie viele Pods ein Instance-Typ

unterstützt, finden Sie unter [the section called “Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen”](#).

 Note

Wenn Sie ein Amazon EKS-optimiertes Amazon Linux 2-AMI v20220406 oder neuer verwenden, können Sie einen neuen Instance-Typ verwenden, ohne auf das neueste AMI aktualisieren zu müssen. Für diese berechnet das AMI automatisch den erforderlichen max-pods Wert AMIs, wenn er nicht in der [eni-max-podsTXT-Datei](#) aufgeführt ist. Instance-Typen, die sich derzeit in der Vorschau befinden, werden möglicherweise von Amazon EKS standardmäßig nicht unterstützt. Werte für max-pods für solche Typen müssen noch zu eni-max-pods.txt in unserem AMI hinzugefügt werden.

[AWS Nitro System-Instance-Typen](#) unterstützen optional deutlich mehr IP-Adressen als Instance-Typen, die nicht von Nitro System stammen. Allerdings sind nicht alle IP-Adressen, die einer Instanz zugewiesen wurden, für Pods verfügbar. Um Ihren Instances eine deutlich größere Anzahl von IP-Adressen zuzuweisen, müssen Sie Version 1.9.0 oder höher des Amazon VPC CNI-Add-ons in Ihrem Cluster installiert und entsprechend konfiguriert haben. Weitere Informationen finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#). Um Ihren Instances die größte Anzahl von IP-Adressen zuzuweisen, müssen Sie Version 1.10.1 oder höher des Amazon VPC CNI-Add-ons in Ihrem Cluster installiert haben und den Cluster mit der IPv6-Familie bereitstellen.

## IP-Familie

Sie können jeden unterstützten Instanztyp verwenden, wenn Sie die IPv4 Familie für einen Cluster verwenden, sodass Ihr Cluster Ihren Pods und Services private IPv4 Adressen zuweisen kann. Wenn Sie jedoch die IPv6-Familie für Ihren Cluster verwenden möchten, müsste Sie die [AWS -Nitro-System](#)-Instance-Typen oder Bare-Metal-Instance-Typen verwenden. Nur IPv4 wird für Windows-Instances unterstützt. Ihr Cluster muss auf dem Version 1.10.1 oder höher des Amazon-VPC-CNI-Add-ons ausgeführt wird. Weitere Informationen zur Verwendung von IPv6 finden Sie unter [the section called “IPv6”](#).

## Version des Amazon VPC CNI-Add-ons, das Sie ausführen

Die aktuelle Version des [Amazon-CNI-Plugins für Kubernetes](#) unterstützt [diese Instance-Typen](#). Möglicherweise müssen Sie Ihre Amazon VPC-CNI-Add-on-Version aktualisieren, um die Vorteile der neuesten unterstützten Instance-Typen zu nutzen. Weitere Informationen finden Sie unter [the section called “Amazon VPC CNI”](#). Die neueste Version unterstützt die neuesten Features

für die Verwendung mit Amazon EKS. Frühere Versionen unterstützen nicht alle Funktionen. Sie können die von verschiedenen Versionen unterstützten Features im [Änderungsverlauf](#) auf GitHub anzeigen.

AWS Region, in der Sie Ihre Knoten erstellen

Nicht alle Instance-Typen sind in allen AWS Regionen verfügbar.

Ob Sie Sicherheitsgruppen für Pods verwenden

Wenn Sie Sicherheitsgruppen für Pods verwenden, werden nur bestimmte Instanztypen unterstützt. Weitere Informationen finden Sie unter [the section called “Sicherheitsgruppen für Pods”](#).

## Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen

Da jedem Pod eine eigene IP-Adresse zugewiesen wird, ist die Anzahl der von einem Instance-Typ unterstützten IP-Adressen ein Faktor bei der Bestimmung der Anzahl der Pods, die auf der Instance ausgeführt werden können. Amazon EKS stellt ein Skript bereit, das Sie herunterladen und ausführen können, um die von Amazon EKS empfohlene maximale Anzahl von Pods zur Ausführung auf jedem Instance-Typ zu bestimmen. Das Skript verwendet Hardwareattribute jeder Instance und Konfigurationsoptionen, um die maximale Pod-Anzahl zu bestimmen. Sie können die in diesen Schritten zurückgegebene Zahl verwenden, um Funktionen wie die [Zuweisung von IP-Adressen zu Pods aus einem anderen Subnetz als dem der Instance und die deutliche Erhöhung der Anzahl der IP-Adressen für Ihre](#) Instance zu aktivieren. Wenn Sie eine verwaltete Knotengruppe mit mehreren Instance-Typen verwenden, verwenden Sie einen Wert, der für alle Instance-Typen funktioniert.

1. Laden Sie ein Skript herunter, mit dem Sie die maximale Anzahl von Pods für jeden Instance-Typ berechnen können.

```
curl -O https://raw.githubusercontent.com/awslabs/amazon-eks-ami/master/templates/a12/runtime/max-pods-calculator.sh
```

2. Markieren Sie das Skript auf Ihrem Computer als ausführbar.

```
chmod +x max-pods-calculator.sh
```

3. Führen Sie das Skript aus und ersetzen Sie *m5.large* durch den Instance-Typ, den Sie bereitstellen möchten, und *1.9.0-eksbuild.1* durch Ihre Amazon-VPC-CNI-Add-on-Version.



Informationen zur Bestimmung Ihrer Add-On-Version finden Sie in den Aktualisierungsverfahren unter [Zuweisen IPs zu Pods mit der Amazon VPC CNI](#).

```
./max-pods-calculator.sh --instance-type m5.large --cni-version 1.9.0-eksbuild.1
```

Eine Beispielausgabe sieht wie folgt aus.

29

Sie können dem Skript die folgenden Optionen hinzufügen, um die maximal unterstützten Pods anzuzeigen, wenn optionale Funktionen verwendet werden.

- `--cni-custom-networking-enabled`— Verwenden Sie diese Option, wenn Sie IP-Adressen aus einem anderen Subnetz als dem Ihrer Instance zuweisen möchten. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Netzwerke”](#). Das Hinzufügen dieser Option zum vorherigen Skript mit denselben Beispielwerten ergibt 20.
- `--cni-prefix-delegation-enabled` – Verwenden Sie diese Option, wenn Sie jeder Elastic-Network-Schnittstelle deutlich mehr IP-Adressen zuweisen möchten. Diese Funktion erfordert eine Amazon Linux-Instance, die auf dem Nitro System und der Version 1.9.0 oder höher des Amazon VPC CNI-Add-ons ausgeführt wird. Weitere Informationen finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#). Das Hinzufügen dieser Option zum vorherigen Skript mit denselben Beispielwerten ergibt 110.

Sie können das Skript auch mit der Option `--help` ausführen, um alle verfügbaren Optionen anzuzeigen.

#### Note

Das Rechnerskript „Max Pods“ begrenzt den Rückgabewert 110 auf die [Skalierbarkeitsgrenzwerte von Kubernetes](#) und die empfohlenen Einstellungen. Wenn Ihr Instance-Typ mehr als 30 V hat CPUs, springt dieses Limit auf eine Zahl 250, die auf internen Tests des Amazon EKS-Skalierbarkeitsteams basiert. Weitere Informationen finden Sie im Blogbeitrag [Amazon VPC CNI plugin increases pods per node limits](#) (VPC-CNI-Plugin von Amazon erhöht Grenzwerte für Pods pro Knoten).

## Überlegungen zum automatischen EKS-Modus

Der automatische EKS-Modus begrenzt die Anzahl der Pods auf Knoten auf den folgenden Wert:

- Hardcap für 110 Pods
- Das Ergebnis der oben beschriebenen Berechnung der maximalen Anzahl an Pods.

## Erstellen Sie Knoten mit vorgefertigten optimierten Images

Sie können Knoten mit vordefinierten Amazon EKS-optimierten [Amazon Machine Images](#) (AMIs) oder Ihren eigenen benutzerdefinierten, AMIs wenn Sie verwaltete Knotengruppen oder selbstverwaltete Knoten verwenden, bereitstellen. Wenn Sie Hybridknoten ausführen, finden Sie weitere Informationen unter [the section called “Bereiten Sie das Betriebssystem vor”](#) Informationen über die einzelnen Typen von Amazon-EKS-optimierten AMIs finden Sie in den folgenden Themen. Anweisungen zum Erstellen eines eigenen benutzerdefinierten AMI finden Sie unter [the section called “Maßgeschneiderte Builds”](#).

Im Amazon EKS Auto Mode verwaltet EKS die EC2 Instance, einschließlich der Auswahl und Aktualisierung des AMI.

### Themen

- [Leitfaden zu den Funktionen von EKS AL2 und AL2 -Accelerated AMIs Transition](#)
- [Knoten mit optimiertem Amazon Linux erstellen AMIs](#)
- [Erstellen Sie Knoten mit optimiertem Bottlerocket AMIs](#)
- [Erstellen Sie Knoten mit optimiertem Ubuntu Linux AMIs](#)
- [Knoten mit optimiertem Windows erstellen AMIs](#)

## Leitfaden zu den Funktionen von EKS AL2 und AL2 -Accelerated AMIs Transition

AWS wird den Support für EKS AL2 — optimiert und AL2 beschleunigt — mit Wirkung zum 26. AMIs November 2025 beenden. Sie können EKS zwar auch AL2 AMIs nach dem end-of-support (EOS-) Datum (26. November 2025) weiter verwenden, nach diesem Datum wird EKS jedoch keine neuen Kubernetes-Versionen oder Updates mehr veröffentlichen AL2 AMIs, einschließlich kleinerer Releases, Patches und Bugfixes. Wir empfehlen ein Upgrade auf Amazon Linux 2023 (AL2023) oder AMIs Bottlerocket:

- AL2023 ermöglicht einen secure-by-default Ansatz mit vorkonfigurierten Sicherheitsrichtlinien SELinux im permissiven Modus, standardmäßig aktiviertem IMDSv2 Nur-Modus, optimierten Startzeiten und verbesserter Paketverwaltung für mehr Sicherheit und Leistung. Er eignet sich gut für Infrastrukturen, die umfangreiche Anpassungen wie direkten Zugriff auf Betriebssystemebene oder umfangreiche Knotenänderungen erfordern.
- Bottlerocket ermöglicht verbesserte Sicherheit, schnellere Startzeiten und eine kleinere Angriffsfläche für mehr Effizienz mit seinem speziell entwickelten, containeroptimierten Design, das sich gut für container-native Ansätze mit minimalen Knotenanpassungen eignet.

Alternativ können Sie [the section called “Maßgeschneiderte Builds”](#) bis zum EOS-Datum (26. November 2025) oder bis zum Amazon Linux 2 EOS-Datum (30. Juni 2026) ein benutzerdefiniertes AMI mit einer Amazon Linux 2-Basisinstanz erstellen. Weitere Informationen finden Sie unter [AL2023 FAQs](#), [Bottlerocket](#). Eine ausführliche Anleitung zur FAQs Migration finden Sie in [the section called “Führen Sie ein Upgrade auf Version AL2 023 durch”](#) unserer [the section called “Bottlerocket”](#) Dokumentation.

## Migration und Support FAQs

Wie migriere ich von meinem AL2 auf ein AL2 023 AMI?

Wir empfehlen, einen Migrationsplan zu erstellen und zu implementieren, der gründliche Anwendungs-Workload-Tests und dokumentierte Rollback-Verfahren umfasst. Folgen Sie anschließend den step-by-step Anweisungen im [Abschnitt Upgrade von Amazon Linux 2 auf Amazon Linux 2023](#) in der offiziellen EKS-Dokumentation.

Kann ich ein benutzerdefiniertes AL2 AMI nach dem EKS end-of-support (EOS) -Datum für EKS Optimized erstellen AL2 AMIs?

Wir empfehlen zwar, auf offiziell unterstütztes und veröffentlichtes EKS umzusteigen, das AMIs für AL2 023 oder Bottlerocket optimiert ist, aber Sie können benutzerdefinierte EKS erstellen, die AMIs bis zum AL2 AL2 AMI-EOS-Datum (26. November 2025) AL2 optimiert und beschleunigt sind. Alternativ können Sie bis zum Amazon Linux 2 EOS-Datum (30. Juni 2026) ein benutzerdefiniertes AMI mit einer Amazon Linux 2-Basis-Instance erstellen. step-by-stepAnweisungen zum Erstellen eines benutzerdefinierten AL2 EKS-optimierten und AL2 -beschleunigten AMI finden Sie unter [Erstellen eines benutzerdefinierten Amazon Linux-AMI](#) in der offiziellen EKS-Dokumentation.

Gilt die Richtlinie zur Unterstützung der EKS Kubernetes-Version für Amazon Linux-Distributionen?

Nein. Das EOS-Datum für EKS AL2 — optimiert und AL2 beschleunigt — AMIs ist unabhängig von den standardmäßigen und erweiterten Supportzeiten für Kubernetes-Versionen von EKS. Sie müssen zu AL2 023 oder Bottlerocket migrieren, auch wenn Sie den erweiterten EKS-Support verwenden.

Wie wirkt sich der Wechsel von cgroupv1 zu cgroupv2 auf meine Migration aus?

Die [Kubernetes-Community](#) hat den cgroupv1 Support (der von verwendet wird AL2) in den Wartungsmodus versetzt, was bedeutet, dass keine neuen Funktionen hinzugefügt werden und nur kritische Sicherheits- und größere Bugfixes bereitgestellt werden. cgroupv2Um Kubernetes einzuführen, müssen Sie die Kompatibilität zwischen Betriebssystem, Kernel, Container-Laufzeit und Kubernetes-Komponenten sicherstellen. Dies erfordert eine cgroupv2 standardmäßig aktivierte Linux-Distribution wie AL2 023, Bottlerocket, Red Hat Enterprise Linux (RHEL) 9+, Ubuntu 22.04+ oder Debian 11+. Diese Distributionen werden mit den Kernelversionen  $\geq 5.8$  ausgeliefert. Dies ist die Mindestanforderung für die Unterstützung in Kubernetes. cgroupv2 [Weitere Informationen finden Sie unter Über cgroup v2.](#)

Was mache ich, wenn ich Neuron in meinem benutzerdefinierten AL2 AMI benötige?

Sie können Ihre vollständigen Neuron-gestützten Anwendungen nicht nativ auf einem Based ausführen. AL2 AMIs Um AWS Neuron auf einem AL2 AMI zu nutzen, müssen Sie Ihre Anwendungen mithilfe eines von NEURON unterstützten Containers mit einer AL2 Nicht-Linux-Distribution (z. B. Ubuntu 22.04, Amazon Linux 2023 usw.) containerisieren und diese Container dann auf einem AL2 basierten AMI bereitstellen, auf dem der Neuron Driver () installiert ist. `aws-neuronx-dkms`

## Kompatibilität und Versionen

### Unterstützte Kubernetes-Versionen für AL2 AMIs

Kubernetes Version 1.32 ist die letzte Version, für die Amazon EKS veröffentlicht wird AL2 (Amazon Linux 2). AMIs Für [unterstützte](#) Kubernetes-Versionen bis 1.32 wird EKS bis zum 26. November 2025 weiterhin Releases AL2 AMIs (AL2\_ARM\_64, \_x86\_64) und -beschleunigte Versionen (AL2\_x86\_64\_GPU) veröffentlichen. AL2 AMIs AL2 Nach diesem Datum wird AL2 AL2 EKS AMIs die Veröffentlichung von -optimierten und -beschleunigten Versionen für alle Kubernetes-Versionen einstellen. Beachten Sie, dass das EOS-Datum für EKS AL2 — optimiert und AL2 beschleunigt — unabhängig von den standardmäßigen und erweiterten Supportzeiten für Kubernetes-Versionen von EKS AMIs ist.

## Vergleich der NVIDIA-Treiber für, 023 und Bottlerocket AL2 AL2 AMIs

| Driver-Branche | Amazon Linux 2-AMI | Amazon Linux 2023 AMI | Bottlerocket AMI  | End-of-Life Datum              |
|----------------|--------------------|-----------------------|-------------------|--------------------------------|
| R535           | Nicht unterstützt  | Nicht unterstützt     | Unterstützt       | <a href="#">September 2027</a> |
| R550           | Unterstützt        | Unterstützt           | Nicht unterstützt | <a href="#">April 2025</a>     |
| R560           | Nicht unterstützt  | Unterstützt           | Nicht unterstützt | <a href="#">März 2025</a>      |
| R570           | Nicht unterstützt  | Unterstützt           | Kommt bald        | <a href="#">Februar 2026</a>   |

Weitere Informationen finden Sie in der [Nvidia-Release-Dokumentation](#).

## Vergleich der NVIDIA CUDA-Versionen für AL2, AL2 023 und Bottlerocket AMIs

| CUDA-Version         | AL2 Support       | AL2023 Support    | Bottlerocket-Unterstützung |
|----------------------|-------------------|-------------------|----------------------------|
| <a href="#">10.1</a> | Unterstützt       | Nicht unterstützt | Nicht unterstützt          |
| <a href="#">11.8</a> | Unterstützt       | Unterstützt       | Unterstützt                |
| <a href="#">12,0</a> | Nicht unterstützt | Unterstützt       | Unterstützt                |
| <a href="#">12,5</a> | Nicht unterstützt | Unterstützt       | Unterstützt                |

Weitere Informationen finden Sie in der [CUDA-Release-Dokumentation](#).

## Vergleich der unterstützten Treiber und Linux-Kernel-Versionen für AL2, AL2 023 und Bottlerocket AMIs

| Komponente                         | AL2 AMI-Quelle | AL2023 AMI-Quelle | Bottlerocket AMI-Quelle |
|------------------------------------|----------------|-------------------|-------------------------|
| Basis-Betriebssystemkompatibilität | RHEL7/CentOS 7 | Fedora/CentOS 9   | N/A                     |

| Komponente         | AL2 AMI-Quelle                 | AL2023 AMI-Quelle                      | Bottlerocket AMI-Quelle                |
|--------------------|--------------------------------|----------------------------------------|----------------------------------------|
| CUDA-Toolkit       | <a href="#">CUDA 11.x—12.x</a> | <a href="#">CUDA 12,5 und höher</a>    | CUDA 11.x (12.5 kommt bald)            |
| NVIDIA-GPU-Treiber | <a href="#">R550</a>           | <a href="#">R565</a> (R570 kommt bald) | <a href="#">R535</a> (R570 kommt bald) |
| AWS Neuron-Treiber | <a href="#">2.19</a>           | <a href="#">2,19+</a>                  | 2,20                                   |
| Linux-Kernel       | <a href="#">5.10</a>           | <a href="#">6,1, 6,12</a>              | 5.15, 6.1 (6.12 kommt bald)            |

## AWS Neuronenkompatibilität mit AL2 AMIs

Ab [AWS der Neuron-Version 2.20](#) unterstützt die von EKS AL-Based verwendete Neuron Runtime (aws-neuronx-runtime-lib) Amazon Linux 2 () nicht AMIs mehr. AL2 Der Neuron-Treiber (aws-neuronx-dkms) ist jetzt das einzige AWS Neuron-Paket, das Amazon Linux 2 unterstützt. Das bedeutet, dass Sie Ihre Neuron-gestützten Anwendungen nicht nativ auf einem AL2 AMI ausführen können. [Informationen zur Einrichtung von Neuron auf AL2 023 AMIs finden Sie in der Neuron-Setup-Anleitung.AWS](#)

## Kubernetes-Kompatibilität mit AL2 AMIs

Die Kubernetes-Community hat den cgroupv1 Support (verwendet von AL2) in den Wartungsmodus versetzt. Das bedeutet, dass keine neuen Funktionen hinzugefügt werden und nur kritische Sicherheits- und größere Bugfixes bereitgestellt werden. Alle Kubernetes-Funktionen, die auf cgroupv2 basieren, wie MemoryQoS und erweiterte Ressourcenisolierung, sind auf nicht verfügbar. AL2 Darüber hinaus war Amazon EKS Kubernetes Version 1.32 die letzte Version, die unterstützt wurde. AL2 AMIs Um die Kompatibilität mit den neuesten Kubernetes-Versionen aufrechtzuerhalten, empfehlen wir die Migration zu AL2 023 oder Bottlerocket, die standardmäßig aktiviert sind.

cgroupv2

## Kompatibilität der Linux-Version mit AL2 AMIs

Amazon Linux 2 (AL2) wird AWS bis zu seinem end-of-support (EOS) Datum am 30. Juni 2026 unterstützt. Mit zunehmendem Alter AL2 wurde der Support für neue Anwendungen und Funktionen durch die breitere Linux-Community jedoch immer eingeschränkter. AL2 AMIs basieren auf dem

[Linux-Kernel 5.10](#), während AL2 023 den [Linux-Kernel](#) 6.10 verwendet. Im Gegensatz zu AL2 023 wird es von der AL2 breiteren Linux-Community nur begrenzt unterstützt. Das bedeutet, dass viele Upstream-Linux-Pakete und -Tools zurückportiert werden müssen, um mit AL2 der älteren Kernel-Version zu arbeiten, einige moderne Linux-Funktionen und Sicherheitsverbesserungen sind aufgrund des älteren Kernels nicht verfügbar, und viele Open-Source-Projekte unterstützen ältere Kernelversionen wie 5.10 nicht mehr oder nur eingeschränkt.

Veraltete Pakete, die nicht in 0.23 enthalten sind AL2

Zu den gängigsten Paketen, die nicht enthalten sind oder die in Version AL2 023 geändert wurden, gehören:

- Einige [Quell-Binärpakete in Amazon Linux 2](#) sind in Amazon Linux 2023 nicht mehr verfügbar
- Änderungen in der Art und Weise, wie Amazon Linux verschiedene Versionen von Paketen (z. B. [amazon-linux-extras System](#)) in AL2 023 unterstützt
- [Zusätzliche Pakete für Enterprise Linux \(EPEL\) werden in Version](#) 023 nicht unterstützt AL2
- [32-Bit-Anwendungen](#) werden in 023 nicht unterstützt AL2
- AL2023 erstellt keine [Mate-Desktop-Pakete](#)

Weitere Informationen finden Sie unter Comparing und 023. [AL2 AL2](#)

Vergleich der FIPS-Validierung zwischen AL2 023 AL2 und Bottlerocket

Amazon Linux 2 (AL2), Amazon Linux 2023 (AL2023) und Bottlerocket unterstützen die Einhaltung der Federal Information Processing Standards (FIPS).

- AL2 ist nach FIPS 140-2 zertifiziert und 023 ist nach FIPS 140-3 zertifiziert. AL2 Um den FIPS-Modus auf AL2 023 zu aktivieren, installieren Sie die erforderlichen Pakete auf Ihrer EC2 Amazon-Instance und befolgen Sie die Konfigurationsschritte anhand der Anweisungen unter [FIPS-Modus aktivieren](#) auf 023. AL2 [Weitere Informationen finden Sie unter 023. AL2 FAQs](#)
- Bottlerocket bietet speziell für FIPS entwickelte Varianten, die die Kernel- und Userspace-Komponenten auf die Verwendung von kryptografischen Modulen beschränken, die beim FIPS 140-3 Cryptographic Module Validation Program eingereicht wurden.

EKS AMI-Treiber und Versionsänderungsprotokoll

Eine vollständige Liste aller EKS AMI-Komponenten und ihrer Versionen finden Sie in den [Amazon EKS AMI-Versionshinweisen](#) unter GitHub.

## Knoten mit optimiertem Amazon Linux erstellen AMIs

Das für Amazon EKS optimierte Amazon Linux AMIs basiert auf Amazon Linux 2 (AL2) und Amazon Linux 2023 (AL2023). Sie sind so konfiguriert, dass sie als Basis-Images für Amazon EKS-Knoten dienen. Sie AMIs sind für die Verwendung mit Amazon EKS konfiguriert und enthalten die folgenden Komponenten:

- kubelet
- AWS IAM-Authentifikator
- containerd

### Note

- Sie können Sicherheits- oder Datenschutzereignisse für Amazon Linux im [Amazon Linux-Sicherheitszentrum](#) verfolgen, indem Sie den Tab für Ihre gewünschte Version auswählen. Sie können auch den entsprechenden RSS-Feed abonnieren. Sicherheits- oder Datenschutzereignisse enthalten eine Übersicht über das Problem, welche Pakete betroffen sind und wie Sie Ihre Instances aktualisieren, um das Problem zu beheben.
- Bevor Sie ein beschleunigtes AMI oder ein ARM-AMI bereitstellen, lesen Sie die Informationen in [Amazon EKS, optimiertes, beschleunigtes Amazon Linux AMIs](#) und [the section called "Amazon EKS-optimierter Arm Amazon Linux AMIs"](#).
- EC2 P2Amazon-Instances werden auf Amazon EKS nicht unterstützt, da sie NVIDIA Treiberversion 470 oder früher benötigen.
- Alle neu erstellten verwalteten Knotengruppen in Clustern der Version 1.30 oder neuer verwenden automatisch standardmäßig AL2 023 als Knotenbetriebssystem. Bisher wurde für neue Knotengruppen standardmäßig die Option verwendet. AL2 Sie können ihn weiterhin verwenden, AL2 indem Sie ihn beim Erstellen einer neuen Knotengruppe als AMI-Typ auswählen.
- Amazon EKS wird AMIs nach dem 26. November 2025 kein EKS-optimiertes Amazon Linux 2 (AL2) mehr veröffentlichen. Darüber hinaus 1.32 ist die Kubernetes-Version die letzte Version, für die Amazon EKS veröffentlicht wird. AL2 AMIs 1.33Ab Version 2 wird Amazon EKS weiterhin Version AL2 023 veröffentlichen und auf Bottlerocket basieren. AMIs



## Amazon EKS hat Amazon Linux optimiert und beschleunigt AMIs

Das für Amazon EKS optimierte, beschleunigte Amazon Linux AMIs basiert auf dem standardmäßigen Amazon EKS-optimierten Amazon Linux AMIs. Sie sind so konfiguriert, dass sie als optionale Images für Amazon EKS-Knoten zur Unterstützung von GPU-, [Inferentia](#) - und [Trainium-basierten](#) Workloads dienen.

Neben der standardmäßigen, für Amazon EKS optimierten AMI-Konfiguration AMIs umfassen die beschleunigten Konfigurationen Folgendes:

- NVIDIA-Treiber
- `nvidia-container-toolkit`
- AWS Neuron-Treiber

Eine Liste der neuesten Komponenten, die in der beschleunigten Version enthalten sind AMIs, finden Sie in den `amazon-eks-ami` [Releases](#) am GitHub.

### Note

- Stellen Sie sicher, dass Sie den entsprechenden Instanztyp in Ihrer AWS CloudFormation Knotenvorlage angeben. Durch die Nutzung von Amazon EKS Optimized Accelerated AMIs stimmen Sie [der Cloud-Endbenutzer-Lizenzvereinbarung \(EULA\) von NVIDIA](#) zu.
- Die für Amazon EKS optimierten AMIs Beschleunigungen wurden zuvor als Amazon EKS bezeichnet, die AMIs mit GPU-Unterstützung optimiert wurden.
- In früheren Versionen von Amazon EKS Optimized Accelerated AMIs wurde das `nvidia-docker` Repository installiert. Das Repository ist nicht mehr im Amazon EKS-AMI Version `v20200529` und höher enthalten.

Einzelheiten zur Ausführung von Workloads auf Amazon EKS-optimiertem beschleunigtem Amazon Linux finden Sie AMIs unter [the section called “Führen Sie Linux GPU aus AMIs”](#).

## Amazon EKS-optimierter Arm Amazon Linux AMIs

Arm-Instances führen zu deutlichen Kosteneinsparungen für skalierbare und Arm-basierte Anwendungen wie Webserver, Container-Microservices, Zwischenspeicherflotten und verteilte

Datenspeicher. Beachten Sie beim Hinzufügen von Arm-Knoten zu Ihrem Cluster die folgenden Überlegungen.

- Wenn Ihr Cluster vor dem 17. August 2020 bereitgestellt wurde, müssen Sie ein einmaliges Upgrade kritischer Cluster-Add-on-Manifeste durchführen. Dies ist so, dass Kubernetes für jede Hardwarearchitektur, die in Ihrem Cluster verwendet wird, das richtige Image abrufen kann. Weitere Informationen zum Aktualisieren von Cluster-Add-ons finden Sie unter [the section called “Schritt 1: Bereiten Sie das Upgrade vor”](#). Wenn Sie Ihren Cluster am oder nach dem 17. August 2020 bereitgestellt haben, sind Ihre CoreDNS- und Amazon VPC CNI-Plug-ins für Kubernetes bereits multiarchitekturfähig. kube-proxy
- Anwendungen, die auf Arm-Knoten bereitgestellt werden, müssen für Arm kompiliert werden.
- Wenn Sie DaemonSets diese in einem vorhandenen Cluster bereitgestellt haben oder sie in einem neuen Cluster bereitstellen möchten, in dem Sie auch ARM-Knoten bereitstellen möchten, stellen Sie sicher, dass Sie auf allen Hardwarearchitekturen in Ihrem Cluster ausgeführt DaemonSet werden können.
- Sie können Arm-Knotengruppen und x86-Knotengruppen im selben Cluster ausführen. Wenn ja, sollten Sie erwägen, Container-Images mit mehreren Architekturen in einem Container-Repository wie Amazon Elastic Container Registry bereitzustellen und dann Node-Selectoren zu Ihren Manifesten hinzuzufügen, damit Kubernetes weiß, auf welcher Hardwarearchitektur ein Pod bereitgestellt werden kann. Weitere Informationen finden Sie unter [Übertragen eines Multi-Architektur-Images](#) im Amazon-ECR-Benutzerhandbuch und im Blogbeitrag [Einführung in Multi-Architektur-Container-Images für Amazon ECR](#).

## Weitere Informationen

Weitere Informationen zur Verwendung von Amazon EKS-optimiertem Amazon Linux AMIs finden Sie in den folgenden Abschnitten:

- Informationen zur Verwendung von Amazon Linux mit verwalteten Knotengruppen finden Sie unter [the section called “Verwaltete Knotengruppen”](#).
- Informationen zum Starten selbstverwalteter Amazon-Linux-Knoten finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).
- Versionsinformationen finden Sie unter [the section called “Versionsinformationen abrufen”](#).
- Informationen zum Abrufen der neuesten Version IDs des für Amazon EKS optimierten Amazon Linux AMIs finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).

- Informationen zu Open-Source-Skripten, die zur Erstellung der Amazon EKS-optimierten Version verwendet werden AMIs, finden Sie unter [the section called “Maßgeschneiderte Builds”](#).

## Upgrade von Amazon Linux 2 auf Amazon Linux 2023

Die für Amazon EKS optimierten AMIs Produkte sind in zwei Familien erhältlich, die auf AL2 und AL2 023 basieren. AL2023 ist ein neues Linux-basiertes Betriebssystem, das eine sichere, stabile und leistungsstarke Umgebung für Ihre Cloud-Anwendungen bietet. Es ist die nächste Generation von Amazon Linux von Amazon Web Services und ist in allen unterstützten Amazon EKS-Versionen verfügbar.

AL2023 bietet mehrere Verbesserungen gegenüber AL2. Einen vollständigen Vergleich finden Sie unter [AL2 Comparing and Amazon Linux 2023](#) im Amazon Linux 2023-Benutzerhandbuch. Es wurden mehrere Pakete hinzugefügt, aktualisiert und entfernt AL2. Es wird dringend empfohlen, Ihre Anwendungen vor dem Upgrade mit AL2 023 zu testen. Eine Liste aller Paketänderungen in Version AL2 023 finden Sie unter [Paketänderungen in Amazon Linux 2023](#) in den Versionshinweisen zu Amazon Linux 2023.

Zusätzlich zu diesen Änderungen sollten Sie Folgendes beachten:

- AL2023 führt einen neuen Knoteninitialisierungsprozess `enodeadm`, der ein YAML-Konfigurationsschema verwendet. Wenn Sie selbstverwaltete Knotengruppen oder ein AMI mit einer Startvorlage verwenden, müssen Sie jetzt beim Erstellen einer neuen Knotengruppe explizit zusätzliche Cluster-Metadaten angeben. Ein [Beispiel](#) für die mindestens erforderlichen Parameter lautet wie folgt, wobei `apiServerEndpointcertificateAuthority`, und `Service` jetzt erforderlich `cidr` sind:

```

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: my-cluster
 apiServerEndpoint: https://example.com
 certificateAuthority: Y2VydG1maWNhdGVBdXR0b3JpdHk=
 cidr: 10.100.0.0/16
```

AL2In wurden die Metadaten dieser Parameter aus dem Amazon `DescribeCluster` EKS-API-Aufruf ermittelt. Mit AL2 023 hat sich dieses Verhalten geändert, da durch den zusätzlichen API-

Aufruf die Gefahr einer Drosselung bei der Skalierung großer Knoten besteht. Diese Änderung hat keine Auswirkungen auf Sie, wenn Sie verwaltete Knotengruppen ohne Startvorlage verwenden oder wenn Sie Karpenter verwenden. Weitere Informationen zu `certificateAuthority` und `Service cidr` finden Sie [DescribeCluster](#) in der Amazon EKS API-Referenz.

- Für AL2 023 wird `nodeadm` auch das Format geändert, in dem Parameter `kubelet` für jeden verwendeten [NodeConfigSpec](#) Knoten angewendet werden. In AL2, das wurde mit dem `--kubelet-extra-args` Parameter gemacht. Dies wird häufig verwendet, um Knoten Beschriftungen und Markierungen hinzuzufügen. Ein Beispiel unten zeigt, wie `maxPods` und auf `--node-labels` den Knoten angewendet wird.

```

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: test-cluster
 apiServerEndpoint: https://example.com
 certificateAuthority: Y2Vy dG lmaWNhdGV BdXRob3JpdHk=
 cidr: 10.100.0.0/16
 kubelet:
 config:
 maxPods: 110
 flags:
 - --node-labels=karpenter.sh/capacity-type=on-demand,karpenter.sh/nodepool=test
```

- Amazon VPC CNI-Version 1.16.2 oder höher ist für AL2 023 erforderlich.
- AL2023 erfordert standardmäßig IMDSv2. IMDSv2 hat mehrere Vorteile, die zur Verbesserung der Sicherheitslage beitragen. Es verwendet eine sitzungsorientierte Authentifizierungsmethode, die die Erstellung eines geheimen Tokens in einer einfachen HTTP-PUT-Anfrage erfordert, um die Sitzung zu starten. Das Token einer Sitzung kann zwischen 1 Sekunde und 6 Stunden gültig sein. Weitere Informationen zum Übergang von IMDSv1 zu IMDSv2 finden Sie unter [Umstellung auf Instance Metadata Service Version 2](#) und [Nutzen Sie alle Vorteile IMDSv2 und deaktivieren Sie Ihre IMDSv1 gesamte AWS Infrastruktur](#). Wenn Sie es verwenden möchten, können Sie dies dennoch tun IMDSv1, indem Sie die Einstellungen mithilfe der Starteigenschaften der Instanz-Metadatenoption manuell überschreiben.

 Note

Für IMDSv2 ist die Standard-Hop-Anzahl für verwaltete Knotengruppen auf 1 gesetzt. Das bedeutet, dass Container mithilfe von IMDS keinen Zugriff auf die Anmeldeinformationen des Knotens haben. Wenn Sie Container-Zugriff auf die Anmeldeinformationen des Knotens benötigen, können Sie dies trotzdem tun, indem Sie die `HttpPutResponseHopLimit` in einer [benutzerdefinierten EC2 Amazon-Startvorlage](#) manuell überschreiben und sie auf 2 erhöhen. Alternativ können Sie [Amazon EKS Pod Identity](#) verwenden, um Anmeldeinformationen bereitzustellen, anstatt IMDSv2

- AL2023 bietet die nächste Generation einheitlicher Kontrollgruppenhierarchien (`cgroupv2`). `cgroupv2` wird verwendet, um eine Container-Laufzeit zu implementieren, und `vonsystemd`. AL2023 enthält zwar immer noch Code, mit dem das System ausgeführt werden kann `cgroupv1`, dies ist jedoch keine empfohlene oder unterstützte Konfiguration. Diese Konfiguration wird in einer future Hauptversion von Amazon Linux vollständig entfernt.
- `eksctl` Für `eksctl` die Unterstützung von AL2 0.23 ist eine Version `0.176.0` oder höher erforderlich.

Für bereits bestehende verwaltete Knotengruppen können Sie entweder ein direktes Upgrade oder ein blaues/grünes Upgrade durchführen, je nachdem, wie Sie eine Startvorlage verwenden:

- Wenn Sie ein benutzerdefiniertes AMI mit einer verwalteten Knotengruppe verwenden, können Sie ein direktes Upgrade durchführen, indem Sie die AMI-ID in der Startvorlage austauschen. Sie sollten sicherstellen, dass Ihre Anwendungen und alle Benutzerdaten zuerst auf AL2 023 übertragen werden, bevor Sie diese Upgrade-Strategie durchführen.
- Wenn Sie verwaltete Knotengruppen entweder mit der Standard-Startvorlage oder mit einer benutzerdefinierten Startvorlage verwenden, die die AMI-ID nicht angibt, müssen Sie ein Upgrade durchführen. Ein blue/green strategy. A blue/green Upgrade ist in der Regel komplexer und beinhaltet die Erstellung einer völlig neuen Knotengruppe, bei der Sie AL2 023 als AMI-Typ angeben würden. Die neue Knotengruppe muss anschließend sorgfältig konfiguriert werden, um sicherzustellen, dass alle benutzerdefinierten Daten aus der AL2 Knotengruppe mit dem neuen Betriebssystem kompatibel sind. Sobald die neue Knotengruppe mit Ihren Anwendungen getestet und validiert wurde, können Pods von der alten Knotengruppe zur neuen Knotengruppe migriert werden. Sobald die Migration abgeschlossen ist, können Sie die alte Knotengruppe löschen.

Wenn Sie Karpenter verwenden und AL2 023 verwenden möchten, müssen Sie das `EC2NodeClass` `amiFamily` Feld mit 023 ändern. AL2 Standardmäßig ist Drift in Karpenter aktiviert. Das bedeutet, dass Karpenter, sobald das `amiFamily` Feld geändert wurde, Ihre Worker-Knoten automatisch auf das neueste AMI aktualisiert, sofern verfügbar.

## Amazon Linux AMI-Versionsinformationen abrufen

Für Amazon EKS optimierte Amazon Linux-Versionen AMIs werden nach Kubernetes-Version und Veröffentlichungsdatum des AMI im folgenden Format versioniert:

```
k8s_major_version.k8s_minor_version.k8s_patch_version-release_date
```

[Jede AMI-Version enthält verschiedene Versionen von Kubelet, dem Linux-Kernel und Containerd.](#)

Die beschleunigten Versionen enthalten AMIs auch verschiedene Versionen des NVIDIA-Treibers. Diese Informationen finden Sie im [Changelog](#) (Änderungsprotokoll) in GitHub.

## Rufen Sie das empfohlene Amazon Linux AMI ab IDs

Bei der Bereitstellung von Knoten können Sie eine ID für ein vorgefertigtes Amazon EKS-optimiertes Amazon Machine Image (AMI) angeben. Um eine AMI-ID abzurufen, die Ihrer gewünschten Konfiguration entspricht, fragen Sie die AWS Systems Manager Parameter Store-API ab. Durch die Verwendung dieser API entfällt die Notwendigkeit, manuell nach Amazon EKS-optimiertem AMI zu suchen IDs. Weitere Informationen finden Sie unter [GetParameter](#). Das von Ihnen verwendete [IAM-Prinzipal](#) muss über die `ssm:GetParameter`-IAM-Berechtigung zum Abrufen der Amazon EKS-optimierten AMI-Metadaten verfügen.

Sie können die Image-ID des neuesten empfohlenen Amazon EKS-optimierten Amazon Linux-AMIs mit dem folgenden Befehl abrufen, der den Unterparameter `image_id` verwendet. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:

- `<kubernetes-version>`Durch eine unterstützte [Amazon EKS-Version](#) ersetzen.
- ***ami-type*** Ersetzen Sie durch eine der folgenden Optionen. Informationen zu den Typen von EC2 Amazon-Instances finden Sie unter [EC2 Amazon-Instance-Typen](#).
  - Wird ***amazon-linux-2023/x86\_64/standard*** für Amazon Linux 2023 (AL2023) x86 -basierte Instances verwendet.
  - Wird ***amazon-linux-2023/arm64/standard*** für AL2 023 ARM-Instances verwendet, z. B. [AWS Graviton-basierte](#) Instances.

- Wird *amazon-linux-2023/x86\_64/nvidia* für die neuesten genehmigten AL2 023 x86 NVIDIA-basierten Instances verwendet.
- Wird *amazon-linux-2023/arm64/nvidia* für die neuesten genehmigten AL2 023 arm64 NVIDIA-basierten Instanzen verwendet.
- Wird *amazon-linux-2023/x86\_64/neuron* für die neuesten AL2 023 [AWS Neuron-Instanzen](#) verwendet.
- Wird *amazon-linux-2* für Amazon Linux 2 (AL2) x86 -basierte Instances verwendet.
- Wird *amazon-linux-2-arm64* für AL2 ARM-Instances wie [AWS Graviton-basierte](#) Instances verwendet.
- Wird *amazon-linux-2-gpu* für AL2 [hardwarebeschleunigte](#) Instanzen für NVIDIA-GPU-, [Inferentia](#) - und x86 [Trainium-basierte](#) Workloads verwendet.
- <region-code> Ersetzen Sie durch eine von [Amazon EKS unterstützte AWS Region](#), für die Sie die AMI-ID benötigen.

```
aws ssm get-parameter --name /aws/service/eks/optimized-ami/<kubernetes-version>/<ami-type>/recommended/image_id \
 --region <region-code> --query "Parameter.Value" --output text
```

Hier ist ein Beispielbefehl, nachdem Platzhalter ersetzt wurden.

```
aws ssm get-parameter --name /aws/service/eks/optimized-ami/1.31/amazon-
linux-2023/x86_64/standard/recommended/image_id \
 --region us-west-2 --query "Parameter.Value" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
ami-1234567890abcdef0
```

Erstellen Sie ein benutzerdefiniertes Amazon Linux AMI

#### Important

Amazon EKS wird AMIs nach dem 26. November 2025 kein EKS-optimiertes Amazon Linux 2 (AL2) mehr veröffentlichen. Darüber hinaus 1.32 ist die Kubernetes-Version die letzte

Version, für die Amazon EKS veröffentlicht wird. AL2 AMIs 1.33 Ab Version 2 wird Amazon EKS weiterhin Version AL2 023 veröffentlichen und auf Bottlerocket basieren. AMIs

Das für Amazon EKS optimierte Amazon Linux (AL) AMIs basiert auf AL2 und AL2 023 und wurde speziell für die Verwendung als Knoten in Amazon EKS-Clustern entwickelt. Amazon EKS stellt Open-Source-Build-Skripte im [Amazon EKS AMI Build Specification-Repository](#) bereit, die Sie auf folgende Weise verwenden können: \* Sehen Sie sich die Konfigurationen für `kubenet`, die Laufzeit und den AWS IAM Authenticator für Kubernetes an. \* Erstellen Sie Ihr eigenes AL-basiertes AMI von Grund auf neu.

Dieses Repository enthält das spezielle [Bootstrap-Skript und das Nodeadm-Skript](#), das beim Booten ausgeführt wird. Diese Skripts konfigurieren die Zertifikatsdaten Ihrer Instanz, den Endpunkt der Kontrollebene, den Clusternamen und mehr. Die Skripts gelten als Informationsquelle für Amazon EKS-optimierte AMI-Builds, sodass Sie dem GitHub Repository folgen können, um Änderungen an unseren zu überwachen AMIs.

### Voraussetzungen

- [Installieren Sie die AWS CLI](#)
- [Installieren Sie HashiCorp Packer v1.9.4+](#)
- [Installieren Sie GNU Make](#)

### Quickstart

Dieser Abschnitt zeigt Ihnen die Befehle zum Erstellen eines benutzerdefinierten AMI in Ihrem AWS Konto. Weitere Informationen zu den Konfigurationen, die zur Anpassung Ihres AMI verfügbar sind, finden Sie in den Vorlagenvariablen auf der [Amazon Linux 2023-Seite](#).

### Schritt 1. Richten Sie Ihre Umgebung ein

Klonen oder forken Sie das offizielle Amazon EKS AMI-Repository. Zum Beispiel:

```
git clone https://github.com/aws-labs/amazon-eks-ami.git
cd amazon-eks-ami
```

Stellen Sie sicher, dass Packer installiert ist:

```
packer --version
```



## Schritt 2. So erstellen Sie ein benutzerdefiniertes -AMI

Im Folgenden finden Sie Beispielbefehle für verschiedene benutzerdefinierte AMIs Befehle.

### Grundlegendes AL2 NVIDIA-AMI:

```
make k8s=1.31 os_distro=al2 \
 enable_accelerator=nvidia \
 nvidia_driver_major_version=560 \
 enable_efa=true
```

### Grundlegendes NVIDIA AL2 023 AMI:

```
make k8s=1.31 os_distro=al2023 \
 enable_accelerator=nvidia \
 nvidia_driver_major_version=560 \
 enable_efa=true
```

### STIG-konformes Neuron 023 AMI AL2:

```
make k8s=1.31 os_distro=al2023 \
 enable_accelerator=neuron \
 enable_fips=true \
 source_ami_id=ami-0abcd1234efgh5678 \
 kms_key_id=alias/aws-stig
```

Nachdem Sie diese Befehle ausgeführt haben, geht Packer wie folgt vor: \* Startet eine temporäre EC2 Amazon-Instance. \* Installieren Sie Kubernetes-Komponenten, -Treiber und Konfigurationen. \* Erstellen Sie das AMI in Ihrem AWS Konto.

## Schritt 3. Standardwerte anzeigen

Führen Sie den folgenden Befehl aus, um Standardwerte und zusätzliche Optionen anzuzeigen:

```
make help
```

## Erstellen Sie Knoten mit optimiertem Bottlerocket AMIs

[Bottlerocket](#) ist eine Open-Source-Linux-Distribution, die von gesponsert und unterstützt wird. AWS Bottlerocket wurde speziell für das Hosten von Container-Workloads entwickelt. Mit Bottlerocket können Sie die Verfügbarkeit containerisierter Bereitstellungen verbessern und die Betriebskosten

senken, indem Sie Updates Ihrer Container-Infrastruktur automatisieren. Bottlerocket enthält nur die für den Betrieb von Containern unverzichtbare Software, wodurch die Ressourcennutzung verbessert, Sicherheitsbedrohungen reduziert und der Verwaltungsaufwand gesenkt wird. Das Bottlerocket AMI umfasst `containerd`, `kubelet`, und AWS IAM Authenticator. [Neben verwalteten Knotengruppen und selbstverwalteten Knoten wird Bottlerocket auch von Karpenter unterstützt.](#)

## Vorteile

Die Verwendung von Bottlerocket mit Ihrem Amazon-EKS-Cluster hat die folgenden Vorteile:

- Höhere Verfügbarkeit bei niedrigeren Betriebskosten und geringerer Verwaltungskomplexität — Bottlerocket hat einen geringeren Ressourcenbedarf, kürzere Startzeiten und ist weniger anfällig für Sicherheitsbedrohungen als andere Linux-Distributionen. Der geringere Platzbedarf von Bottlerocket trägt zur Kostensenkung bei, da weniger Speicher-, Rechen- und Netzwerkressourcen benötigt werden.
- Verbesserte Sicherheit durch automatische Betriebssystemupdates – Updates für Bottlerocket werden als eine Einheit installiert, die bei Bedarf rückgängig gemacht werden kann. Dadurch wird das Risiko beschädigter oder fehlgeschlagener Updates vermieden, die das System in einen unbrauchbaren Zustand versetzen können. Mit Bottlerocket können Sicherheitsupdates automatisch installiert werden, sobald sie verfügbar sind, und das bei minimalen Unterbrechungen. Bei Ausfällen können sie rückgängig gemacht werden.
- Premium-Support — AWS sofern Versionen von Bottlerocket auf Amazon EC2 verfügbar sind, fallen unter dieselben AWS Support-Pläne, die auch AWS Services wie Amazon EC2, Amazon EKS und Amazon ECR abdecken.

## Überlegungen

Beachten Sie Folgendes, wenn Sie Bottlerocket für Ihren AMI-Typ verwenden:

- Bottlerocket unterstützt EC2 Amazon-Instances mit x86\_64 und Prozessoren. arm64 Das Bottlerocket AMI wird nicht für die Verwendung mit EC2 Amazon-Instances mit einem Inferentia-Chip empfohlen.
- Bottlerocket-Images enthalten weder einen SSH-Server noch eine Shell. Sie können out-of-band Zugriffsmethoden verwenden, um SSH zuzulassen. Diese Ansätze ermöglichen es dem Administrator-Container, einige Bootstrapping-Konfigurationsschritte mit Benutzerdaten zu übergeben. Weitere Informationen finden Sie in den folgenden Abschnitten von [Bottlerocket](#) OS unter: GitHub

- [Exploration](#) (Erkundung)
- [Administrator-Container](#)
- [Kubernetes-Einstellungen](#)
- Bottlerocket verwendet verschiedene Containertypen:
  - Standardmäßig ist ein [Steuerungs-Container](#) aktiviert. In diesem Container wird der [AWS Systems Manager Manager-Agent](#) ausgeführt, mit dem Sie Befehle ausführen oder Shell-Sitzungen auf Amazon EC2 Bottlerocket-Instances starten können. Weitere Informationen finden Sie unter [Setting up Session Manager](#) im AWS Systems Manager Manager-Benutzerhandbuch.
  - Wenn bei der Erstellung der Knotengruppe ein SSH-Schlüssel angegeben wird, wird ein Admin-Container aktiviert. Wir empfehlen, den Administrator-Container nur für Entwicklungs- und Testszenarien zu verwenden. Es wird nicht empfohlen, es für Produktionsumgebungen zu verwenden. Weitere Informationen finden Sie unter [Administrator-Container](#) auf GitHub.

## Weitere Informationen

Weitere Informationen zur Verwendung des für Amazon EKS optimierten Bottlerocket AMIs finden Sie in den folgenden Abschnitten:

- [Einzelheiten zu Bottlerocket finden Sie in der Bottlerocket-Dokumentation.](#)
- Ressourcen zu Versionsinformationen finden Sie unter. [the section called “Versionsinformationen abrufen”](#)
- Informationen zur Verwendung von Bottlerocket mit verwalteten Knotengruppen finden Sie unter. [the section called “Verwaltete Knotengruppen”](#)
- Informationen zum Starten von selbstverwalteten Bottlerocket-Knoten finden Sie unter. [the section called “Bottlerocket”](#)
- Informationen zum Abrufen der neuesten Version IDs des für Amazon EKS optimierten Bottlerocket AMIs finden Sie unter. [the section called “Holen Sie sich die neuesten IDs”](#)
- Einzelheiten zur Compliance-Unterstützung finden Sie unter [the section called “Compliance-Unterstützung”](#).

## Bottlerocket AMI-Versionsinformationen abrufen

[Jede Bottlerocket-AMI-Version enthält verschiedene Versionen von Kubelet, dem Bottlerocket-Kernel und Containerd.](#) Zu den beschleunigten AMI-Varianten gehören auch verschiedene Versionen

des NVIDIA-Treibers. Sie finden diese Versionsinformationen im Thema [Betriebssystem](#) der Bottlerocket-Dokumentation. Navigieren Sie von dieser Seite aus zum entsprechenden Unterthema Versionsinformationen.

Die Bottlerocket-Dokumentation kann manchmal hinter den Versionen zurückbleiben, die auf verfügbar sind. GitHub [Eine Liste der Änderungen für die neuesten Versionen finden Sie in den Versionen unter](#). GitHub

## Rufen Sie das empfohlene Bottlerocket-AMI ab IDs

Bei der Bereitstellung von Knoten können Sie eine ID für ein vorgefertigtes Amazon EKS-optimiertes Amazon Machine Image (AMI) angeben. Um eine AMI-ID abzurufen, die Ihrer gewünschten Konfiguration entspricht, fragen Sie die AWS Systems Manager Parameter Store-API ab. Durch die Verwendung dieser API entfällt die Notwendigkeit, manuell nach Amazon EKS-optimiertem AMI zu suchen IDs. Weitere Informationen finden Sie unter [GetParameter](#). Das von Ihnen verwendete [IAM-Prinzipal](#) muss über die `ssm:GetParameter`-IAM-Berechtigung zum Abrufen der Amazon EKS-optimierten AMI-Metadaten verfügen.

Sie können die Image-ID des neuesten empfohlenen Amazon EKS-optimierten Bottlerocket-AMIs mit dem folgenden AWS CLI-Befehl abrufen, der den Unterparameter verwendet. `image_id` Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:

- *kubernetes-version* Durch eine unterstützte [Amazon EKS-Version](#) ersetzen.
- *-flavor* Ersetzen Sie durch eine der folgenden Optionen.
  - *-flavor* Bei Varianten ohne GPU entfernen.
  - Wird *-nvidia* für GPU-fähige Varianten verwendet.
  - Wird *-fips* für FIPS-fähige Varianten verwendet.
- Ersetzen Sie *architecture* durch eine der folgenden Optionen.
  - Wird *x86\_64* für x86 basierte Instances verwendet.
  - *arm64* Für ARM-Instanzen verwenden.
- *region-code* Ersetzen Sie durch eine von [Amazon EKS unterstützte AWS Region](#), für die Sie die AMI-ID benötigen.

```
aws ssm get-parameter --name /aws/service/bottlerocket/aws-k8s-kubernetes-version-flavor/architecture/latest/image_id \
```

```
--region region-code --query "Parameter.Value" --output text
```

Hier ist ein Beispielbefehl, nachdem Platzhalter ersetzt wurden.

```
aws ssm get-parameter --name /aws/service/bottlerocket/aws-k8s-1.31/x86_64/latest/
image_id \
--region us-west-2 --query "Parameter.Value" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
ami-1234567890abcdef0
```

## Erfüllen Sie die Compliance-Anforderungen mit Bottlerocket

Bottlerocket entspricht den Empfehlungen verschiedener Organisationen:

- Für Bottlerocket ist ein [CIS-Benchmark](#) definiert. In einer Standardkonfiguration verfügt das Bottlerocket-Image über die meisten Steuerelemente, die für das CIS Level 1-Konfigurationsprofil erforderlich sind. Sie können die für ein CIS-Level-2-Konfigurationsprofil erforderlichen Steuerungen implementieren. Weitere Informationen finden Sie im Blog unter [Validierung des für Amazon EKS optimierten Bottlerocket-AMI anhand des CIS-Benchmarks](#). AWS
- Der optimierte Funktionsumfang und die reduzierte Angriffsfläche bedeuten, dass Bottlerocket-Instances weniger Konfiguration benötigen, um die PCI-DSS-Anforderungen zu erfüllen. Der [CIS Benchmark for Bottlerocket](#) ist eine hervorragende Informationsquelle für Sicherheitslösungen und unterstützt Ihre Anforderungen an sichere Konfigurationsstandards gemäß PCI DSS-Anforderung 2.2. Sie können [Fluent Bit](#) auch nutzen, um Ihre Anforderungen an die Audit-Protokollierung auf Betriebssystemebene gemäß der PCI DSS-Anforderung 10.2 zu erfüllen. AWS veröffentlicht regelmäßig neue (gepatchte) Bottlerocket-Instanzen, um Ihnen zu helfen, die PCI DSS-Anforderungen 6.2 (für v3.2.1) und die Anforderung 6.3.3 (für v4.0) zu erfüllen.
- Bottlerocket ist eine HIPAA-fähige Funktion, die für die Verwendung mit regulierten Workloads sowohl für Amazon als auch für Amazon EKS autorisiert ist. EC2 [Weitere Informationen finden Sie unter HIPAA-Referenz für qualifizierte Dienste](#).
- Bottlerocket AMIs sind verfügbar, die für die Verwendung von FIPS 140-3-validierten kryptografischen Modulen vorkonfiguriert sind. Dazu gehören das Amazon Linux 2023 Kernel Cryptographic API Cryptographic Module und das AWS-LC Cryptographic Module. Weitere Informationen finden Sie unter [the section called "Bottlerocket FIPS AMIs"](#).

## Machen Sie Ihre Worker-Nodes FIPS-fähig mit Bottlerocket FIPS AMIs

Die Publikation 140-3 des Federal Information Processing Standard (FIPS) ist ein Regierungsstandard der Vereinigten Staaten und Kanadas, der die Sicherheitsanforderungen für kryptografische Module zum Schutz vertraulicher Informationen festlegt. Bottlerocket erleichtert die Einhaltung von FIPS, indem es mit einem FIPS-Kernel anbietet. AMIs

Diese AMIs sind für die Verwendung von FIPS 140-3-validierten kryptografischen Modulen vorkonfiguriert. Dazu gehören das Amazon Linux 2023 Kernel Cryptographic API Cryptographic Module und das AWS-LC Cryptographic Module.

Durch die Verwendung von Bottlerocket FIPS sind Ihre Worker-Knoten AMIs zwar „FIPS-fähig“, aber nicht automatisch „FIPS-konform“. Weitere Informationen finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

### Überlegungen

- Wenn Ihr Cluster isolierte Subnetze verwendet, ist der Amazon ECR FIPS-Endpunkt möglicherweise nicht zugänglich. Dies kann dazu führen, dass der Knoten-Bootstrap fehlschlägt. Stellen Sie sicher, dass Ihre Netzwerkkonfiguration den Zugriff auf die erforderlichen FIPS-Endpunkte ermöglicht. Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter [Zugreifen auf eine Ressource über einen VPC-Endpunkt](#) für Ressourcen.
- Wenn Ihr Cluster ein Subnetz mit verwendet [PrivateLink](#), schlagen Image-Pulls fehl, weil Amazon ECR FIPS-Endpunkte nicht über verfügbar sind. PrivateLink

Erstellen Sie eine verwaltete Knotengruppe mit einem Bottlerocket FIPS AMI

Das Bottlerocket FIPS AMI ist in zwei Varianten erhältlich, um Ihre Workloads zu unterstützen:

- BOTTLEROCKET\_x86\_64\_FIPS
- BOTTLEROCKET\_ARM\_64\_FIPS

Um eine verwaltete Knotengruppe mit einem Bottlerocket FIPS-AMI zu erstellen, wählen Sie während des Erstellungsprozesses den entsprechenden AMI-Typ aus. Weitere Informationen finden Sie unter [the section called “Erstellen”](#).

Weitere Informationen zur Auswahl von FIPS-fähigen Varianten finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#)

## Deaktivieren Sie den FIPS-Endpunkt für nicht unterstützte Regionen AWS

Bottlerocket FIPS AMIs werden in den Vereinigten Staaten, einschließlich AWS GovCloud (US-) Regionen, direkt unterstützt. AWS In Regionen, in denen sie verfügbar AMIs sind, aber nicht direkt unterstützt werden, können Sie sie trotzdem verwenden, AMIs indem Sie eine verwaltete Knotengruppe mit einer Startvorlage erstellen.

Das Bottlerocket FIPS AMI stützt sich beim Bootstrap auf den Amazon ECR FIPS-Endpunkt, der außerhalb der Vereinigten Staaten nicht allgemein verfügbar ist. Um das AMI für seinen FIPS-Kernel in AWS Regionen zu verwenden, in denen der Amazon ECR-FIPS-Endpunkt nicht verfügbar ist, gehen Sie wie folgt vor, um den FIPS-Endpunkt zu deaktivieren:

1. Erstellen Sie eine neue Konfigurationsdatei mit dem folgenden Inhalt oder integrieren Sie den Inhalt in Ihre bestehende Konfigurationsdatei.

```
[default]
use_fips_endpoint=false
```

1. Kodieren Sie den Dateiinhalt im Base64-Format.
2. Fügen Sie in Ihren Startvorlagen die UserData folgende kodierte Zeichenfolge im TOML-Format hinzu:

```
[settings.aws]
config = "<your-base64-encoded-string>"
```

[Weitere Einstellungen finden Sie in der Beschreibung der Einstellungen von Bottlerocket unter GitHub](#)

Hier ist ein Beispiel für eine UserData Startvorlage:

```
[settings]
motd = "Hello from eksctl!"
[settings.aws]
config = "W2RlZmF1bHRdCnVzZV9maXBzX2VuZHBvaW50PWZhbnHNlCg==" # Base64-encoded string.
[settings.kubernetes]
api-server = "<api-server-endpoint>"
cluster-certificate = "<cluster-certificate-authority>"
cluster-name = "<cluster-name>"
```

```
...<other-settings>
```

Weitere Informationen zum Erstellen einer Startvorlage mit Benutzerdaten finden Sie unter [the section called “Startvorlagen”](#).

## Erstellen Sie Knoten mit optimiertem Ubuntu Linux AMIs

Canonical hat sich mit Amazon EKS zusammengetan, um Knoten zu erstellen AMIs , die Sie in Ihren Clustern verwenden können.

[Canonical](#) liefert ein built-for-purpose Kubernetes Node OS-Image. Dieses minimierte Ubuntu-Image ist für Amazon EKS optimiert und enthält den benutzerdefinierten AWS Kernel, der gemeinsam mit AWS entwickelt wurde. Weitere Informationen finden Sie unter [Ubuntu auf Amazon Elastic Kubernetes Service \(EKS\)](#) und. [the section called “Ubuntu Linux”](#) Informationen zum Support finden Sie im Abschnitt [Drittanbieter-Software](#) des AWS Premium-Supports FAQs.

## Knoten mit optimiertem Windows erstellen AMIs

Windows Amazon EKS Optimized AMIs basiert auf Windows Server 2019 und Windows Server 2022. Sie sind so konfiguriert, dass sie als Basis-Image für Amazon-EKS-Knoten dienen. Standardmäßig AMIs enthalten sie die folgenden Komponenten:

- [Kubelet](#)
- [kube-proxy](#)
- [AWS IAM-Authentifikator für Kubernetes](#)
- [CSI-Proxy](#)
- [containerd](#)

### Note

Sie können Sicherheits- oder Datenschutzereignisse für Windows Server mit dem [Microsoft Security Update Guide](#) verfolgen.

Amazon EKS-Angebote AMIs , die für Windows-Container optimiert sind, gibt es in den folgenden Varianten:

- Amazon-EKS-optimierte Windows-Server-2019-Core-AMI



- Amazon-EKS-optimierte Windows-Server-2019-Full-AMI
- Amazon EKS-optimiertes Windows Server 2022 Core-AMI
- Vollständiges AMI für Amazon EKS für Windows Server 2022

### Important

- Das Amazon EKS-optimierte Windows Server 20H2 Core AMI ist veraltet. Es werden keine neuen Versionen dieses AMI veröffentlicht.
- Um sicherzustellen, dass Sie standardmäßig über die neuesten Sicherheitsupdates verfügen, hat Amazon EKS AMIs Windows in den letzten 4 Monaten optimiert. Jedes neue AMI wird ab dem Zeitpunkt der ersten Veröffentlichung für 4 Monate verfügbar sein. Nach Ablauf dieses Zeitraums AMIs werden ältere Dateien als privat eingestuft und sind nicht mehr zugänglich. Wir empfehlen, die neuesten Versionen AMIs zu verwenden, um Sicherheitslücken zu vermeiden und den Zugriff auf ältere Versionen zu vermeiden AMIs , die das Ende ihrer unterstützten Lebensdauer erreicht haben. Wir können zwar nicht garantieren, dass wir Zugriff auf privat gemachte AMIs Inhalte gewähren können, aber du kannst den Zugriff beantragen, indem du ein Ticket beim AWS Support einreichst.

## Veröffentlichungskalender

In der folgenden Tabelle sind die Veröffentlichungs- und Daten für das Ende der Unterstützung für Windows-Versionen auf Amazon EKS aufgeführt. Wenn ein Enddatum leer ist, liegt das daran, dass die Version weiterhin unterstützt wird.

| Windows-Version          | Amazon-EKS-Version | Ende der Unterstützung für Amazon EKS |
|--------------------------|--------------------|---------------------------------------|
| Windows Server 2022 Kern | 17.10.2022         |                                       |
| Windows Server 2022 Voll | 17.10.2022         |                                       |
| Windows Server 20H2 Core | 12.8.2021          | 9.8.2022                              |
| Windows Server 2004 Core | 19.8.2020          | 14.12.2021                            |
| Windows Server 2019 Kern | 7.10.2019          |                                       |

| Windows-Version          | Amazon-EKS-Version | Ende der Unterstützung für Amazon EKS |
|--------------------------|--------------------|---------------------------------------|
| Windows Server 2019 Full | 7.10.2019          |                                       |
| Windows Server 1909 Core | 7.10.2019          | 8.12.2020                             |

## Bootstrap-Skript-Konfigurationsparameter

Wenn Sie einen Windows-Knoten erstellen, befindet sich auf dem Knoten ein Skript, mit dem Sie verschiedene Parameter konfigurieren können. Abhängig von Ihrem Setup kann dieses Skript auf dem Knoten an einem Ort gefunden werden, der ähnlich ist wie: `C:\Program Files\Amazon\EKS\Start-EKSBootstrap.ps1`. Sie können benutzerdefinierte Parameterwerte angeben, indem Sie sie als Argumente für das Bootstrap-Skript angeben. So können Sie beispielsweise die Benutzerdaten in der Startvorlage aktualisieren. Weitere Informationen finden Sie unter [the section called “EC2 Amazon-Benutzerdaten”](#).

Das Skript enthält die folgenden Befehlszeilenparameter:

- `-EKSClusterName` - Gibt den Namen des Amazon-EKS-Clusters an, dem dieser Worker-Knoten beitreten soll.
- `-KubeletExtraArgs` - Gibt zusätzliche Argumente für `kubelet` an (optional).
- `-KubeProxyExtraArgs` - Gibt zusätzliche Argumente für `kube-proxy` an (optional).
- `-APIServerEndpoint` - Gibt den Amazon-EKS-Cluster-API-Server-Endpunkt an (optional). Nur gültig bei Verwendung mit `-Base64ClusterCA`. Umgehung des Aufrufs `Get-EKSCluster`.
- `-Base64ClusterCA` - Gibt den base64-codierten Cluster-CA-Inhalt an (optional). Nur gültig bei Verwendung mit `-APIServerEndpoint`. Umgehung des Aufrufs `Get-EKSCluster`.
- `-DNSClusterIP` - Überschreibt die IP-Adresse, die für DNS-Abfragen innerhalb des Clusters verwendet werden soll (optional). Der Standardwert ist `10.100.0.10` oder `172.20.0.10`, basierend auf der IP-Adresse der primären Schnittstelle.
- `-ServiceCIDR`— Überschreibt den IP-Adressbereich des Kubernetes-Dienstes, von dem aus Clusterdienste adressiert werden. Der Standardwert ist `172.20.0.0/16` oder `10.100.0.0/16`, basierend auf der IP-Adresse der primären Schnittstelle.
- `-ExcludedSnatCIDRs`— Eine Liste von Dateien IPv4 CIDRs, die von der Source Network Address Translation (SNAT) ausgeschlossen werden sollen. Dies bedeutet, dass die private Pod-

IP, die über VPC adressierbar ist, nicht in die IP-Adresse der primären IPv4 Adresse der Instanz ENI für ausgehenden Datenverkehr übersetzt wird. Standardmäßig wird der IPv4 CIDR der VPC für den Amazon EKS-Windows-Knoten hinzugefügt. Die Angabe CIDRs dieses Parameters schließt zusätzlich den angegebenen Parameter aus. CIDRs Weitere Informationen finden Sie unter [the section called “Ausgehender Verkehr”](#).

Zusätzlich zu den Befehlszeilenparametern können Sie auch einige Parameter für Umgebungsvariablen angeben. Wenn Sie einen Befehlszeilenparameter angeben, hat dieser Vorrang vor der jeweiligen Umgebungsvariablen. Die Umgebungsvariablen sollten als Maschinen- (oder System-) Bereich definiert werden, da das Bootstrap-Skript nur maschinenspezifische Variablen liest.

Das Skript berücksichtigt die folgenden Umgebungsvariablen:

- SERVICE\_IPV4\_CIDR – Die Definition finden Sie im ServiceCIDR-Befehlszeilenparameter.
- EXCLUDED\_SNAT\_CIDRS – Sollte eine durch Kommas getrennte Zeichenfolge sein. Die Definition finden Sie im ExcludedSnatCIDRs-Befehlszeilenparameter.

## Unterstützung gMSA gMSA-Authentifizierung

Amazon EKS Windows Pods ermöglichen verschiedene Arten der Gruppenauthentifizierung für Managed Service Account (gMSA).

- Amazon EKS unterstützt Active Directory-Domänenidentitäten für die Authentifizierung. Weitere Informationen zu domänengebundenen GmSA finden Sie im Blog unter [Windows-Authentifizierung auf Amazon EKS Windowspods](#). AWS
- Amazon EKS bietet ein Plug-in, mit dem non-domain-joined Windows-Knoten gMSA-Anmeldeinformationen mit einer portablen Benutzeridentität abrufen können. Weitere Informationen zu domainless gMSA finden Sie im Blog unter [Domainless Windows Authentication for Amazon EKS Windowspods](#). AWS

## Zwischengespeicherte Container-Images

Amazon EKS ist für Windows optimiert und AMLs hat bestimmte Container-Images für die containerd Laufzeit zwischengespeichert. Container-Images werden zwischengespeichert, wenn benutzerdefinierte Images AMLs mit von Amazon verwalteten Build-Komponenten erstellt werden. Weitere Informationen finden Sie unter [the section called “Verwenden der von Amazon verwalteten Build-Komponente”](#).

Die folgenden zwischengespeicherten Container-Images sind für die `containerd`-Laufzeit bestimmt:

- `amazonaws.com/eks/pause-windows`
- `mcr.microsoft.com/windows/nanoserver`
- `mcr.microsoft.com/windows/servercore`

## Weitere Informationen

Weitere Informationen zur Verwendung von Amazon EKS-optimiertem Windows AMIs finden Sie in den folgenden Abschnitten:

- Einzelheiten zur Ausführung von Workloads auf Amazon EKS-optimiertem beschleunigtem Windows finden Sie AMIs unter [the section called “Führen Sie Windows GPU aus AMIs”](#).
- Informationen zur Verwendung von Windows mit verwalteten Knotengruppen finden Sie unter [the section called “Verwaltete Knotengruppen”](#).
- Informationen zum Starten von selbstverwalteten Windows-Knoten finden Sie unter [the section called “Windows”](#).
- Versionsinformationen finden Sie unter [the section called “Versionsinformationen abrufen”](#).
- Informationen zum Abrufen der neuesten Version IDs des für Amazon EKS optimierten Windows AMIs finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).
- Informationen zur Verwendung von Amazon EC2 Image Builder zur Erstellung benutzerdefinierter AMIs, für Amazon EKS optimierter Windows finden Sie unter [the section called “Benutzerdefinierte Builds”](#).
- Bewährte Methoden finden Sie unter [Optimiertes Windows AMI-Management von Amazon EKS](#) im EKS Best Practices Guide.

## Erstellen Sie selbstverwaltete Windows Server 2022-Knoten mit **eksctl**

Sie können Folgendes `test-windows-2022.yaml` als Referenz für die Erstellung selbstverwalteter Windows Server 2022-Knoten verwenden. Ersetzen Sie jede *example value* durch Ihre eigenen Werte.

 Note

Sie müssen eksctl Version [0.116.0](#) oder höher verwenden, um selbstverwaltete Windows Server 2022-Knoten auszuführen.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: windows-2022-cluster
 region: region-code
 version: '1.33'

nodeGroups:
 - name: windows-ng
 instanceType: m5.2xlarge
 amiFamily: WindowsServer2022FullContainer
 volumeSize: 100
 minSize: 2
 maxSize: 3
 - name: linux-ng
 amiFamily: AmazonLinux2
 minSize: 2
 maxSize: 3
```

Die Knotengruppen können dann mit dem folgenden Befehl erstellt werden.

```
eksctl create cluster -f test-windows-2022.yaml
```

## Windows AMI-Versionsinformationen abrufen

[In diesem Thema werden Versionen des für Amazon EKS optimierten Windows AMIs und die entsprechenden Versionen von Kubelet, Containerd und csi-proxy aufgeführt.](#)

Die Amazon-EKS-optimierten AMI-Metadaten, einschließlich der AMI-ID für jede Variante, können programmgesteuert abgerufen werden. Weitere Informationen finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).

AMIs werden nach der Kubernetes-Version und dem Veröffentlichungsdatum des AMI im folgenden Format versioniert:

`k8s_major_version.k8s_minor_version-release_date`**Note**

Von Amazon EKS verwaltete Knotengruppen unterstützen die Windows-Versionen November 2022 und spätere Versionen AMIs.

Um Benachrichtigungen über alle Änderungen an der Quelldatei auf dieser speziellen Dokumentationsseite zu erhalten, können Sie die folgende URL mit einem RSS-Reader abonnieren:

<https://github.com/awsdocs/amazon-eks-user-guide/commits/mainline/latest/ug/nodes/eks-ami-versions-windows.adoc.atom>

## Amazon EKS-optimiertes Windows Server 2022 Core-AMI

In den folgenden Tabellen sind die aktuellen und früheren Versionen des für Amazon EKS optimierten Windows Server 2022 Core AMI aufgeführt.

### Example

#### Kubernetes Version 1.33

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.33-2025<br>.06.13 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |
| 1.33-2025<br>.05.17 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |

## Kubernetes-Version 1.32

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.32-2025<br>.06.13 | 1.32.5          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.32-2025<br>.05.17 | 1.32.5          | 1.7.20                | 1.2.1                 |                                                     |
| 1.32-2025<br>.04.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |
| 1.32-2025<br>.03.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |
| 1.32-2025<br>.02.18 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |
| 1.32-2025<br>.01.15 | 1.32.0          | 1.7.20                | 1.1.3                 |                                                     |

## Kubernetes-Version 1.31

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.31-2025<br>.06.13 | 1.31.9          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.31-2025<br>.05.17 | 1.31.9          | 1.7.20                | 1.2.1                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                             |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------|
| 1.31-2025<br>.04.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2025<br>.03.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2025<br>.02.15 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2025<br>.01.15 | 1.31.4          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2025<br>.01.01 | 1.31.4          | 1.7.20                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 . |
| 1.31-2024<br>.12.13 | 1.31.3          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2024<br>.11.12 | 1.31.1          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2024<br>.10.08 | 1.31.1          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2024<br>.10.01 | 1.31.1          | 1.7.20                | 1.1.3                 |                                                  |
| 1.31-2024<br>.09.10 | 1.31.0          | 1.7.20                | 1.1.3                 |                                                  |



## Kubernetes-Version 1.30

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2025<br>.06.13 | 1.30.13         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.30-2025<br>.05.17 | 1.30.13         | 1.7.20                | 1.2.1                 |                                                     |
| 1.30-2025<br>.04.14 | 1.30.9          | 1.7.20                | 1.1.3                 |                                                     |
| 1.30-2025<br>.03.14 | 1.30.9          | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.30-2025<br>.02.15 | 1.30.9          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2025<br>.01.15 | 1.30.8          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2025<br>.01.01 | 1.30.8          | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.30-2024<br>.12.11 | 1.30.7          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.11.12 | 1.30.4          | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2024<br>.10.08 | 1.30.4          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.09.10 | 1.30.2          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.08.13 | 1.30.2          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.07.10 | 1.30.2          | 1.7.14                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .    |
| 1.30-2024<br>.06.17 | 1.30.0          | 1.7.14                | 1.1.2                 | container<br>d wurde<br>auf 1.7.14<br>aktualisiert. |
| 1.30-2024<br>.05.15 | 1.30.0          | 1.6.28                | 1.1.2                 |                                                     |

## Kubernetes-Version 1.29

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.29-2025<br>.06.13 | 1.29.15         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.29-2025<br>.05.17 | 1.29.15         | 1.7.20                | 1.2.1                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.29-2025<br>.04.14 | 1.29.13         | 1.7.20                | 1.1.3                 |                                                     |
| 1.29-2025<br>.03.14 | 1.29.13         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.29-2025<br>.02.15 | 1.29.13         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2025<br>.01.15 | 1.29.12         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2025<br>.01.01 | 1.29.12         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.29-2024<br>.12.11 | 1.29.10         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2024<br>.11.12 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2024<br>.10.08 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2024<br>.09.10 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2024<br>.08.13 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.07.10 | 1.29.6          | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                                           |
| 1.29-2024<br>.06.17 | 1.29.3          | 1.7.11                | 1.1.2                 |                                                                                                                            |
| 1.29-2024<br>.05.15 | 1.29.3          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.<br>kubelet wurde<br>auf 1.29.3<br>aktualisiert.                        |
| 1.29-2024<br>.04.09 | 1.29.0          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.29-2024<br>.03.12 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                            |
| 1.29-2024<br>.02.13 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                           |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.02.06 | 1.29.0          | 1.6.25                | 1.1.2                 | Es wurde ein Fehler behoben, bei dem das Pause-Bild fälschlicherweise beim kubelet Garbage-Collection-Prozess gelöscht wurde.                                                                                                                                                  |
| 1.29-2024<br>.01.11 | 1.29.0          | 1.6.18                | 1.1.2                 | Ausgeschlossen ist das eigenständige Windows Update <a href="#">KB5034439</a> auf Windows Server 2022 Core AMIs. Die KB gilt nur für Windows-Installationen mit einer separaten WinRE-Partition, die in keinem unserer für Amazon EKS optimierten Windows AMIs enthalten sind. |

## Kubernetes Version 1.28

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.28-2025<br>.06.13 | 1.28.15         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.28-2025<br>.05.17 | 1.28.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.28-2025<br>.04.14 | 1.28.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.28-2025<br>.03.14 | 1.28.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.28-2025<br>.02.15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>.01.15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>-01-01 | 1.28.15         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.28-2024<br>.12.11 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.11.12 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.10.08 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.09.10 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.08.13 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.07.10 | 1.28.11         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                    |
| 1.28-2024<br>.06.17 | 1.28.8          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                 |
| 1.28-2024<br>.05.14 | 1.28.8          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.28.8<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.04.09 | 1.28.5          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.28-2024<br>.03.12 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2024<br>.02.13 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                                                                                        |
|---------------------|-----------------|-----------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.01.11 | 1.28.5          | 1.6.18                | 1.1.2                 | Ausgeschl<br>ossen ist das<br>eigenständige<br>Windows-<br>Update<br><a href="#">KB5034439</a><br>auf Windows<br>Server 2022<br>Core. AMIs<br>Die KB gilt nur<br>für Windows-I<br>nstallationen mit<br>einer separaten<br>WinRE-Par<br>tition, die in<br>keinem unserer<br>für Amazon<br>EKS optimierten<br>Windows AMIs<br>enthalten sind. |
| 1.28-2023<br>.12.12 | 1.28.3          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                                                                                                                                             |
| 1.28-2023<br>.11.14 | 1.28.3          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.28-2023<br>.10.19 | 1.28.2          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.28-2023<br>-09.27 | 1.28.2          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |
| 1.28-2023<br>.09.12 | 1.28.1          | 1.6.6                 | 1.1.2                 |                                                                                                                                                                                                                       |

## Kubernetes Version 1.27

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.06.13 | 1.27.16         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.05.17 | 1.27.16         | 1.7.20                | 1.2.1                 |                                                     |
| 1.27-2025<br>.04.14 | 1.27.16         | 1.7.20                | 1.1.3                 |                                                     |
| 1.27-2025<br>.03.14 | 1.27.16         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.27-2025<br>.02.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.01 | 1.27.16         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.27-2024<br>.12.11 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.11.12 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.10.08 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.09.10 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.08.13 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.07.10 | 1.27.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                                           |
| 1.27-2024<br>.06.17 | 1.27.12         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.27-2024<br>.05.14 | 1.27.12         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.27.12<br>aktualisiert.                       |
| 1.27-2024<br>.04.09 | 1.27.9          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.27-2024<br>.03.12 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2024<br>.02.13 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                                                                                        |
|---------------------|-----------------|-----------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.01.11 | 1.27.9          | 1.6.18                | 1.1.2                 | Ausgeschl<br>ossen ist das<br>eigenständige<br>Windows-<br>Update<br><a href="#">KB5034439</a><br>auf Windows<br>Server 2022<br>Core. AMIs<br>Die KB gilt nur<br>für Windows-I<br>nstallationen mit<br>einer separaten<br>WinRE-Par<br>tition, die in<br>keinem unserer<br>für Amazon<br>EKS optimierten<br>Windows AMIs<br>enthalten sind. |
| 1.27-2023<br>.12.12 | 1.27.7          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                                                                                                                                             |
| 1.27-2023<br>.11.14 | 1.27.7          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.10.19 | 1.27.6          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.27-2023<br>-09.27 | 1.27.6          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                             |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.09.12 | 1.27.4          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connector-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.27-2023<br>.08.17 | 1.27.4          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                       |
| 1.27-2023<br>.08.08 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |
| 1.27-2023<br>.07.11 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.06.20 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                       |
| 1.27-2023<br>.06.14 | 1.27.1          | 1.6.6                 | 1.1.1                 | Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt.           |
| 1.27-2023<br>.06.06 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das <a href="#">Problem #2042</a> von containerd-roadmap, das dazu führte, dass Knoten private Amazon-ECR-Images nicht abrufen konnten, wurde behoben. |
| 1.27-2023<br>.05.17 | 1.27.1          | 1.6.6                 | 1.1.1                 |                                                                                                                                                        |



## Kubernetes Version 1.26

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.26-2025<br>.05.17 | 1.26.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.26-2025<br>.04.14 | 1.26.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.26-2025<br>.03.14 | 1.26.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.26-2025<br>.02.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2025<br>.01.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.12.11 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.11.12 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.10.08 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.09.10 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.08.13 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.07.10 | 1.26.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
|                     |                 |                       |                       | CVE-2024-5321 .                                                                                                            |
| 1.26-2024<br>.06.17 | 1.26.15         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.26-2024<br>.05.14 | 1.26.15         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.15<br>aktualisiert.                       |
| 1.26-2024<br>.04.09 | 1.26.12         | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.26-2024<br>.03.12 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.02.13 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                                                                                        |
|---------------------|-----------------|-----------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2024<br>.01.11 | 1.26.12         | 1.6.18                | 1.1.2                 | Ausgeschl<br>ossen ist das<br>eigenständige<br>Windows-<br>Update<br><a href="#">KB5034439</a><br>auf Windows<br>Server 2022<br>Core. AMIs<br>Die KB gilt nur<br>für Windows-I<br>nstallationen mit<br>einer separaten<br>WinRE-Par<br>tition, die in<br>keinem unserer<br>für Amazon<br>EKS optimierten<br>Windows AMIs<br>enthalten sind. |
| 1.26-2023<br>.12.12 | 1.26.10         | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                                                                                                                                             |
| 1.26-2023<br>.11.14 | 1.26.10         | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.10.19 | 1.26.9          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.9<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                 |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.09.12 | 1.26.7          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connect- oder-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.26-2023<br>.08.17 | 1.26.7          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                           |
| 1.26-2023<br>.08.08 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |
| 1.26-2023<br>.07.11 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.06.20 | 1.26.4          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                                                       |
| 1.26-2023<br>.06.14 | 1.26.4          | 1.6.6                 | 1.1.1                 | Kubernetes wurde aktualisiert auf 1.26.4. Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                            |
|---------------------|-----------------|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.05.09 | 1.26.2          | 1.6.6                 | 1.1.1                 | Ein Fehler wurde behoben, der das Netzwerkverbindungssproblem <a href="#">#1126</a> auf Pods nach dem Neustart des Knotens verursachte. Ein neuer <a href="#">Bootstrap-Skriptkonfigurationsparameter</a> (ExcludedSnatCIDs ) wurde eingeführt. |
| 1.26-2023<br>.04.26 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |
| 1.26-2023<br>.04.11 | 1.26.2          | 1.6.6                 | 1.1.1                 | Wiederherstellungsmechanismus für kubelet und kube-proxy bei einem Serviceabsturz hinzugefügt.                                                                                                                                                  |
| 1.26-2023<br>.03.24 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |

## Amazon EKS-optimiertes Windows Server 2022 Vollständiges AMI

In den folgenden Tabellen sind die aktuellen und früheren Versionen des für Amazon EKS optimierten Windows Server 2022 Full AMI aufgeführt.

### Example

#### Kubernetes Version 1.33

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.33-2025<br>.06.13 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |
| 1.33-2025<br>.05.17 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |

#### Kubernetes-Version 1.32

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                           |
|---------------------|-----------------|-----------------------|-----------------------|------------------------------------------------|
| 1.32-2025<br>.06.13 | 1.32.5          | 1.7.27                | 1.2.1                 | Wurde aktualisi<br>ert containrd<br>auf 1.7.27 |
| 1.32-2025<br>.05.17 | 1.32.5          | 1.7.20                | 1.2.1                 |                                                |
| 1.32-2025<br>.04.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                |
| 1.32-2025<br>.03.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                |
| 1.32-2025<br>.02.18 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.32-2025<br>.01.01 | 1.32.0          | 1.7.20                | 1.1.3                 |                      |

## Kubernetes Version 1.31

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.31-2025<br>.06.13 | 1.31.9          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.31-2025<br>.05.17 | 1.31.9          | 1.7.20                | 1.2.1                 |                                                     |
| 1.31-2025<br>.04.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.03.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.02.15 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.01.15 | 1.31.4          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.01.01 | 1.31.4          | 1.7.20                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.31-2024<br>.12.13 | 1.31.3          | 1.7.20                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.31-2024<br>.11.12 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.10.08 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.10.01 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.09.10 | 1.31.0          | 1.7.20                | 1.1.3                 |                      |

### Kubernetes-Version 1.30

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2025<br>.06.13 | 1.30.13         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.30-2025<br>.05.17 | 1.30.13         | 1.7.20                | 1.2.1                 |                                                     |
| 1.30-2025<br>.04.14 | 1.30.9          | 1.7.20                | 1.1.3                 |                                                     |
| 1.30-2025<br>.03.14 | 1.30.9          | 1.7.20                | 1.1.3                 | contianer<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.30-2025<br>.02.15 | 1.30.9          | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2025<br>.01.15 | 1.30.8          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2025<br>.01.01 | 1.30.8          | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.30-2024<br>.12.11 | 1.30.7          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.11.12 | 1.30.4          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.10.08 | 1.30.4          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.09.10 | 1.30.2          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.08.13 | 1.30.2          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.07.10 | 1.30.2          | 1.7.14                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .    |
| 1.30-2024<br>.06.17 | 1.30.0          | 1.7.14                | 1.1.2                 | container<br>d wurde<br>auf 1.7.14<br>aktualisiert. |
| 1.30-2024<br>.05.15 | 1.30.0          | 1.6.28                | 1.1.2                 |                                                     |

## Kubernetes-Version 1.29

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.29-2025<br>.06.13 | 1.29.15         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.29-2025<br>.05.17 | 1.29.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.29-2025<br>.04.14 | 1.29.13         | 1.7.20                | 1.1.3                 |                                                     |
| 1.29-2025<br>.03.14 | 1.29.13         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.29-2025<br>.02.15 | 1.29.13         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2025<br>.01.15 | 1.29.12         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2025<br>.01.01 | 1.29.12         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.29-2024<br>.12.11 | 1.29.10         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2024<br>.11.12 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.10.08 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                                                                                            |
| 1.29-2024<br>.09.10 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                                                                                            |
| 1.29-2024<br>.08.13 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                                                                                            |
| 1.29-2024<br>.07.10 | 1.29.6          | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                                           |
| 1.29-2024<br>.06.17 | 1.29.3          | 1.7.11                | 1.1.2                 |                                                                                                                            |
| 1.29-2024<br>.05.15 | 1.29.3          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.<br>kubelet wurde<br>auf 1.29.3<br>aktualisiert.                        |
| 1.29-2024<br>.04.09 | 1.29.0          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                          |
|---------------------|-----------------|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.03.12 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                               |
| 1.29-2024<br>.02.13 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                               |
| 1.29-2024<br>.02.06 | 1.29.0          | 1.6.25                | 1.1.2                 | Es wurde ein Fehler behoben, bei dem das Pause-Bild fälschlicherweise beim kubelet Garbage-Collection-Prozess gelöscht wurde. |
| 1.29-2024<br>.01.09 | 1.29.0          | 1.6.18                | 1.1.2                 |                                                                                                                               |

## Kubernetes Version 1.28

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                      |
|---------------------|-----------------|-----------------------|-----------------------|-------------------------------------------|
| 1.28-2025<br>.06.13 | 1.28.15         | 1.7.27                | 1.2.1                 | containerd wurde auf 1.7.27 aktualisiert. |
| 1.28-2025<br>.05.17 | 1.28.15         | 1.7.20                | 1.2.1                 |                                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.28-2025<br>.04.14 | 1.28.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.28-2025<br>.03.14 | 1.28.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.28-2025<br>.02.15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>.01.15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>.01.01 | 1.28.15         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.28-2024<br>.12.11 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.11.12 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.10.08 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.09.10 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.08.13 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.07.10 | 1.28.11         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                                           |
| 1.28-2024<br>.06.17 | 1.28.8          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.28-2024<br>.05.14 | 1.28.8          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.28.8<br>aktualisiert.                        |
| 1.28-2024<br>.04.09 | 1.28.5          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.28-2024<br>.03.12 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2024<br>.02.13 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.01.09 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                       |
| 1.28-2023<br>.12.12 | 1.28.3          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                       |
| 1.28-2023<br>.11.14 | 1.28.3          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                      |
| 1.28-2023<br>.10.19 | 1.28.2          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.28-2023<br>-09.27 | 1.28.2          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |
| 1.28-2023<br>.09.12 | 1.28.1          | 1.6.6                 | 1.1.2                 |                                                                                                                                                                                                                       |

## Kubernetes Version 1.27

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.06.13 | 1.27.16         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.27-2025<br>.05.17 | 1.27.16         | 1.7.20                | 1.2.1                 |                                                     |
| 1.27-2025<br>.04.14 | 1.27.16         | 1.7.20                | 1.1.3                 |                                                     |
| 1.27-2025<br>.03.14 | 1.27.16         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.27-2025<br>.02.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.01 | 1.27.16         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.27-2024<br>.12.11 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.11.12 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                 |
|---------------------|-----------------|-----------------------|-----------------------|------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.10.08 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                                                                      |
| 1.27-2024<br>.09.10 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                                                                      |
| 1.27-2024<br>.08.13 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                                                                      |
| 1.27-2024<br>.07.10 | 1.27.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                     |
| 1.27-2024<br>.06.17 | 1.27.12         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                  |
| 1.27-2024<br>.05.14 | 1.27.12         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.27.12<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.04.09 | 1.27.9          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.27-2024<br>.03.12 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2024<br>.02.13 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2024<br>.01.09 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2023<br>.12.12 | 1.27.7          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2023<br>.11.14 | 1.27.7          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.10.19 | 1.27.6          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.27-2023<br>-09.27 | 1.27.6          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                             |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.09.12 | 1.27.4          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connector-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.27-2023<br>.08.17 | 1.27.4          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                       |
| 1.27-2023<br>.08.08 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |
| 1.27-2023<br>.07.11 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.06.20 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                       |
| 1.27-2023<br>.06.14 | 1.27.1          | 1.6.6                 | 1.1.1                 | Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt.           |
| 1.27-2023<br>.06.06 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das <a href="#">Problem #2042</a> von containerd-roadmap, das dazu führte, dass Knoten private Amazon-ECR-Images nicht abrufen konnten, wurde behoben. |
| 1.27-2023<br>.05.18 | 1.27.1          | 1.6.6                 | 1.1.1                 |                                                                                                                                                        |

## Kubernetes Version 1.26

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.26-2025<br>.05.17 | 1.26.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.26-2025<br>.04.14 | 1.26.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.26-2025<br>.03.14 | 1.26.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.26-2025<br>.02.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2025<br>.01.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.12.11 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.11.12 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.10.08 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.09.10 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.08.13 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.07.10 | 1.26.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für                           |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
|                     |                 |                       |                       | CVE-2024-5321 .                                                                                                            |
| 1.26-2024<br>.06.17 | 1.26.15         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.26-2024<br>.05.14 | 1.26.15         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.15<br>aktualisiert.                       |
| 1.26-2024<br>.04.09 | 1.26.12         | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.26-2024<br>.03.12 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.02.13 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.01.09 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.12.12 | 1.26.10         | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                                                                       |
| 1.26-2023<br>.11.14 | 1.26.10         | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                                                                      |
| 1.26-2023<br>.10.19 | 1.26.9          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.9<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                 |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.09.12 | 1.26.7          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connect- oder-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.26-2023<br>.08.17 | 1.26.7          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                           |
| 1.26-2023<br>.08.08 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |
| 1.26-2023<br>.07.11 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.06.20 | 1.26.4          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                                                       |
| 1.26-2023<br>.06.14 | 1.26.4          | 1.6.6                 | 1.1.1                 | Kubernetes wurde aktualisiert auf 1.26.4. Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                            |
|---------------------|-----------------|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.05.09 | 1.26.2          | 1.6.6                 | 1.1.1                 | Ein Fehler wurde behoben, der das Netzwerkverbindungssproblem <a href="#">#1126</a> auf Pods nach dem Neustart des Knotens verursachte. Ein neuer <a href="#">Bootstrap-Skriptkonfigurationsparameter</a> (ExcludedSnatCIDs ) wurde eingeführt. |
| 1.26-2023<br>.04.26 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |
| 1.26-2023<br>.04.11 | 1.26.2          | 1.6.6                 | 1.1.1                 | Wiederherstellungsmechanismus für kubelet und kube-proxy bei einem Serviceabsturz hinzugefügt.                                                                                                                                                  |
| 1.26-2023<br>.03.24 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |

## Amazon-EKS-optimierte Windows-Server-2019-Core-AMI

In den folgenden Tabellen sind die aktuellen und früheren Versionen des für Amazon EKS optimierten Windows Server 2019 Core AMI aufgeführt.

### Example

#### Kubernetes Version 1.33

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.33-2025<br>.06.13 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |
| 1.33-2025<br>.05.17 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |

#### Kubernetes-Version 1.32

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.32-2025<br>.06.13 | 1.32.5          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.32-2025<br>.05.17 | 1.32.5          | 1.7.20                | 1.2.1                 |                                                     |
| 1.32-2025<br>.04.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |
| 1.32-2025<br>.03.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.32-2025<br>.02.18 | 1.32.1          | 1.7.20                | 1.1.3                 |                      |
| 1.32-2025<br>.01.15 | 1.32.4          | 1.7.20                | 1.1.3                 |                      |

### Kubernetes-Version 1.31

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.31-2025<br>.06.13 | 1.31.9          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.31-2025<br>.05.17 | 1.31.9          | 1.7.20                | 1.2.1                 |                                                     |
| 1.31-2025<br>.04.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.03.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.02.15 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.01.15 | 1.31.4          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.01.01 | 1.31.4          | 1.7.20                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.31-2024<br>.12.13 | 1.31.3          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.11.12 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.10.08 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.10.01 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.09.10 | 1.31.0          | 1.7.20                | 1.1.3                 |                      |

### Kubernetes-Version 1.30

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2025<br>.06.13 | 1.30.13         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.30-2025<br>.05.17 | 1.30.13         | 1.7.20                | 1.2.1                 |                                                     |
| 1.30-2025<br>.04.14 | 1.30.9          | 1.7.20                | 1.1.3                 |                                                     |
| 1.30-2025<br>.03.14 | 1.30.9          | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |



| AMI-Version     | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                      |
|-----------------|-----------------|-----------------------|-----------------------|-------------------------------------------|
| 1.30-2025-02-15 | 1.30.9          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2025.01.15 | 1.30.8          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2025.01.01 | 1.30.8          | 1.7.14                | 1.1.3                 | Beinhaltet Patches für CVE-2024-9042 .    |
| 1.30-2024.12.11 | 1.30.7          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2024.11.12 | 1.30.4          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2024.10.08 | 1.30.4          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2024.09.10 | 1.30.2          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2024.08.13 | 1.30.2          | 1.7.14                | 1.1.3                 |                                           |
| 1.30-2024.07.10 | 1.30.2          | 1.7.14                | 1.1.2                 | Beinhaltet Patches für CVE-2024-5321 .    |
| 1.30-2024.06.17 | 1.30.0          | 1.7.14                | 1.1.2                 | containerd wurde auf 1.7.14 aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.30-2024<br>.05.15 | 1.30.0          | 1.6.28                | 1.1.2                 |                      |

## Kubernetes-Version 1.29

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.29-2025<br>.06.13 | 1.29.15         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.29-2025<br>.05.17 | 1.29.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.29-2025<br>.04.14 | 1.29.13         | 1.7.20                | 1.1.3                 |                                                     |
| 1.29-2025<br>.03.14 | 1.29.13         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.29-2025<br>.02.15 | 1.29.13         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2025<br>.01.15 | 1.29.12         | 1.7.14                | 1.1.3                 |                                                     |
| 1.29-2025<br>.01.01 | 1.29.12         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.12.11 | 1.29.10         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.11.12 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.10.08 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.09.10 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.08.13 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.07.10 | 1.29.6          | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                    |
| 1.29-2024<br>.06.17 | 1.29.3          | 1.7.11                | 1.1.2                 |                                                                                                     |
| 1.29-2024<br>.05.15 | 1.29.3          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.<br>kubelet wurde<br>auf 1.29.3<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                            |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.04.09 | 1.29.0          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1                                      |
| 1.29-2024<br>.03.13 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                                                                 |
| 1.29-2024<br>.02.13 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                                                                 |
| 1.29-2024<br>.02.06 | 1.29.0          | 1.6.25                | 1.1.2                 | Es wurde ein<br>Fehler behoben,<br>bei dem das<br>Pause-Bil<br>d fälschlic<br>herweise beim<br>kubelet<br>Garbage-<br>Collection<br>-Prozess<br>gelöscht wurde. |
| 1.29-2024<br>.01.09 | 1.29.0          | 1.6.18                | 1.1.2                 |                                                                                                                                                                 |

## Kubernetes Version 1.28

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.28-2025<br>.06.13 | 1.28.15         | 1.7.20                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.28-2025<br>.05.17 | 1.28.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.28-2025<br>.04.14 | 1.28.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.28-2025<br>.03.14 | 1.28.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.28-2025<br>.02.15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>-01-15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>-01-01 | 1.28.15         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.28-2024<br>.12.11 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.11.12 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.10.08 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.09.10 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.08.13 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.07.10 | 1.28.11         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                    |
| 1.28-2024<br>.06.17 | 1.28.8          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                 |
| 1.28-2024<br>.05.14 | 1.28.8          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.28.8<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.04.09 | 1.28.5          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.28-2024<br>.03.13 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2024<br>.02.13 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2024<br>.01.09 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2023<br>.12.12 | 1.28.3          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2023<br>.11.14 | 1.28.3          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.28-2023<br>.10.19 | 1.28.2          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.28-2023<br>-09.27 | 1.28.2          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |
| 1.28-2023<br>.09.12 | 1.28.1          | 1.6.6                 | 1.1.2                 |                                                                                                                                                                                                                       |

## Kubernetes Version 1.27

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.06.13 | 1.27.16         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.05.17 | 1.27.16         | 1.7.20                | 1.2.1                 |                                                     |
| 1.27-2025<br>.04.14 | 1.27.16         | 1.7.20                | 1.1.3                 |                                                     |
| 1.27-2025<br>.03.14 | 1.27.16         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.27-2025<br>.02.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.01 | 1.27.16         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.27-2024<br>.12.11 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.11.12 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.10.08 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.09.10 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.08.13 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.07.10 | 1.27.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                                           |
| 1.27-2024<br>.06.17 | 1.27.12         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.27-2024<br>.05.14 | 1.27.12         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.27.12<br>aktualisiert.                       |
| 1.27-2024<br>.04.09 | 1.27.9          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.27-2024<br>.03.13 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2024<br>.02.13 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.01.09 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                       |
| 1.27-2023<br>.12.12 | 1.27.7          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                       |
| 1.27-2023<br>.11.14 | 1.27.7          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                      |
| 1.27-2023<br>.10.19 | 1.27.6          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.27-2023<br>-09.27 | 1.27.6          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                             |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.09.12 | 1.27.4          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connector-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.27-2023<br>.08.17 | 1.27.4          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                       |
| 1.27-2023<br>.08.08 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |
| 1.27-2023<br>.07.11 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.06.20 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                       |
| 1.27-2023<br>.06.14 | 1.27.1          | 1.6.6                 | 1.1.1                 | Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt.           |
| 1.27-2023<br>.06.06 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das <a href="#">Problem #2042</a> von containerd-roadmap, das dazu führte, dass Knoten private Amazon-ECR-Images nicht abrufen konnten, wurde behoben. |
| 1.27-2023<br>.05.18 | 1.27.1          | 1.6.6                 | 1.1.1                 |                                                                                                                                                        |

## Kubernetes Version 1.26

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.26-2025<br>.05.17 | 1.26.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.26-2025<br>.04.14 | 1.26.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.26-2025<br>.03.14 | 1.26.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.26-2025<br>.02.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2025<br>.01.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.12.11 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.11.12 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.10.09 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.09.10 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.08.13 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.07.10 | 1.26.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
|                     |                 |                       |                       | CVE-2024-5321 .                                                                                                            |
| 1.26-2024<br>.06.17 | 1.26.15         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.26-2024<br>.05.14 | 1.26.15         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.15<br>aktualisiert.                       |
| 1.26-2024<br>.04.09 | 1.26.12         | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.26-2024<br>.03.13 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.02.13 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.01.09 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.12.12 | 1.26.10         | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                                                                       |
| 1.26-2023<br>.11.14 | 1.26.10         | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                                                                      |
| 1.26-2023<br>.10.19 | 1.26.9          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.9<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                 |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.09.12 | 1.26.7          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connect- oder-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.26-2023<br>.08.17 | 1.26.7          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                           |
| 1.26-2023<br>.08.08 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |
| 1.26-2023<br>.07.11 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.06.20 | 1.26.4          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                                                       |
| 1.26-2023<br>.06.14 | 1.26.4          | 1.6.6                 | 1.1.1                 | Kubernetes wurde aktualisiert auf 1.26.4. Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                            |
|---------------------|-----------------|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.05.09 | 1.26.2          | 1.6.6                 | 1.1.1                 | Ein Fehler wurde behoben, der das Netzwerkverbindungssproblem <a href="#">#1126</a> auf Pods nach dem Neustart des Knotens verursachte. Ein neuer <a href="#">Bootstrap-Skriptkonfigurationsparameter</a> (ExcludedSnatCIDs ) wurde eingeführt. |
| 1.26-2023<br>.04.26 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |
| 1.26-2023<br>.04.11 | 1.26.2          | 1.6.6                 | 1.1.1                 | Wiederherstellungsmechanismus für kubelet und kube-proxy bei einem Serviceabsturz hinzugefügt.                                                                                                                                                  |
| 1.26-2023<br>.03.24 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |

## Amazon-EKS-optimierte Windows-Server-2019-Full-AMI

In den folgenden Tabellen sind die aktuellen und früheren Versionen des für Amazon EKS optimierten Windows Server 2019 Full AMI aufgeführt.

### Example

#### Kubernetes Version 1.33

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.33-2025<br>.06.13 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |
| 1.33-2025<br>.05.17 | 1.33.1          | 1.7.27                | 1.2.1                 |                      |

#### Kubernetes-Version 1.32

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.32-2025<br>.06.13 | 1.32.5          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.32-2025<br>.05.17 | 1.32.5          | 1.7.20                | 1.2.1                 |                                                     |
| 1.32-2025<br>.04.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |
| 1.32-2025<br>.03.14 | 1.32.1          | 1.7.20                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.32-2025<br>.02.18 | 1.32.1          | 1.7.20                | 1.1.3                 |                      |
| 1.32-2025<br>.01.15 | 1.32.0          | 1.7.20                | 1.1.3                 |                      |

## Kubernetes-Version 1.31

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.31-2025<br>.06.13 | 1.31.9          | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.31-2025<br>.05.17 | 1.31.9          | 1.7.20                | 1.2.1                 |                                                     |
| 1.31-2025<br>.04.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.03.14 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.02.15 | 1.31.5          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.01.15 | 1.31.4          | 1.7.20                | 1.1.3                 |                                                     |
| 1.31-2025<br>.01.01 | 1.31.4          | 1.7.20                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise |
|---------------------|-----------------|-----------------------|-----------------------|----------------------|
| 1.31-2024<br>.12.13 | 1.31.3          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.11.12 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.10.08 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.10.01 | 1.31.1          | 1.7.20                | 1.1.3                 |                      |
| 1.31-2024<br>.09.10 | 1.31.0          | 1.7.20                | 1.1.3                 |                      |

### Kubernetes-Version 1.30

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2025<br>.06.13 | 1.30.13         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.30-2025<br>.05.17 | 1.30.13         | 1.7.20                | 1.2.1                 |                                                     |
| 1.30-2025<br>.04.14 | 1.30.9          | 1.7.20                | 1.1.3                 |                                                     |
| 1.30-2025<br>.03.14 | 1.30.9          | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.30-2025<br>.02.15 | 1.30.9          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2025<br>.01.15 | 1.30.8          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2025<br>.01.01 | 1.30.8          | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.30-2024<br>.12.11 | 1.30.7          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.11.12 | 1.30.4          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.10.08 | 1.30.4          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.09.10 | 1.30.2          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.08.13 | 1.30.2          | 1.7.14                | 1.1.3                 |                                                     |
| 1.30-2024<br>.07.10 | 1.30.2          | 1.7.14                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .    |
| 1.30-2024<br>.06.17 | 1.30.0          | 1.7.14                | 1.1.2                 | container<br>d wurde<br>auf 1.7.14<br>aktualisiert. |

| AMI-Version | Kubelet-Version | Version containerd | CSI-Proxy-Version | Versionshinweise |
|-------------|-----------------|--------------------|-------------------|------------------|
|-------------|-----------------|--------------------|-------------------|------------------|

|                 |        |        |       |  |
|-----------------|--------|--------|-------|--|
| 1.30-2024.05.15 | 1.30.0 | 1.6.28 | 1.1.2 |  |
|-----------------|--------|--------|-------|--|

Kubernetes-Version 1.29

| AMI-Version | Kubelet-Version | Version containerd | CSI-Proxy-Version | Versionshinweise |
|-------------|-----------------|--------------------|-------------------|------------------|
|-------------|-----------------|--------------------|-------------------|------------------|

|                 |         |        |       |                                           |
|-----------------|---------|--------|-------|-------------------------------------------|
| 1.29-2025.06.13 | 1.29.15 | 1.7.27 | 1.2.1 | containerd wurde auf 1.7.27 aktualisiert. |
|-----------------|---------|--------|-------|-------------------------------------------|

|                 |         |        |       |  |
|-----------------|---------|--------|-------|--|
| 1.29-2025.05.17 | 1.29.15 | 1.7.20 | 1.2.1 |  |
|-----------------|---------|--------|-------|--|

|                 |         |        |       |  |
|-----------------|---------|--------|-------|--|
| 1.29-2025.04.14 | 1.29.13 | 1.7.20 | 1.1.3 |  |
|-----------------|---------|--------|-------|--|

|                 |         |        |       |                                           |
|-----------------|---------|--------|-------|-------------------------------------------|
| 1.29-2025.03.14 | 1.29.13 | 1.7.20 | 1.1.3 | containerd wurde auf 1.7.20 aktualisiert. |
|-----------------|---------|--------|-------|-------------------------------------------|

|                 |         |        |       |  |
|-----------------|---------|--------|-------|--|
| 1.29-2025.02.15 | 1.29.13 | 1.7.14 | 1.1.3 |  |
|-----------------|---------|--------|-------|--|

|                 |         |        |       |  |
|-----------------|---------|--------|-------|--|
| 1.29-2025.01.15 | 1.29.12 | 1.7.14 | 1.1.3 |  |
|-----------------|---------|--------|-------|--|

|                 |         |        |       |                                        |
|-----------------|---------|--------|-------|----------------------------------------|
| 1.29-2025.01.01 | 1.29.12 | 1.7.14 | 1.1.3 | Beinhaltet Patches für CVE-2024-9042 . |
|-----------------|---------|--------|-------|----------------------------------------|



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.12.11 | 1.29.10         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.11.12 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.10.08 | 1.29.8          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.09.10 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.08.13 | 1.29.6          | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.29-2024<br>.07.10 | 1.29.6          | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                    |
| 1.29-2024<br>.06.17 | 1.29.3          | 1.7.11                | 1.1.2                 |                                                                                                     |
| 1.29-2024<br>.05.15 | 1.29.3          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.<br>kubelet wurde<br>auf 1.29.3<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                            |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.29-2024<br>.04.09 | 1.29.0          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1                                      |
| 1.29-2024<br>.03.13 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                                                                 |
| 1.29-2024<br>.02.13 | 1.29.0          | 1.6.25                | 1.1.2                 |                                                                                                                                                                 |
| 1.29-2024<br>.02.06 | 1.29.0          | 1.6.25                | 1.1.2                 | Es wurde ein<br>Fehler behoben,<br>bei dem das<br>Pause-Bil<br>d fälschlic<br>herweise beim<br>kubelet<br>Garbage-<br>Collection<br>-Prozess<br>gelöscht wurde. |
| 1.29-2024<br>.01.09 | 1.29.0          | 1.6.18                | 1.1.2                 |                                                                                                                                                                 |

## Kubernetes Version 1.28

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.28-2025<br>.06.13 | 1.28.15         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |
| 1.28-2025<br>.05.17 | 1.28.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.28-2025<br>.04.14 | 1.28.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.28-2025<br>.03.14 | 1.28.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.28-2025<br>.02.15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>-01-15 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2025<br>-01-01 | 1.28.15         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.28-2024<br>.12.11 | 1.28.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.28-2024<br>.11.12 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.10.08 | 1.28.13         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.09.10 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.08.13 | 1.28.11         | 1.7.14                | 1.1.3                 |                                                                                                     |
| 1.28-2024<br>.07.10 | 1.28.11         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                    |
| 1.28-2024<br>.06.17 | 1.28.8          | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                 |
| 1.28-2024<br>.05.14 | 1.28.8          | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.28.8<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.28-2024<br>.04.09 | 1.28.5          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.28-2024<br>.03.13 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2024<br>.02.13 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2024<br>.01.09 | 1.28.5          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2023<br>.12.12 | 1.28.3          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.28-2023<br>.11.14 | 1.28.3          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.28-2023<br>.10.19 | 1.28.2          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.28-2023<br>-09.27 | 1.28.2          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |
| 1.28-2023<br>.09.12 | 1.28.1          | 1.6.6                 | 1.1.2                 |                                                                                                                                                                                                                       |

## Kubernetes Version 1.27

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.06.13 | 1.27.16         | 1.7.27                | 1.2.1                 | container<br>d wurde<br>auf 1.7.27<br>aktualisiert. |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.27-2025<br>.05.17 | 1.27.16         | 1.7.20                | 1.2.1                 |                                                     |
| 1.27-2025<br>.04.14 | 1.27.16         | 1.7.20                | 1.1.3                 |                                                     |
| 1.27-2025<br>.03.14 | 1.27.16         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.27-2025<br>.02.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.15 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2025<br>.01.01 | 1.27.16         | 1.7.14                | 1.1.3                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>9042 .    |
| 1.27-2024<br>.12.11 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.11.12 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.10.08 | 1.27.16         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.09.10 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.27-2024<br>.08.13 | 1.27.15         | 1.7.14                | 1.1.3                 |                                                     |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.07.10 | 1.27.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2024-<br>5321 .                                                                           |
| 1.27-2024<br>.06.17 | 1.27.12         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.27-2024<br>.05.14 | 1.27.12         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.27.12<br>aktualisiert.                       |
| 1.27-2024<br>.04.09 | 1.27.9          | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.27-2024<br>.03.13 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.27-2024<br>.02.13 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                            |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2024<br>.01.09 | 1.27.9          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                       |
| 1.27-2023<br>.12.12 | 1.27.7          | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                       |
| 1.27-2023<br>.11.14 | 1.27.7          | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                      |
| 1.27-2023<br>.10.19 | 1.27.6          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |
| 1.27-2023<br>-09.27 | 1.27.6          | 1.6.6                 | 1.1.2                 | Ein <a href="#">Security<br/>Advisory</a> wurde<br>in kubelet<br>behooben.                                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                             |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.09.12 | 1.27.4          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connector-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.27-2023<br>.08.17 | 1.27.4          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                       |
| 1.27-2023<br>.08.08 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |
| 1.27-2023<br>.07.11 | 1.27.3          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                  |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.27-2023<br>.06.20 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                       |
| 1.27-2023<br>.06.14 | 1.27.1          | 1.6.6                 | 1.1.1                 | Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt.           |
| 1.27-2023<br>.06.06 | 1.27.1          | 1.6.6                 | 1.1.1                 | Das <a href="#">Problem #2042</a> von containerd-roadmap, das dazu führte, dass Knoten private Amazon-ECR-Images nicht abrufen konnten, wurde behoben. |
| 1.27-2023<br>.05.17 | 1.27.1          | 1.6.6                 | 1.1.1                 |                                                                                                                                                        |

## Kubernetes Version 1.26

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------|
| 1.26-2025<br>.05.17 | 1.26.15         | 1.7.20                | 1.2.1                 |                                                     |
| 1.26-2025<br>.04.14 | 1.26.15         | 1.7.20                | 1.1.3                 |                                                     |
| 1.26-2025<br>.03.14 | 1.26.15         | 1.7.20                | 1.1.3                 | container<br>d wurde<br>auf 1.7.20<br>aktualisiert. |
| 1.26-2025<br>.02.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2025<br>.01.15 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.12.11 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.11.12 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.10.08 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.09.10 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.08.13 | 1.26.15         | 1.7.14                | 1.1.3                 |                                                     |
| 1.26-2024<br>.07.10 | 1.26.15         | 1.7.11                | 1.1.2                 | Beinhaltet<br>Patches für                           |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                       |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
|                     |                 |                       |                       | CVE-2024-5321 .                                                                                                            |
| 1.26-2024<br>.06.17 | 1.26.15         | 1.7.11                | 1.1.2                 | container<br>d wurde<br>auf 1.7.11<br>aktualisiert.                                                                        |
| 1.26-2024<br>.05.14 | 1.26.15         | 1.6.28                | 1.1.2                 | container<br>d wurde<br>auf 1.6.28<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.15<br>aktualisiert.                       |
| 1.26-2024<br>.04.09 | 1.26.12         | 1.6.25                | 1.1.2                 | container<br>d wurde<br>auf 1.6.25<br>aktualisiert.<br>CNI neu erstellt<br>und verwendet<br>.csi-proxy<br>golang<br>1.22.1 |
| 1.26-2024<br>.03.13 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.02.13 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |
| 1.26-2024<br>.01.09 | 1.26.12         | 1.6.18                | 1.1.2                 |                                                                                                                            |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                                                  |
|---------------------|-----------------|-----------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.12.12 | 1.26.10         | 1.6.18                | 1.1.2                 |                                                                                                                                                                                                                                                                       |
| 1.26-2023<br>.11.14 | 1.26.10         | 1.6.18                | 1.1.2                 | Beinhaltet<br>Patches für<br>CVE-2023-<br>5528 .                                                                                                                                                                                                                      |
| 1.26-2023<br>.10.19 | 1.26.9          | 1.6.18                | 1.1.2                 | container<br>d wurde<br>auf 1.6.18<br>aktualisiert.<br>kubelet wurde<br>auf 1.26.9<br>aktualisi<br>ert. Neue<br><a href="#">Umgebungs<br/>variablen für<br/>Bootstrap<br/>-Skripte</a><br>hinzugefügt<br>(SERVICE_I<br>PV4_CIDR<br>und EXCLUDED_<br>SNAT_CIDR<br>S ). |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                 |
|---------------------|-----------------|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.09.12 | 1.26.7          | 1.6.6                 | 1.1.2                 | Das Amazon VPC CNI-Plugin wurde aktualisiert, sodass es die Kubernetes-Connect- oder-Binärdatei verwendet, die die Pod-IP-Adresse vom Kubernetes-API-Server erhält. Die <a href="#">Pull-Anforderung #100</a> wurde zusammengeführt. |
| 1.26-2023<br>.08.17 | 1.26.7          | 1.6.6                 | 1.1.2                 | Beinhaltet Patches für CVE-2023-3676 , CVE-2023-3893 , und CVE-2023-3955 .                                                                                                                                                           |
| 1.26-2023<br>.08.08 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |
| 1.26-2023<br>.07.11 | 1.26.6          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                      |

| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                   |
|---------------------|-----------------|-----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.06.20 | 1.26.4          | 1.6.6                 | 1.1.1                 | Das Problem, das dazu führte, dass die DNS-Suffix-Suchliste falsch gefüllt wurde, wurde behoben.                                                                                       |
| 1.26-2023<br>.06.14 | 1.26.4          | 1.6.6                 | 1.1.1                 | Kubernetes wurde aktualisiert auf 1.26.4. Die Unterstützung für die Zuordnung von Host-Ports in CNI wurde hinzugefügt. Die Pull-Anforderung <a href="#">#93</a> wurde zusammengeführt. |



| AMI-Version         | Kubelet-Version | Version<br>containerd | CSI-Proxy-<br>Version | Versionsh<br>inweise                                                                                                                                                                                                                            |
|---------------------|-----------------|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.26-2023<br>.05.09 | 1.26.2          | 1.6.6                 | 1.1.1                 | Ein Fehler wurde behoben, der das Netzwerkverbindungssproblem <a href="#">#1126</a> auf Pods nach dem Neustart des Knotens verursachte. Ein neuer <a href="#">Bootstrap-Skriptkonfigurationsparameter</a> (ExcludedSnatCIDs ) wurde eingeführt. |
| 1.26-2023<br>.04.26 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |
| 1.26-2023<br>.04.11 | 1.26.2          | 1.6.6                 | 1.1.1                 | Wiederherstellungsmechanismus für kubelet und kube-proxy bei einem Serviceabsturz hinzugefügt.                                                                                                                                                  |
| 1.26-2023<br>.03.24 | 1.26.2          | 1.6.6                 | 1.1.1                 |                                                                                                                                                                                                                                                 |

## Rufen Sie das empfohlene Microsoft Windows AMI ab IDs

Bei der Bereitstellung von Knoten können Sie eine ID für ein vorgefertigtes Amazon EKS-optimiertes Amazon Machine Image (AMI) angeben. Um eine AMI-ID abzurufen, die Ihrer gewünschten Konfiguration entspricht, fragen Sie die AWS Systems Manager Parameter Store-API ab. Durch die Verwendung dieser API entfällt die Notwendigkeit, manuell nach Amazon EKS-optimiertem AMI zu suchen IDs. Weitere Informationen finden Sie unter [GetParameter](#). Das von Ihnen verwendete [IAM-Prinzipal](#) muss über die `ssm:GetParameter`-IAM-Berechtigung zum Abrufen der Amazon EKS-optimierten AMI-Metadaten verfügen.

Sie können die Image-ID des neuesten empfohlenen Amazon EKS-optimierten Windows-AMIs mit dem folgenden Befehl abrufen, der den Unterparameter `image_id` verwendet. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:

- *release* Ersetzen Sie durch eine der folgenden Optionen.
  - *2022* Für Windows Server 2022 verwenden.
  - *2019* Für Windows Server 2019 verwenden.
- *installation-option* Ersetzen Sie durch eine der folgenden Optionen. Weitere Informationen finden Sie unter [Was ist die Server Core-Installationsoption in Windows Server](#).
  - Verwenden Sie diese Option *Core* für eine Minimalinstallation mit einer kleineren Angriffsfläche.
  - Wird verwendet *Full*, um das Windows-Desktop-Erlebnis einzubeziehen.
- *kubernetes-version* Durch eine unterstützte [Amazon EKS-Version](#) ersetzen.
- *region-code* Ersetzen Sie durch eine von [Amazon EKS unterstützte AWS Region](#), für die Sie die AMI-ID benötigen.

```
aws ssm get-parameter --name /aws/service/ami-windows-latest/Windows_Server-release-
English-installation-option-EKS_Optimized-kubernetes-version/image_id \
--region region-code --query "Parameter.Value" --output text
```

Hier ist ein Beispielbefehl, nachdem Platzhalter ersetzt wurden.

```
aws ssm get-parameter --name /aws/service/ami-windows-latest/Windows_Server-2022-
English-Core-EKS_Optimized-k8s-n-2/image_id \
--region us-west-2 --query "Parameter.Value" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
ami-1234567890abcdef0
```

## Erstellen Sie ein benutzerdefiniertes Windows-AMI mit Image Builder

Sie können EC2 Image Builder verwenden, um benutzerdefinierte, für Amazon EKS optimierte Windows AMIs mit einer der folgenden Optionen zu erstellen:

- [Verwenden eines für Amazon EKS optimierten Windows-AMI als Basis](#)
- [Verwenden der von Amazon verwalteten Build-Komponente](#)

Bei beiden Methoden müssen Sie Ihr eigenes Image-Builder-Rezept erstellen. Weitere Informationen finden Sie unter [Erstellen einer neuen Version eines Bildrezeptes](#) im Image-Builder-Benutzerhandbuch.

### Important

Die folgenden von Amazon verwalteten Komponenten für eks enthalten Patches für CVE-2024-5321.

- 1.26.4 und höher
- 1.27.2 und höher
- 1.28.2 und höher
- 1.29.2 und höher
- 1.30.1 und höher

## Verwenden eines für Amazon EKS optimierten Windows-AMI als Basis

Diese Option ist die empfohlene Methode, um Ihr benutzerdefiniertes Windows zu erstellen AMIs. Das von AMIs uns bereitgestellte Amazon EKS-optimierte Windows wird häufiger aktualisiert als die von Amazon verwaltete Build-Komponente.

1. Starten Sie ein neues Image-Builder-Rezept.

- a. Öffnen Sie die EC2 Image Builder Builder-Konsole unter <https://console.aws.amazon.com/imagebuilder>.

- b. Wählen Sie im linken Navigationsbereich Image recipes (Image-Rezepte) aus.
  - c. Wählen Sie Create image recipe (Image-Rezept erstellen) aus.
2. Geben Sie im Abschnitt Recipe details (Rezeptdetails) einen Namen und eine Version ein.
3. Geben Sie die ID des für Amazon EKS optimierten Windows-AMI im Abschnitt Basis-Image an.
  - a. Wählen Sie Enter custom AMI ID (Benutzerdefinierte AMI-ID eingeben) aus.
  - b. Rufen Sie die AMI-ID für die Windows-Betriebssystemversion ab, die Sie benötigen. Weitere Informationen finden Sie unter [the section called “Holen Sie sich die neuesten IDs”](#).
  - c. Geben Sie die benutzerdefinierte AMI-ID ein. Wenn die AMI-ID nicht gefunden wird, stellen Sie sicher, dass die AWS Region für die AMI-ID mit der AWS Region übereinstimmt, die oben rechts auf Ihrer Konsole angezeigt wird.
4. (Optional) Um die neuesten Sicherheitsupdates zu erhalten, fügen Sie die update-windows-Komponente im Abschnitt Build components – (Build-Komponenten – ) hinzu.
  - a. Wählen Sie in der Dropdownliste rechts neben dem Suchfeld Find components by name (Komponenten nach Namen suchen) Amazon-managed (Von Amazon verwaltet) aus.
  - b. Geben Sie im Suchfeld Find components by name (Komponenten nach Namen suchen) update-windows ein.
  - c. Aktivieren Sie das Kontrollkästchen des **update-windows**Suchergebnisses. Diese Komponente enthält die neuesten Windows-Patches für das Betriebssystem.
5. Füllen Sie die verbleibenden Image-Rezepteingaben mit Ihren erforderlichen Konfigurationen aus. Weitere Informationen finden Sie unter [Erstellen einer neuen Version eines Image-Rezeptes \(Konsole\)](#) im Image-Builder-Benutzerhandbuch.
6. Wählen Sie Create Recipe (Rezept erstellen) aus.
7. Verwenden Sie das neue Image-Rezept in einer neuen oder vorhandenen Image-Pipeline. Sobald Ihre Image-Pipeline erfolgreich ausgeführt wurde, wird Ihr benutzerdefiniertes AMI als Ausgabe-Image aufgeführt und ist einsatzbereit. Weitere Informationen finden Sie unter [Erstellen einer Image-Pipeline mit dem EC2 Image Builder Builder-Konsolenassistenten](#).

## Verwenden der von Amazon verwalteten Build-Komponente

Wenn die Verwendung eines für Amazon EKS optimierten Windows-AMI als Basis nicht praktikabel ist, können Sie stattdessen die von Amazon verwaltete Build-Komponente verwenden. Diese Option kann hinter den zuletzt unterstützten Kubernetes-Versionen zurückbleiben.

1. Starten Sie ein neues Image-Builder-Rezept.

- a. Öffnen Sie die EC2 Image Builder Builder-Konsole unter <https://console.aws.amazon.com/imagebuilder>.
- b. Wählen Sie im linken Navigationsbereich Image recipes (Image-Rezepte) aus.
- c. Wählen Sie Create image recipe (Image-Rezept erstellen) aus.
2. Geben Sie im Abschnitt Recipe details (Rezeptdetails) einen Namen und eine Version ein.
3. Legen Sie im Abschnitt Base image (Basis-Image) fest, welche Option Sie verwenden werden, um Ihr benutzerdefiniertes AMI zu erstellen:
  - Select managed images (Verwaltete Images auswählen) – Wählen Sie Windows als Ihr Image Operating System (OS) (Image-Betriebssystem (OS)) aus. Wählen Sie dann eine der folgenden Optionen für Image origin (Image-Ursprung) aus:
    - Schnellstart (von Amazon verwaltet) — Wählen Sie in der Dropdownliste Image-Name eine von Amazon EKS unterstützte Windows Server-Version aus. Weitere Informationen finden Sie unter [the section called “Windows”](#).
    - Images owned by me (Bilder in meinem Besitz) – Wählen Sie für Image-Name den ARN Ihres eigenen Image mit Ihrer eigenen Lizenz aus. In dem von Ihnen bereitgestellten Image dürfen noch keine Amazon EKS-Komponenten installiert sein.
  - Enter custom AMI ID (Benutzerdefinierte AMI-ID eingeben) – Geben Sie für AMI-ID die ID für Ihr AMI mit Ihrer eigenen Lizenz ein. In dem von Ihnen bereitgestellten Image dürfen noch keine Amazon EKS-Komponenten installiert sein.
4. Gehen Sie im Abschnitt Build components – Windows (Komponenten erstellen – Windows) wie folgt vor:
  - a. Wählen Sie in der Dropdownliste rechts neben dem Suchfeld Find components by name (Komponenten nach Namen suchen) Amazon-managed (Von Amazon verwaltet) aus.
  - b. Geben Sie im Suchfeld Find components by name (Komponenten nach Namen suchen) eks ein.
  - c. Aktivieren Sie das Kontrollkästchen für das **eks-optimized-ami-windows**Suchergebnis, auch wenn das zurückgegebene Ergebnis möglicherweise nicht die von Ihnen gewünschte Version ist.
  - d. Geben Sie im Suchfeld Find components by name (Komponenten nach Namen suchen) update-windows ein.
  - e. Markieren Sie das Kontrollkästchen des Suchergebnisses update-windows. Diese Komponente enthält die neuesten Windows-Patches für das Betriebssystem.

5. Gehen Sie im Abschnitt Selected components (Ausgewählte Komponenten) wie folgt vor:

- a. Wählen Sie Versionierungsoptionen für **eks-optimized-ami-windows**.
  - b. Wählen Sie Specify component version (Komponentenversion angeben) aus.
  - c. Geben Sie **version.x** im Feld Komponentenversion Folgendes ein: **version** Ersetzen durch eine unterstützte Kubernetes-Version. Wenn Sie **x** für einen Teil der Versionsnummer eingeben, wird die neueste Komponentenversion verwendet, die auch mit dem Teil der Version übereinstimmt, den Sie explizit definieren. Achten Sie auf die Konsolenausgabe, da sie Sie darüber informiert, ob Ihre gewünschte Version als verwaltete Komponente verfügbar ist. Beachten Sie, dass die neuesten Kubernetes-Versionen möglicherweise nicht für die Build-Komponente verfügbar sind. Weitere Informationen zu den verfügbaren Versionen finden Sie unter [the section called “Abrufen von Informationen zu eks-optimized-ami-windows-Komponentenversionen”](#).
6. Füllen Sie die verbleibenden Image-Rezepteingaben mit Ihren erforderlichen Konfigurationen aus. Weitere Informationen finden Sie unter [Erstellen einer neuen Version eines Image-Rezeptes \(Konsole\)](#) im Image-Builder-Benutzerhandbuch.
  7. Wählen Sie Create Recipe (Rezept erstellen) aus.
  8. Verwenden Sie das neue Image-Rezept in einer neuen oder vorhandenen Image-Pipeline. Sobald Ihre Image-Pipeline erfolgreich ausgeführt wurde, wird Ihr benutzerdefiniertes AMI als Ausgabe-Image aufgeführt und ist einsatzbereit. Weitere Informationen finden Sie unter [Erstellen einer Image-Pipeline mit dem EC2 Image Builder Builder-Konsolenassistenten](#).

#### Abrufen von Informationen zu **eks-optimized-ami-windows**-Komponentenversionen

Sie können spezifische Informationen darüber abrufen, was mit den einzelnen Komponenten installiert ist. Sie können beispielsweise überprüfen, welche kubelet-Version installiert ist. Die Komponenten werden auf den von Amazon EKS unterstützten Windows-Betriebssystemversionen Funktionstests unterzogen. Weitere Informationen finden Sie unter [the section called “Veröffentlichungskalender”](#). Alle anderen Windows-Betriebssystemversionen, die nicht als unterstützt aufgeführt sind oder deren Support abgelaufen ist, sind möglicherweise nicht mit der Komponente kompatibel.

1. Öffnen Sie die EC2 Image Builder Builder-Konsole unter <https://console.aws.amazon.com/imagebuilder>.
2. Wählen Sie im linken Navigationsbereich Components (Komponenten) aus.

3. Ändern Sie in der Dropdownliste rechts neben dem Suchfeld Find components by name (Komponenten nach Namen suchen) Owned by me (In meinem Besitz) zu Quick start (Amazon-managed) (Schnellstart (Von Amazon verwaltet)).
4. Geben Sie im Feld Komponenten nach Name suchen eks ein.
5. (Optional) Wenn Sie eine aktuelle Version verwenden, sortieren Sie die Spalte Version in absteigender Reihenfolge, indem Sie sie zweimal auswählen.
6. Wählen Sie den **eks-optimized-ami-windows** Link mit der gewünschten Version.

Unter Description (Beschreibung) auf der resultierenden Seite werden die spezifischen Informationen angezeigt.

## Aktivieren Sie die auto Knotenreparatur und untersuchen Sie Probleme mit dem Knotenstatus

Der Zustand eines Knotens bezieht sich auf den Betriebsstatus und die Fähigkeit eines Knotens, Workloads effektiv auszuführen. Ein fehlerfreier Knoten behält die erwartete Konnektivität bei, verfügt über ausreichende Ressourcen und kann Pods ohne Unterbrechung erfolgreich ausführen. Informationen zum Abrufen von Details zu Ihren Knoten finden Sie unter [the section called “Zustand des Knotens anzeigen”](#) und [the section called “Holen Sie sich Knotenprotokolle”](#).

Um die Aufrechterhaltung fehlerfreier Knoten zu unterstützen, bietet Amazon EKS den Node Monitoring Agent und die auto Knotenreparatur an.

### Important

Der Node Monitoring Agent und Node Auto Repair sind nur unter Linux verfügbar. Diese Funktionen sind unter Windows nicht verfügbar.

## Agent zur Knotenüberwachung

Der Node Monitoring Agent liest automatisch Knotenprotokolle, um bestimmte Gesundheitsprobleme zu erkennen. Er analysiert Knotenprotokolle, um Fehler zu erkennen, und zeigt verschiedene Statusinformationen zu Worker-Knoten an. Für jede Kategorie von erkannten Problemen, z. B. Speicher- und Netzwerkprobleme, wird auf die Worker-Knoten ein eigener NodeCondition Fehler

angewendet. Beschreibungen der erkannten Gesundheitsprobleme werden im Observability-Dashboard zur Verfügung gestellt. Weitere Informationen finden Sie unter [the section called “Probleme mit dem Zustand des Knotens”](#).

Der Node Monitoring Agent ist als Funktion für alle Amazon EKS Auto Mode-Cluster enthalten. Für andere Clustertypen können Sie den Monitoring-Agenten als Amazon EKS-Add-on hinzufügen. Weitere Informationen finden Sie unter [the section called “Erstellen Sie ein Add-on”](#).

## auto Knotenreparatur

Die auto Reparatur von Knoten ist eine zusätzliche Funktion, die kontinuierlich den Zustand von Knoten überwacht, automatisch auf erkannte Probleme reagiert und Knoten nach Möglichkeit ersetzt. Dadurch wird die Gesamtverfügbarkeit des Clusters bei minimalem manuellem Eingriff verbessert. Wenn eine Zustandsprüfung fehlschlägt, wird der Knoten automatisch gesperrt, sodass keine neuen Pods auf dem Knoten geplant werden.

Die auto Reparatur von Knoten allein kann auf den Ready Zustand der kubelet und aller manuell gelöschten Knotenobjekte reagieren. In Kombination mit dem Node Monitoring Agent kann Node Auto Repair auf mehr Bedingungen reagieren, die sonst nicht erkannt würden. Zu diesen zusätzlichen Bedingungen gehören `KernelReadyNetworkingReady`, und `StorageReady`.

Diese automatische Knotenwiederherstellung behebt automatisch sporadisch auftretende Knotenprobleme wie Fehler beim Beitritt zum Cluster, nicht reagierende Kubelets und vermehrte Beschleunigerfehler (Gerätefehler). Die verbesserte Zuverlässigkeit trägt dazu bei, Ausfallzeiten von Anwendungen zu reduzieren und den Clusterbetrieb zu verbessern. Die auto Knotenreparatur kann bestimmte gemeldete Probleme wie `DiskPressureMemoryPressure`, und nicht `behandelnPIDPressure`. Amazon EKS wartet 10 Minuten, bevor es auf die Bedingungen reagiert `AcceleratedHardwareReadyNodeConditions`, und 30 Minuten, wenn es sich um alle anderen Bedingungen handelt.

In zwei Szenarien deaktivieren verwaltete Knotengruppen aus Sicherheitsgründen außerdem automatisch die Reparatur von Knoten. Alle Reparaturvorgänge, die zuvor ausgeführt wurden, werden in beiden Situationen fortgesetzt.

- Wenn durch den Application Recovery Controller (ARC) eine Zonenverschiebung für Ihren Cluster ausgelöst wurde, werden alle nachfolgenden Reparaturvorgänge angehalten.
- Wenn Ihre Knotengruppe mehr als fünf Knoten umfasst und sich mehr als 20% der Knoten in Ihrer Knotengruppe in einem fehlerhaften Zustand befinden, werden die Reparaturvorgänge angehalten.



Sie können die auto Knotenreparatur aktivieren, wenn Sie eine verwaltete Knotengruppe erstellen oder bearbeiten.

- Wenn Sie die Amazon EKS-Konsole verwenden, aktivieren Sie das Kontrollkästchen auto Reparatur von Knoten aktivieren für die verwaltete Knotengruppe. Weitere Informationen finden Sie unter [the section called “Erstellen”](#).
- Wenn Sie die AWS CLI verwenden, fügen Sie `--node-repair-config enabled=true` dem [eks update-nodegroup-config](#) Befehl [eks create nodegroup](#) oder den hinzu.
- Ein Beispiel `eksctlClusterConfig`, das eine verwaltete Knotengruppe mit auto Knotenreparatur verwendet, finden Sie unter [44-node-repair.yaml](#) on. GitHub

## Probleme mit dem Zustand des Knotens

In den folgenden Tabellen werden Probleme mit dem Knotenstatus beschrieben, die vom Node Monitoring Agent erkannt werden können. Es gibt zwei Arten von Problemen:

- Zustand — Ein Terminalproblem, das eine Behebungsmaßnahme wie den Austausch einer Instanz oder einen Neustart rechtfertigt. Wenn die auto Reparatur aktiviert ist, führt Amazon EKS eine Reparaturaktion durch, entweder als Knotenersatz oder als Neustart. Weitere Informationen finden Sie unter [the section called “Bedingungen der Knoten”](#).
- Ereignis — Ein vorübergehendes Problem oder eine suboptimale Knotenkonfiguration. Es werden keine Autoreparaturmaßnahmen durchgeführt. Weitere Informationen finden Sie unter [the section called “Knotenereignisse”](#).

## Probleme mit dem Zustand des Kernelknotens

| Name               | Schweregrad | Beschreibung                                                                                                                                                                                               |
|--------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ForkFailedOutOfPID | Bedingung   | Ein Fork- oder Exec-Aufruf ist fehlgeschlagen, weil das System keinen Prozess IDs - oder Speicherzugriff mehr hatte. Dies kann durch Zombie-Prozesse oder physische Speichererschöpfung verursacht werden. |

| Name                    | Schweregrad | Beschreibung                                                                                                                                                                                 |
|-------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AppBlocked              | Ereignis    | Die Aufgabe wurde über einen längeren Zeitraum von der Planung blockiert, was in der Regel darauf zurückzuführen ist, dass sie bei der Eingabe oder Ausgabe blockiert wurde.                 |
| AppCrash                | Ereignis    | Eine Anwendung auf dem Knoten ist abgestürzt.                                                                                                                                                |
| ApproachingKernelPidMax | Ereignis    | Die Anzahl der Prozesse nähert sich der maximalen Anzahl PIDs, die gemäß der aktuellen kernel.pids_max-Einstellung verfügbar sind. Danach können keine Prozesse mehr gestartet werden.       |
| ApproachingMaxOpenFiles | Ereignis    | Die Anzahl der geöffneten Dateien nähert sich angesichts der aktuellen Kernel-Einstellungen der maximalen Anzahl möglicher geöffneter Dateien. Danach schlägt das Öffnen neuer Dateien fehl. |
| ConntrackExceededKernel | Ereignis    | Die Verbindungsverfolgung hat das Maximum für den Kernel überschritten und es konnten keine neuen Verbindungen hergestellt werden, was zu Paketverlusten führen kann.                        |

| Name                     | Schweregrad | Beschreibung                                                                                                                                                                                                                         |
|--------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ExcessiveZombieProcesses | Ereignis    | Prozesse, die nicht vollständig zurückgewonnen werden können, häufen sich in großer Zahl, was auf Anwendungsprobleme hindeutet und dazu führen kann, dass die Prozessgrenzen des Systems erreicht werden.                            |
| KernelBug                | Ereignis    | Ein Kernelfehler wurde vom Linux-Kernel selbst entdeckt und gemeldet. Dieser Fehler kann jedoch manchmal durch Knoten mit hoher CPU- oder Speicherauslastung verursacht werden, was zu einer verzögerten Ereignisverarbeitung führt. |
| LargeEnvironment         | Ereignis    | Die Anzahl der Umgebungsvariablen für diesen Prozess ist größer als erwartet, was möglicherweise darauf zurückzuführen ist, dass viele Dienste auf true enableServiceLinks gesetzt sind, was zu Leistungsproblemen führen kann.      |

| Name       | Schweregrad | Beschreibung                                                                                                                                                                     |
|------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RapidCron  | Ereignis    | Ein Cron-Job wird auf diesem Knoten schneller als alle fünf Minuten ausgeführt, was sich negativ auf die Leistung auswirken kann, wenn der Job erhebliche Ressourcen verbraucht. |
| SoftLockup | Ereignis    | Die CPU ist für eine bestimmte Zeit ins Stocken geraten.                                                                                                                         |

## Probleme mit dem Zustand des Netzwirknotens

| Name                     | Schweregrad | Beschreibung                                                                                                          |
|--------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------|
| InterfaceNotRunning      | Bedingung   | Diese Schnittstelle scheint nicht zu laufen oder es liegen Netzwerkprobleme vor.                                      |
| InterfaceNotUp           | Bedingung   | Diese Schnittstelle scheint nicht zu funktionieren oder es liegen Netzwerkprobleme vor.                               |
| IPAMDNotBereit           | Bedingung   | IPAMD kann keine Verbindung zum API-Server herstellen.                                                                |
| IPAMDNotWird ausgeführt  | Bedingung   | Es wurde nicht festgestellt, dass der <code>aws-k8s-agent</code> Prozess läuft.                                       |
| MissingLoopbackInterface | Bedingung   | Die Loopback-Schnittstelle fehlt in dieser Instanz, was je nach lokaler Konnektivität zum Ausfall von Diensten führt. |

| Name                           | Schweregrad | Beschreibung                                                                                                                                                           |
|--------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BandwidthInExceeded            | Ereignis    | Pakete wurden in die Warteschlange gestellt oder verworfen, weil die Gesamtbandbreite für eingehende Nachrichten das Maximum für die Instanz überschritten hat.        |
| BandwidthOutExceeded           | Ereignis    | Pakete wurden in die Warteschlange gestellt oder verworfen, weil die Gesamtbandbreite für ausgehende Nachrichten das Maximum für die Instance überschritten hat.       |
| ConntrackExceeded              | Ereignis    | Die Verbindungsverfolgung hat das Maximum für die Instanz überschritten und es konnten keine neuen Verbindungen hergestellt werden, was zu Paketverlusten führen kann. |
| IPAMNoIPs                      | Ereignis    | IPAM-D hat keine IP-Adressen mehr.                                                                                                                                     |
| IPAMDRepeatedlyStarten Sie neu | Ereignis    | Der IPAMD-Dienst wurde mehrfach neu gestartet.                                                                                                                         |
| KubeProxyNotReady              | Ereignis    | Der Kube-Proxy konnte keine Ressourcen überwachen oder auflisten.                                                                                                      |

| Name                         | Schweregrad | Beschreibung                                                                                                                                                                                         |
|------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LinkLocalExceeded            | Ereignis    | Pakete wurden verworfen, weil die PPS des Datenverkehrs zu lokalen Proxydiensten das Maximum der Netzwerkschnittstelle überschritten haben.                                                          |
| MissingDefaultRoutes         | Ereignis    | Es fehlen Standardroutenregeln.                                                                                                                                                                      |
| FehltIPRules, fehlt IPRoutes | Ereignis    | In der Routentabelle fehlen Routenregeln für IPs des folgenden Pod.                                                                                                                                  |
| NetworkSysctl                | Ereignis    | Die Netzwerk-Sysctl-Einstellungen dieses Knotens sind möglicherweise falsch.                                                                                                                         |
| PortConflict                 | Ereignis    | Wenn ein Pod HostPort verwendet, kann er iptables-Regeln schreiben, die die bereits gebundenen Ports des Hosts außer Kraft setzen und so möglicherweise den API-Serverzugriff verhindern.<br>kubelet |
| PPSExceeded                  | Ereignis    | Pakete wurden in die Warteschlange gestellt oder verworfen, weil das bidirektionale PPS das Maximum für die Instanz überschritten hat.                                                               |

| Name                 | Schweregrad | Beschreibung                                                                                                                    |
|----------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| UnexpectedRejectRule | Ereignis    | In den iptables wurde eine unerwartete REJECT DROP OR-Regel gefunden, die möglicherweise den erwarteten Datenverkehr blockiert. |

## Probleme mit der Gesundheit von Neuronenknoten

| Name                           | Schweregrad | Beschreibung                                                                                             |
|--------------------------------|-------------|----------------------------------------------------------------------------------------------------------|
| Neuron DMAError                | Bedingung   | Bei einer DMA-Engine ist ein nicht behebbarer Fehler aufgetreten.                                        |
| HBMUncorrectableNeuronenfehler | Bedingung   | Ein HBM ist auf einen nicht behebbaren Fehler gestoßen und hat zu falschen Ergebnissen geführt.          |
| NCUncorrectableNeuronenfehler  | Bedingung   | Es wurde ein nicht behebbarer Speicherfehler in Neuron Core festgestellt.                                |
| SRAMUncorrectableNeuron-Fehler | Bedingung   | Bei einem SRAM auf dem Chip ist ein Paritätsfehler aufgetreten, der zu falschen Ergebnissen geführt hat. |

## Probleme mit dem Zustand von NVIDIA-Knoten

Wenn die auto Reparatur aktiviert ist, beginnen die aufgeführten Reparaturaktionen 10 Minuten, nachdem das Problem erkannt wurde. Weitere Informationen zu XID-Fehlern finden Sie unter [Xid-Fehler](#) in der Dokumentation zur Bereitstellung und Verwaltung von NVIDIA-GPUs. Weitere

Informationen zu den einzelnen XID-Meldungen finden Sie unter [Grundlegendes zu Xid-Meldungen](#) in der Dokumentation zur Bereitstellung und Verwaltung von NVIDIA-GPUs.

| Name                 | Schweregrad | Beschreibung                                                                                                | Aktion reparieren |
|----------------------|-------------|-------------------------------------------------------------------------------------------------------------|-------------------|
| NvidiaDoubleBitError | Bedingung   | Der GPU-Treiber hat einen Double-Bit-Fehler verursacht.                                                     | Ersetzen          |
| NVLinkNvidia-Fehler  | Bedingung   | NVLink Fehler wurden vom GPU-Treiber gemeldet.                                                              | Ersetzen          |
| XID13Nvidia-Fehler   | Bedingung   | Es gibt eine Ausnahme für die Grafik-Engine.                                                                | Neustart          |
| XID31Nvidia-Fehler   | Bedingung   | Es bestehen vermutete Hardwareprobleme.                                                                     | Neustart          |
| XID48Nvidia-Fehler   | Bedingung   | Double-Bit-ECC-Fehler werden vom Treiber gemeldet.                                                          | Neustart          |
| Nvidia-Fehler XID63  | Bedingung   | Es wurde eine Seite zurückgezogen oder die Zeile neu zugewiesen.                                            | Neustart          |
| Nvidia-Fehler XID64  | Bedingung   | Beim Versuch, eine Seite zurückzuziehen oder eine Node-Neuzuordnung durchzuführen, sind Fehler aufgetreten. | Neustart          |
| Nvidia-Fehler XID74  | Bedingung   | Es besteht ein Problem mit einer                                                                            | Ersetzen          |



| Name                 | Schweregrad | Beschreibung                                                                                                                                                                                                                      | Aktion reparieren |
|----------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
|                      |             | Verbindung von der GPU zu einer anderen GPU oder einer anderen NVSwitch GPU NVLink. Dies kann auf einen Hardwarefehler mit der Verbindung selbst oder auf ein Problem mit dem Gerät am entfernten Ende der Verbindung hinweisen . |                   |
| XID79Nvidia-Fehler   | Bedingung   | Der GPU-Treiber hat versucht, über seine PCI-Express-Verbindung auf die GPU zuzugreifen, und hat festgestellt, dass auf die GPU nicht zugegriffen werden kann.                                                                    | Ersetzen          |
| XID94Nvidia-Fehler   | Bedingung   | Es gibt ECC-Speicherfehler.                                                                                                                                                                                                       | Neustart          |
| Nvidia-Fehler XID95  | Bedingung   | Es gibt ECC-Speicherfehler.                                                                                                                                                                                                       | Neustart          |
| Nvidia-Fehler XID119 | Bedingung   | Das GSP hat bei der Reaktion auf RPC-Anfragen von anderen Bits im Treiber eine Zeitüberschreitung erlitten.                                                                                                                       | Ersetzen          |

| Name                  | Schweregrad | Beschreibung                                                                                                                                                                                                            | Aktion reparieren |
|-----------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| XID12Nvidia: 0 Fehler | Bedingung   | Das GSP hat rechtzeitig geantwortet, aber mit einem Fehler.                                                                                                                                                             | Ersetzen          |
| Nvidia-Fehler XID121  | Bedingung   | C2C ist eine Chip-Verbindung. Es ermöglicht die gemeinsame Nutzung von Speicher zwischen CPUs Beschleunigern und mehr.                                                                                                  | Ersetzen          |
| Nvidia 0 Fehler XID14 | Bedingung   | Der GPU-Treiber hat möglicherweise nicht behebbare Fehler im GPU-Speicher festgestellt, sodass der GPU-Treiber nicht mehr in der Lage ist, Seiten für dynamisches Seitenofflining oder Zeilenneuzuweisung zu markieren. | Ersetzen          |
| NvidiaPageRetirement  | Ereignis    | Der GPU-Treiber hat eine Speicherseite als veraltet markiert. Dies kann der Fall sein, wenn ein einzelner Doppelbitfehler oder zwei Einzelbitfehler an derselben Adresse auftreten.                                     | Keine             |

| Name                        | Schweregrad | Beschreibung                                                                                                             | Aktion reparieren |
|-----------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------|-------------------|
| nvidiaxID [Code]<br>Warnung | Ereignis    | Jedes Auftreten XIDs anderer als der in dieser Liste definierten Ereignisse führt zu diesem Ereignis.                    | Keine             |
| DCGMError                   | Bedingung   | Die Verbindung zum Data Center GPU Manager (DCGM) - Hostprozess wurde unterbrochen oder konnte nicht hergestellt werden. | Keine             |
| DCGMDiagnosticFehler        | Bedingung   | Beim Ausführen der aktiven DCGM-Diagnose ist ein Problem aufgetreten.                                                    | Keine             |
| DCGMDiagnosticEin Fehler    | Bedingung   | Ein Testfall aus der DCGM Active Diagnostics Test Suite ist fehlgeschlagen.                                              | Keine             |

## Probleme mit dem Zustand des Laufzeitknotens

| Name                | Schweregrad | Beschreibung                                                                                                                                                        |
|---------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PodStuckTerminating | Bedingung   | Ein Pod steckt oder war hängen geblieben und hat zu lange gekündigt. Dies kann durch CRI-Fehler verursacht werden, die das Fortschreiten des Pod-Status verhindern. |

| Name                   | Schweregrad | Beschreibung                                                                                                                                                                                     |
|------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %sRepeatedRestart      | Ereignis    | Startet alle Systemd-Dienste auf dem Knoten neu (formatiert unter Verwendung des Unit-Namens in Titelbuchstaben).                                                                                |
| ContainerRuntimeFailed | Ereignis    | Die Container-Laufzeit konnte keinen Container erstellen, was wahrscheinlich auf gemeldete Probleme zurückzuführen ist, wenn sie wiederholt auftreten.                                           |
| KubeletFailed          | Ereignis    | Das Kubelet ist in einen ausgefallenen Zustand übergegangen.                                                                                                                                     |
| LivenessProbeFailures  | Ereignis    | Es wurde ein Fehler bei der Verfügbarkeitsprüfung festgestellt, der möglicherweise auf Probleme mit dem Anwendungscode oder unzureichende Timeout-Werte hindeutet, falls er wiederholt auftritt. |
| ReadinessProbeFailures | Ereignis    | Es wurde ein Fehler bei der Bereitschaftsprüfung festgestellt, der möglicherweise auf Probleme mit dem Anwendungscode oder unzureichende Timeoutwerte hindeutet, falls er wiederholt auftritt.   |
| ServiceFailedToStart   | Ereignis    | Eine Systemd-Einheit konnte nicht gestartet werden.                                                                                                                                              |

## Probleme mit dem Zustand des Speicherknotens

| Name                       | Schweregrad | Beschreibung                                                                                                                                                                                                                      |
|----------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| XFSSmallAverageClusterSize | Bedingung   | Die durchschnittliche XFS-Clustergröße ist klein, was auf eine übermäßige Fragmentierung des freien Speicherplatzes hindeutet, die trotz verfügbarer Inodes oder freiem Speicherplatz die Erstellung von Dateien verhindern kann. |
| EtcHostsMountFailed        | Ereignis    | Das Mounten des generierten Kubelets ist <code>/etc/hosts</code> fehlgeschlagen, da Benutzerdaten während des Kubelet-Container-Betriebs erneut bereitgestellt wurden. <code>/var/lib/kubelet/pods</code>                         |
| IODelays                   | Ereignis    | In einem Prozess wurde eine Eingabe- oder Ausgabeverzögerung festgestellt, was möglicherweise auf eine unzureichende Bereitstellung von Eingabe und Ausgabe hindeutet, falls diese zu hoch ist.                                   |
| KubeletDiskUsageSlow       | Ereignis    | Kubelet meldet eine langsame Festplattennutzung beim Versuch, auf das Dateisystem zuzugreifen, was möglicherweise auf unzureichende Festplatteneingabe- und                                                                       |

| Name | Schweregrad | Beschreibung                                             |
|------|-------------|----------------------------------------------------------|
|      |             | -ausgabeprobleme oder auf Dateisystemprobleme hindeutet. |

## Sehen Sie sich den Gesundheitsstatus Ihrer Knoten an

In diesem Thema werden die Tools und Methoden erklärt, die für die Überwachung des Knotenzustands in Amazon EKS-Clustern verfügbar sind. Die Informationen behandeln Knotenbedingungen, Ereignisse und Erkennungsfälle, die Ihnen helfen, Probleme auf Knotenebene zu identifizieren und zu diagnostizieren. Verwenden Sie die hier beschriebenen Befehle und Muster, um die Knotenintegritätsressourcen zu überprüfen, Statusbedingungen zu interpretieren und Knotenereignisse für die betriebliche Fehlerbehebung zu analysieren.

Mit Kubernetes-Befehlen für alle Knoten können Sie einige Informationen zum Zustand des Knotens abrufen. Und wenn Sie den Node Monitoring Agent über den Amazon EKS Auto Mode oder das Amazon EKS Managed Add-on verwenden, erhalten Sie eine größere Auswahl an Knotensignalen, die Ihnen bei der Fehlerbehebung helfen. Beschreibungen der vom Node Monitoring Agent erkannten Gesundheitsprobleme werden auch im Observability-Dashboard zur Verfügung gestellt. Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).

## Bedingungen der Knoten

Bei den Knotenbedingungen handelt es sich um Terminalprobleme, die Behebungsmaßnahmen wie den Austausch von Instanzen oder einen Neustart erfordern.

Um die Bedingungen für alle Knoten abzurufen:

```
kubectl get nodes -o 'custom-
columns=NAME:.metadata.name,CONDITIONS:.status.conditions[*].type,STATUS:.status.conditions[*].
```

Um detaillierte Bedingungen für einen bestimmten Knoten zu erhalten

```
kubectl describe node node-name
```

Beispiel für die Ausgabe einer Bedingung für einen fehlerfreien Knoten:

```
- lastHeartbeatTime: "2024-11-21T19:07:40Z"
 lastTransitionTime: "2024-11-08T03:57:40Z"
 message: Monitoring for the Networking system is active
 reason: NetworkingIsReady
 status: "True"
 type: NetworkingReady
```

Beispiel für einen Zustand eines fehlerhaften Knotens mit einem Netzwerkproblem:

```
- lastHeartbeatTime: "2024-11-21T19:12:29Z"
 lastTransitionTime: "2024-11-08T17:04:17Z"
 message: IPAM-D has failed to connect to API Server which could be an issue with
 IPTable rules or any other network configuration.
 reason: IPAMDNotReady
 status: "False"
 type: NetworkingReady
```

## Knotenereignisse

Knotenereignisse deuten auf vorübergehende Probleme oder suboptimale Konfigurationen hin.

Um alle Ereignisse abzurufen, die vom Node-Monitoring-Agenten gemeldet werden

Wenn der Node Monitoring Agent verfügbar ist, können Sie den folgenden Befehl ausführen.

```
kubectl get events --field-selector=reportingComponent=eks-node-monitoring-agent
```

Beispielausgabe:

| LAST SEEN         | TYPE    | REASON     | OBJECT                                            |
|-------------------|---------|------------|---------------------------------------------------|
| MESSAGE           |         |            |                                                   |
| 4s                | Warning | SoftLockup | node/ip-192-168-71-251.us-west-2.compute.internal |
| CPU stuck for 23s |         |            |                                                   |

Um Ereignisse für alle Knoten abzurufen

```
kubectl get events --field-selector involvedObject.kind=Node
```

Um Ereignisse für einen bestimmten Knoten abzurufen

```
kubectl get events --field-selector involvedObject.kind=Node,involvedObject.name=node-name
```

Um Ereignisse in Echtzeit zu verfolgen

```
kubectl get events -w --field-selector involvedObject.kind=Node
```

Beispiel für eine Ereignisausgabe:

| LAST SEEN | TYPE    | REASON         | OBJECT      | MESSAGE                           |
|-----------|---------|----------------|-------------|-----------------------------------|
| 2m        | Warning | MemoryPressure | Node/node-1 | Node experiencing memory pressure |
| 5m        | Normal  | NodeReady      | Node/node-1 | Node became ready                 |

## Allgemeine Befehle zur Fehlerbehebung

```
Get comprehensive node status
kubectl get node node-name -o yaml

Watch node status changes
kubectl get nodes -w

Get node metrics
kubectl top node
```

## Rufen Sie mit kubectl und S3 Knotenprotokolle für einen verwalteten Knoten ab

Erfahren Sie, wie Sie Knotenprotokolle für einen von Amazon EKS verwalteten Knoten abrufen, der über den Knotenüberwachungsagenten verfügt.

## Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein vorhandener Amazon EKS-Cluster mit dem Knotenüberwachungsagenten. Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).
- Das `kubectl` Befehlszeilentool wurde für die Kommunikation mit Ihrem Cluster installiert und konfiguriert.



- Die AWS CLI wurde installiert und hat sich mit ausreichenden Berechtigungen angemeldet, um S3-Buckets und -Objekte zu erstellen.
- Eine aktuelle Version von Python 3 ist installiert
- Das AWS SDK für Python 3, Boto 3, ist installiert.

## Schritt 1: S3-Bucket-Ziel erstellen (optional)

Wenn Sie noch keinen S3-Bucket zum Speichern der Protokolle haben, erstellen Sie einen. Verwenden Sie den folgenden AWS CLI-Befehl. Der Bucket verwendet standardmäßig die `private` Zugriffskontrollliste. Ersetzen Sie es durch *bucket-name* den von Ihnen gewählten eindeutigen Bucket-Namen.

```
aws s3api create-bucket --bucket bucket-name
```

## Schritt 2: Erstellen Sie eine vorsignierte S3-URL für HTTP Put

Amazon EKS gibt die Knotenprotokolle zurück, indem es einen HTTP-PUT-Vorgang an eine von Ihnen angegebene URL ausführt. In diesem Tutorial werden wir eine vorsignierte S3-HTTP-PUT-URL generieren.

Die Protokolle werden als Gzip-Tarball mit der Erweiterung zurückgegeben. `.tar.gz`

### Note

Sie müssen die AWS API oder ein SDK verwenden, um die vorsignierte S3-Upload-URL zu erstellen, damit EKS die Protokolldatei hochladen kann. Sie können mit der AWS CLI keine vorsignierte S3-Upload-URL erstellen.

1. Ermitteln Sie, wo im Bucket Sie die Protokolle speichern möchten. Sie könnten es beispielsweise `2024-11-12/logs1.tar.gz` als Schlüssel verwenden.
2. Speichern Sie den folgenden Python-Code in der `Dateipresign-upload.py`. Ersetze `<bucket-name>` und `<key>`. Der Schlüssel sollte enden mit `.tar.gz`.

```
import boto3; print(boto3.client('s3').generate_presigned_url(
 ClientMethod='put_object',
```

```
Params={'Bucket': '<bucket-name>', 'Key': '<key>'},
ExpiresIn=1000
)
```

### 3. Führen Sie das Skript mit aus

```
python presign-upload.py
```

### 4. Notieren Sie sich die URL-Ausgabe. Verwenden Sie diesen Wert im nächsten Schritt als `http-put-destination`.

Weitere Informationen finden Sie unter [Generieren einer vorsignierten URL zum Hochladen einer Datei](#) in der Dokumentation zum AWS Boto3-SDK für Python.

## Schritt 3: Ressource erstellen NodeDiagnostic

Identifizieren Sie den Namen des Knotens, von dem Sie Protokolle sammeln möchten.

Erstellen Sie ein `NodeDiagnostic` Manifest, das den Namen des Knotens als Namen der Ressource verwendet und ein HTTP-PUT-URL-Ziel bereitstellt.

```
apiVersion: eks.amazonaws.com/v1alpha1
kind: NodeDiagnostic
metadata:
 name: node-name
spec:
 logCapture:
 destination: http-put-destination
```

Wenden Sie die Manifestdatei auf Ihren Cluster an.

```
kubectl apply -f nodediagnostic.yaml
```

Sie können den Status der Sammlung überprüfen, indem Sie die `NodeDiagnostic` Ressource beschreiben:

- Der Status `Success` oder `SuccessWithErrors` gibt an, dass die Aufgabe abgeschlossen und die Protokolle an das angegebene Ziel hochgeladen wurden (`SuccessWithErrors` weist darauf hin, dass einige Protokolle möglicherweise fehlen)

- Wenn der Status Fehlgeschlagen lautet, vergewissern Sie sich, dass die Upload-URL korrekt formatiert und nicht abgelaufen ist.

```
kubectl describe nodediagnostics.eks.amazonaws.com/node-name
```

## Schritt 4: Laden Sie die Protokolle von S3 herunter

Warten Sie etwa eine Minute, bevor Sie versuchen, die Protokolle herunterzuladen. Verwenden Sie dann die S3-CLI, um die Protokolle herunterzuladen.

```
Once NodeDiagnostic shows Success status, download the logs
aws s3 cp s3://bucket-name/key ./node-logs.tar.gz
```

## Schritt 5: NodeDiagnostic Ressource bereinigen

- NodeDiagnosticRessourcen werden nicht automatisch gelöscht. Sie sollten diese selbst bereinigen, nachdem Sie Ihre Log-Artefakte erhalten haben

```
Delete the NodeDiagnostic resource
kubectl delete nodediagnostics.eks.amazonaws.com/node-name
```

# Überblick über Amazon EKS-Hybridknoten

Mit Amazon EKS Hybrid Nodes können Sie Ihre lokale Infrastruktur und Ihre Edge-Infrastruktur als Knoten in Amazon EKS-Clustern verwenden. AWS verwaltet die AWS gehostete Kubernetes-Steuerebene des Amazon EKS-Clusters, und Sie verwalten die Hybridknoten, die in Ihren lokalen oder Edge-Umgebungen ausgeführt werden. Dadurch wird das Kubernetes-Management in Ihren Umgebungen vereinheitlicht und die Verwaltung der Kubernetes-Steuerebene auf Ihre lokalen und Edge-Anwendungen verlagert. AWS

Amazon EKS Hybrid Nodes funktioniert mit jeder lokalen Hardware oder virtuellen Maschinen und bietet die Effizienz, Skalierbarkeit und Verfügbarkeit von Amazon EKS überall dort, wo Ihre Anwendungen ausgeführt werden müssen. Sie können eine Vielzahl von Amazon EKS-Funktionen mit Amazon EKS-Hybridknoten verwenden, darunter Amazon EKS-Add-Ons, Amazon EKS Pod Identity, Cluster-Zugriffseinträge, Cluster-Einblicke und erweiterte Kubernetes-Versionsunterstützung.

Amazon EKS Hybrid Nodes lässt sich nativ in AWS Services wie AWS Systems Manager, AWS IAM Roles Anywhere, Amazon Managed Service for Prometheus und Amazon CloudWatch für zentrale Überwachung, Protokollierung und Identitätsverwaltung integrieren.

Bei Amazon EKS-Hybridknoten gibt es keine Vorabverpflichtungen oder Mindestgebühren, und die vCPU-Ressourcen Ihrer Hybridknoten, wenn sie an Ihre Amazon EKS-Cluster angeschlossen sind, werden Ihnen pro Stunde berechnet. Weitere Preisinformationen finden Sie unter [Amazon EKS-Preise](#).

## Features

EKS Hybrid Nodes bietet die folgenden Funktionen auf hoher Ebene:

- **Verwaltete Kubernetes-Steuerebene:** AWS verwaltet die AWS gehostete Kubernetes-Steuerebene des EKS-Clusters, und Sie verwalten die Hybridknoten, die in Ihren lokalen oder Edge-Umgebungen ausgeführt werden. Dadurch wird das Kubernetes-Management in Ihren Umgebungen vereinheitlicht und die Verwaltung der Kubernetes-Steuerebene auf Ihre lokalen und Edge-Anwendungen verlagert. AWS Durch die Umstellung der Kubernetes-Steuerungsebene auf diese können Sie lokale Kapazität für Ihre Anwendungen sparen und darauf vertrauen AWS, dass die Kubernetes-Steuerungsebene mit Ihren Workloads skaliert.
- **Konsistentes EKS-Erlebnis:** Die meisten EKS-Funktionen werden mit EKS-Hybridknoten unterstützt, um ein einheitliches EKS-Erlebnis in Ihren lokalen und Cloud-Umgebungen zu gewährleisten, einschließlich EKS-Add-Ons, EKS Pod Identity, Clusterzugriffseinträgen, Cluster-Erkennnissen, erweiterter Kubernetes-Versionsunterstützung und mehr. [the section called “Add-Ons konfigurieren”](#) Weitere Informationen zu den EKS-Add-Ons, die von EKS Hybrid Nodes unterstützt werden, finden Sie unter.
- **Zentralisierte Beobachtbarkeit und Identitätsmanagement:** EKS Hybrid Nodes lässt sich nativ in AWS Dienste wie AWS Systems Manager, AWS IAM Roles Anywhere, Amazon Managed Service for Prometheus und Amazon CloudWatch für zentrale Überwachung, Protokollierung und Identitätsverwaltung integrieren.
- **Burst-to-cloud oder lokale Kapazität hinzufügen:** Ein einziger EKS-Cluster kann verwendet werden, um Hybridknoten und Knoten in AWS Regionen, AWS Local Zones oder AWS Outposts zu betreiben oder lokale Kapazität zu burst-to-cloud Ihren EKS-Clustern hinzuzufügen. Weitere Informationen finden Sie unter [Überlegungen zu Clustern im gemischten Modus](#).
- **Flexible Infrastruktur:** EKS Hybrid Nodes folgt einem Bring Your Own Infrastructure-Ansatz und ist unabhängig von der Infrastruktur, die Sie für Hybridknoten verwenden. Sie können Hybridknoten

auf physischen oder virtuellen Maschinen sowie auf x86- und ARM-Architekturen ausführen, sodass Sie lokale Workloads, die auf Hybridknoten ausgeführt werden, über verschiedene Infrastrukturtypen hinweg migrieren können.

- **Flexibles Networking:** Mit EKS-Hybridknoten wird die Kommunikation zwischen der EKS-Steuerungsebene und den Hybridknoten über die VPC und die Subnetze geleitet, die Sie bei der Clustererstellung übergeben, was auf dem [bestehenden Mechanismus](#) in EKS für die Vernetzung von Kontrollebene zu Knoten aufbaut. Dies ist flexibel für Ihre bevorzugte Methode, Ihre lokalen Netzwerke mit einer VPC in zu verbinden. AWS Es stehen mehrere [dokumentierte Optionen](#) zur Verfügung, darunter AWS Site-to-Site VPN, AWS Direct Connect oder Ihre eigene VPN-Lösung, und Sie können die Methode wählen, die am besten zu Ihrem Anwendungsfall passt.

## Einschränkungen

- Pro Cluster werden bis zu 15 CIDRs für Remote Node Networks und 15 CIDRs für Remote Pod Networks unterstützt.

## Überlegungen

- EKS-Hybridknoten können mit neuen oder vorhandenen EKS-Clustern verwendet werden.
- EKS Hybrid Nodes ist in allen AWS Regionen verfügbar, mit Ausnahme der Regionen AWS GovCloud (USA) und der Regionen AWS China.
- EKS-Hybridknoten müssen über eine zuverlässige Verbindung zwischen Ihrer lokalen Umgebung und AWS verfügen. EKS-Hybridknoten eignen sich nicht für Umgebungen mit Unterbrechungen, Unterbrechungen, Unterbrechungen oder Einschränkungen (DDIL). Wenn Sie in einer DDIL-Umgebung arbeiten, sollten Sie [Amazon EKS](#) Anywhere in Betracht ziehen. Informationen darüber, wie sich [Hybridknoten bei Netzwerkunterbrechungen verhalten, finden Sie in den Best Practices für EKS-Hybridknoten](#).
- Das Ausführen von EKS-Hybridknoten in der Cloud-Infrastruktur, einschließlich AWS Regionen, AWS Local Zones, AWS Outposts oder in anderen Clouds, wird nicht unterstützt. Ihnen wird die Gebühr für Hybridknoten berechnet, wenn Sie Hybridknoten auf EC2 Amazon-Instances ausführen.
- Die Abrechnung für Hybridknoten beginnt, wenn die Knoten dem EKS-Cluster beitreten, und endet, wenn die Knoten aus dem Cluster entfernt werden. Achten Sie darauf, Ihre Hybridknoten aus Ihrem EKS-Cluster zu entfernen, wenn Sie sie nicht verwenden.

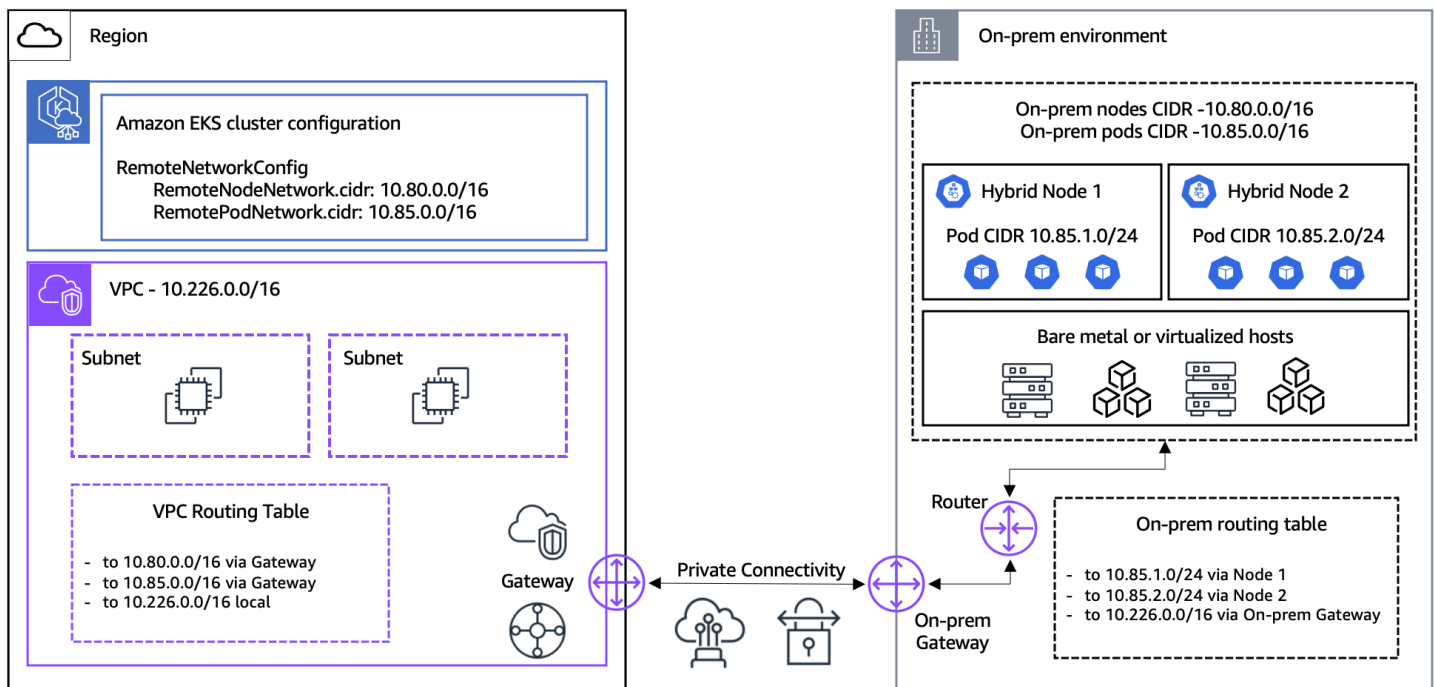
## Weitere Ressourcen

- [EKS-Hybridknoten-Workshop](#): Step-by-step Anweisungen zur Bereitstellung von EKS-Hybridknoten in einer Demo-Umgebung.
- [AWS re:Invent: EKS Hybrid Nodes](#): AWS re:Invent-Sitzung, in der die Markteinführung von EKS Hybrid Nodes vorgestellt wird. Ein Kunde zeigt, wie er EKS-Hybridknoten in seiner Umgebung einsetzt.
- [AWS re:POST: Clusternetzwerke für EKS-Hybridknoten](#): Artikel, in dem verschiedene Methoden zum Einrichten von Netzwerken für EKS-Hybridknoten erläutert werden.
- [AWS Blog: Führen Sie die GenAI-Inferenz mit EKS-Hybridknoten umgebungsübergreifend](#) aus: Blogbeitrag, der zeigt, wie Sie die GenAI-Inferenz mit EKS-Hybridknoten umgebungsübergreifend ausführen können.

## Vorbereitende Einrichtung für Hybridknoten

Um Amazon EKS-Hybridknoten verwenden zu können, müssen Sie private Konnektivität von Ihrer lokalen Umgebung zu/von AWS Bare-Metal-Servern oder virtuellen Maschinen mit einem unterstützten Betriebssystem haben und AWS IAM Roles Anywhere- oder AWS Systems Manager (SSM) -Hybridaktivierungen konfiguriert haben. Sie sind dafür verantwortlich, diese Voraussetzungen während des gesamten Lebenszyklus der Hybridknoten zu verwalten.

- Hybride Netzwerkkonnektivität von Ihrer lokalen Umgebung zu/von AWS
- Infrastruktur in Form von physischen oder virtuellen Maschinen
- Betriebssystem, das mit Hybridknoten kompatibel ist
- Lokaler Anbieter für IAM-Anmeldeinformationen konfiguriert



## Hybride Netzwerkkonnektivität

Die Kommunikation zwischen der Amazon EKS-Kontrollebene und den Hybridknoten wird über die VPC und die Subnetze geleitet, die Sie bei der Clustererstellung übergeben, was auf dem [bestehenden Mechanismus](#) in Amazon EKS für die Vernetzung von Kontrollebene zu Knoten aufbaut. Es stehen mehrere [dokumentierte Optionen](#) zur Verfügung, mit denen Sie Ihre lokale Umgebung mit Ihrer VPC verbinden können, darunter AWS Site-to-Site VPN, AWS Direct Connect oder Ihre eigene VPN-Verbindung. Weitere Informationen zur Verwendung dieser Lösungen für Ihre hybride Netzwerkverbindung finden Sie in den [AWS Site-to-Site VPN](#) - und [AWS Direct Connect-Benutzerhandbüchern](#).

Für ein optimales Erlebnis empfehlen wir eine zuverlässige Netzwerkkonnektivität von mindestens 100 Mbit/s und eine maximale Round-Trip-Latenz von 200 ms für die Verbindung der Hybridknoten mit der AWS Region. Dies ist eine allgemeine Anleitung, die für die meisten Anwendungsfälle geeignet ist, aber keine strikte Anforderung ist. Die Anforderungen an Bandbreite und Latenz können je nach Anzahl der Hybridknoten und Ihren Workload-Merkmalen variieren, z. B. Größe des Anwendungsimages, Anwendungselastizität, Überwachungs- und Protokollierungskonfigurationen und Anwendungsabhängigkeiten beim Zugriff auf Daten, die in anderen AWS Diensten gespeichert sind. Wir empfehlen, dass Sie vor der Bereitstellung in der Produktion Tests mit Ihren eigenen Anwendungen und Umgebungen durchführen, um sicherzustellen, dass Ihr Netzwerk-Setup den Anforderungen für Ihre Workloads entspricht.

## Netzwerkconfiguration vor Ort

Sie müssen den eingehenden Netzwerkzugriff von der Amazon EKS-Steuerebene auf Ihre lokale Umgebung aktivieren, damit die Amazon EKS-Steuerebene mit den auf Hybridknoten `kubelet` ausgeführten Knoten und optional mit Webhooks, die auf Ihren Hybridknoten ausgeführt werden, kommunizieren kann. Darüber hinaus müssen Sie den ausgehenden Netzwerkzugriff für Ihre Hybridknoten und die darauf ausgeführten Komponenten aktivieren, um mit der Amazon EKS-Steuerebene zu kommunizieren. Sie können diese Kommunikation so konfigurieren, dass sie für Ihre AWS Direct Connect-, AWS Site-to-Site VPN- oder Ihre eigene VPN-Verbindung vollständig privat bleibt.

Die CIDR-Bereiche (Classless Inter-Domain Routing), die Sie für Ihre lokalen Knoten- und Pod-Netzwerke verwenden, müssen RFC-1918-Adressbereiche verwenden IPv4. Ihr lokaler Router muss mit Routen zu Ihren lokalen Knoten und optional zu Pods konfiguriert sein. [the section called "Netzwerkconfiguration vor Ort"](#) Weitere Informationen zu den lokalen Netzwerkanforderungen, einschließlich der vollständigen Liste der erforderlichen Ports und Protokolle, die in Ihrer Firewall und Ihrer lokalen Umgebung aktiviert sein müssen, finden Sie unter.

## EKS-Cluster-Konfiguration

Um die Latenz zu minimieren, empfehlen wir Ihnen, Ihren Amazon EKS-Cluster in der AWS Region zu erstellen, die Ihrer lokalen Umgebung oder Edge-Umgebung am nächsten liegt. Sie übergeben Ihren lokalen Knoten und Pod CIDRs während der Amazon EKS-Clustererstellung über zwei API-Felder: `RemoteNodeNetwork` und `RemotePodNetwork`. Möglicherweise müssen Sie mit Ihrem lokalen Netzwerkteam darüber sprechen, wie Sie Ihren lokalen Knoten und Pod identifizieren können. CIDRs Der Knoten-CIDR wird von Ihrem lokalen Netzwerk zugewiesen, und der Pod-CIDR wird von dem Container Network Interface (CNI) zugewiesen, das Sie verwenden, wenn Sie ein Overlay-Netzwerk für Ihr CNI verwenden. Cilium und Calico verwenden standardmäßig Overlay-Netzwerke.

Der lokale Knoten und der Pod, die CIDRs Sie über die `RemotePodNetwork` Felder `RemoteNodeNetwork` und konfigurieren, werden verwendet, um die Amazon EKS-Steuerebene so zu konfigurieren, dass der Datenverkehr über Ihre VPC zu den `kubelet` und den Pods geleitet wird, die auf Ihren Hybridknoten ausgeführt werden. Ihr lokaler Knoten und Ihr Pod CIDRs dürfen sich nicht miteinander, mit der VPC-CIDR, die Sie bei der Clustererstellung übergeben, oder mit der IPv4 Servicekonfiguration für Ihren Amazon EKS-Cluster überschneiden.

Wir empfehlen, für den Amazon EKS Kubernetes API-Serverendpunkt entweder öffentlichen oder privaten Endpunktzugriff zu verwenden. Wenn Sie „Öffentlich und privat“ wählen, wird der Amazon EKS Kubernetes API-Serverendpunkt IPs für Hybridknoten, die außerhalb Ihrer VPC laufen, immer



öffentlich aufgelöst, wodurch verhindert werden kann, dass Ihre Hybridknoten dem Cluster beitreten. Wenn Sie den öffentlichen Endpunktzugriff verwenden, wird der Kubernetes-API-Serverendpunkt öffentlich aufgelöst IPs und die Kommunikation von Hybridknoten zur Amazon EKS-Kontrollebene wird über das Internet geleitet. Wenn Sie privaten Endpunktzugriff wählen, wird der Kubernetes-API-Serverendpunkt in privat aufgelöst IPs und die Kommunikation von Hybridknoten zur Amazon EKS-Kontrollebene wird über Ihre private Konnektivitätsverbindung, in den meisten Fällen AWS Direct Connect oder VPN, geleitet. AWS Site-to-Site

## VPC-Konfiguration

Sie müssen die VPC, die Sie bei der Erstellung des Amazon EKS-Clusters übergeben, mit Routen in der Routing-Tabelle für Ihren lokalen Knoten und optional mit Pod-Netzwerken mit Ihrem Virtual Private Gateway (VGW) oder Transit Gateway (TGW) als Ziel konfigurieren. Es folgt ein Beispiel. Ersetzen Sie `REMOTE_NODE_CIDR` und durch die Werte für `REMOTE_POD_CIDR` Ihr lokales Netzwerk.

| Bestimmungsort                | Ziel             | Beschreibung                                              |
|-------------------------------|------------------|-----------------------------------------------------------|
| 10.226.0.0/16                 | local            | Lokaler Verkehr zu den VPC-Routen innerhalb der VPC       |
| <code>REMOTE_NODE_CIDR</code> | tgw-abcdef123456 | CIDR am lokalen Knoten, leitet den Verkehr zum TGW weiter |
| <code>REMOTE_POD_CIDR</code>  | tgw-abcdef123456 | CIDR vor Ort, leitet den Verkehr zum TGW weiter           |

## Sicherheitsgruppenkonfiguration

Wenn Sie einen Cluster erstellen, erstellt Amazon EKS eine Sicherheitsgruppe mit einem Namen `eks-cluster-sg-<cluster-name>-<uniqueID>`. Sie können die Regeln für eingehende Nachrichten dieser Cluster-Sicherheitsgruppe nicht ändern, aber Sie können die Regeln für ausgehenden Datenverkehr einschränken. Sie müssen Ihrem Cluster eine zusätzliche Sicherheitsgruppe hinzufügen, damit das Kubelet und optional Webhooks, die auf Ihren Hybridknoten ausgeführt werden, die Amazon EKS-Kontrollebene kontaktieren können. Die erforderlichen Regeln für eingehende Nachrichten für diese zusätzliche Sicherheitsgruppe sind unten aufgeführt. Ersetzen Sie `REMOTE_NODE_CIDR` und `REMOTE_POD_CIDR` durch die Werte für Ihr lokales Netzwerk.

| Name                       | Regel-ID der Sicherheitsgruppe | IP-Version | Typ   | Protocol (Protokoll) | Port-Bereich | Quelle           |
|----------------------------|--------------------------------|------------|-------|----------------------|--------------|------------------|
| Eingehender On-Prem-Knoten | sgr-abcdef123456               | IPv4       | HTTPS | TCP                  | 443          | REMOTE_NODE_CIDR |
| Eingehender On-Prem-Pod    | sgr-abcdef654321               | IPv4       | HTTPS | TCP                  | 443          | REMOTE_POD_CIDR  |

## Infrastruktur

Sie müssen über Bare-Metal-Server oder virtuelle Maschinen verfügen, die Sie als Hybridknoten verwenden können. Hybridknoten sind unabhängig von der zugrunde liegenden Infrastruktur und unterstützen x86- und ARM-Architekturen. Amazon EKS Hybrid Nodes folgt einem „Bring Your Own Infrastructure“-Ansatz, bei dem Sie für die Bereitstellung und Verwaltung der Bare-Metal-Server oder virtuellen Maschinen verantwortlich sind, die Sie für Hybridknoten verwenden. Es gibt zwar keine strengen Mindestressourcenanforderungen, wir empfehlen jedoch, Hosts mit mindestens 1 vCPU und 1 GiB RAM für Hybridknoten zu verwenden.

## Betriebssystem

Bottlerocket, Amazon Linux 2023 (AL2023), Ubuntu und RHEL werden fortlaufend für die Verwendung als Knotenbetriebssystem für Hybridknoten validiert. Bottlerocket wird nur AWS in VMware vSphere-Umgebungen unterstützt. AL2023 ist nicht durch AWS Supportpläne abgedeckt, wenn sie außerhalb von Amazon EC2 ausgeführt werden. AL2023 kann nur in lokalen virtualisierten Umgebungen verwendet werden. Weitere Informationen finden Sie im [Amazon Linux 2023 User Guide](#). AWS unterstützt die Integration von Hybridknoten mit Ubuntu- und RHEL-Betriebssystemen, bietet jedoch keine Unterstützung für das Betriebssystem selbst.

Sie sind für die Bereitstellung und Verwaltung des Betriebssystems verantwortlich. Wenn Sie Hybridknoten zum ersten Mal testen, ist es am einfachsten, die Amazon EKS Hybrid Nodes CLI (nodeadm) auf einem bereits bereitgestellten Host auszuführen. Für Produktionsbereitstellungen

empfehlen wir, dass Sie `nodeadm` in Ihr goldenes Betriebssystem Images aufnehmen, die so konfiguriert sind, dass sie als `Systemd-Service` ausgeführt werden, um Hosts beim Host-Start automatisch mit Amazon EKS-Clustern zu verbinden.

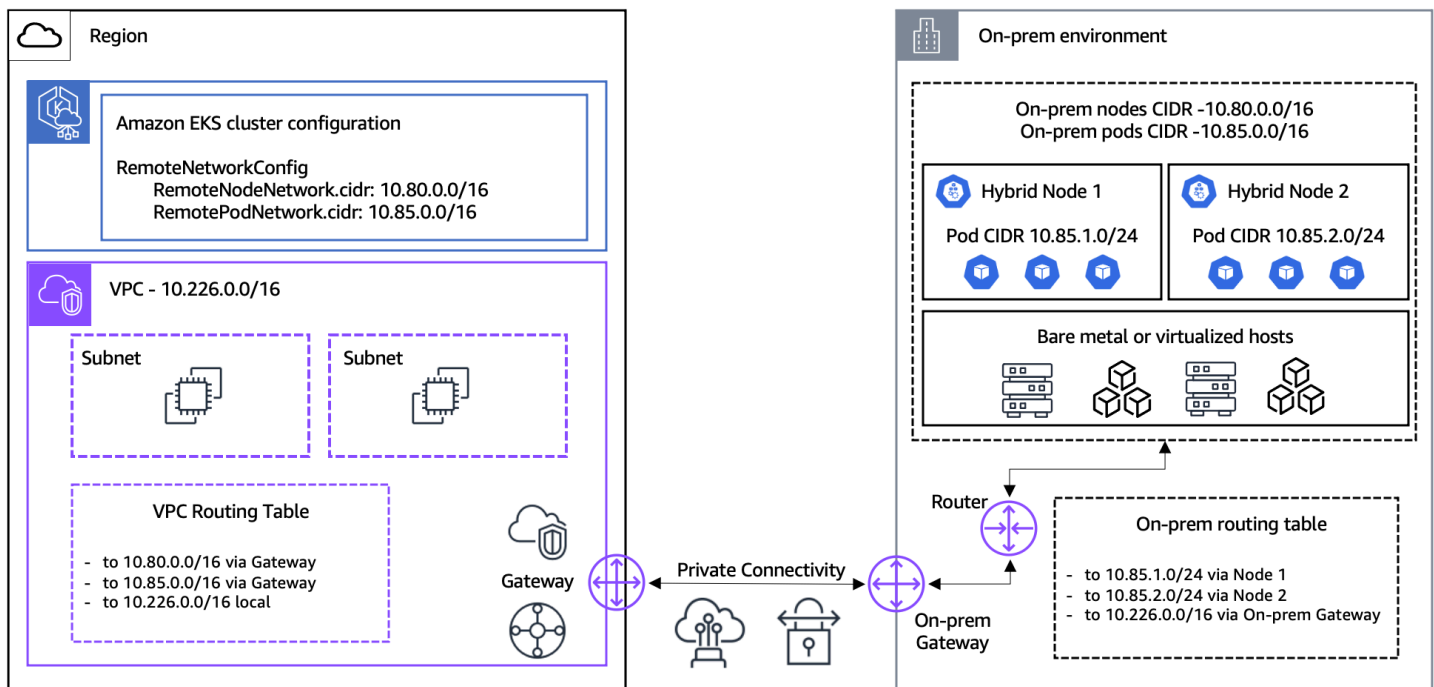
## Anbieter von IAM-Anmeldeinformationen vor Ort

Amazon EKS-Hybridknoten verwenden temporäre IAM-Anmeldeinformationen, die durch AWS SSM-Hybrid-Aktivierungen oder AWS IAM Roles Anywhere bereitgestellt werden, um sich beim Amazon EKS-Cluster zu authentifizieren. Sie müssen entweder AWS SSM-Hybrid-Aktivierungen oder AWS IAM Roles Anywhere mit der Amazon EKS Hybrid Nodes CLI () verwenden. `nodeadm` Wir empfehlen, AWS SSM-Hybrid-Aktivierungen zu verwenden, wenn Sie nicht über eine bestehende Public Key-Infrastruktur (PKI) mit einer Zertifizierungsstelle (CA) und Zertifikaten für Ihre lokalen Umgebungen verfügen. Wenn Sie bereits über PKI und Zertifikate vor Ort verfügen, verwenden Sie IAM Roles Anywhere. AWS

Ähnlich wie bei Knoten, die auf Amazon laufen EC2, erstellen Sie eine IAM-Rolle [the section called “Knoten-IAM-Rolle”](#) für Hybridknoten mit den erforderlichen Berechtigungen, um Hybridknoten mit Amazon EKS-Clustern zu verbinden. Wenn Sie AWS IAM Roles Anywhere verwenden, konfigurieren Sie eine Vertrauensrichtlinie, die es AWS IAM Roles Anywhere ermöglicht, die IAM-Rolle Hybrid Nodes zu übernehmen, und konfigurieren Sie Ihr AWS IAM Roles Anywhere-Profil mit der Hybrid Nodes IAM-Rolle als wahrscheinlicher Rolle. Wenn Sie AWS SSM verwenden, konfigurieren Sie eine Vertrauensrichtlinie, die es AWS SSM ermöglicht, die IAM-Rolle Hybrid Nodes zu übernehmen und die Hybrid-Aktivierung mit der Hybrid Nodes IAM-Rolle zu erstellen. Informationen [the section called “Bereiten Sie die Anmeldeinformationen vor”](#) zum Erstellen der IAM-Rolle Hybrid Nodes mit den erforderlichen Berechtigungen finden Sie unter.

## Bereiten Sie das Netzwerk für Hybridknoten vor

Dieses Thema bietet einen Überblick über die Netzwerkkonfiguration, die Sie konfiguriert haben müssen, bevor Sie Ihren Amazon EKS-Cluster erstellen und Hybridknoten anhängen. In diesem Leitfaden wird davon ausgegangen, dass Sie die Voraussetzungen für Hybrid-Netzwerkkonnektivität mit [AWS Site-to-Site VPN](#), [AWS Direct Connect](#) oder Ihrer eigenen VPN-Lösung erfüllt haben.



## Netzwerkconfiguration vor Ort

### Mindestanforderungen an das Netzwerk

Für ein optimales Erlebnis empfehlen wir eine zuverlässige Netzwerkkonnektivität von mindestens 100 Mbit/s und eine maximale Round-Trip-Latenz von 200 ms für die Verbindung der Hybridknoten mit der AWS Region. Dies ist eine allgemeine Anleitung, die für die meisten Anwendungsfälle geeignet ist, aber keine strikte Anforderung ist. Die Anforderungen an Bandbreite und Latenz können je nach Anzahl der Hybridknoten und Ihren Workload-Merkmalen variieren, z. B. Größe des Anwendungsimages, Anwendungselastizität, Überwachungs- und Protokollierungskonfigurationen und Anwendungsabhängigkeiten beim Zugriff auf Daten, die in anderen AWS Diensten gespeichert sind. Wir empfehlen, dass Sie vor der Bereitstellung in der Produktion Tests mit Ihren eigenen Anwendungen und Umgebungen durchführen, um sicherzustellen, dass Ihr Netzwerk-Setup den Anforderungen für Ihre Workloads entspricht.

### Lokaler Knoten und Pod CIDRs

Identifizieren Sie den Knoten und den Pod, den CIDRs Sie für Ihre Hybridknoten und die darauf ausgeführten Workloads verwenden werden. Der Node-CIDR wird von Ihrem lokalen Netzwerk zugewiesen und der Pod-CIDR wird von Ihrem Container Network Interface (CNI) zugewiesen, wenn Sie ein Overlay-Netzwerk für Ihr CNI verwenden. Sie übergeben Ihren lokalen Knoten CIDRs und Pod CIDRs als Eingaben, wenn Sie Ihren EKS-Cluster mit den Feldern und erstellen. RemoteNodeNetwork RemotePodNetwork Ihr lokaler Knoten CIDRs muss in Ihrem lokalen

Netzwerk routingfähig sein. Im folgenden Abschnitt finden Sie Informationen zur Routbarkeit des lokalen Pod-CIDR-Pods.

Die lokalen Knoten- und Pod-CIDR-Blöcke müssen die folgenden Anforderungen erfüllen:

1. Innerhalb eines der folgenden IPv4 RFC-1918-Bereiche liegen: `10.0.0.0/8`, oder `172.16.0.0/12` `192.168.0.0/16`
2. Überschneiden Sie sich nicht miteinander, mit dem VPC-CIDR für Ihren EKS-Cluster oder Ihrem Kubernetes-Dienst-CIDR. IPv4

## Pod-Netzwerk-Routing vor Ort

Wenn Sie EKS-Hybridknoten verwenden, empfehlen wir generell, Ihren lokalen Pod in Ihrem lokalen Netzwerk CIDRs routingfähig zu machen, um die vollständige Cluster-Kommunikation und Funktionalität zwischen Cloud- und lokalen Umgebungen zu ermöglichen.

## Routbare Pod-Netzwerke

Wenn Sie Ihr Pod-Netzwerk in Ihrem lokalen Netzwerk routingfähig machen können, folgen Sie den nachstehenden Anweisungen.

1. Konfigurieren Sie das `RemotePodNetwork` Feld für Ihren EKS-Cluster mit Ihrem lokalen Pod-CIDR, Ihre VPC-Routing-Tabellen mit Ihrem lokalen Pod-CIDR und Ihre EKS-Cluster-Sicherheitsgruppe mit Ihrem lokalen Pod-CIDR.
2. Es gibt verschiedene Techniken, mit denen Sie Ihren lokalen Pod-CIDR in Ihrem lokalen Netzwerk routingfähig machen können, darunter Border Gateway Protocol (BGP), statische Routen oder andere benutzerdefinierte Routing-Lösungen. BGP ist die empfohlene Lösung, da sie skalierbarer und einfacher zu verwalten ist als alternative Lösungen, die eine benutzerdefinierte oder manuelle Routenkonfiguration erfordern. AWS unterstützt die BGP-Funktionen von Cilium und Calico für Werbe-Pods CIDRs. Weitere Informationen finden Sie unter [the section called "CNI konfigurieren"](#) und [the section called "Routbarer Remote-Pod CIDRs"](#).
3. Webhooks können auf Hybridknoten ausgeführt werden, da die EKS-Steuerebene mit den Pod-IP-Adressen kommunizieren kann, die den Webhooks zugewiesen sind.
4. Workloads, die auf Cloud-Knoten ausgeführt werden, können direkt mit Workloads kommunizieren, die auf Hybridknoten im selben EKS-Cluster ausgeführt werden.
5. Andere AWS Dienste, wie AWS Application Load Balancers und Amazon Managed Service for Prometheus, können mit Workloads kommunizieren, die auf Hybridknoten ausgeführt werden, um den Netzwerkverkehr auszugleichen und Pod-Metriken auszuwerten.

## Pod-Netzwerke, die nicht routbar sind

Wenn Sie Ihre Pod-Netzwerke in Ihrem lokalen Netzwerk nicht routingfähig machen können, folgen Sie den nachstehenden Anweisungen.

1. Webhooks können nicht auf Hybridknoten ausgeführt werden, da Webhooks Konnektivität von der EKS-Steuerebene zu den Pod-IP-Adressen erfordern, die den Webhooks zugewiesen sind. In diesem Fall empfehlen wir, Webhooks auf Cloud-Knoten im selben EKS-Cluster wie Ihre Hybridknoten auszuführen. Weitere Informationen finden Sie unter [the section called “Webhooks konfigurieren”](#).
2. Workloads, die auf Cloud-Knoten ausgeführt werden, können nicht direkt mit Workloads kommunizieren, die auf Hybridknoten ausgeführt werden, wenn VPC CNI für Cloud-Knoten und Cilium oder Calico für Hybridknoten verwendet werden.
3. Verwenden Sie Service Traffic Distribution, um den Datenverkehr lokal in der Zone zu halten, aus der er stammt. Weitere Informationen zur Verteilung des Dienstverkehrs finden Sie unter [the section called “Konfigurieren Sie die Verteilung des Servicedatenverkehrs”](#).
4. Konfigurieren Sie Ihr CNI so, dass Egress Masquerade oder Network Address Translation (NAT) für den Pod-Verkehr verwendet wird, wenn dieser Ihre lokalen Hosts verlässt. Dies ist in Cilium standardmäßig aktiviert. Calico muss `natOutgoing` auf eingestellt sein. `true`
5. Andere AWS Dienste, wie AWS Application Load Balancers und Amazon Managed Service for Prometheus, können nicht mit Workloads kommunizieren, die auf Hybridknoten ausgeführt werden.

Während der Installation und des Upgrades des Hybridknotens ist Zugriff erforderlich

Während des Installationsvorgangs, bei dem Sie die Abhängigkeiten der Hybridknoten auf Ihren Hosts installieren, müssen Sie Zugriff auf die folgenden Domänen haben. Dieser Vorgang kann einmal ausgeführt werden, wenn Sie Ihre Betriebssystem-Images erstellen, oder er kann auf jedem Host zur Laufzeit ausgeführt werden. Dazu gehören die Erstinstallation und das Upgrade der Kubernetes-Version Ihrer Hybridknoten.

| Komponente               | URL                                                 | Protokoll | Port |
|--------------------------|-----------------------------------------------------|-----------|------|
| EKS-Knotenartefakte (S3) | <code>https://hybrid-asset.eks.amazonaws.com</code> | HTTPS     | 443  |

| Komponente                                    | URL                                                                                                                        | Protokoll | Port |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-----------|------|
| <a href="#">EKS-Dienstendpunkte</a>           | https://eks.<br><i>region</i> .amazonaws.com                                                                               | HTTPS     | 443  |
| <a href="#">ECR-Serviceendpunkte</a>          | https://api.ecr.<br><i>region</i> .amazonaws.com                                                                           | HTTPS     | 443  |
| EKS ECR-Endpunkte                             | Informationen zu regionalen <a href="#">the section called “Amazon-Bildregister anzeigen”</a> Endpunkten finden Sie unter. | HTTPS     | 443  |
| Binärer SSM-Endpunkt 1                        | https://amazon-ssm - <i>region</i> .s3.<br><i>region</i> .amazonaws.com                                                    | HTTPS     | 443  |
| <a href="#">SSM-Dienstendpunkt 1</a>          | https://ssm.<br><i>region</i> .amazonaws.com                                                                               | HTTPS     | 443  |
| Binärer IAM Anywhere-Endpunkt 2               | https://rolesanywhere.amazonaws.com                                                                                        | HTTPS     | 443  |
| <a href="#">IAM Anywhere-Dienstendpunkt 2</a> | https://rolesanywhere.<br><i>region</i> .amazonaws.com                                                                     | HTTPS     | 443  |

### Note

<sup>1</sup> Der Zugriff auf die AWS SSM-Endpunkte ist nur erforderlich, wenn Sie SSM-Hybrid-Aktivierungen für Ihren lokalen AWS IAM-Anmeldeinformationsanbieter verwenden.

<sup>2</sup> Der Zugriff auf die AWS IAM-Endpunkte ist nur erforderlich, wenn Sie IAM Roles Anywhere für Ihren lokalen AWS IAM-Anmeldeinformationsanbieter verwenden.

Für den laufenden Clusterbetrieb ist Zugriff erforderlich

Der folgende Netzwerkzugriff für Ihre lokale Firewall ist für den laufenden Clusterbetrieb erforderlich.

**⚠ Important**

Je nachdem, für welches CNI Sie sich entscheiden, müssen Sie zusätzliche Netzwerkzugriffsregeln für die CNI-Ports konfigurieren. Einzelheiten finden Sie in der [Cilium-Dokumentation](#) und der [Calico-Dokumentation](#).

| Typ   | Protokoll | Richtung  | Port | Quelle                     | Ziel                               | Verwendung                                                                      |
|-------|-----------|-----------|------|----------------------------|------------------------------------|---------------------------------------------------------------------------------|
| HTTPS | TCP       | Ausgehend | 443  | CIDR (s) für Remote-Knoten | EKS-Cluster 1 IPs                  | Kubelet-zu-Kubernetes-API-Server                                                |
| HTTPS | TCP       | Ausgehend | 443  | CIDR (s) für Remote-Pods   | EKS-Cluster 1 IPs                  | Vom Pod zum Kubernetes-API-Server                                               |
| HTTPS | TCP       | Ausgehend | 443  | CIDR (s) für Remote-Knoten | <a href="#">SSM-Dienstendpunkt</a> | SSM-Hybrid-Aktivierungen, Aktualisierung der Anmeldeinformationen und SSM-Heart |



| Typ   | Protokoll | Richtung  | Port  | Quelle                     | Ziel                                                               | Verwendung                                                                        |
|-------|-----------|-----------|-------|----------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|       |           |           |       |                            |                                                                    | beats alle 5 Minuten                                                              |
| HTTPS | TCP       | Ausgehend | 443   | CIDR (s) für Remote-Knoten | <a href="#">IAM Anywhere-Dienstendpunkt</a>                        | Aktualisierung der Anmeldeinformationen für IAM Roles Anywhere                    |
| HTTPS | TCP       | Ausgehend | 443   | CIDR (s) für Remote-Pods   | <a href="#">Regionaler STS-Endpunkt</a>                            | Pod zum STS-Endpunkt, nur für IRSA erforderlich                                   |
| HTTPS | TCP       | Ausgehend | 443   | CIDR (s) für Remote-Knoten | <a href="#">Endpunkt des Amazon EKS-Authentifizierungsdienstes</a> | Knoten zum Amazon EKS Auth-Endpunkt, nur für Amazon EKS Pod Identity erforderlich |
| HTTPS | TCP       | Eingehend | 10250 | EKS-Cluster 1 IPs          | CIDR (s) für Remote-Knoten                                         | Vom Kubernetes-API-Server zum Kubelet                                             |

| Typ               | Protokoll         | Richtung             | Port               | Quelle                   | Ziel                     | Verwendung                                                                                                                                                 |
|-------------------|-------------------|----------------------|--------------------|--------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPS             | TCP               | Eingehend            | Webhook-Anschlüsse | EKS-Cluster 1 IPs        | CIDR (s) für Remote-Pods | Kubernetes-API-Server für Webhooks                                                                                                                         |
| HTTPS             | TCP, UDP          | Eingehend, Ausgehend | 53                 | CIDR (s) für Remote-Pods | CIDR (s) für Remote-Pods | Pod zu CoreDNS. Wenn Sie mindestens ein CoreDNS-Replikat in der Cloud ausführen, müssen Sie DNS-Verkehr zur VPC zulassen, auf der CoreDNS ausgeführt wird. |
| Benutzerdefiniert | Benutzerdefiniert | Eingehend, Ausgehend | App-Ports          | CIDR (s) für Remote-Pods | CIDR (s) für Remote-Pods | Pod zu Pod                                                                                                                                                 |

 Note

<sup>1</sup> Der IPs des EKS-Clusters. Weitere Informationen finden Sie im folgenden Abschnitt über elastische Netzwerkschnittstellen von Amazon EKS.

## Amazon EKS-Netzwerkschnittstellen

Amazon EKS fügt Netzwerkschnittstellen an die Subnetze in der VPC an, die Sie bei der Clustererstellung übergeben haben, um die Kommunikation zwischen der EKS-Steuerebene und Ihrer VPC zu ermöglichen. Die Netzwerkschnittstellen, die Amazon EKS erstellt, finden Sie nach der Cluster-Erstellung in der EC2 Amazon-Konsole oder mit der AWS CLI. Die ursprünglichen Netzwerkschnittstellen werden gelöscht und neue Netzwerkschnittstellen werden erstellt, wenn Änderungen an Ihrem EKS-Cluster vorgenommen werden, z. B. bei Upgrades der Kubernetes-Version. Sie können den IP-Bereich für die Amazon EKS-Netzwerkschnittstellen einschränken, indem Sie eingeschränkte Subnetzgrößen für die Subnetze verwenden, die Sie bei der Clustererstellung passieren. Dies macht es einfacher, Ihre lokale Firewall so zu konfigurieren, dass inbound/outbound Konnektivität zu dieser bekannten, eingeschränkten Gruppe von Verbindungen möglich ist. IPs Um zu kontrollieren, in welchen Subnetzen Netzwerkschnittstellen erstellt werden, können Sie die Anzahl der Subnetze einschränken, die Sie bei der Erstellung eines Clusters angeben, oder Sie können die Subnetze nach der Erstellung des Clusters aktualisieren.

Die von Amazon EKS bereitgestellten Netzwerkschnittstellen haben eine Beschreibung des Formats `Amazon EKS your-cluster-name`. Im folgenden Beispiel finden Sie einen AWS CLI-Befehl, mit dem Sie die IP-Adressen der Netzwerkschnittstellen ermitteln können, die Amazon EKS bereitstellt. `VPC_ID` Ersetzen Sie durch die ID der VPC, die Sie bei der Clustererstellung übergeben haben.

```
aws ec2 describe-network-interfaces \
--query 'NetworkInterfaces[?(VpcId == VPC_ID && contains(Description,Amazon
EKS))].PrivateIpAddress'
```

## AWS VPC- und Subnetz-Setup

Die bestehenden [VPC- und Subnetzanforderungen](#) für Amazon EKS gelten für Cluster mit Hybridknoten. Darüber hinaus darf sich Ihr VPC-CIDR nicht mit Ihrem lokalen Knoten und Pod überschneiden. CIDRs Sie müssen Routen in Ihrer VPC-Routingtabelle für Ihren lokalen Knoten und optional den Pod konfigurieren. CIDRs Diese Routen müssen so eingerichtet werden, dass der Verkehr an das Gateway weitergeleitet wird, das Sie für Ihre hybride Netzwerkkonnektivität verwenden. Dabei handelt es sich in der Regel um ein Virtual Private Gateway (VGW) oder Transit Gateway (TGW). Wenn Sie TGW oder VGW verwenden, um Ihre VPC mit Ihrer lokalen Umgebung zu verbinden, müssen Sie einen TGW- oder VGW-Anhang für Ihre VPC erstellen. Ihre VPC muss DNS-Hostnamen und die DNS-Auflösung unterstützen.

Die folgenden Schritte verwenden die AWS CLI. Sie können diese Ressourcen auch in AWS Management Console oder mit anderen Schnittstellen wie AWS CloudFormation AWS CDK oder Terraform erstellen.

## Schritt 1: VPC erstellen

1. Führen Sie den folgenden Befehl aus, um eine VPC zu erstellen. `VPC_CIDR` Ersetzen Sie es durch einen CIDR-Bereich IPv4 gemäß RFC-1918 (privat) oder einen CIDR-Bereich außerhalb von RFC-1918 (öffentlich) (z. B.). `10.0.0.0/16` Hinweis: Die DNS-Auflösung, die eine EKS-Anforderung ist, ist standardmäßig für die VPC aktiviert.

```
aws ec2 create-vpc --cidr-block VPC_CIDR
```

2. Aktivieren Sie DNS-Hostnamen für Ihre VPC. Beachten Sie, dass die DNS-Auflösung standardmäßig für die VPC aktiviert ist. `VPC_ID` Ersetzen Sie durch die ID der VPC, die Sie im vorherigen Schritt erstellt haben.

```
aws ec2 modify-vpc-attribute --vpc-id VPC_ID --enable-dns-hostnames
```

## Schritt 2: Subnetze erstellen

Erstellen Sie mindestens 2 Subnetze. Amazon EKS verwendet diese Subnetze für die Cluster-Netzwerkschnittstellen. Weitere Informationen finden Sie unter [Anforderungen und Überlegungen zu Subnetzen](#).

1. Sie können die Verfügbarkeitszonen für eine AWS Region mit dem folgenden Befehl ermitteln. Ersetze es `us-west-2` durch deine Region.

```
aws ec2 describe-availability-zones \
 --query 'AvailabilityZones[?(RegionName == us-west-2)].ZoneName'
```

2. Erstellen Sie ein Subnetz. `VPC_ID` Ersetzen Sie durch die ID der VPC. `SUBNET_CIDR` Ersetzen Sie durch den CIDR-Block für Ihr Subnetz (z. B. `10.0.1.0/24`). `AZ` Ersetzen Sie es durch die Availability Zone, in der das Subnetz erstellt wird (z. B. `us-west-2a`). Die Subnetze, die Sie erstellen, müssen sich in mindestens 2 verschiedenen Verfügbarkeitszonen befinden.

```
aws ec2 create-subnet \
 --vpc-id VPC_ID \
```

```
--cidr-block SUBNET_CIDR \
--availability-zone AZ
```

(Optional) Schritt 3: Verbinden Sie VPC mit Amazon VPC Transit Gateway (TGW) oder AWS Direct Connect Virtual Private Gateway (VGW)

Wenn Sie ein TGW oder VGW verwenden, schließen Sie Ihre VPC an das TGW oder VGW an. Weitere Informationen finden Sie unter [Amazon VPC-Anlagen in Amazon VPC Transit Gateways- oder AWS Direct Connect Virtual Private Gateway-Verknüpfungen](#).

### Transit-Gateway

Führen Sie den folgenden Befehl aus, um ein Transit Gateway anzuhängen. VPC\_ID Ersetzen Sie durch die ID der VPC. Ersetzen Sie SUBNET\_ID1 und SUBNET\_ID2 durch die IDs der Subnetze, die Sie im vorherigen Schritt erstellt haben. TGW\_ID Ersetzen Sie es durch die ID Ihres TGW.

```
aws ec2 create-transit-gateway-vpc-attachment \
--vpc-id VPC_ID \
--subnet-ids SUBNET_ID1 SUBNET_ID2 \
--transit-gateway-id TGW_ID
```

### Virtuelles privates Gateway

Führen Sie den folgenden Befehl aus, um ein Transit Gateway anzuhängen. VPN\_ID Ersetzen Sie es durch die ID Ihres VGW. VPC\_ID Ersetzen Sie durch die ID der VPC.

```
aws ec2 attach-vpn-gateway \
--vpn-gateway-id VPN_ID \
--vpc-id VPC_ID
```

### (Optional) Schritt 4: Routentabelle erstellen

Sie können die Hauptroutentabelle für die VPC ändern oder eine benutzerdefinierte Routentabelle erstellen. Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Routing-Tabelle mit den Routen zum lokalen Knoten und Pod. CIDRs Weitere Informationen finden Sie unter [Subnetz-Routentabellen](#). VPC\_ID Ersetzen Sie durch die ID der VPC.

```
aws ec2 create-route-table --vpc-id VPC_ID
```

## Schritt 5: Erstellen Sie Routen für lokale Knoten und Pods

Erstellen Sie Routen in der Routentabelle für jeden Ihrer lokalen Remote-Knoten. Sie können die Hauptroutentabelle für die VPC ändern oder die benutzerdefinierte Routentabelle verwenden, die Sie im vorherigen Schritt erstellt haben.

Die folgenden Beispiele zeigen, wie Sie Routen für Ihren lokalen Knoten und Pod erstellen. CIDRs In den Beispielen wird ein Transit Gateway (TGW) verwendet, um die VPC mit der lokalen Umgebung zu verbinden. Wenn Sie mehrere lokale Knoten und Pods haben CIDRs, wiederholen Sie die Schritte für jeden CIDR.

- Wenn Sie ein Internet-Gateway oder ein Virtual Private Gateway (VGW) verwenden, ersetzen Sie es durch. `--transit-gateway-id --gateway-id`
- `RT_ID` Ersetzen Sie es durch die ID der Routing-Tabelle, die Sie im vorherigen Schritt erstellt haben.
- `REMOTE_NODE_CIDR` Ersetzen Sie es durch den CIDR-Bereich, den Sie für Ihre Hybridknoten verwenden werden.
- `REMOTE_POD_CIDR` Ersetzen Sie es durch den CIDR-Bereich, den Sie für die Pods verwenden werden, die auf Hybridknoten ausgeführt werden. Der Pod-CIDR-Bereich entspricht der Container Networking Interface (CNI) -Konfiguration, bei der am häufigsten ein lokales Overlay-Netzwerk verwendet wird. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#).
- Ersetzen Sie es `TGW_ID` durch die ID Ihres TGW.

## Netzwerk mit Remote-Knoten

```
aws ec2 create-route \
 --route-table-id RT_ID \
 --destination-cidr-block REMOTE_NODE_CIDR \
 --transit-gateway-id TGW_ID
```

## Remote-Pod-Netzwerk

```
aws ec2 create-route \
 --route-table-id RT_ID \
 --destination-cidr-block REMOTE_POD_CIDR \
 --transit-gateway-id TGW_ID
```

```
--destination-cidr-block REMOTE_POD_CIDR \
--transit-gateway-id TGW_ID
```

### (Optional) Schritt 6: Ordnen Sie Subnetze der Routentabelle zu

Wenn Sie im vorherigen Schritt eine benutzerdefinierte Routing-Tabelle erstellt haben, ordnen Sie jedes der Subnetze, die Sie im vorherigen Schritt erstellt haben, Ihrer benutzerdefinierten Routentabelle zu. Wenn Sie die VPC-Hauptroutentabelle ändern, werden die Subnetze automatisch der Hauptroutentabelle der VPC zugeordnet, und Sie können diesen Schritt überspringen.

Führen Sie den folgenden Befehl für jedes der Subnetze aus, die Sie in den vorherigen Schritten erstellt haben. *RT\_ID* ersetzen Sie es durch die Routing-Tabelle, die Sie im vorherigen Schritt erstellt haben. *SUBNET\_ID* ersetzen Sie durch die ID eines Subnetzes.

```
aws ec2 associate-route-table --route-table-id RT_ID --subnet-id SUBNET_ID
```

### Konfiguration der Cluster-Sicherheitsgruppe

Der folgende Zugriff für Ihre EKS-Cluster-Sicherheitsgruppe ist für den laufenden Clusterbetrieb erforderlich.

| Typ   | Protokoll | Richtung  | Port | Quelle                     | Ziel | Verwendung                                                               |
|-------|-----------|-----------|------|----------------------------|------|--------------------------------------------------------------------------|
| HTTPS | TCP       | Eingehend | 443  | CIDR (s) für Remote-Knoten | N/A  | Kubelet- zu-Kubernetes-API-Server                                        |
| HTTPS | TCP       | Eingehend | 443  | CIDR (s) für Remote-Pods   | N/A  | Pods, die Zugriff auf den API-Server von K8 benötigen, wenn das CNI kein |

| Typ   | Protokoll | Richtung  | Port               | Quelle | Ziel                       | Verwendung                                                                               |
|-------|-----------|-----------|--------------------|--------|----------------------------|------------------------------------------------------------------------------------------|
|       |           |           |                    |        |                            | NAT für den Pod-Verkehr verwendet.                                                       |
| HTTPS | TCP       | Ausgehend | 10250              | N/A    | CIDR (s) für Remote-Knoten | Kubernetes-API-Server zu Kubelet                                                         |
| HTTPS | TCP       | Ausgehend | Webhook-Anschlüsse | N/A    | CIDR (s) für Remote-Pods   | Vom Kubernetes-API-Server zum Webhook (wenn Webhooks auf Hybridknoten ausgeführt werden) |

Führen Sie die folgenden Befehle aus, um eine Sicherheitsgruppe mit den Regeln für den eingehenden Zugriff zu erstellen. Diese Sicherheitsgruppe muss übergeben werden, wenn Sie Ihren Amazon EKS-Cluster erstellen. Standardmäßig erstellt der folgende Befehl eine Sicherheitsgruppe, die den gesamten ausgehenden Zugriff ermöglicht. Sie können den ausgehenden Zugriff so einschränken, dass er nur die oben genannten Regeln einbezieht. Wenn Sie erwägen, die Regeln für ausgehenden Datenverkehr einzuschränken, empfehlen wir Ihnen, alle Ihre Anwendungen und die Pod-Konnektivität gründlich zu testen, bevor Sie Ihre geänderten Regeln auf einen Produktionscluster anwenden.

- Ersetzen Sie den Befehl im ersten Befehl SG\_NAME durch einen Namen für Ihre Sicherheitsgruppe



- Ersetzen Sie im ersten Befehl VPC\_ID durch die ID der VPC, die Sie im vorherigen Schritt erstellt haben
- Ersetzen Sie im zweiten Befehl SG\_ID durch die ID der Sicherheitsgruppe, die Sie im ersten Befehl erstellt haben
- Ersetzen Sie im zweiten Befehl REMOTE\_NODE\_CIDR und REMOTE\_POD\_CIDR durch die Werte für Ihre Hybridknoten und Ihr lokales Netzwerk.

```
aws ec2 create-security-group \
 --group-name SG_NAME \
 --description "security group for hybrid nodes" \
 --vpc-id VPC_ID
```

```
aws ec2 authorize-security-group-ingress \
 --group-id SG_ID \
 --ip-permissions '[{"IpProtocol": "tcp", "FromPort": 443, "ToPort": 443,
"IpRanges": [{"CidrIp": "REMOTE_NODE_CIDR"}, {"CidrIp": "REMOTE_POD_CIDR"}]]']
```

## Betriebssystem für Hybridknoten vorbereiten

Bottlerocket, Amazon Linux 2023 (AL2023), Ubuntu und RHEL werden fortlaufend für die Verwendung als Knotenbetriebssystem für Hybridknoten validiert. Bottlerocket wird nur AWS in VMware vSphere-Umgebungen unterstützt. AL2023 ist nicht durch AWS Supportpläne abgedeckt, wenn sie außerhalb von Amazon EC2 ausgeführt werden. AL2023 kann nur in lokalen virtualisierten Umgebungen verwendet werden. Weitere Informationen finden Sie im [Amazon Linux 2023 User Guide](#). AWS unterstützt die Integration von Hybridknoten mit Ubuntu- und RHEL-Betriebssystemen, bietet jedoch keine Unterstützung für das Betriebssystem selbst.

Sie sind für die Bereitstellung und Verwaltung des Betriebssystems verantwortlich. Wenn Sie Hybridknoten zum ersten Mal testen, ist es am einfachsten, die Amazon EKS Hybrid Nodes CLI (nodeadm) auf einem bereits bereitgestellten Host auszuführen. Für Produktionsbereitstellungen empfehlen wir, dass Sie Images nodeadm in Ihr Betriebssystem aufnehmen, die so konfiguriert sind, dass sie als Systemd-Service ausgeführt werden, um Hosts beim Host-Start automatisch mit Amazon EKS-Clustern zu verbinden. Wenn Sie Bottlerocket als Ihr Node-Betriebssystem auf vSphere verwenden, müssen Sie es nicht verwenden, nodeadm da Bottlerocket bereits die für Hybridknoten erforderlichen Abhängigkeiten enthält und beim Host-Start automatisch eine Verbindung zu dem Cluster herstellt, den Sie konfigurieren.

## Versionskompatibilität

In der folgenden Tabelle sind die Betriebssystemversionen aufgeführt, die kompatibel sind und für die Verwendung als Knotenbetriebssystem für Hybridknoten validiert wurden. Wenn Sie andere Betriebssystemvarianten oder Versionen verwenden, die nicht in dieser Tabelle enthalten sind, wird die Kompatibilität von Hybridknoten mit Ihrer Betriebssystemvariante oder -version nicht vom AWS Support abgedeckt. Hybridknoten sind unabhängig von der zugrunde liegenden Infrastruktur und unterstützen x86- und ARM-Architekturen.

| Betriebssystem           | Versionen                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------|
| Amazon Linux             | Amazon Linux 2023 (AL2023)                                                                |
| Bottlerocket             | v1.37.0 und höhere VMware Varianten, auf denen Kubernetes v1.28 und höher ausgeführt wird |
| Ubuntu                   | Ubuntu 20.04, Ubuntu 22.04, Ubuntu 24.04                                                  |
| Red Hat Enterprise Linux | REGEL 8, REGEL 9                                                                          |

## Überlegungen zum Betriebssystem

### Allgemeines

- Die Amazon EKS Hybrid Nodes CLI (nodeadm) kann verwendet werden, um die Installation und Konfiguration der Komponenten und Abhängigkeiten der Hybridknoten zu vereinfachen. Sie können den `nodeadm install` Prozess während der Image-Build-Pipelines Ihres Betriebssystems oder zur Laufzeit auf jedem lokalen Host ausführen. Weitere Informationen zu den Komponenten, die nodeadm installiert werden, finden Sie unter [the section called “Hybridknoten nodeadm”](#)
- Wenn Sie in Ihrer lokalen Umgebung einen Proxy verwenden, um auf das Internet zuzugreifen, ist für die Installations- und Upgrade-Prozesse eine zusätzliche Betriebssystemkonfiguration erforderlich, um Ihren Paketmanager für die Verwendung des Proxys zu konfigurieren. Detaillierte Anweisungen finden Sie unter [the section called “Proxy konfigurieren”](#).

## Bottlerocket

- Die Schritte und Tools zum Herstellen einer Verbindung mit einem Bottlerocket-Knoten unterscheiden sich von den Schritten für andere Betriebssysteme und werden nicht unter [the section called “Connect Hybridknoten mit Bottlerocket”](#), sondern unter beschrieben. [the section called “Hybridknoten Connect”](#)
- Die Schritte für Bottlerocket verwenden nicht das CLI-Tool für Hybridknoten, `nodeadm`
- Nur VMware Varianten von Bottlerocket Version v1.37.0 und höher werden mit EKS-Hybridknoten unterstützt. VMware Varianten von Bottlerocket sind für die Kubernetes-Versionen v1.28 und höher verfügbar. [Andere Bottlerocket-Varianten](#) werden als Betriebssystem für Hybridknoten nicht unterstützt. HINWEIS: VMware Varianten von Bottlerocket sind nur für die x86\_64-Architektur verfügbar.

## Enthalten

- Containerd ist die standardmäßige Kubernetes-Container-Laufzeit und eine Abhängigkeit für Hybridknoten sowie für alle Amazon EKS-Knotenberechnungstypen. Die Amazon EKS Hybrid Nodes CLI (`nodeadm`) versucht, containerd während des `nodeadm install` Vorgangs zu installieren. Sie können die containerd-Installation zur `nodeadm install` Laufzeit mit der `--containerd-source` Befehlszeilenoption konfigurieren. Gültige Optionen sind `nonedistro`, `unddocker`. Wenn Sie RHEL verwenden, `distro` ist dies keine gültige Option und Sie können entweder so konfigurieren `nodeadm`, dass der containerd-Build aus den Docker-Repos installiert wird, oder Sie können containerd manuell installieren. Wenn Sie AL2 023 oder Ubuntu verwenden, wird containerd `nodeadm` standardmäßig aus der Betriebssystemdistribution installiert. Wenn Sie nicht möchten, dass `nodeadm` containerd installiert, verwenden Sie die Option. `--containerd-source none`

## Ubuntu

- Wenn Sie Ubuntu 20.04 verwenden, müssen Sie AWS Systems Manager Manager-Hybridaktivierungen als Ihren Anmeldeinformationsanbieter verwenden. AWS IAM Roles Anywhere wird unter Ubuntu 20.04 nicht unterstützt.
- [Wenn Sie Ubuntu 24.04 verwenden, müssen Sie möglicherweise Ihre Version von containerd aktualisieren oder Ihre AppArmor Konfiguration ändern, um einen Fix zu implementieren, mit dem Pods ordnungsgemäß beendet werden können, siehe Ubuntu #2065423.](#) Ein Neustart ist erforderlich, um die Änderungen am Profil zu übernehmen. AppArmor Die neueste Version von

Ubuntu 24.04 hat eine aktualisierte Containerd-Version in ihrem Paketmanager mit dem Fix (containerd-Version 1.7.19+).

## RHEL

- Wenn Sie RHEL 8 verwenden, müssen Sie AWS Systems Manager Manager-Hybridaktivierungen als Ihren Anmeldeinformationsanbieter verwenden. AWS IAM Roles Anywhere wird auf RHEL 8 nicht unterstützt.

## ARM

- Wenn Sie ARM-Hardware verwenden, ist ein ARMv8 2.2-kompatibler Prozessor mit der Cryptography Extension (ARMv8.2+crypto) erforderlich, um Version 1.31 und höher des EKS-Kube-Proxy-Add-ons auszuführen. Alle Raspberry Pi-Systeme vor dem Raspberry Pi 5 sowie Prozessoren auf Cortex-A72-Basis erfüllen diese Anforderung nicht. Um das Problem zu umgehen, können Sie Version 1.30 des EKS Kube-Proxy Add-ons weiter verwenden, bis der erweiterte Support im Juli 2026 ausläuft. Sehen [the section called “Amazon-EKS-Kubernetes-Veröffentlichungskalender”](#) Sie sich dazu ein benutzerdefiniertes Kube-Proxy-Image von Upstream an oder verwenden Sie es.
- Die folgende Fehlermeldung im Kube-Proxy-Protokoll weist auf diese Inkompatibilität hin:

```
Fatal glibc error: This version of Amazon Linux requires a newer ARM64 processor
compliant with at least ARM architecture 8.2-a with Cryptographic extensions. On EC2
this is Graviton 2 or later.
```

## Betriebssystem-Images erstellen

Amazon EKS bietet [Beispiel-Packer-Vorlagen](#), mit denen Sie Betriebssystem-Images erstellen können, die diese enthalten nodeadm und für die Ausführung beim Host-Start konfigurieren können. Dieser Prozess wird empfohlen, um zu vermeiden, dass die Abhängigkeiten der Hybridknoten einzeln auf jedem Host abgerufen werden, und um den Bootstrap-Prozess der Hybridknoten zu automatisieren. Sie können die Packer-Beispielvorlagen mit einem Ubuntu 22.04-, Ubuntu 24.04-, RHEL 8- oder RHEL 9-ISO-Image verwenden und Bilder in den folgenden Formaten ausgeben: OVA, Qcow2 oder RAW.

## Voraussetzungen

Bevor Sie die Packer-Beispielvorlagen verwenden können, müssen Sie auf dem Computer, von dem aus Sie Packer ausführen, Folgendes installiert haben.

- Packer-Version 1.11.0 oder höher. Anweisungen zur Installation von Packer finden [Sie unter Install Packer in der Packer-Dokumentation](#).
- Beim Erstellen das OVAs VMware vSphere-Plug-in 1.4.0 oder höher
- Wenn Sie Images Qcow2 oder Rohbilder erstellen, QEMU-Plug-in Version 1.x

## Festlegen von Umgebungsvariablen

Bevor Sie den Packer-Build ausführen, legen Sie die folgenden Umgebungsvariablen auf dem Computer fest, von dem aus Sie Packer ausführen.

## Allgemeines

Die folgenden Umgebungsvariablen müssen für die Erstellung von Images mit allen Betriebssystemen und Ausgabeformaten festgelegt werden.

| Umgebungsvariable | Typ    | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PKR_SSH_PASSWORD  | String | Packer verwendet die <code>ssh_password</code> Variablen <code>ssh_username</code> und, um bei der Bereitstellung per SSH auf die erstellte Maschine zuzugreifen. Dies muss mit den Passwörtern übereinstimmen, die zur Erstellung des ersten Benutzers in den Kickstart- oder Benutzerdateien des jeweiligen Betriebssystems verwendet wurden. Die Standardinstellung ist je nach Betriebssystem auf „Builder“ oder „Ubuntu“ eingestellt. Achten |

| Umgebungsvariable | Typ    | Beschreibung                                                                                                                                                                                          |
|-------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |        | Sie beim Einstellen Ihres Passworts darauf, es in der entsprechenden user-data Datei <code>ks.cfg</code> oder Datei entsprechend zu ändern.                                                           |
| ISO_URL           | String | URL der zu verwendenden ISO-Datei. Kann ein Weblink zum Herunterladen von einem Server oder ein absoluter Pfad zu einer lokalen Datei sein                                                            |
| ISO_CHECKSUM      | String | Zugeordnete Prüfsumme für das bereitgestellte ISO.                                                                                                                                                    |
| CREDITAL_PROVIDER | String | Anbieter von Anmeldeinformationen für Hybridknoten. Gültige Werte sind <code>ssm</code> (Standard) für SSM-Hybrid-Aktivierungen und <code>iam</code> für IAM Roles Anywhere                           |
| K8S_VERSION       | String | Kubernetes-Version für Hybridknoten (zum Beispiel) <code>1.31</code> . Informationen zu unterstützten Kubernetes-Versionen finden Sie unter <a href="#">the section called “Kubernetes-Versionen”</a> |
| NODEADM_ARCH      | String | Architektur für <code>nodeadm</code> installieren. Wählen Sie <code>amd</code> oder <code>arm</code> .                                                                                                |

## RHEL

Wenn Sie RHEL verwenden, müssen die folgenden Umgebungsvariablen gesetzt werden.

| Umgebungsvariable | Typ    | Beschreibung                                                      |
|-------------------|--------|-------------------------------------------------------------------|
| RH_USERNAME       | String | Benutzername für den RHEL-Abonnementmanager                       |
| RH_PASSWORD       | String | Passwort für den RHEL-Abonnementmanager                           |
| RHEL_VERSION      | String | Die RHEL-ISO-Version wird verwendet. Gültige Werte sind 8 oder 9. |

## Ubuntu

Es sind keine Ubuntu-spezifischen Umgebungsvariablen erforderlich.

## vSphere

Wenn Sie eine VMware vSphere-OVA erstellen, müssen die folgenden Umgebungsvariablen festgelegt werden.

| Umgebungsvariable  | Typ    | Beschreibung                    |
|--------------------|--------|---------------------------------|
| VSPHERE_SERVER     | String | vSphere-Serveradresse           |
| VSPHERE_USER       | String | vSphere-Benutzername            |
| VSPHERE_PASSWORD   | String | vSphere-Passwort                |
| VSPHERE_DATACENTER | String | Name des vSphere-Rechenzentrums |
| VSPHERE_CLUSTER    | String | Name des vSphere-Clusters       |
| VSPHERE_DATASTORE  | String | Name des vSphere-Datenspeichers |
| VSPHERE_NETWORK    | String | vSphere-Netzwerkname            |

| Umgebungsvariable     | Typ    | Beschreibung                           |
|-----------------------|--------|----------------------------------------|
| VSPHERE_OUTPUT_FOLDER | String | vSphere-Ausgabeordner für die Vorlagen |

## QEMU

| Umgebungsvariable    | Typ    | Beschreibung                                                                                     |
|----------------------|--------|--------------------------------------------------------------------------------------------------|
| PACKER_AUSGABEFORMAT | String | Ausgabeformat für den QEMU-Builder. Gültige Werte sind <code>qcow2</code> und <code>raw</code> . |

## Vorlage validieren

Bevor Sie Ihren Build ausführen, validieren Sie Ihre Vorlage mit dem folgenden Befehl, nachdem Sie Ihre Umgebungsvariablen festgelegt haben. Ersetzen Sie es, `template.pkr.hcl` wenn Sie einen anderen Namen für Ihre Vorlage verwenden.

```
packer validate template.pkr.hcl
```

## Erstellen Sie Bilder

Erstellen Sie Ihre Images mit den folgenden Befehlen und verwenden Sie das `-only` Flag, um das Ziel und das Betriebssystem für Ihre Images anzugeben. Ersetzen Sie es, `template.pkr.hcl` wenn Sie einen anderen Namen für Ihre Vorlage verwenden.

## vSphere OVAs

### Note

Wenn Sie RHEL mit vSphere verwenden, müssen Sie die Kickstart-Dateien in ein OEMDRV-Image konvertieren und es als ISO übergeben, von dem aus gestartet werden kann. Weitere Informationen finden Sie in der [Packer-Readme-Datei im EKS Hybrid Nodes Repository](#).  
GitHub



## Ubuntu 22.04 OVA

```
packer build -only=general-build.vsphere-iso.ubuntu22 template.pkr.hcl
```

## Ubuntu 24.04 OVA

```
packer build -only=general-build.vsphere-iso.ubuntu24 template.pkr.hcl
```

## RHEL 8 OVA

```
packer build -only=general-build.vsphere-iso.rhel8 template.pkr.hcl
```

## RHEL 9 OVA

```
packer build -only=general-build.vsphere-iso.rhel9 template.pkr.hcl
```

## QEMU

### Note

Wenn Sie ein Image für eine bestimmte Host-CPU erstellen, die nicht zu Ihrem Builder-Host passt, finden Sie in der [QEMU-Dokumentation](#) den Namen, der zu Ihrer Host-CPU passt, und verwenden Sie das `-cpu` Flag mit dem Namen der Host-CPU, wenn Sie die folgenden Befehle ausführen.

## Ubuntu 22.04 Qcow2//Raw

```
packer build -only=general-build.qemu.ubuntu22 template.pkr.hcl
```

## Ubuntu 24.04 Qcow2//Raw

```
packer build -only=general-build.qemu.ubuntu24 template.pkr.hcl
```

## RHEL 8 Qcow2//Raw

```
packer build -only=general-build.qemu.rhel8 template.pkr.hcl
```

## RHEL 9 Qcow2//Raw

```
packer build -only=general-build.qemu.rhel9 template.pkr.hcl
```

## Übergibt die Nodeadm-Konfiguration über Benutzerdaten

Sie können die Konfiguration für nodeadm in Ihren Benutzerdaten über cloud-init übergeben, um Hybridknoten zu konfigurieren und beim Host-Start automatisch mit Ihrem EKS-Cluster zu verbinden. Im Folgenden finden Sie ein Beispiel dafür, wie Sie dies erreichen können, wenn Sie VMware vSphere als Infrastruktur für Ihre Hybridknoten verwenden.

1. Installieren Sie die govc CLI gemäß den Anweisungen in der [Govc-Readme-Datei unter](#). GitHub
2. Nachdem Sie den Packer-Build im vorherigen Abschnitt ausgeführt und Ihre Vorlage bereitgestellt haben, können Sie Ihre Vorlage klonen, um mehrere verschiedene Knoten zu erstellen. Gehen Sie dazu wie folgt vor. Sie müssen die Vorlage für jede neue VM klonen, die Sie erstellen und die für Hybridknoten verwendet wird. Ersetzen Sie die Variablen im folgenden Befehl durch die Werte für Ihre Umgebung. Der VM\_NAME Befehl unten wird als Ihr verwendet, NODE\_NAME wenn Sie die Namen für Sie VMs über Ihre metadata.yaml Datei eingeben.

```
govc vm.clone -vm "/PATH/TO/TEMPLATE" -ds="YOUR_DATASTORE" \
 -on=false -template=false -folder=/FOLDER/TO/SAVE/VM "VM_NAME"
```

3. Nachdem Sie die Vorlage für jedes Ihrer neuen geklont haben VMs, erstellen Sie ein userdata.yaml und metadata.yaml für Ihre. VMs Sie VMs können dasselbe teilen userdata.yaml metadata.yaml und Sie werden diese in den folgenden Schritten für jede VM einzeln ausfüllen. Die nodeadm Konfiguration wird im write\_files Abschnitt Ihres userdata.yaml erstellt und definiert. Im folgenden Beispiel werden AWS SSM-Hybrid-Aktivierungen als lokaler Anbieter von Anmeldeinformationen für Hybridknoten verwendet. Weitere Informationen zur nodeadm Konfiguration finden Sie im. [the section called "Hybridknoten nodeadm"](#)

userdata.yaml:

```
#cloud-config
users:
 - name: # username for login. Use 'builder' for RHEL or 'ubuntu' for Ubuntu.
 passwd: # password to login. Default is 'builder' for RHEL.
 groups: [adm, cdrom, dip, plugdev, lxd, sudo]
 lock-passwd: false
 sudo: ALL=(ALL) NOPASSWD:ALL
 shell: /bin/bash
```

```

write_files:
 - path: /usr/local/bin/nodeConfig.yaml
 permissions: '0644'
 content: |
 apiVersion: node.eks.aws/v1alpha1
 kind: NodeConfig
 spec:
 cluster:
 name: # Cluster Name
 region: # AWS region
 hybrid:
 ssm:
 activationCode: # Your ssm activation code
 activationId: # Your ssm activation id

runcmd:
 - /usr/local/bin/nodeadm init -c file:///usr/local/bin/nodeConfig.yaml >> /var/log/
 nodeadm-init.log 2>&1

```

metadata.yaml:

Erstellen Sie eine für Ihre Umgebung `metadata.yaml`. Behalten Sie das "\$NODE\_NAME" Variablenformat in der Datei bei, da diese in einem nachfolgenden Schritt mit Werten gefüllt wird.

```

instance-id: "$NODE_NAME"
local-hostname: "$NODE_NAME"
network:
 version: 2
 ethernet:
 nics:
 match:
 name: ens*
 dhcp4: yes

```

4. Fügen Sie die `metadata.yaml` Dateien `userdata.yaml` und als `gzip+base64` Zeichenfolgen mit den folgenden Befehlen hinzu. Die folgenden Befehle sollten für jeden Befehl ausgeführt werden, den VMs Sie gerade erstellen. `VM_NAME` Ersetzen Sie es durch den Namen der VM, die Sie aktualisieren.

```

export NODE_NAME="VM_NAME"
export USER_DATA=$(gzip -c9 <userdata.yaml | base64)

```

```
govc vm.change -dc="YOUR_DATASTORE" -vm "$NODE_NAME" -e
 guestinfo.userdata="${USER_DATA}"
govc vm.change -dc="YOUR_DATASTORE" -vm "$NODE_NAME" -e
 guestinfo.userdata.encoding=gzip+base64

envsubst '$NODE_NAME' < metadata.yaml > metadata.yaml.tmp
export METADATA=$(gzip -c9 <metadata.yaml.tmp | base64)

govc vm.change -dc="YOUR_DATASTORE" -vm "$NODE_NAME" -e
 guestinfo.metadata="${METADATA}"
govc vm.change -dc="YOUR_DATASTORE" -vm "$NODE_NAME" -e
 guestinfo.metadata.encoding=gzip+base64
```

5. Schalten Sie Ihren neuen ein VMs, der automatisch eine Verbindung zu dem von Ihnen konfigurierten EKS-Cluster herstellen sollte.

```
govc vm.power -on "${NODE_NAME}"
```

## Anmeldedaten für Hybridknoten vorbereiten

Amazon EKS-Hybridknoten verwenden temporäre IAM-Anmeldeinformationen, die durch AWS SSM-Hybrid-Aktivierungen oder AWS IAM Roles Anywhere bereitgestellt werden, um sich beim Amazon EKS-Cluster zu authentifizieren. Sie müssen entweder AWS SSM-Hybrid-Aktivierungen oder AWS IAM Roles Anywhere mit der Amazon EKS Hybrid Nodes CLI () verwenden. `nodeadm` Sie sollten nicht sowohl AWS SSM-Hybrid-Aktivierungen als auch IAM-Rollen Anywhere verwenden. AWS Wir empfehlen, AWS SSM-Hybrid-Aktivierungen zu verwenden, wenn Sie nicht über eine bestehende Public Key-Infrastruktur (PKI) mit einer Zertifizierungsstelle (CA) und Zertifikaten für Ihre lokalen Umgebungen verfügen. Wenn Sie bereits über PKI und Zertifikate vor Ort verfügen, verwenden Sie IAM Roles Anywhere. AWS

### IAM-Rolle für Hybridknoten

Bevor Sie Hybridknoten mit Ihrem Amazon EKS-Cluster verbinden können, müssen Sie eine IAM-Rolle erstellen, die mit AWS SSM-Hybrid-Aktivierungen oder AWS IAM Roles Anywhere für Ihre Hybridknoten-Anmeldeinformationen verwendet wird. Nach der Clustererstellung verwenden Sie diese Rolle mit einem Amazon EKS-Zugriffseintrag oder `aws-auth ConfigMap` einem Eintrag, um die IAM-Rolle Kubernetes Role-Based Access Control (RBAC) zuzuordnen. Weitere Informationen zur Verknüpfung der IAM-Rolle Hybrid Nodes mit Kubernetes RBAC finden Sie unter [the section called "Bereiten Sie den Clusterzugriff vor"](#)

Die IAM-Rolle Hybrid Nodes muss über die folgenden Berechtigungen verfügen.

- Berechtigungen für nodeadm die Verwendung der `eks:DescribeCluster` Aktion zum Sammeln von Informationen über den Cluster, der für die Verbindung von Hybridknoten mit dem Cluster verwendet wird. Wenn Sie die `eks:DescribeCluster` Aktion nicht aktivieren, müssen Sie Ihren Kubernetes-API-Endpunkt, das Cluster-CA-Bundle und den IPv4 Service-CIDR in der Knotenkonfiguration übergeben, an die Sie nodeadm bei der Ausführung von `init` übergeben. nodeadm
- [Berechtigungen für das Kubelet zur Verwendung von Container-Images aus Amazon Elastic Container Registry \(Amazon ECR\), wie in der Amazon-Richtlinie definiert. EC2 ContainerRegistryPullOnly](#)
- [Bei Verwendung von AWS SSM: Berechtigungen für nodeadm init zur Verwendung von AWS SSM-Hybrid-Aktivierungen, wie in der Richtlinie `aws-managed-policy latest/reference/AmazonSSMManagedInstanceCore` definiert.](#)
- Bei Verwendung von AWS SSM: Berechtigungen zur Verwendung der `ssm:DeregisterManagedInstance` Aktion und `ssm:DescribeInstanceInformation` Aktion für zum Abmelden von Instanzen. nodeadm `uninstall`
- (Optional) Berechtigungen für den Amazon EKS Pod Identity Agent zum Verwenden der Aktion `eks-auth:AssumeRoleForPodIdentity`, um Anmeldeinformationen für Pods abzurufen.

Richten Sie SSM-Hybrid-Aktivierungen AWS ein

Bevor Sie AWS SSM-Hybrid-Aktivierungen einrichten, müssen Sie eine IAM-Rolle für Hybrid Nodes erstellt und konfiguriert haben. Weitere Informationen finden Sie unter [the section called “Erstellen Sie die IAM-Rolle Hybrid Nodes”](#). Folgen Sie den Anweisungen unter [Hybrid-Aktivierung erstellen, um Knoten bei Systems Manager zu registrieren im AWS Systems Manager](#) Manager-Benutzerhandbuch, um eine AWS SSM-Hybrid-Aktivierung für Ihre Hybridknoten zu erstellen. Der Aktivierungscode und die ID, die Sie erhalten, werden zusammen verwendet, nodeadm wenn Sie Ihre Hosts als Hybridknoten in Ihrem Amazon EKS-Cluster registrieren. Sie können zu einem späteren Zeitpunkt zu diesem Schritt zurückkehren, nachdem Sie Ihre Amazon EKS-Cluster für Hybridknoten erstellt und vorbereitet haben.

 **Important**

Systems Manager übergibt den Aktivierungscode und die ID sofort an die Konsole oder das Befehlsfenster, je nachdem, wie Sie die Aktivierung erstellt haben. Kopieren Sie diese Informationen und speichern Sie sie an einem sicheren Ort. Wenn Sie die Konsole verlassen

oder das Befehlsfenster schließen, können diese Informationen verloren gehen. Wenn Sie die Informationen verlieren, müssen Sie eine neue Aktivierung erstellen.

Standardmäßig sind AWS SSM-Hybrid-Aktivierungen 24 Stunden lang aktiv. Alternativ können Sie --expiration-date bei der Erstellung Ihrer Hybrid-Aktivierung eine im Zeitstempelformat angeben, z. B. 2024-08-01T00:00:00 Wenn Sie AWS SSM als Ihren Anmeldeinformationsanbieter verwenden, ist der Knotenname für Ihre Hybridknoten nicht konfigurierbar und wird automatisch von SSM generiert. AWS Sie können die von AWS SSM verwalteten Instanzen in der AWS Systems Manager-Konsole unter Fleet Manager anzeigen und verwalten. Sie können bis zu 1.000 standardmäßige, [hybridaktivierte Knoten](#) pro Konto und AWS Region ohne zusätzliche Kosten registrieren. Um mehr als 1 000 Hybrid-Knoten zu registrieren, müssen Sie jedoch das Advanced-Instances-Kontingent aktivieren. Für die Nutzung des Advanced-Instance-Tarifs fällt eine Gebühr an, die nicht in den Preisen für [Amazon EKS Hybrid Nodes](#) enthalten ist. Weitere Informationen finden Sie unter [AWS Systems Manager Manager-Preise](#).

Im folgenden Beispiel erfahren Sie, wie Sie eine AWS SSM-Hybrid-Aktivierung mit Ihrer Hybrid Nodes IAM-Rolle erstellen. Wenn Sie AWS SSM-Hybrid-Aktivierungen für Ihre Anmeldeinformationen für Hybridknoten verwenden, haben die Namen Ihrer Hybridknoten das gleiche Format mi-012345678abcdefgh und die von AWS SSM bereitgestellten temporären Anmeldeinformationen sind 1 Stunde lang gültig. Sie können den Knotennamen oder die Dauer der Anmeldeinformationen nicht ändern, wenn Sie AWS SSM als Ihren Anmeldeinformationsanbieter verwenden. Die temporären Anmeldeinformationen werden von AWS SSM automatisch rotiert, und die Rotation hat keine Auswirkungen auf den Status Ihrer Knoten oder Anwendungen.

Wir empfehlen, dass Sie eine AWS SSM-Hybrid-Aktivierung pro EKS-Cluster verwenden, um die AWS ssm:DeregisterManagedInstance SSM-Berechtigungen der IAM-Rolle Hybrid Nodes so festzulegen, dass nur Instances abgemeldet werden können, die mit Ihrer SSM-Hybrid-Aktivierung verknüpft sind. AWS In dem Beispiel auf dieser Seite wird ein Tag mit dem EKS-Cluster-ARN verwendet, das verwendet werden kann, um Ihre AWS SSM-Hybridaktivierung dem EKS-Cluster zuzuordnen. Sie können alternativ Ihr bevorzugtes Tag und Ihre bevorzugte Methode verwenden, um den Umfang der AWS SSM-Berechtigungen auf der Grundlage Ihrer Berechtigungsgrenzen und Anforderungen festzulegen. Die REGISTRATION\_LIMIT Option im folgenden Befehl ist eine Ganzzahl, die verwendet wird, um die Anzahl der Maschinen zu begrenzen, die die AWS SSM-Hybridaktivierung verwenden können (zum Beispiel) 10

```
aws ssm create-activation \
 --region AWS_REGION \
 --tags TagKey=tag-value
```

```
--default-instance-name eks-hybrid-nodes \
--description "Activation for EKS hybrid nodes" \
--iam-role AmazonEKSHybridNodesRole \
--tags Key=EKSclusterARN,Value=arn:aws: eks:AWS_REGION:AWS_ACCOUNT_ID:cluster/
CLUSTER_NAME \
--registration-limit REGISTRATION_LIMIT
```

Weitere Informationen [zu den verfügbaren Konfigurationseinstellungen für AWS SSM-Hybrid-Aktivierungen finden Sie in den Anweisungen unter Hybrid-Aktivierung erstellen, um Knoten bei Systems Manager zu registrieren.](#)

Richten Sie AWS IAM-Rollen überall ein

Folgen Sie den Anweisungen unter [Erste Schritte mit IAM Roles Anywhere](#) im IAM Roles Anywhere-Benutzerhandbuch, um den Vertrauensanker und das Profil einzurichten, die Sie für temporäre IAM-Anmeldeinformationen für Ihre Hybrid Nodes IAM-Rolle verwenden werden. Wenn Sie Ihr Profil erstellen, können Sie es erstellen, ohne Rollen hinzuzufügen. Sie können dieses Profil erstellen, zu diesen Schritten zurückkehren, um Ihre Hybrid Nodes IAM-Rolle zu erstellen, und Ihre Rolle dann Ihrem Profil hinzufügen, nachdem sie erstellt wurde. Sie können auch die AWS CloudFormation Schritte weiter unten auf dieser Seite verwenden, um Ihr IAM Roles Anywhere-Setup für Hybridknoten abzuschließen.

Wenn Sie Ihrem Profil die IAM-Rolle Hybrid Nodes hinzufügen, wählen Sie im Bereich Sitzungsname für benutzerdefinierte Rolle unten auf der Seite Profil bearbeiten in der AWS IAM Roles Anywhere-Konsole die Option Sitzungsname der benutzerdefinierten Rolle akzeptieren aus. Dies entspricht dem Feld „[acceptRoleSessionName](#)“ der CreateProfile API. Auf diese Weise können Sie in der Konfiguration, an die Sie nodeadm während des Bootstrap-Prozesses übergeben, einen benutzerdefinierten Knotennamen für Ihre Hybridknoten angeben. Die Übergabe eines benutzerdefinierten Knotennamens während des nodeadm init Vorgangs ist erforderlich. Sie können Ihr Profil nach der Erstellung Ihres Profils so aktualisieren, dass es einen Sitzungsnamen mit einer benutzerdefinierten Rolle akzeptiert.

Sie können die Gültigkeitsdauer der Anmeldeinformationen mit AWS IAM Roles Anywhere über das Feld [DurationSeconds](#) Ihres AWS IAM Roles Anywhere-Profiles konfigurieren. Die Standarddauer beträgt 1 Stunde mit einem Maximum von 12 Stunden. Die MaxSessionDuration Einstellung in Ihrer IAM-Rolle Hybrid Nodes muss größer sein als die durationSeconds Einstellung in Ihrem AWS IAM Roles Anywhere-Profil. Weitere Informationen dazu finden Sie in der MaxSessionDuration [UpdateRole API-Dokumentation](#).

Die Zertifikate und Schlüssel pro Computer, die Sie von Ihrer Zertifizierungsstelle (CA) generieren, müssen in dem `/etc/iam/pki` Verzeichnis auf jedem Hybridknoten mit den Dateinamen `server.pem` für das Zertifikat und `server.key` für den Schlüssel abgelegt werden.

## Erstellen Sie die IAM-Rolle Hybrid Nodes

Um die Schritte in diesem Abschnitt auszuführen, muss der IAM-Principal, der die AWS Konsole oder AWS CLI verwendet, über die folgenden Berechtigungen verfügen.

- `iam:CreatePolicy`
- `iam:CreateRole`
- `iam:AttachRolePolicy`
- Wenn Sie AWS IAM Roles Anywhere verwenden
  - `rolesanywhere:CreateTrustAnchor`
  - `rolesanywhere:CreateProfile`
  - `iam:PassRole`

## AWS CloudFormation

Installieren und konfigurieren Sie die AWS CLI, falls Sie dies noch nicht getan haben. Siehe [Installation oder Aktualisierung auf die letzte Version der AWS CLI](#).

## Schritte für AWS SSM-Hybrid-Aktivierungen

Der CloudFormation Stack erstellt die IAM-Rolle Hybrid Nodes mit den oben beschriebenen Berechtigungen. Die CloudFormation Vorlage erstellt die AWS SSM-Hybrid-Aktivierung nicht.

1. Laden Sie die AWS CloudFormation SSM-Vorlage für Hybridknoten herunter:

```
curl -OL 'https://raw.githubusercontent.com/aws/eks-hybrid/refs/heads/main/example/hybrid-ssm-cfn.yaml'
```

2. Erstellen Sie eine `cfn-ssm-parameters.json` mit den folgenden Optionen:
  - a. `ROLE_NAME` Ersetzen Sie es durch den Namen für Ihre Hybrid Nodes IAM-Rolle. Standardmäßig verwendet `AmazonEKSHybridNodesRole` die CloudFormation Vorlage den Namen der Rolle, die sie erstellt, wenn Sie keinen Namen angeben.
  - b. `TAG_KEY` Ersetzen Sie es durch den AWS SSM-Ressourcen-Tag-Schlüssel, den Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung verwendet haben. Die Kombination aus Tag-



Schlüssel und Tag-Wert wird in der Bedingung verwendet, dass nur die IAM-Rolle Hybrid Nodes die Registrierung der mit AWS SSM verwalteten Instanzen, die mit Ihrer SSM-Hybrid-Aktivierung verknüpft sind, aufheben darf. `ssm:DeregisterManagedInstance` AWS In der Vorlage ist der Standardwert `CloudFormation . TAG_KEY EKSClusterARN`

- c. `TAG_VALUE` Ersetzen Sie es durch den Wert des AWS SSM-Ressourcen-Tags, den Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung verwendet haben. Die Kombination aus Tag-Schlüssel und Tag-Wert wird in der Bedingung verwendet, dass nur die IAM-Rolle Hybrid Nodes die Registrierung der mit AWS SSM verwalteten Instanzen, die mit Ihrer SSM-Hybrid-Aktivierung verknüpft sind, aufheben darf. `ssm:DeregisterManagedInstance` AWS Wenn Sie den Standard `TAG_KEY` von `verwendenEKSClusterARN`, übergeben Sie Ihren EKS-Cluster-ARN als `TAG_VALUE`. EKS-Cluster ARNs haben das Format `arn:aws:eks:AWS_REGION:AWS_ACCOUNT_ID:cluster/CLUSTER_NAME`.

```
{
 "Parameters": {
 "RoleName": "ROLE_NAME",
 "SSMDeregisterConditionTagKey": "TAG_KEY",
 "SSMDeregisterConditionTagValue": "TAG_VALUE"
 }
}
```

3. Stellen Sie den CloudFormation Stack bereit. `STACK_NAME` Ersetzen Sie ihn durch Ihren Namen für den CloudFormation Stack.

```
aws cloudformation deploy \
 --stack-name STACK_NAME \
 --template-file hybrid-ssm-cfn.yaml \
 --parameter-overrides file://cfn-ssm-parameters.json \
 --capabilities CAPABILITY_NAMED_IAM
```

## Schritte für AWS IAM Roles Anywhere

Der CloudFormation Stack erstellt den AWS IAM Roles Anywhere-Vertrauensanker mit der von Ihnen konfigurierten Zertifizierungsstelle (CA), erstellt das AWS IAM Roles Anywhere-Profil und erstellt die IAM-Rolle Hybrid Nodes mit den zuvor beschriebenen Berechtigungen.

1. So richten Sie eine Zertifizierungsstelle (CA) ein

- a. Um eine AWS private CA-Ressource zu verwenden, öffnen Sie die [AWS Private Certificate Authority-Konsole](#). Folgen Sie den Anweisungen im [AWS Private CA-Benutzerhandbuch](#).
  - b. Um eine externe Zertifizierungsstelle zu verwenden, folgen Sie den Anweisungen der Zertifizierungsstelle. Sie geben die Zertifizierungsstelle in einem späteren Schritt an.
  - c. Öffentlich ausgestellte Zertifikate CAs können nicht als Vertrauensanker verwendet werden.
2. Laden Sie die AWS IAM Roles CloudFormation Anywhere-Vorlage für Hybridknoten herunter

```
curl -OL 'https://raw.githubusercontent.com/aws/eks-hybrid/refs/heads/main/example/hybrid-ira-cfn.yaml'
```

3. Erstellen Sie eine `cfn-iamra-parameters.json` mit den folgenden Optionen:
- a. `ROLE_NAME` Ersetzen Sie es durch den Namen für Ihre Hybrid Nodes IAM-Rolle. Standardmäßig verwendet AmazonEKSHybridNodesRole die CloudFormation Vorlage den Namen der Rolle, die sie erstellt, wenn Sie keinen Namen angeben.
  - b. `CERT_ATTRIBUTE` Ersetzen Sie es durch das Zertifikatsattribut pro Computer, das Ihren Host eindeutig identifiziert. Das von Ihnen verwendete Zertifikatsattribut muss mit dem `NodeName` übereinstimmen, den Sie für die `nodeadm` Konfiguration verwenden, wenn Sie Hybridknoten mit Ihrem Cluster verbinden. Weitere Informationen hierzu finden Sie unter [the section called "Hybridknoten nodeadm"](#). Standardmäßig verwendet die CloudFormation Vorlage `${aws:PrincipalTag/x509Subject/CN}` als `CERT_ATTRIBUTE`, was dem CN-Feld Ihrer Computerzertifikate entspricht. Sie können es auch `$(aws:PrincipalTag/x509SAN/Name/CN)` als Ihr `CERT_ATTRIBUTE` Passwort übergeben.
  - c. `CA_CERT_BODY` Ersetzen Sie es durch die Zertifizierungsstelle Ihrer Zertifizierungsstelle ohne Zeilenumbrüche. Das `CA_CERT_BODY` muss im PEM-Format (Privacy Enhanced Mail) vorliegen. Wenn Sie über ein CA-Zertifikat im PEM-Format verfügen, entfernen Sie die Zeilenumbrüche und die Zeilen `BEGIN CERTIFICATE` und `END CERTIFICATE`, bevor Sie den Hauptteil des CA-Zertifikats in Ihre `cfn-iamra-parameters.json` Datei einfügen.

```
{
 "Parameters": {
 "RoleName": "ROLE_NAME",
 "CertAttributeTrustPolicy": "CERT_ATTRIBUTE",
 "CABundleCert": "CA_CERT_BODY"
 }
}
```

4. Stellen Sie die CloudFormation Vorlage bereit. STACK\_NAME Ersetzen Sie es durch Ihren Namen für den CloudFormation Stack.

```
aws cloudformation deploy \
 --stack-name STACK_NAME \
 --template-file hybrid-ira-cfn.yaml \
 --parameter-overrides file://cfn-iamra-parameters.json \
 --capabilities CAPABILITY_NAMED_IAM
```

## AWS CLI

Installieren und konfigurieren Sie die AWS CLI, falls Sie dies noch nicht getan haben. Siehe [Installation oder Aktualisierung auf die letzte Version der AWS CLI](#).

Erstellen Sie die EKS Describe Cluster-Richtlinie

1. Erstellen Sie eine Datei `eks-describe-cluster-policy.json` mit dem folgenden Inhalt:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "eks:DescribeCluster"
],
 "Resource": "*"
 }
]
}
```

2. Erstellen Sie die Richtlinie mit dem folgenden Befehl:

```
aws iam create-policy \
 --policy-name EKSDescribeClusterPolicy \
 --policy-document file://eks-describe-cluster-policy.json
```

## Schritte für AWS SSM-Hybrid-Aktivierungen

1. Erstellen Sie eine Datei mit dem Namen `eks-hybrid-ssm-policy.json` und dem folgenden Inhalt. Die Richtlinie gewährt die Genehmigung für zwei Aktionen `ssm:DescribeInstanceInformation` und `ssm:DeregisterManagedInstance`. Die Richtlinie schränkt die `ssm:DeregisterManagedInstance` Berechtigung auf AWS SSM-verwaltete Instanzen ein, die mit Ihrer AWS SSM-Hybridaktivierung verknüpft sind, und zwar auf der Grundlage des Ressourcen-Tags, das Sie in Ihrer Vertrauensrichtlinie angeben.
  - a. Ersetzen Sie es `AWS_REGION` durch die AWS Region für Ihre AWS SSM-Hybrid-Aktivierung.
  - b. Ersetzen Sie `AWS_ACCOUNT_ID` durch Ihre AWS Konto-ID.
  - c. `TAG_KEY` Ersetzen Sie es durch den AWS SSM-Ressourcen-Tag-Schlüssel, den Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung verwendet haben. Die Kombination aus Tag-Schlüssel und Tag-Wert wird in der Bedingung verwendet, dass nur die IAM-Rolle Hybrid Nodes die Registrierung der mit AWS SSM verwalteten Instanzen, die mit Ihrer SSM-Hybrid-Aktivierung verknüpft sind, aufheben darf. `ssm:DeregisterManagedInstance` AWS In der Vorlage ist der Standardwert `CloudFormation`. `TAG_KEY` `EKSclusterARN`
  - d. `TAG_VALUE` Ersetzen Sie es durch den Wert des AWS SSM-Ressourcen-Tags, den Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung verwendet haben. Die Kombination aus Tag-Schlüssel und Tag-Wert wird in der Bedingung verwendet, dass nur die IAM-Rolle Hybrid Nodes die Registrierung der mit AWS SSM verwalteten Instanzen, die mit Ihrer SSM-Hybrid-Aktivierung verknüpft sind, aufheben darf. `ssm:DeregisterManagedInstance` AWS Wenn Sie den Standard `TAG_KEY` von verwenden `EKSclusterARN`, übergeben Sie Ihren EKS-Cluster-ARN als `TAG_VALUE`. EKS-Cluster ARNs haben das Format `arn:aws:eks:AWS_REGION:AWS_ACCOUNT_ID:cluster/CLUSTER_NAME`.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ssm:DescribeInstanceInformation",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ssm:DeregisterManagedInstance",
 "Resource": "arn:aws:ssm:AWS_REGION:AWS_ACCOUNT_ID:managed-instance/*",
 "Condition": {
 "StringEquals": {

```

```

 "ssm:resourceTag/TAG_KEY": "TAG_VALUE"
 }
 }
]
}

```

2. Erstellen Sie die Richtlinie mit dem folgenden Befehl

```

aws iam create-policy \
 --policy-name EKSHybridSSMPolicy \
 --policy-document file://eks-hybrid-ssm-policy.json

```

3. Erstellen Sie eine Datei namens `eks-hybrid-ssm-trust.json`. `AWS_REGION` Ersetzen Sie es durch die AWS Region Ihrer AWS SSM-Hybrid-Aktivierung und `AWS_ACCOUNT_ID` durch Ihre AWS Konto-ID.

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "AWS_ACCOUNT_ID"
 },
 "ArnEquals": {
 "aws:SourceArn": "arn:aws:ssm:AWS_REGION:AWS_ACCOUNT_ID:*"
 }
 }
 }
]
}

```

4. Erstellen Sie die Rolle mit dem folgenden Befehl.

```

aws iam create-role \
 --role-name AmazonEKSHybridNodesRole \

```

```
--assume-role-policy-document file://eks-hybrid-ssm-trust.json
```

5. Hängen Sie das EKSDescribeClusterPolicy und das anEKSHybridSSMPolicy, das Sie in den vorherigen Schritten erstellt haben. AWS\_ACCOUNT\_ID ersetzen Sie es durch Ihre AWS Konto-ID.

```
aws iam attach-role-policy \
 --role-name AmazonEKSHybridNodesRole \
 --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/EKSDescribeClusterPolicy
```

```
aws iam attach-role-policy \
 --role-name AmazonEKSHybridNodesRole \
 --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/EKSHybridSSMPolicy
```

6. Hängen Sie die AmazonEC2ContainerRegistryPullOnly und die AmazonSSMManagedInstanceCore AWS verwalteten Richtlinien an.

```
aws iam attach-role-policy \
 --role-name AmazonEKSHybridNodesRole \
 --policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly
```

```
aws iam attach-role-policy \
 --role-name AmazonEKSHybridNodesRole \
 --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

## Schritte für AWS IAM Roles Anywhere

Um AWS IAM Roles Anywhere verwenden zu können, müssen Sie Ihren AWS IAM Roles Anywhere-Vertrauensanker einrichten, bevor Sie die IAM-Rolle Hybrid Nodes erstellen. Detaillierte Anweisungen finden Sie unter [the section called “Richten Sie AWS IAM-Rollen überall ein”](#).

1. Erstellen Sie eine Datei namens eks-hybrid-iamra-trust.json. TRUST\_ANCHOR ARN ersetzen Sie ihn durch den ARN des Vertrauensankers, den Sie in den [the section called “Richten Sie AWS IAM-Rollen überall ein”](#) Schritten erstellt haben. Die Bedingung in dieser Vertrauensrichtlinie schränkt die Fähigkeit von AWS IAM Roles Anywhere ein, die IAM-Rolle Hybrid Nodes anzunehmen und temporäre IAM-Anmeldeinformationen nur auszutauschen, wenn der Name der Rollensitzung mit dem CN im x509-Zertifikat übereinstimmt, das auf Ihren Hybridknoten installiert ist. Sie können auch andere Zertifikatsattribute verwenden, um Ihren

Knoten eindeutig zu identifizieren. Das Zertifikatsattribut, das Sie in der Vertrauensrichtlinie verwenden, muss dem entsprechen, das nodeName Sie in Ihrer nodeadm Konfiguration festgelegt haben. Weitere Informationen hierzu finden Sie unter [the section called “Hybridknoten nodeadm”](#).

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "rolesanywhere.amazonaws.com"
 },
 "Action": [
 "sts:TagSession",
 "sts:SetSourceIdentity"
],
 "Condition": {
 "ArnEquals": {
 "aws:SourceArn": "TRUST_ANCHOR_ARN"
 }
 }
 },
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "rolesanywhere.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "sts:RoleSessionName": "${aws:PrincipalTag/x509Subject/CN}"
 },
 "ArnEquals": {
 "aws:SourceArn": "TRUST_ANCHOR_ARN"
 }
 }
 }
]
}
```

2. Erstellen Sie die Rolle mit dem folgenden Befehl.

```
aws iam create-role \
```

```
--role-name AmazonEKSHybridNodesRole \
--assume-role-policy-document file:///eks-hybrid-iamra-trust.json
```

3. Hängen EKSDescribeClusterPolicy Sie die an, die Sie in den vorherigen Schritten erstellt haben. AWS\_ACCOUNT\_ID Ersetzen Sie es durch Ihre AWS Konto-ID.

```
aws iam attach-role-policy \
--role-name AmazonEKSHybridNodesRole \
--policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/EKSDescribeClusterPolicy
```

4. Hängen Sie die AmazonEC2ContainerRegistryPullOnly AWS verwaltete Richtlinie an

```
aws iam attach-role-policy \
--role-name AmazonEKSHybridNodesRole \
--policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly
```

## AWS Management Console

Erstellen Sie die EKS Describe Cluster-Richtlinie

1. Öffnen Sie die [Amazon IAM-Konsole](#)
2. Wählen Sie im linken Navigationsbereich die Option Policies aus.
3. Wählen Sie auf der Seite Richtlinien die Option Richtlinie erstellen.
4. Wählen Sie auf der Seite „Berechtigungen angeben“ im Bereich Service auswählen die Option EKS aus.
  - a. Filtern Sie Aktionen nach DescribeCluster und wählen Sie die Aktion DescribeClusterLesen aus.
  - b. Wählen Sie Weiter aus.
5. Auf der Seite Überprüfen und erstellen
  - a. Geben Sie einen Richtliniennamen für Ihre Richtlinie ein, EKSDescribeClusterPolicy z. B.
  - b. Wählen Sie Richtlinie erstellen aus.

## Schritte für AWS SSM-Hybrid-Aktivierungen

1. Öffnen Sie die [Amazon IAM-Konsole](#)
2. Wählen Sie im linken Navigationsbereich die Option Policies aus.
3. Wählen Sie auf der Seite Richtlinien die Option Richtlinie erstellen.



4. Wählen Sie auf der Seite „Berechtigungen angeben“ im Richtlinien-Editor oben rechts die Option JSON aus. Fügen Sie das folgende Snippet ein. `AWS_REGION` ersetzen Sie es durch die AWS Region Ihrer AWS SSM-Hybrid-Aktivierung und `AWS_ACCOUNT_ID` ersetzen Sie es durch Ihre AWS Konto-ID. Ersetzen Sie `TAG_KEY` und `TAG_VALUE` durch den AWS SSM-Ressourcen-Tag-Schlüssel, den Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung verwendet haben.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ssm:DescribeInstanceInformation",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ssm:DeregisterManagedInstance",
 "Resource": "arn:aws:ssm:AWS_REGION:AWS_ACCOUNT_ID:managed-instance/*",
 "Condition": {
 "StringEquals": {
 "ssm:resourceTag/TAG_KEY": "TAG_VALUE"
 }
 }
 }
]
}
```

- a. Wählen Sie Weiter aus.
5. Auf der Seite Überprüfen und erstellen.
  - a. Geben Sie einen Richtliniennamen für Ihre Richtlinie ein, z. B. `EKSHybridSSMPolicy`
  - b. Wählen Sie Richtlinie erstellen aus.
6. Wählen Sie im linken Navigationsbereich Roles aus.
7. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
8. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
  - a. Wählen Sie im Abschnitt Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus. Fügen Sie Folgendes in den Editor für benutzerdefinierte Vertrauensrichtlinien ein. `AWS_REGION` ersetzen Sie es durch die AWS Region Ihrer AWS SSM-Hybrid-Aktivierung und `AWS_ACCOUNT_ID` durch Ihre AWS Konto-ID.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "AWS_ACCOUNT_ID"
 },
 "ArnEquals": {
 "aws:SourceArn": "arn:aws:ssm:AWS_REGION:AWS_ACCOUNT_ID:*"
 }
 }
 }
]
}
```

b. Wählen Sie Weiter aus.

9. Führen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die folgenden Schritte aus:

- a. Geben Sie in das Feld Richtlinien filtern den Namen der Richtlinie einEKSDescribeClusterPolicy, die Sie oben erstellt haben. Aktivieren Sie in den Suchergebnissen das Kontrollkästchen links neben Ihrem Richtliniennamen.
- b. Geben Sie in das Feld Richtlinien filtern den Namen der Richtlinie einEKSHybridSSMPolicy, die Sie oben erstellt haben. Aktivieren Sie in den Suchergebnissen das Kontrollkästchen links neben Ihrem Richtliniennamen.
- c. Geben Sie im Feld Filter policies (Filterrichtlinien) AmazonEC2ContainerRegistryPullOnly ein. Aktivieren Sie das Kontrollkästchen links neben AmazonEC2ContainerRegistryPullOnly den Suchergebnissen.
- d. Geben Sie im Feld Filter policies (Filterrichtlinien) AmazonSSMManagedInstanceCore ein. Aktivieren Sie das Kontrollkästchen links neben AmazonSSMManagedInstanceCore den Suchergebnissen.
- e. Wählen Sie Weiter aus.

10. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:

- a. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. AmazonEKSHybridNodesRole.
- b. Ersetzen Sie unter Description (Beschreibung) den aktuellen Text durch beschreibenden Text wie beispielsweise Amazon EKS - Hybrid Nodes role.
- c. Wählen Sie Rolle erstellen aus.

## Schritte für AWS IAM Roles Anywhere

Um AWS IAM Roles Anywhere verwenden zu können, müssen Sie Ihren AWS IAM Roles Anywhere-Vertrauensanker einrichten, bevor Sie die IAM-Rolle Hybrid Nodes erstellen. Detaillierte Anweisungen finden Sie unter [the section called "Richten Sie AWS IAM-Rollen überall ein"](#).

1. Öffnen Sie die [Amazon IAM-Konsole](#)
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
  - a. Wählen Sie im Abschnitt Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus. Fügen Sie Folgendes in den Editor für benutzerdefinierte Vertrauensrichtlinien ein. TRUST\_ANCHOR ARN Ersetzen Sie ihn durch den ARN des Vertrauensankers, den Sie in den [the section called "Richten Sie AWS IAM-Rollen überall ein"](#) Schritten erstellt haben. Die Bedingung in dieser Vertrauensrichtlinie schränkt die Fähigkeit von AWS IAM Roles Anywhere ein, die IAM-Rolle Hybrid Nodes anzunehmen und temporäre IAM-Anmeldeinformationen nur auszutauschen, wenn der Name der Rollensitzung mit dem CN im x509-Zertifikat übereinstimmt, das auf Ihren Hybridknoten installiert ist. Sie können auch andere Zertifikatsattribute verwenden, um Ihren Knoten eindeutig zu identifizieren. Das Zertifikatsattribut, das Sie in der Vertrauensrichtlinie verwenden, muss dem NodeName entsprechen, den Sie in Ihrer nodeadm-Konfiguration festgelegt haben. Weitere Informationen hierzu finden Sie unter [the section called "Hybridknoten nodeadm"](#).

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
```

```

 "Principal": {
 "Service": "rolesanywhere.amazonaws.com"
 },
 "Action": [
 "sts:TagSession",
 "sts:SetSourceIdentity"
],
 "Condition": {
 "ArnEquals": {
 "aws:SourceArn": "TRUST_ANCHOR_ARN"
 }
 }
 },
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "rolesanywhere.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "sts:RoleSessionName": "${aws:PrincipalTag/x509Subject/CN}"
 },
 "ArnEquals": {
 "aws:SourceArn": "TRUST_ANCHOR_ARN"
 }
 }
 }
]
}

```

b. Wählen Sie Weiter aus.

5. Führen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die folgenden Schritte aus:

- a. Geben Sie in das Feld Richtlinien filtern den Namen der Richtlinie einEKSDescribeClusterPolicy, die Sie oben erstellt haben. Aktivieren Sie in den Suchergebnissen das Kontrollkästchen links neben Ihrem Richtliniennamen.
- b. Geben Sie im Feld Filter policies (Filterrichtlinien) AmazonEC2ContainerRegistryPullOnly ein. Aktivieren Sie das Kontrollkästchen links neben AmazonEC2ContainerRegistryPullOnly den Suchergebnissen.
- c. Wählen Sie Weiter aus.

6. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
  - a. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. AmazonEKSHybridNodesRole.
  - b. Ersetzen Sie unter Description (Beschreibung) den aktuellen Text durch beschreibenden Text wie beispielsweise Amazon EKS - Hybrid Nodes role.
  - c. Wählen Sie Rolle erstellen aus.

## Erstellen Sie einen Amazon EKS-Cluster mit Hybridknoten

Dieses Thema bietet einen Überblick über die verfügbaren Optionen und beschreibt, was zu beachten ist, wenn Sie einen Amazon EKS-Cluster mit Hybridknoten erstellen. EKS-Hybridknoten bieten dieselbe [Unterstützung für Kubernetes-Versionen](#) wie Amazon EKS-Cluster mit Cloud-Knoten, einschließlich Standard- und erweiterter Unterstützung.

Wenn Sie nicht planen, EKS-Hybridknoten zu verwenden, finden Sie weitere Informationen in der primären Amazon EKS-Dokumentation zum Erstellen von Clustern unter [the section called “Erstellen eines -Clusters”](#).

### Voraussetzungen

- Das [the section called “Voraussetzungen”](#) abgeschlossene. Bevor Sie Ihren Cluster mit aktivierten Hybridknoten erstellen, müssen Sie Ihren lokalen Knoten und optional Ihren Pod CIDRs identifizieren, Ihre VPC und Subnetze gemäß den EKS-Anforderungen und den Anforderungen der Hybridknoten erstellt haben und Ihre Sicherheitsgruppe mit eingehenden Regeln für Ihren lokalen und optionalen Pod. CIDRs Weitere Informationen zu diesen Voraussetzungen finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#)
- Die neueste Version der AWS Befehlszeilenschnittstelle (AWS CLI) ist auf Ihrem Gerät installiert und konfiguriert. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version`. Paketmanager wie yum, apt-get oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der CLI. AWS Informationen zur Installation der neuesten Version finden Sie unter [Installation oder Aktualisierung auf die letzte Version der AWS CLI](#) und [Konfigurieren von Einstellungen für die AWS CLI](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- Ein [IAM-Prinzipal](#) mit Berechtigungen zum Erstellen von IAM-Rollen und zum Anhängen von Richtlinien sowie zum Erstellen und Beschreiben von EKS-Clustern

## Überlegungen

- Ihr Cluster muss entweder API oder API\_AND\_CONFIG\_MAP für den Cluster-Authentifizierungsmodus verwenden.
- Ihr Cluster muss die IPv4 Adressfamilie verwenden.
- Ihr Cluster muss entweder öffentliche oder private Cluster-Endpunktkonnektivität verwenden. Ihr Cluster kann die Cluster-Endpunktkonnektivität „öffentlich und privat“ nicht verwenden, da der Amazon EKS Kubernetes API-Serverendpunkt IPs für Hybridknoten, die außerhalb Ihrer VPC laufen, öffentlich auflöst.
- Die OIDC-Authentifizierung wird für EKS-Cluster mit Hybridknoten unterstützt.
- Sie können die Hybridknotenkonfiguration eines vorhandenen Clusters hinzufügen, ändern oder entfernen. Weitere Informationen finden Sie unter [the section called “Bestehender Cluster”](#).

## Schritt 1: Cluster-IAM-Rolle erstellen

Wenn Sie bereits über eine Cluster-IAM-Rolle verfügen oder Ihren Cluster mit `eksctl` oder erstellen möchten AWS CloudFormation, können Sie diesen Schritt überspringen. Standardmäßig erstellt die AWS CloudFormation Vorlage die Cluster-IAM-Rolle für Sie. `eksctl`

1. Führen Sie den folgenden Befehl aus, um eine JSON-Datei für eine IAM-Vertrauensrichtlinie zu erstellen.

```
cat >eks-cluster-role-trust-policy.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "eks.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
EOF
```

2. Erstellen Sie die Amazon-EKS-Cluster-IAM-Rolle. Geben Sie bei Bedarf als Präfix `eks-cluster-role-trust-policy.json` den Pfad auf Ihrem Computer ein, in den Sie die Datei im vorherigen Schritt

geschrieben haben. Der Befehl verknüpft die im vorherigen Schritt erstellte Vertrauensrichtlinie mit der Rolle. Um eine IAM-Rolle zu erstellen, muss dem [IAM-Prinzipal](#), der die Rolle erstellt, die `iam:CreateRole`-Aktion (Berechtigung) zugewiesen werden.

```
aws iam create-role \
 --role-name myAmazonEKSClusterRole \
 --assume-role-policy-document file://"eks-cluster-role-trust-policy.json"
```

3. Sie können entweder die von Amazon EKS verwaltete Richtlinie zuweisen oder Ihre eigene benutzerdefinierte Richtlinie erstellen. Informationen zu den Mindestberechtigungen, die Sie in Ihrer benutzerdefinierten Richtlinie verwenden müssen, finden Sie unter [the section called "Knoten-IAM-Rolle"](#). Hängen Sie die von Amazon EKS verwaltete Richtlinie `AmazonEKSClusterPolicy` an die Rolle an. Um eine IAM-Richtlinie an einen [IAM-Prinzipal](#) anzuhängen, muss der Prinzipal, der die Richtlinie anhängt, eine der folgenden IAM-Aktionen (Berechtigungen) zugewiesen werden: `iam:AttachUserPolicy` oder `iam:AttachRolePolicy`.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy \
 --role-name myAmazonEKSClusterRole
```

## Schritt 2: Erstellen Sie einen Cluster mit aktivierten Hybridknoten

Sie können einen Cluster erstellen, indem Sie Folgendes verwenden:

- [eksctl](#)
- [AWS CloudFormation](#)
- [AWS CLI](#)
- [AWS Management Console](#)

### Erstellen Sie einen Cluster mit aktivierten Hybridknoten - eksctl

Sie müssen die neueste Version des Befehlszeilentools installieren. `eksctl` Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).

1. Erstellen `cluster-config.yaml`, um einen Amazon IPv4 EKS-Cluster mit Hybridknoten zu definieren. Nehmen Sie die folgenden Ersetzungen in Ihrem `cluster-config.yaml` Eine vollständige Liste der Einstellungen finden Sie in der [eksctl-Dokumentation](#).
  - a. Ersetzen Sie `CLUSTER_NAME` durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Sie muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
  - b. `AWS_REGION` Ersetzen Sie es durch die AWS Region, in der Sie Ihren Cluster erstellen möchten.
  - c. Ersetzen Sie `K8S_VERSION` durch eine von [Amazon EKS unterstützte Version](#).
  - d. `CREDS_PROVIDER` Ersetzen Sie durch `ssm` oder `ira` basierend auf dem Anmeldeinformationsanbieter, den Sie in den Schritten für [the section called "Bereiten Sie die Anmeldeinformationen vor"](#) konfiguriert haben.
  - e. Ersetzen Sie `CA_BUNDLE_CERT`, wenn Ihr Anmeldeinformationsanbieter auf eingestellt ist `ira`, der AWS IAM Roles Anywhere als Anmeldeinformationsanbieter verwendet. `CA_BUNDLE_CERT` ist die Zertifizierungsstelle der Zertifizierungsstelle (CA) und hängt von Ihrer Wahl der Zertifizierungsstelle ab. Das Zertifikat muss im PEM-Format (Privacy Enhanced Mail) vorliegen.
  - f. `GATEWAY_ID` Ersetzen Sie es durch die ID Ihres Virtual Private Gateways oder Transit-Gateways, das an Ihre VPC angehängt werden soll.
  - g. `REMOTE_NODE_CIDR` Ersetzen Sie es durch den lokalen Node CIDR für Ihre Hybridknoten.
  - h. `REMOTE_POD_CIDR` Ersetzen Sie es durch das lokale Pod-CIDR für Workloads, die auf Hybridknoten ausgeführt werden, oder entfernen Sie die Zeile aus Ihrer Konfiguration, wenn Sie keine Webhooks auf Hybridknoten ausführen. Sie müssen Ihre Konfiguration vornehmen, `REMOTE_POD_CIDRS` falls Ihr CNI keine Network Address Translation (NAT) oder Masquerading für Pod-IP-Adressen verwendet, wenn der Pod-Verkehr Ihre lokalen Hosts verlässt. Sie müssen konfigurieren, `REMOTE_POD_CIDRS` ob Sie Webhooks auf Hybridknoten ausführen. Weitere Informationen finden Sie unter. [the section called "Webhooks konfigurieren"](#)
  - i. Ihre lokalen Knoten- und Pod-CIDR-Blöcke müssen die folgenden Anforderungen erfüllen:
    - i. Innerhalb eines der IPv4 RFC-1918-Bereiche liegen: `10.0.0.0/8`, oder. `172.16.0.0/12` `192.168.0.0/16`
    - ii. Überschneiden Sie sich nicht miteinander, das CIDR VPC CIDR für Ihren Cluster oder Ihren Kubernetes-Service IPv4



```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: CLUSTER_NAME
 region: AWS_REGION
 version: "K8S_VERSION"

remoteNetworkConfig:
 iam:
 provider: CREDENTIALS_PROVIDER # default SSM, can also be set to IRA
 # caBundleCert: CA_BUNDLE_CERT
 vpcGatewayID: GATEWAY_ID
 remoteNodeNetworks:
 - cidrs: ["REMOTE_NODE_CIDRS"]
 remotePodNetworks:
 - cidrs: ["REMOTE_POD_CIDRS"]
```

2. Führen Sie den folgenden Befehl aus:

```
eksctl create cluster -f cluster-config.yaml
```

Die Clusterbereitstellung dauert mehrere Minuten. Während der Cluster erstellt wird, werden mehrere Ausgabezeilen angezeigt. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] EKS cluster "CLUSTER_NAME" in "REGION" region is ready
```

3. Fahren Sie fort mit [the section called "Schritt 3: Kubeconfig aktualisieren"](#).

Erstellen Sie einen Cluster mit aktivierten Hybridknoten - AWS CloudFormation

Der CloudFormation Stack erstellt die IAM-Rolle des EKS-Clusters und einen EKS-Cluster mit dem von Ihnen angegebenen RemoteNodeNetwork und RemotePodNetwork. Ändern Sie die CloudFormation Vorlage, wenn Sie Einstellungen für Ihren EKS-Cluster anpassen müssen, die nicht in der CloudFormation Vorlage verfügbar gemacht werden.

1. Laden Sie die CloudFormation Vorlage herunter.

```
curl -OL 'https://raw.githubusercontent.com/aws/eks-hybrid/refs/heads/main/example/hybrid-eks-cfn.yaml'
```

2. Erstellen Sie eine `cfn-eks-parameters.json` und geben Sie Ihre Konfiguration für jeden Wert an.
  - a. `CLUSTER_NAME`: Name des EKS-Clusters, der erstellt werden soll
  - b. `CLUSTER_ROLE_NAME`: Name der EKS-Cluster-IAM-Rolle, die erstellt werden soll. Die Standardeinstellung in der Vorlage ist „EKSClusterRolle“.
  - c. `SUBNET1_ID`: Die ID des ersten Subnetzes, das Sie in den erforderlichen Schritten erstellt haben
  - d. `SUBNET2_ID`: Die ID des zweiten Subnetzes, das Sie in den erforderlichen Schritten erstellt haben
  - e. `SG_ID`: Die Sicherheitsgruppen-ID, die Sie in den erforderlichen Schritten erstellt haben
  - f. `REMOTE_NODE_CIDRS`: der CIDR für den lokalen Knoten für Ihre Hybridknoten
  - g. `REMOTE_POD_CIDRS`: das lokale Pod-CIDR für Workloads, die auf Hybridknoten ausgeführt werden. Sie müssen Ihre Konfiguration vornehmen, `REMOTE_POD_CIDRS` falls Ihr CNI keine Network Address Translation (NAT) oder Masquerading für Pod-IP-Adressen verwendet, wenn der Pod-Verkehr Ihre lokalen Hosts verlässt. Sie müssen konfigurieren, `REMOTE_POD_CIDRS` ob Sie Webhooks auf Hybridknoten ausführen. Weitere Informationen finden Sie unter [the section called “Webhooks konfigurieren”](#)
  - h. Ihre lokalen Knoten- und Pod-CIDR-Blöcke müssen die folgenden Anforderungen erfüllen:
    - i. Innerhalb eines der IPv4 RFC-1918-Bereiche liegen: `10.0.0.0/8`, oder `172.16.0.0/12` `192.168.0.0/16`
    - ii. Überschneiden Sie sich nicht miteinander, weder mit dem CIDR VPC CIDR für Ihren Cluster noch mit Ihrem Kubernetes-Service. IPv4
  - i. `CLUSTER_AUTH`: der Cluster-Authentifizierungsmodus für Ihren Cluster. Gültige Werte sind `API` und `API_AND_CONFIG_MAP`. Die Standardeinstellung in der Vorlage ist `API_AND_CONFIG_MAP`.
  - j. `CLUSTER_ENDPOINT`: Die Cluster-Endpunktkonnektivität für Ihren Cluster. Gültige Werte sind „Public“ und „Private“. Die Standardeinstellung in der Vorlage ist Privat, was bedeutet, dass Sie nur von Ihrer VPC aus eine Verbindung zum Kubernetes-API-Endpunkt herstellen können.
  - k. `K8S_VERSION`: Die Kubernetes-Version, die Sie für Ihren Cluster verwenden möchten. Siehe [the section called “Kubernetes-Versionen”](#).

```
{
 "Parameters": {
 "ClusterName": "CLUSTER_NAME",
 "ClusterRoleName": "CLUSTER_ROLE_NAME",
 "SubnetId1": "SUBNET1_ID",
 "SubnetId2": "SUBNET2_ID",
 "SecurityGroupId": "SG_ID",
 "RemoteNodeCIDR": "REMOTE_NODE_CIDRS",
 "RemotePodCIDR": "REMOTE_POD_CIDRS",
 "ClusterAuthMode": "CLUSTER_AUTH",
 "ClusterEndpointConnectivity": "CLUSTER_ENDPOINT",
 "K8sVersion": "K8S_VERSION"
 }
}
```

3. Stellen Sie den CloudFormation Stack bereit. STACK\_NAME Ersetzen Sie ihn durch Ihren Namen für den CloudFormation Stack und AWS\_REGION durch Ihre AWS Region, in der der Cluster erstellt werden soll.

```
aws cloudformation deploy \
 --stack-name STACK_NAME \
 --region AWS_REGION \
 --template-file hybrid-eks-cfn.yaml \
 --parameter-overrides file://cfn-eks-parameters.json \
 --capabilities CAPABILITY_NAMED_IAM
```

Die Clusterbereitstellung dauert mehrere Minuten. Sie können den Status Ihres Stacks mit dem folgenden Befehl überprüfen. STACK\_NAME Ersetzen Sie ihn durch Ihren Namen für den CloudFormation Stack und AWS\_REGION durch Ihre AWS Region, in der der Cluster erstellt werden soll.

```
aws cloudformation describe-stacks \
 --stack-name STACK_NAME \
 --region AWS_REGION \
 --query 'Stacks[].StackStatus'
```

4. Fahren Sie fort mit [the section called “Schritt 3: Kubeconfig aktualisieren”](#).

## Cluster mit Hybridknoten erstellen — CLI AWS

1. Führen Sie den folgenden Befehl aus, um einen EKS-Cluster mit Hybridknoten zu erstellen. Bevor Sie den Befehl ausführen, ersetzen Sie Folgendes durch Ihre Einstellungen. Eine vollständige Liste der Einstellungen finden Sie in der [the section called “Erstellen eines -Clusters”](#) Dokumentation.
  - a. CLUSTER\_NAME: Name des EKS-Clusters, der erstellt werden soll
  - b. AWS\_REGION: AWS Region, in der der Cluster erstellt wird.
  - c. K8S\_VERSION: Die Kubernetes-Version, die Sie für Ihren Cluster verwenden möchten. Weitere Informationen finden Sie unter Unterstützte Versionen von Amazon EKS.
  - d. ROLE\_ARN: Die Amazon EKS-Clusterrolle, die Sie für Ihren Cluster konfiguriert haben. Weitere Informationen finden Sie unter Amazon EKS-Cluster-IAM-Rolle.
  - e. SUBNET1\_ID: Die ID des ersten Subnetzes, das Sie in den erforderlichen Schritten erstellt haben
  - f. SUBNET2\_ID: Die ID des zweiten Subnetzes, das Sie in den erforderlichen Schritten erstellt haben
  - g. SG\_ID: Die Sicherheitsgruppen-ID, die Sie in den erforderlichen Schritten erstellt haben
  - h. Sie können API und API\_AND\_CONFIG\_MAP für Ihren Cluster-Zugriffs-Authentifizierungsmodus verwenden. Im folgenden Befehl ist der Authentifizierungsmodus für den Clusterzugriff auf eingestelltAPI\_AND\_CONFIG\_MAP.
  - i. Sie können die endpointPrivateAccess Parameter endpointPublicAccess und verwenden, um den öffentlichen und privaten Zugriff auf den Kubernetes-API-Serverendpunkt Ihres Clusters zu aktivieren oder zu deaktivieren. Im folgenden Befehl endpointPublicAccess ist der Wert auf false gesetzt und auf endpointPrivateAccess true gesetzt.
  - j. REMOTE\_NODE\_CIDRS: der CIDR für den lokalen Knoten für Ihre Hybridknoten.
  - k. REMOTE\_POD\_CIDRS(optional): das lokale Pod-CIDR für Workloads, die auf Hybridknoten ausgeführt werden.
  - l. Ihre lokalen Knoten- und Pod-CIDR-Blöcke müssen die folgenden Anforderungen erfüllen:
    - i. Innerhalb eines der IPv4 RFC-1918-Bereiche liegen:10.0.0.0/8,, oder. 172.16.0.0/12  
192.168.0.0/16
    - ii. Keine Überschneidungen miteinander, weder VPC CIDR für Ihren Amazon EKS-Cluster noch für Ihren Kubernetes-Service IPv4 CIDR.

```
aws eks create-cluster \
 --name CLUSTER_NAME \
 --region AWS_REGION \
 --kubernetes-version K8S_VERSION \
 --role-arn ROLE_ARN \
 --resources-vpc-config
subnetIds=SUBNET1_ID,SUBNET2_ID,securityGroupIds=SG_ID,endpointPrivateAccess=true,endpointPublicAccess=true \
 --access-config authenticationMode=API_AND_CONFIG_MAP \
 --remote-network-config '{"remoteNodeNetworks":[{"cidrs":["REMOTE_NODE_CIDRS"]}],"remotePodNetworks":[{"cidrs":["REMOTE_POD_CIDRS"]}]}'
```

- Die Bereitstellung des Clusters dauert mehrere Minuten. Sie können den Status Ihres Clusters mit dem folgenden Befehl überprüfen. CLUSTER\_NAME Ersetzen Sie ihn durch den Namen des Clusters, den Sie erstellen, und AWS\_REGION durch die AWS Region, in der der Cluster erstellt wird. Fahren Sie erst mit dem nächsten Schritt fort, wenn die zurückgegebene ACTIVE Ausgabe

```
aws eks describe-cluster \
 --name CLUSTER_NAME \
 --region AWS_REGION \
 --query "cluster.status"
```

- Fahren Sie fort mit [the section called “Schritt 3: Kubeconfig aktualisieren”](#).

Erstellen Sie einen Cluster mit aktivierten Hybridknoten - AWS Management Console

- Öffnen Sie die Amazon EKS-Konsole auf der [Amazon EKS-Konsole](#).
- Wählen Sie Cluster hinzufügen und dann Erstellen aus.
- Füllen Sie auf der Seite Configure cluster (Cluster konfigurieren) die folgenden Felder aus:
  - Name – Ein Name für Ihren Cluster. Der Name darf nur alphanumerische Zeichen (Groß- und Kleinschreibung beachten), Bindestriche und Unterstriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
  - Cluster-IAM-Rolle — Wählen Sie die Amazon EKS-Cluster-IAM-Rolle aus, die Sie erstellt haben, damit die Kubernetes-Steuerebene AWS Ressourcen in Ihrem Namen verwalten kann.
  - Kubernetes-Version – Die Kubernetes-Version, die für den Cluster verwendet wird. Wir empfehlen, die frühere Version auszuwählen, es sei denn, Sie benötigen eine ältere Version.

- d. Upgrade-Richtlinie — Wählen Sie entweder Erweitert oder Standard.
    - i. Erweitert: Diese Option unterstützt die Kubernetes-Version für 26 Monate nach dem Veröffentlichungsdatum. Für den erweiterten Supportzeitraum fallen zusätzliche stündliche Kosten an, die nach Ablauf des Standard-Supportzeitraums beginnen. Wenn der erweiterte Support endet, wird Ihr Cluster auto auf die nächste Version aktualisiert.
    - ii. Standard: Diese Option unterstützt die Kubernetes-Version für 14 Monate nach dem Veröffentlichungsdatum. Es fallen keine zusätzlichen Kosten an. Wenn die Standardunterstützung endet, wird Ihr Cluster auto auf die nächste Version aktualisiert.
  - e. Clusterzugriff — Geben Sie an, ob Sie den Cluster-Administratorzugriff zulassen oder verbieten möchten, und wählen Sie einen Authentifizierungsmodus aus. Die folgenden Authentifizierungsmodi werden für Cluster mit aktivierten Hybridknoten unterstützt.
    - i. EKS-API: Der Cluster bezieht authentifizierte IAM-Prinzipale nur aus dem EKS-Zugriffseintrag. APIs
    - ii. EKS-API und ConfigMap: Der Cluster bezieht authentifizierte IAM-Prinzipale sowohl aus dem EKS-Zugriffseintrag als auch aus dem. APIs aws-auth ConfigMap
  - f. Secrets-Verschlüsselung – (Optional) Aktivieren Sie die Secrets-Verschlüsselung von Kubernetes-Secrets mithilfe eines KMS-Schlüssels. Sie können diese auch aktivieren, nachdem Sie Ihren Cluster erstellt haben. Bevor Sie diese Funktion aktivieren, stellen Sie sicher, dass Sie mit den Informationen in vertraut sind. [the section called “Aktivieren Sie die geheime Verschlüsselung”](#)
  - g. ARC Zonal Shift — Wenn diese Option aktiviert ist, registriert EKS Ihren Cluster bei ARC Zonal Shift, sodass Sie mithilfe von Zonal Shift den Anwendungsdatenverkehr von einer AZ wegverlagern können.
  - h. Tags – (Optional) Fügen Sie Ihrem Cluster beliebige Tags hinzu. Weitere Informationen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#).
  - i. Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.
4. Wählen Sie auf der Seite Specify networking (Netzwerk angeben) die Werte für die folgenden Felder aus:
- a. VPC — Wählen Sie eine bestehende VPC, die die Anforderungen von [Amazon EKS Hybrid Nodes](#) erfüllt [the section called “VPC- und Subnetz-Anforderungen”](#). Bevor Sie sich für eine VPC entscheiden, empfehlen wir Ihnen, sich mit allen Anforderungen und Überlegungen in View Amazon EKS-Netzwerkanforderungen für VPC, Subnetze und Hybridknoten vertraut zu machen. Sie können nach der Clustererstellung nicht ändern, welche VPC Sie verwenden möchten. Wenn keine aufgeführt VPCs sind, müssen Sie zuerst eine erstellen.

Weitere Informationen finden Sie unter [the section called “Erstellen einer VPC”](#) und in den [Netzwerkanforderungen für Amazon EKS Hybrid Nodes](#).

- b. Subnetze – Standardmäßig sind alle im vorherigen Feld angegebenen Subnetze in der VPC vorausgewählt. Sie müssen mindestens zwei auswählen.
- c. Security groups (Sicherheitsgruppen) – (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die Amazon EKS den erstellten Netzwerkschnittstellen zuordnen soll. Für mindestens eine der von Ihnen angegebenen Sicherheitsgruppen müssen Regeln für eingehenden Datenverkehr für Ihren lokalen Knoten und optional für Ihren Pod gelten. CIDRs Weitere Informationen finden Sie in den [Netzwerkanforderungen für Amazon EKS Hybrid Nodes](#). Unabhängig davon, ob Sie Sicherheitsgruppen wählen oder nicht, erstellt Amazon EKS eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der von Amazon EKS erstellten Cluster-Sicherheitsgruppe finden [the section called “Anforderungen an Sicherheitsgruppen”](#) Sie unter Sie können die Regeln in der von Amazon EKS erstellten Clustersicherheitsgruppe ändern.
- d. Cluster-IP-Adressfamilie wählen — Sie müssen sich IPv4 für Cluster mit aktivierten Hybridknoten entscheiden.
- e. (Optional) Wählen Sie „Kubernetes Service IP-Adressbereich konfigurieren“ und geben Sie einen Dienstbereich an. IPv4
- f. Wählen Sie Remotenetzwerke konfigurieren, um Hybridknoten zu aktivieren, und geben Sie Ihren lokalen Knoten und Pod CIDRs für Hybridknoten an.
- g. Sie müssen Ihr Remote-Pod-CIDR konfigurieren, wenn Ihr CNI keine Network Address Translation (NAT) oder Masquerading für Pod-IP-Adressen verwendet, wenn der Pod-Verkehr Ihre lokalen Hosts verlässt. Sie müssen den Remote-Pod-CIDR konfigurieren, wenn Sie Webhooks auf Hybridknoten ausführen.
- h. Ihre lokalen Knoten- und Pod-CIDR-Blöcke müssen die folgenden Anforderungen erfüllen:
  - i. Innerhalb eines der IPv4 RFC-1918-Bereiche liegen: 10.0.0.0/8,, oder. 172.16.0.0/12 192.168.0.0/16
  - ii. Überschneiden Sie sich nicht miteinander, das CIDR VPC CIDR für Ihren Cluster oder Ihren Kubernetes-Service IPv4
- i. Wählen Sie eine Option für den Cluster-Endpointzugriff aus. Nachdem Ihr Cluster erstellt wurde, können Sie diese Option ändern. Für Cluster mit aktivierten Hybridknoten müssen Sie entweder „Öffentlich“ oder „Privat“ wählen. Bevor Sie eine nicht standardmäßige Option

auswählen, sollten Sie sich mit den Optionen und deren Auswirkungen vertraut machen.

Weitere Informationen finden Sie unter [the section called “Cluster-Endpunktzugriff”](#).

j. Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

5. (Optional) Wählen Sie auf der Seite „Observability konfigurieren“ aus, welche Optionen für die Protokollierung von Metriken und Kontrollebenen aktiviert werden sollen. Standardmäßig sind alle Protokollierungstypen deaktiviert.

a. Weitere Informationen zur Option Prometheus-Metriken finden Sie unter. [the section called “Prometheus-Metriken”](#)

b. Weitere Informationen zu den Protokollierungsoptionen der EKS-Steuerung finden Sie unter. [the section called “Protokolle der Kontrollebene”](#)

c. Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

6. Wählen Sie auf der Seite Select add-ons (Add-Ons auswählen) die Add-Ons aus, die Sie Ihrem Cluster hinzufügen möchten.

a. Sie können so viele Amazon EKS-Add-Ons und AWS Marketplace-Add-Ons auswählen, wie Sie benötigen. Amazon EKS-Add-Ons, die nicht mit Hybridknoten kompatibel sind, sind mit „Nicht kompatibel mit Hybridknoten“ gekennzeichnet und die Add-Ons verfügen über eine Anti-Affinitätsregel, die verhindert, dass sie auf Hybridknoten ausgeführt werden. Weitere Informationen finden Sie unter Konfiguration von Add-Ons für Hybridknoten. Wenn die AWS Marketplace-Add-Ons, die Sie installieren möchten, nicht aufgeführt sind, können Sie nach verfügbaren AWS Marketplace-Add-Ons suchen, indem Sie Text in das Suchfeld eingeben. Sie können auch nach category (Kategorie), vendor (Anbieter) oder pricing model (Preismodell) suchen und dann die Add-Ons aus den Suchergebnissen auswählen.

b. Einige Add-Ons wie CoreDNS und Kube-Proxy sind standardmäßig installiert. Wenn Sie eines der Standard-Add-Ons deaktivieren, kann dies Ihre Fähigkeit beeinträchtigen, Kubernetes-Anwendungen auszuführen.

c. Wenn Sie mit dieser Seite fertig sind, wählen Sie. Next

7. Wählen Sie auf der Seite Einstellungen für ausgewählte Add-ons konfigurieren die Version aus, die Sie installieren möchten.

a. Sie können nach der Clustererstellung jederzeit auf eine neuere Version aktualisieren. Sie können die Konfiguration jedes Add-Ons nach der Cluster-Erstellung aktualisieren. Weitere Informationen zum Konfigurieren eines Add-Ons finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#). Informationen zu den Versionen der Add-ons, die mit Hybridknoten kompatibel sind, finden Sie unter [the section called “Add-Ons konfigurieren”](#).

b. Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.



8. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die Informationen, die Sie auf den vorherigen Seiten eingegeben oder ausgewählt haben. Wenn Sie Änderungen vornehmen müssen, wählen Sie Edit (Bearbeiten). Wenn Sie zufrieden sind, wählen Sie Create. Das Feld Status zeigt CREATING (WIRD ERSTELLT) an, während der Cluster bereitgestellt wird. Die Clusterbereitstellung dauert mehrere Minuten.
9. Fahren Sie fort mit [the section called “Schritt 3: Kubeconfig aktualisieren”](#).

### Schritt 3: Kubeconfig aktualisieren

Wenn Sie Ihren Cluster mit `eksctl` erstellt haben, können Sie diesen Schritt überspringen. Das liegt daran, dass `eksctl` diesen Schritt bereits für Sie durchgeführt hat. Aktivieren Sie `kubectl` die Kommunikation mit Ihrem Cluster, indem Sie der `kubectl` Konfigurationsdatei einen neuen Kontext hinzufügen. Weitere Informationen zum Erstellen und Aktualisieren der Datei finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).

```
aws eks update-kubeconfig --name CLUSTER_NAME --region AWS_REGION
```

Eine Beispielausgabe sieht wie folgt aus.

```
Added new context arn:aws: eks:AWS_REGION:111122223333:cluster/CLUSTER_NAME to /home/username/.kube/config
```

Bestätigen Sie die Kommunikation mit Ihrem Cluster, indem Sie den folgenden Befehl ausführen.

```
kubectl get svc
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME       | TYPE      | CLUSTER-IP | EXTERNAL-IP | PORT(S) | AGE |
|------------|-----------|------------|-------------|---------|-----|
| kubernetes | ClusterIP | 10.100.0.1 | <none>      | 443/TCP | 28h |

### Schritt 4: Cluster-Setup

Im nächsten Schritt erfahren Sie, wie Sie [the section called “Bereiten Sie den Clusterzugriff vor”](#) den Zugriff für Ihre Hybridknoten aktivieren, um Ihrem Cluster beizutreten.

## Aktivieren Sie Hybridknoten auf einem vorhandenen Amazon EKS-Cluster oder ändern Sie die Konfiguration

Dieses Thema bietet einen Überblick über die verfügbaren Optionen und beschreibt, was zu beachten ist, wenn Sie die Hybridknotenkonfiguration für einen Amazon EKS-Cluster hinzufügen, ändern oder entfernen.

Um einem Amazon EKS-Cluster die Verwendung von Hybridknoten zu ermöglichen, fügen Sie der Konfiguration die IP-Adress-CIDR-Bereiche Ihres lokalen Knotens und optional des RemoteNetworkConfig Pod-Netzwerks hinzu. EKS verwendet diese Liste von CIDRs, um die Konnektivität zwischen dem Cluster und Ihren lokalen Netzwerken zu aktivieren. Eine vollständige Liste der Optionen bei der Aktualisierung Ihrer Cluster-Konfiguration finden Sie [UpdateClusterConfig](#) in der Amazon EKS API-Referenz.

Sie können jede der folgenden Aktionen an der Netzwerkkonfiguration von EKS Hybrid Nodes in einem Cluster durchführen:

- [Fügen Sie eine Remote-Netzwerkkonfiguration hinzu, um EKS-Hybridknoten in einem vorhandenen Cluster zu aktivieren.](#)
- [Fügen Sie die Remote-Knoten-Netzwerke oder die Remote-Pod-Netzwerke in einem vorhandenen Cluster hinzu, ändern oder entfernen Sie sie.](#)
- [Entfernen Sie alle CIDR-Bereiche des Remote-Knoten-Netzwerks, um EKS-Hybridknoten in einem vorhandenen Cluster zu deaktivieren.](#)

### Voraussetzungen

- Bevor Sie Ihren Amazon EKS-Cluster für Hybridknoten aktivieren, stellen Sie sicher, dass Ihre Umgebung die unter [the section called “Voraussetzungen”](#), [the section called “Bereiten Sie das Netzwerk vor”](#), [the section called “Bereiten Sie das Betriebssystem vor”](#), und [beschriebenen Anforderungen erfüllt](#) [the section called “Bereiten Sie die Anmeldeinformationen vor”](#).
- Ihr Cluster muss die IPv4 Adressfamilie verwenden.
- Ihr Cluster muss entweder API oder API\_AND\_CONFIG\_MAP für den Cluster-Authentifizierungsmodus verwenden. Das Verfahren zum Ändern des Cluster-Authentifizierungsmodus wird unter [beschrieben](#) [the section called “Authentifizierungsmodus”](#).
- Wir empfehlen, entweder öffentlichen oder privaten Endpunktzugriff für den Amazon EKS Kubernetes API-Serverendpunkt zu verwenden, aber nicht beide. Wenn Sie „Öffentlich und

privat“ wählen, wird der Amazon EKS Kubernetes API-Serverendpunkt IPs für Hybridknoten, die außerhalb Ihrer VPC laufen, immer öffentlich aufgelöst, wodurch verhindert werden kann, dass Ihre Hybridknoten dem Cluster beitreten. Das Verfahren zur Änderung des Netzwerkzugriffs auf Ihren Cluster wird unter beschrieben. [the section called “Cluster-Endpunktzugriff”](#)

- Die neueste Version der AWS Befehlszeilenschnittstelle (AWS CLI) ist auf Ihrem Gerät installiert und konfiguriert. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version`. Paketmanager wie yum, apt-get oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der CLI. AWS Informationen zur Installation der neuesten Version finden Sie unter [Installation oder Aktualisierung auf die neueste Version der AWS CLI](#) und [Konfigurieren von Einstellungen für die AWS CLI](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- Ein [IAM-Principal](#) mit der Berechtigung, Ihren [UpdateClusterConfig](#) Amazon EKS-Cluster aufzurufen.
- Aktualisieren Sie Add-Ons auf Versionen, die mit Hybridknoten kompatibel sind. Die Versionen der Add-ons, die mit Hybridknoten kompatibel sind, finden Sie unter [the section called “Add-Ons konfigurieren”](#).
- Wenn Sie Add-Ons ausführen, die nicht mit Hybridknoten kompatibel sind, stellen Sie sicher, dass für das Add-On [DaemonSet](#) oder die [Bereitstellung](#) die folgende Affinitätsregel gilt, um die Bereitstellung auf Hybridknoten zu verhindern. Fügen Sie die folgende Affinitätsregel hinzu, falls sie noch nicht vorhanden ist.

```
affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
```

## Überlegungen

Das `remoteNetworkConfig` JSON-Objekt verhält sich während einer Aktualisierung wie folgt:

- Jeder vorhandene Teil der Konfiguration, den Sie nicht angeben, bleibt unverändert. Wenn Sie keinen der beiden Parameter `remoteNodeNetworks` oder `angebenremotePodNetworks`, bleibt dieser Teil unverändert.

- Wenn Sie eine der `remotePodNetworks` Listen `remoteNodeNetworks` oder von ändern CIDRs, müssen Sie in Ihrer endgültigen Konfiguration die vollständige Liste angeben CIDRs , die Sie möchten. Wenn Sie eine Änderung an der `remotePodNetworks` CIDR-Liste `remoteNodeNetworks` oder angeben, ersetzt EKS die ursprüngliche Liste während der Aktualisierung.
- Ihre lokalen Knoten- und Pod-CIDR-Blöcke müssen die folgenden Anforderungen erfüllen:
  1. Innerhalb eines der IPv4 RFC-1918-Bereiche liegen: 10.0.0.0/8, 172.16.0.0/12 oder 192.168.0.0/16.
  2. Keine Überschneidungen miteinander, mit CIDRs der gesamten VPC für Ihren Amazon EKS-Cluster oder mit Ihrem Kubernetes-Service CIDR. IPv4

Aktivieren Sie Hybridknoten auf einem vorhandenen Cluster

Sie können EKS-Hybridknoten in einem vorhandenen Cluster aktivieren, indem Sie Folgendes verwenden:

- [AWS CloudFormation](#)
- [AWS CLI](#)
- [AWS Management Console](#)

Aktivieren Sie EKS-Hybridknoten in einem vorhandenen Cluster - AWS CloudFormation

1. Um EKS-Hybridknoten in Ihrem Cluster zu aktivieren, fügen Sie Ihrer CloudFormation Vorlage das `RemoteNodeNetwork` und (optional) `RemotePodNetwork` hinzu und aktualisieren Sie den Stack. Beachten Sie, dass `RemoteNodeNetwork` es sich um eine Liste mit maximal einem `Cidrs` Element und um eine Liste mit mehreren IP-CIDR-Bereichen `Cidrs` handelt.

```
RemoteNetworkConfig:
 RemoteNodeNetworks:
 - Cidrs: [RemoteNodeCIDR]
 RemotePodNetworks:
 - Cidrs: [RemotePodCIDR]
```

2. Fahren Sie fort mit [the section called “Bereiten Sie den Clusterzugriff vor”](#).

## Aktivieren Sie EKS-Hybridknoten in einem vorhandenen Cluster — AWS CLI

1. Führen Sie den folgenden Befehl aus, um RemoteNetworkConfig die EKS-Hybridknoten für Ihren EKS-Cluster zu aktivieren. Bevor Sie den Befehl ausführen, ersetzen Sie Folgendes durch Ihre Einstellungen. Eine vollständige Liste der Einstellungen finden Sie [UpdateClusterConfig](#) in der Amazon EKS API-Referenz.
  - a. CLUSTER\_NAME: Name des EKS-Clusters, der aktualisiert werden soll.
  - b. AWS\_REGION: AWS Region, in der der EKS-Cluster ausgeführt wird.
  - c. REMOTE\_NODE\_CIDRS: der CIDR für den lokalen Knoten für Ihre Hybridknoten.
  - d. REMOTE\_POD\_CIDRS(optional): das lokale Pod-CIDR für Workloads, die auf Hybridknoten ausgeführt werden.

```
aws eks update-cluster-config \
 --name CLUSTER_NAME \
 --region AWS_REGION \
 --remote-network-config '{"remoteNodeNetworks":[{"cidrs":
["REMOTE_NODE_CIDRS"]}], "remotePodNetworks":[{"cidrs":["REMOTE_POD_CIDRS"]}]}'
```

2. Die Aktualisierung des Clusters dauert mehrere Minuten. Sie können den Status Ihres Clusters mit dem folgenden Befehl überprüfen. CLUSTER\_NAME Ersetzen Sie durch den Namen des Clusters, den Sie ändern, und AWS\_REGION durch die AWS Region, in der der Cluster ausgeführt wird. Fahren Sie erst mit dem nächsten Schritt fort, wenn die zurückgegebene Ausgabe lautet ACTIVE.

```
aws eks describe-cluster \
 --name CLUSTER_NAME \
 --region AWS_REGION \
 --query "cluster.status"
```

3. Fahren Sie fort mit [the section called “Bereiten Sie den Clusterzugriff vor”](#).

## Aktivieren Sie EKS-Hybridknoten in einem vorhandenen Cluster - AWS Management Console

1. Öffnen Sie die Amazon EKS-Konsole auf der [Amazon EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, um Ihre Cluster-Informationen anzuzeigen.
3. Wählen Sie die Registerkarte Netzwerk und dann Verwalten.
4. Wählen Sie in der Dropdownliste die Option Remote-Netzwerke aus.

5. Wählen Sie Remotenetzwerke konfigurieren, um Hybridknoten zu aktivieren, und geben Sie Ihren lokalen Knoten und Pod CIDRs für Hybridknoten an.
6. Wählen Sie Änderungen speichern, um den Vorgang abzuschließen. Warten Sie, bis der Clusterstatus wieder Aktiv ist.
7. Fahren Sie fort mit [the section called “Bereiten Sie den Clusterzugriff vor”](#).

Aktualisieren Sie die Konfiguration der Hybridknoten in einem vorhandenen Cluster

Sie können Änderungen `remoteNetworkConfig` in einem vorhandenen Hybridcluster vornehmen, indem Sie eine der folgenden Methoden verwenden:

- [AWS CloudFormation](#)
- [AWS CLI](#)
- [AWS Management Console](#)

Hybridkonfiguration in einem vorhandenen Cluster aktualisieren - AWS CloudFormation

1. Aktualisieren Sie Ihre CloudFormation Vorlage mit den neuen Netzwerk-CIDR-Werten.

```
RemoteNetworkConfig:
 RemoteNodeNetworks:
 - Cidrs: [NEW_REMOTE_NODE_CIDRS]
 RemotePodNetworks:
 - Cidrs: [NEW_REMOTE_POD_CIDRS]
```

#### Note

Nehmen Sie bei der Aktualisierung `RemoteNodeNetworks` von `RemotePodNetworks` CIDR-Listen alle CIDRs (neue und bestehende) auf. EKS ersetzt bei Aktualisierungen die gesamte Liste. Wenn Sie diese Felder in der Aktualisierungsanforderung weglassen, bleiben ihre vorhandenen Konfigurationen erhalten.

2. Aktualisieren Sie Ihren CloudFormation Stack mit der geänderten Vorlage und warten Sie, bis das Stack-Update abgeschlossen ist.

## Hybridkonfiguration in einem vorhandenen Cluster aktualisieren — AWS CLI

1. Führen Sie den folgenden Befehl aus CIDRs, um das Remote-Netzwerk zu ändern. Ersetzen Sie die Werte durch Ihre Einstellungen:

```
aws eks update-cluster-config
--name CLUSTER_NAME
--region AWS_REGION
--remote-network-config '{"remoteNodeNetworks":[{"cidrs":
["NEW_REMOTE_NODE_CIDRS"]}],"remotePodNetworks":[{"cidrs":
["NEW_REMOTE_POD_CIDRS"]}]}'
```

### Note

Schließen Sie bei der Aktualisierung `remoteNodeNetworks` von `remotePodNetworks` CIDR-Listen alle CIDRs (neue und bestehende) mit ein. EKS ersetzt bei Aktualisierungen die gesamte Liste. Wenn Sie diese Felder in der Aktualisierungsanforderung weglassen, bleiben ihre vorhandenen Konfigurationen erhalten.

2. Warten Sie, bis der Clusterstatus wieder AKTIV ist, bevor Sie fortfahren.

## Hybridkonfiguration in einem vorhandenen Cluster aktualisieren - AWS Management Console

1. Öffnen Sie die Amazon EKS-Konsole auf der [Amazon EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, um Ihre Cluster-Informationen anzuzeigen.
3. Wählen Sie die Registerkarte Netzwerk und dann Verwalten.
4. Wählen Sie in der Dropdownliste die Option Remote-Netzwerke aus.
5. Aktualisieren Sie die CIDRs unter Remote node networks und nach Remote pod networks - Optional Bedarf.
6. Wählen Sie Änderungen speichern und warten Sie, bis der Clusterstatus wieder Aktiv ist.

## Deaktivieren Sie Hybridknoten in einem vorhandenen Cluster

Sie können EKS-Hybridknoten in einem vorhandenen Cluster wie folgt deaktivieren:

- [AWS CloudFormation](#)
- [AWS CLI](#)

- [AWS Management Console](#)

Deaktivieren Sie EKS-Hybridknoten in einem vorhandenen Cluster - AWS CloudFormation

1. Um EKS-Hybridknoten in Ihrem Cluster RemotePodNetworks zu deaktivieren, legen Sie Arrays in Ihrer CloudFormation Vorlage fest RemoteNodeNetworks und leeren Sie sie und aktualisieren Sie den Stack.

```
RemoteNetworkConfig:
 RemoteNodeNetworks: []
 RemotePodNetworks: []
```

Deaktivieren Sie EKS-Hybridknoten in einem vorhandenen Cluster — AWS CLI

1. Führen Sie den folgenden Befehl aus, um ihn RemoteNetworkConfig aus Ihrem EKS-Cluster zu entfernen. Bevor Sie den Befehl ausführen, ersetzen Sie Folgendes durch Ihre Einstellungen. Eine vollständige Liste der Einstellungen finden Sie [UpdateClusterConfig](#) in der Amazon EKS API-Referenz.
  - a. CLUSTER\_NAME: Name des EKS-Clusters, der aktualisiert werden soll.
  - b. AWS\_REGION: AWS Region, in der der EKS-Cluster ausgeführt wird.

```
aws eks update-cluster-config \
 --name CLUSTER_NAME \
 --region AWS_REGION \
 --remote-network-config '{"remoteNodeNetworks":[],"remotePodNetworks":[]}'
```

2. Die Aktualisierung des Clusters dauert mehrere Minuten. Sie können den Status Ihres Clusters mit dem folgenden Befehl überprüfen. CLUSTER\_NAME Ersetzen Sie durch den Namen des Clusters, den Sie ändern, und AWS\_REGION durch die AWS Region, in der der Cluster ausgeführt wird. Fahren Sie erst mit dem nächsten Schritt fort, wenn die zurückgegebene Ausgabe lautet ACTIVE.

```
aws eks describe-cluster \
 --name CLUSTER_NAME \
 --region AWS_REGION \
 --query "cluster.status"
```



Deaktivieren Sie EKS-Hybridknoten in einem vorhandenen Cluster - AWS Management Console

1. Öffnen Sie die Amazon EKS-Konsole auf der [Amazon EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, um Ihre Cluster-Informationen anzuzeigen.
3. Wählen Sie die Registerkarte Netzwerk und dann Verwalten.
4. Wählen Sie in der Dropdownliste die Option Remote-Netzwerke aus.
5. Wählen Sie Remotenetzwerke konfigurieren, um Hybridknoten zu aktivieren, und entfernen Sie alle CIDRs Unter Remote node networks - und Remote pod networks - Optional.
6. Wählen Sie Änderungen speichern, um den Vorgang abzuschließen. Warten Sie, bis der Clusterstatus wieder Aktiv ist.

## Clusterzugriff für Hybridknoten vorbereiten

Bevor Sie Hybridknoten mit Ihrem Amazon EKS-Cluster verbinden, müssen Sie Ihre Hybrid Nodes IAM-Rolle mit Kubernetes-Berechtigungen aktivieren, um dem Cluster beizutreten. Informationen [the section called “Bereiten Sie die Anmeldeinformationen vor”](#) zur Erstellung der IAM-Rolle Hybrid Nodes finden Sie unter. Amazon EKS unterstützt zwei Möglichkeiten, IAM-Prinzipale mit Kubernetes Role-Based Access Control (RBAC), Amazon EKS-Zugriffseinträgen und dem zu verknüpfen. aws-auth ConfigMap Weitere Informationen zur Amazon EKS-Zugriffsverwaltung finden Sie unter [the section called “Kubernetes-API-Zugriff”](#).

Verwenden Sie die folgenden Verfahren, um Ihre IAM-Rolle Hybrid Nodes mit Kubernetes-Berechtigungen zu verknüpfen. Um Amazon EKS-Zugriffseinträge verwenden zu können, muss Ihr Cluster mit den API\_AND\_CONFIG\_MAP Authentifizierungsmodi API oder erstellt worden sein. Um den verwenden zu können aws-auth ConfigMap, muss Ihr Cluster im API\_AND\_CONFIG\_MAP Authentifizierungsmodus erstellt worden sein. Der Authentifizierungsmodus „CONFIG\_MAPNur“ wird für Amazon EKS-Cluster, die Hybridknoten aktivieren, nicht unterstützt.

### Verwenden von Amazon EKS-Zugriffseinträgen für die IAM-Rolle Hybrid Nodes

Es gibt einen Amazon EKS-Zugriffseintragstyp für Hybridknoten namens HYBRID\_LINUX, der mit einer IAM-Rolle verwendet werden kann. Bei diesem Zugriffseintragstyp wird der Benutzername automatisch auf system:node: {} gesetzt. SessionName Weitere Informationen zum Erstellen von Zugriffseinträgen finden Sie unter. [the section called “Zugangseinträge erstellen”](#)

## AWS CLI

1. Sie müssen die neueste Version der AWS CLI auf Ihrem Gerät installiert und konfiguriert haben. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version`. Paketmanager wie `yum`, `apt-get` oder `Homebrew` für macOS liegen oft mehrere Versionen hinter der neuesten Version der CLI. AWS Informationen zur Installation der neuesten Version finden Sie unter Installation und Schnellkonfiguration mit `aws configure` im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
2. Erstellen Sie Ihren Zugangseintrag mit dem folgenden Befehl. Ersetzen Sie `CLUSTER_NAME` durch den Namen Ihres Clusters und `HYBRID_NODES_ROLE_ARN` durch den ARN der Rolle, die Sie in den Schritten für erstellt haben. [the section called “Bereiten Sie die Anmeldeinformationen vor”](#)

```
aws eks create-access-entry --cluster-name CLUSTER_NAME \
 --principal-arn HYBRID_NODES_ROLE_ARN \
 --type HYBRID_LINUX
```

## AWS Management Console

1. Öffnen Sie die Amazon EKS-Konsole auf der [Amazon EKS-Konsole](#).
2. Wählen Sie den Namen Ihres Clusters, für den Hybridknoten aktiviert sind.
3. Wählen Sie die Registerkarte Zugriff aus.
4. Wählen Sie Zugriffseintrag erstellen aus.
5. Wählen Sie als IAM-Prinzipal die IAM-Rolle Hybrid Nodes aus, die Sie in den Schritten für erstellt haben. [the section called “Bereiten Sie die Anmeldeinformationen vor”](#)
6. Wählen Sie als Typ Hybrid Linux aus.
7. (Optional) Weisen Sie dem Zugriffseintrag unter Tags Beschriftungen zu. So können Sie beispielsweise ganz einfach nach allen Ressourcen mit dem gleichen Tag suchen.
8. Wählen Sie „Zur Überprüfung und Erstellung überspringen“. Sie können dem Hybrid-Linux-Zugriffseintrag keine Richtlinien hinzufügen oder seinen Zugriffsbereich ändern.
9. Überprüfen Sie die Konfiguration für Ihren Zugriffseintrag. Sollten Sie einen Fehler entdecken, wählen Sie Zurück aus, um schrittweise zurück zu navigieren und den Fehler zu korrigieren. Ist die Konfiguration korrekt, wählen Sie Erstellen aus.

## Verwenden von aws-auth ConfigMap für die IAM-Rolle Hybrid Nodes

In den folgenden Schritten erstellen oder aktualisieren Sie die IAM-Rolle aws-auth ConfigMap mit dem ARN der Hybrid Nodes IAM-Rolle, die Sie in den Schritten für [the section called “Bereiten Sie die Anmeldeinformationen vor”](#) erstellt haben.

1. Prüfen Sie, ob aws-auth ConfigMap für Ihren Cluster bereits eine vorhanden ist. Beachten Sie, dass Sie das --kubeconfig Flag verwenden müssen, wenn Sie eine bestimmte kubeconfig Datei verwenden.

```
kubectl describe configmap -n kube-system aws-auth
```

2. Wenn Ihnen eine angezeigt wird aws-auth ConfigMap, aktualisieren Sie sie nach Bedarf.
  - a. Öffnen Sie das ConfigMap zur Bearbeitung.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Fügen Sie nach Bedarf einen neuen mapRoles-Eintrag hinzu.  
HYBRID\_NODES\_ROLE\_ARN Ersetzen Sie es durch den ARN Ihrer Hybrid Nodes IAM-Rolle. Hinweis, {{SessionName}} ist das richtige Vorlagenformat zum Speichern in. ConfigMap Ersetzen Sie es nicht durch andere Werte.

```
data:
 mapRoles: |
 - groups:
 - system:bootstrappers
 - system:nodes
 rolearn: HYBRID_NODES_ROLE_ARN
 username: system:node:{{SessionName}}
```

- c. Speichern Sie die Datei und beenden Sie den Text-Editor.
3. Wenn es aws-auth ConfigMap für Ihren Cluster noch keinen gibt, erstellen Sie ihn mit dem folgenden Befehl. HYBRID\_NODES\_ROLE\_ARN Ersetzen Sie es durch den ARN Ihrer Hybrid Nodes IAM-Rolle. Beachten Sie, dass {{SessionName}} dies das richtige Vorlagenformat zum Speichern in ist. ConfigMap Ersetzen Sie es nicht durch andere Werte.

```
kubectl apply -f=/dev/stdin <<-EOF
apiVersion: v1
kind: ConfigMap
metadata:
```

```
name: aws-auth
namespace: kube-system
data:
 mapRoles: |
 - groups:
 - system:bootstrappers
 - system:nodes
 rolearn: HYBRID_NODES_ROLE_ARN
 username: system:node:{{SessionName}}
EOF
```

## Führen Sie lokale Workloads auf Hybridknoten aus

In einem EKS-Cluster mit aktivierten Hybridknoten können Sie lokale Anwendungen und Edge-Anwendungen auf Ihrer eigenen Infrastruktur mit denselben Amazon EKS-Clustern, Funktionen und Tools ausführen, die Sie in der AWS Cloud verwenden.

Die folgenden Abschnitte enthalten step-by-step Anweisungen zur Verwendung von Hybridknoten.

### Themen

- [Hybridknoten Connect](#)
- [Connect Hybridknoten mit Bottlerocket](#)
- [Aktualisieren Sie Hybridknoten für Ihren Cluster](#)
- [Patchen Sie Sicherheitsupdates für Hybridknoten](#)
- [Hybridknoten entfernen](#)

## Hybridknoten Connect

### Note

Die folgenden Schritte gelten für Hybridknoten, auf denen kompatible Betriebssysteme außer Bottlerocket ausgeführt werden. Schritte zum Verbinden eines Hybridknotens, auf dem Bottlerocket ausgeführt wird, finden Sie unter [the section called “Connect Hybridknoten mit Bottlerocket”](#)

In diesem Thema wird beschrieben, wie Hybridknoten mit einem Amazon EKS-Cluster verbunden werden. Nachdem Ihre Hybridknoten dem Cluster beigetreten sind, werden sie in der Amazon EKS-Konsole und in Kubernetes-kompatiblen Tools wie kubectl mit dem Status Nicht bereit angezeigt. Nachdem Sie die Schritte auf dieser Seite abgeschlossen haben, fahren Sie damit fort, Ihre Hybridknoten für [the section called “CNI konfigurieren”](#) die Ausführung von Anwendungen vorzubereiten.

## Voraussetzungen

Bevor Sie Hybridknoten mit Ihrem Amazon EKS-Cluster verbinden, stellen Sie sicher, dass Sie die erforderlichen Schritte abgeschlossen haben.

- Sie haben Netzwerkkonnektivität von Ihrer lokalen Umgebung zur AWS Region, in der Ihr Amazon EKS-Cluster gehostet wird. Weitere Informationen finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#).
- Sie haben ein kompatibles Betriebssystem für Hybridknoten auf Ihren lokalen Hosts installiert. Weitere Informationen finden Sie unter [the section called “Bereiten Sie das Betriebssystem vor”](#).
- Sie haben Ihre IAM-Rolle Hybrid Nodes erstellt und Ihren lokalen Anbieter für Anmeldeinformationen eingerichtet (AWS Systems Manager Manager-Hybridaktivierungen oder AWS IAM Roles Anywhere). Weitere Informationen finden Sie unter [the section called “Bereiten Sie die Anmeldeinformationen vor”](#).
- Sie haben Ihren Amazon EKS-Cluster mit Hybridknoten erstellt. Weitere Informationen finden Sie unter [the section called “Cluster erstellen”](#).
- Sie haben Ihre IAM-Rolle Hybrid Nodes mit den RBAC-Berechtigungen (Role-Based Access Control) von Kubernetes verknüpft. Weitere Informationen finden Sie unter [the section called “Bereiten Sie den Clusterzugriff vor”](#).

Schritt 1: Installieren Sie die Hybridknoten-CLI (**nodeadm**) auf jedem lokalen Host

Wenn Sie die Amazon EKS Hybrid Nodes CLI (nodeadm) in Ihre vorgefertigten Betriebssystem-Images aufnehmen, können Sie diesen Schritt überspringen. Weitere Informationen zur Hybridknoten-Version von finden Sie nodeadm unter [the section called “Hybridknoten nodeadm”](#).

Die Hybridknoten-Version von nodeadm wird in Amazon S3 gehostet, das von Amazon CloudFront bereitgestellt wird. Um nodeadm auf jedem lokalen Host zu installieren, können Sie den folgenden Befehl von Ihren lokalen Hosts aus ausführen.

Für x86\_64-Hosts:

```
curl -OL 'https://hybrid-assets.eks.amazonaws.com/releases/latest/bin/linux/amd64/
nodeadm'
```

## Für ARM-Hosts

```
curl -OL 'https://hybrid-assets.eks.amazonaws.com/releases/latest/bin/linux/arm64/
nodeadm'
```

Fügen Sie der heruntergeladenen Binärdatei auf jedem Host die Berechtigung für eine ausführbare Datei hinzu.

```
chmod +x nodeadm
```

## Schritt 2: Installieren Sie die Abhängigkeiten der Hybridknoten mit **nodeadm**

Wenn Sie die Abhängigkeiten der Hybridknoten in vorgefertigten Betriebssystem-Images installieren, können Sie diesen Schritt überspringen. Der `nodeadm install` Befehl kann verwendet werden, um alle Abhängigkeiten zu installieren, die für Hybridknoten erforderlich sind. Zu den Abhängigkeiten der Hybridknoten gehören containerd-, kubelet-, kubectl- und AWS SSM- oder IAM Roles Anywhere-Komponenten. AWS Weitere Informationen zu [the section called “Hybridknoten nodeadm”](#) den Komponenten und Dateispeicherorten, die von installiert wurden, finden Sie unter. `nodeadm install` Weitere Informationen zu den Domänen, die für diesen `nodeadm install` Vorgang in Ihrer lokalen Firewall zugelassen werden müssen, finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#) Für Hybridknoten.

Führen Sie den folgenden Befehl aus, um die Abhängigkeiten der Hybridknoten auf Ihrem lokalen Host zu installieren. Der folgende Befehl muss mit einem Benutzer ausgeführt werden, der Sudo-/Root-Zugriff auf Ihrem Host hat.

### Important

Die CLI (nodeadm) der Hybridknoten muss mit einem Benutzer ausgeführt werden, der Sudo/Root-Zugriff auf Ihrem Host hat.

- `K8S_VERSION` Ersetzen Sie es beispielsweise durch die Kubernetes-Nebenversion Ihres Amazon EKS-Clusters. 1.31 Eine Liste der unterstützten Kubernetes-Versionen finden Sie unter. [the section called “Kubernetes-Versionen”](#)

- `CREDS_PROVIDER` Ersetzen Sie es durch den lokalen Anbieter für Anmeldeinformationen, den Sie verwenden. Gültige Werte gelten `ssm` für AWS SSM und `iam-ra` für AWS IAM Roles Anywhere.

```
nodeadm install K8S_VERSION --credential-provider CREDS_PROVIDER
```

### Schritt 3: Connect Hybridknoten mit Ihrem Cluster

Bevor Sie Ihre Hybridknoten mit Ihrem Cluster verbinden, stellen Sie sicher, dass Sie den erforderlichen Zugriff in Ihrer lokalen Firewall und in der Sicherheitsgruppe für Ihren Cluster für die Amazon EKS-Kontrollebene zu/von der Hybridknotenkommunikation zugelassen haben. Die meisten Probleme in diesem Schritt beziehen sich auf die Firewall-Konfiguration, die Sicherheitsgruppenkonfiguration oder die IAM-Rollenkonfiguration der Hybridknoten.

#### Important

Die CLI (nodeadm) der Hybridknoten muss mit einem Benutzer ausgeführt werden, der Sudo/Root-Zugriff auf Ihrem Host hat.

1. Erstellen Sie auf jedem Host eine `nodeConfig.yaml` Datei mit den Werten für Ihre Bereitstellung. Eine vollständige Beschreibung der verfügbaren Konfigurationseinstellungen finden Sie unter [the section called “Hybridknoten nodeadm”](#). Wenn Ihre IAM-Rolle Hybrid Nodes keine Berechtigung für die `eks:DescribeCluster` Aktion besitzt, müssen Sie Ihren Kubernetes-API-Endpunkt, das Cluster-CA-Bundle und den Kubernetes-Service IPv4 CIDR im Cluster-Bereich Ihres übergeben. `nodeConfig.yaml`
  - a. Verwenden Sie das folgende `nodeConfig.yaml` Beispiel, wenn Sie AWS SSM-Hybrid-Aktivierungen für Ihren lokalen Anbieter von Anmeldeinformationen verwenden.
    - i. Ersetzen Sie `CLUSTER_NAME` mit dem Namen Ihres Clusters.
    - ii. Ersetzen Sie es `AWS_REGION` durch die AWS Region, in der Ihr Cluster gehostet wird. Beispiel, `us-west-2`.
    - iii. `ACTIVATION_CODE` Ersetzen Sie es durch den Aktivierungscode, den Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung erhalten haben. Weitere Informationen finden Sie unter [the section called “Bereiten Sie die Anmeldeinformationen vor”](#).
    - iv. `ACTIVATION_ID` Ersetzen Sie es durch die Aktivierungs-ID, die Sie bei der Erstellung Ihrer AWS SSM-Hybrid-Aktivierung erhalten haben. Sie können diese Informationen von der AWS

Systems Manager Manager-Konsole oder vom AWS `aws ssm describe-activations` CLI-Befehl abrufen.

```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: CLUSTER_NAME
 region: AWS_REGION
 hybrid:
 ssm:
 activationCode: ACTIVATION_CODE
 activationId: ACTIVATION_ID
```

- b. Verwenden Sie das folgende `nodeConfig.yaml` Beispiel, wenn Sie AWS IAM Roles Anywhere für Ihren lokalen Anbieter von Anmeldeinformationen verwenden.
  - i. Ersetzen Sie `CLUSTER_NAME` mit dem Namen Ihres Clusters.
  - ii. Ersetzen Sie es `AWS_REGION` durch die AWS Region, in der Ihr Cluster gehostet wird. Beispiel, `us-west-2`.
  - iii. `NODE_NAME` Ersetzen Sie durch den Namen Ihres Knotens. Der Knotenname muss mit dem CN des Zertifikats auf dem Host übereinstimmen, wenn Sie die Vertrauensrichtlinie Ihrer IAM-Rolle für Hybrid Nodes mit der `"sts:RoleSessionName": "${aws:PrincipalTag/x509Subject/CN}"` Ressourcenbedingung konfiguriert haben. Der von `nodeName` Ihnen verwendete Text darf nicht länger als 64 Zeichen sein.
  - iv. `TRUST_ANCHOR_ARN` Ersetzen Sie ihn durch den ARN des Vertrauensankers, den Sie in den Schritten zum Vorbereiten von Anmeldeinformationen für Hybridknoten konfiguriert haben.
  - v. `PROFILE_ARN` Ersetzen Sie es durch den ARN des Vertrauensankers, den Sie in den Schritten für konfiguriert haben [the section called "Bereiten Sie die Anmeldeinformationen vor"](#).
  - vi. `ROLE_ARN` Ersetzen Sie es durch den ARN Ihrer Hybrid Nodes IAM-Rolle.
  - vii. `CERTIFICATE_PATH` Ersetzen Sie es durch den Pfad auf der Festplatte zu Ihrem Knotenzertifikat. Wenn Sie es nicht angeben, ist die Standardeinstellung `/etc/iam/pki/server.pem`.
  - viii. `KEY_PATH` Ersetzen Sie es durch den Pfad auf der Festplatte zu Ihrem privaten Schlüssel für Ihr Zertifikat. Wenn Sie ihn nicht angeben, ist der Standardwert `/etc/iam/pki/server.key`.



```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: CLUSTER_NAME
 region: AWS_REGION
 hybrid:
 iamRolesAnywhere:
 nodeName: NODE_NAME
 trustAnchorArn: TRUST_ANCHOR_ARN
 profileArn: PROFILE_ARN
 roleArn: ROLE_ARN
 certificatePath: CERTIFICATE_PATH
 privateKeyPath: KEY_PATH
```

2. Führen Sie den `nodeadm init` Befehl mit Ihrem `ausnodeConfig.yaml`, um Ihre Hybridknoten mit Ihrem Amazon EKS-Cluster zu verbinden.

```
nodeadm init -c file://nodeConfig.yaml
```

Wenn der obige Befehl erfolgreich ausgeführt wird, ist Ihr Hybridknoten Ihrem Amazon EKS-Cluster beigetreten. Sie können dies in der Amazon EKS-Konsole überprüfen, indem Sie zur Registerkarte Compute für Ihren Cluster navigieren ([stellen Sie sicher, dass der IAM-Prinzipal über Anzeigeberechtigungen verfügt](#)) oder mit `kubectl get nodes`

#### Important

Ihre Knoten erhalten dann den erwarteten Status `Not Ready`, der darauf zurückzuführen ist, dass auf Ihren Hybridknoten kein CNI läuft. Wenn Ihre Knoten dem Cluster nicht beigetreten sind, finden Sie weitere Informationen unter [the section called “Fehlerbehebung”](#).

#### Schritt 4: Konfigurieren Sie ein CNI für Hybridknoten

Um Ihre Hybridknoten für die Ausführung von Anwendungen vorzubereiten, fahren Sie mit den Schritten unter [the section called “CNI konfigurieren”](#) fort.

## Connect Hybridknoten mit Bottlerocket

In diesem Thema wird beschrieben, wie Hybridknoten, auf denen Bottlerocket ausgeführt wird, mit einem Amazon EKS-Cluster verbunden werden. [Bottlerocket](#) ist eine Open-Source-Linux-Distribution, die von [Amazon](#) gesponsert und unterstützt wird. AWS Bottlerocket wurde speziell für das Hosten von Container-Workloads entwickelt. Mit Bottlerocket können Sie die Verfügbarkeit containerisierter Bereitstellungen verbessern und die Betriebskosten senken, indem Sie Updates Ihrer Container-Infrastruktur automatisieren. Bottlerocket enthält nur die für den Betrieb von Containern unverzichtbare Software, wodurch die Ressourcennutzung verbessert, Sicherheitsbedrohungen reduziert und der Verwaltungsaufwand gesenkt wird.

Nur VMware Varianten von Bottlerocket Version v1.37.0 und höher werden mit EKS-Hybridknoten unterstützt. VMware Varianten von Bottlerocket sind für die Kubernetes-Versionen v1.28 und höher verfügbar. Die Betriebssystem-Images für diese Varianten beinhalten Kubelet, Containerd, aws-iam-authenticator und andere Softwarevoraussetzungen für EKS-Hybridknoten. Sie können diese Komponenten mithilfe einer [Bottlerocket-Einstellungsdatei](#) konfigurieren, die Base64-kodierte Benutzerdaten für den Bottlerocket-Bootstrap und die Admin-Container enthält. Durch die Konfiguration dieser Einstellungen kann Bottlerocket Ihren Anbieter für Hybrid-Nodes Credentials verwenden, um Hybridknoten in Ihrem Cluster zu authentifizieren. Nachdem Ihre Hybridknoten dem Cluster beigetreten sind, werden sie mit Status Not Ready in der Amazon EKS-Konsole und in Kubernetes-kompatiblen Tools wie z. B. angezeigt. `kubectl` Nachdem Sie die Schritte auf dieser Seite abgeschlossen haben, fahren Sie damit fort, Ihre Hybridknoten [the section called “CNI konfigurieren”](#) für die Ausführung von Anwendungen vorzubereiten.

### Voraussetzungen

Bevor Sie Hybridknoten mit Ihrem Amazon EKS-Cluster verbinden, stellen Sie sicher, dass Sie die erforderlichen Schritte abgeschlossen haben.

- Sie haben Netzwerkkonnektivität von Ihrer lokalen Umgebung zur AWS Region, in der Ihr Amazon EKS-Cluster gehostet wird. Weitere Informationen finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#).
- Sie haben Ihre IAM-Rolle Hybrid Nodes erstellt und Ihren lokalen Anbieter für Anmeldeinformationen eingerichtet (AWS Systems Manager Manager-Hybridaktivierungen oder AWS IAM Roles Anywhere). Weitere Informationen finden Sie unter [the section called “Bereiten Sie die Anmeldeinformationen vor”](#).
- Sie haben Ihren Amazon EKS-Cluster mit Hybridknoten erstellt. Weitere Informationen finden Sie unter [the section called “Cluster erstellen”](#).

- Sie haben Ihre IAM-Rolle Hybrid Nodes mit den RBAC-Berechtigungen (Role-Based Access Control) von Kubernetes verknüpft. Weitere Informationen finden Sie unter [the section called “Bereiten Sie den Clusterzugriff vor”](#).

## Schritt 1: Erstellen Sie die TOML-Datei mit den Bottlerocket-Einstellungen

Um Bottlerocket für Hybridknoten zu konfigurieren, müssen Sie eine Datei mit der erforderlichen Konfiguration erstellen. `settings.toml` Der Inhalt der TOML-Datei unterscheidet sich je nach dem von Ihnen verwendeten Anmeldeinformationsanbieter (SSM oder IAM Roles Anywhere). Diese Datei wird bei der Bereitstellung der Bottlerocket-Instanz als Benutzerdaten übergeben.

### SSM

Wenn Sie AWS Systems Manager als Ihren Anmeldeinformationsanbieter verwenden, erstellen Sie eine `settings.toml` Datei mit dem folgenden Inhalt:

```
[settings.kubernetes]
cluster-name = "<cluster-name>"
api-server = "<api-server-endpoint>"
cluster-certificate = "<cluster-certificate-authority>"
hostname-override = "<hostname>"
provider-id = "eks-hybrid:///<region>/<cluster-name>/<hostname>"
authentication-mode = "aws"

[settings.network]
hostname = "<hostname>"

[settings.aws]
region = "<region>"

[settings.kubernetes.node-labels]
"eks.amazonaws.com/compute-type" = "hybrid"
"eks.amazonaws.com/hybrid-credential-provider" = "ssm"

[settings.host-containers.admin]
enabled = true
user-data = "<base64-encoded-admin-container-userdata>"

[settings.bootstrap-containers.eks-hybrid-setup]
mode = "always"
user-data = "<base64-encoded-bootstrap-container-userdata>"
```

```
[settings.host-containers.control]
enabled = true
```

Ersetzen Sie die Platzhalter durch die folgenden Werte:

- `<cluster-name>`: Der Name Ihres Amazon EKS-Clusters.
- `<api-server-endpoint>`: Der API-Serverendpunkt Ihres Clusters.
- `<cluster-certificate-authority>`: Das Base64-kodierte CA-Bundle Ihres Clusters.
- `<region>`: Die AWS Region, in der Ihr Cluster gehostet wird, zum Beispiel „us-east-1“.
- `<hostname>`: Der Hostname der Bottlerocket-Instanz, der auch als Knotenname konfiguriert wird. Dies kann ein beliebiger eindeutiger Wert Ihrer Wahl sein, muss jedoch den Benennungskonventionen für [Kubernetes-Objekte](#) entsprechen. Außerdem darf der von Ihnen verwendete Hostname nicht länger als 64 Zeichen sein. HINWEIS: Wenn Sie den SSM-Anbieter verwenden, werden dieser Hostname und der Knotenname durch die verwaltete Instanz-ID (z. B. `mi-*` ID) ersetzt, nachdem die Instanz bei SSM registriert wurde.
- `<base64-encoded-admin-container-userdata>`: Der Base64-kodierte Inhalt der Bottlerocket-Admin-Container-Konfiguration. Wenn Sie den Admin-Container aktivieren, können Sie mit SSH eine Verbindung zu Ihrer Bottlerocket-Instanz herstellen, um das System zu erkunden und zu debuggen. Diese Einstellung ist zwar nicht erforderlich, wir empfehlen jedoch, sie zu aktivieren, um die Fehlerbehebung zu vereinfachen. Weitere Informationen zur Authentifizierung mit dem [Admin-Container finden Sie in der Bottlerocket-Admin-Container-Dokumentation](#). Der Admin-Container akzeptiert SSH-Benutzer- und Schlüsseleingaben im JSON-Format, zum Beispiel

```
{
 "user": "<ssh-user>",
 "ssh": {
 "authorized-keys": [
 "<ssh-authorized-key>"
]
 }
}
```

- `<base64-encoded-bootstrap-container-userdata>`: Der Base64-kodierte Inhalt der Bottlerocket-Bootstrap-Container-Konfiguration. Weitere Informationen zu seiner Konfiguration finden Sie in der [Bottlerocket-Bootstrap-Container-Dokumentation](#). Der Bootstrap-Container ist dafür verantwortlich, die Instance als AWS SSM-verwaltete Instance zu registrieren und

ihr als Kubernetes-Knoten in Ihrem Amazon EKS-Cluster beizutreten. Die an den Bootstrap-Container übergebenen Benutzerdaten haben die Form eines Befehlsaufrufs, der den SSM-Hybrid-Aktivierungscode und die ID, die Sie zuvor erstellt haben, als Eingabe akzeptiert:

```
eks-hybrid-ssm-setup --activation-id=<activation-id> --activation-code=<activation-code> --region=<region>
```

## IAM Roles Anywhere

Wenn Sie AWS IAM Roles Anywhere als Ihren Anmeldeinformationsanbieter verwenden, erstellen Sie eine `settings.toml` Datei mit dem folgenden Inhalt:

```
[settings.kubernetes]
cluster-name = "<cluster-name>"
api-server = "<api-server-endpoint>"
cluster-certificate = "<cluster-certificate-authority>"
hostname-override = "<hostname>"
provider-id = "eks-hybrid:///<region>/<cluster-name>/<hostname>"
authentication-mode = "aws"

[settings.network]
hostname = "<hostname>"

[settings.aws]
region = "<region>"
config = "<base64-encoded-aws-config-file>"

[settings.kubernetes.node-labels]
"eks.amazonaws.com/compute-type" = "hybrid"
"eks.amazonaws.com/hybrid-credential-provider" = "iam-ra"

[settings.host-containers.admin]
enabled = true
user-data = "<base64-encoded-admin-container-userdata>"

[settings.bootstrap-containers.eks-hybrid-setup]
mode = "always"
user-data = "<base64-encoded-bootstrap-container-userdata>"
```

Ersetzen Sie die Platzhalter durch die folgenden Werte:

- `<cluster-name>`: Der Name Ihres Amazon EKS-Clusters.
- `<api-server-endpoint>`: Der API-Serverendpunkt Ihres Clusters.
- `<cluster-certificate-authority>`: Das Base64-kodierte CA-Bundle Ihres Clusters.
- `<region>`: Die AWS Region, in der Ihr Cluster gehostet wird, z. B. „us-east-1“
- `<hostname>`: Der Hostname der Bottlerocket-Instanz, der auch als Knotenname konfiguriert wird. Dies kann ein beliebiger eindeutiger Wert Ihrer Wahl sein, muss jedoch den Benennungskonventionen für [Kubernetes-Objekte](#) entsprechen. Außerdem darf der von Ihnen verwendete Hostname nicht länger als 64 Zeichen sein. HINWEIS: Wenn Sie den IAM-RA-Anbieter verwenden, muss der Knotenname mit der CN des Zertifikats auf dem Host übereinstimmen, wenn Sie die Vertrauensrichtlinie Ihrer Hybrid Nodes IAM-Rolle mit der Ressourcenbedingung konfiguriert haben. `"sts:RoleSessionName": "${aws:PrincipalTag/x509Subject/CN}"`
- `<base64-encoded-aws-config-file>`: Der Base64-kodierte Inhalt Ihrer Konfigurationsdatei. AWS Der Inhalt der Datei sollte wie folgt aussehen:

```
[default]
credential_process = aws_signing_helper credential-process --certificate /root/.aws/
node.crt --private-key /root/.aws/node.key --profile-arn <profile-arn> --role-arn
<role-arn> --trust-anchor-arn <trust-anchor-arn> --role-session-name <role-session-
name>
```

- `<base64-encoded-admin-container-userdata>`: Der Base64-kodierte Inhalt der Bottlerocket-Admin-Container-Konfiguration. Wenn Sie den Admin-Container aktivieren, können Sie mit SSH eine Verbindung zu Ihrer Bottlerocket-Instanz herstellen, um das System zu erkunden und zu debuggen. Diese Einstellung ist zwar nicht erforderlich, wir empfehlen jedoch, sie zu aktivieren, um die Fehlerbehebung zu vereinfachen. Weitere Informationen zur Authentifizierung mit dem [Admin-Container finden Sie in der Bottlerocket-Admin-Container-Dokumentation](#). Der Admin-Container akzeptiert SSH-Benutzer- und Schlüsseleingaben im JSON-Format, zum Beispiel

```
{
 "user": "<ssh-user>",
 "ssh": {
 "authorized-keys": [
 "<ssh-authorized-key>"
]
 }
}
```

```
}
```

- `<base64-encoded-bootstrap-container-userdata>`: Der Base64-kodierte Inhalt der Bottlerocket-Bootstrap-Container-Konfiguration. Weitere Informationen zu seiner Konfiguration finden Sie in der [Bottlerocket-Bootstrap-Container-Dokumentation](#). Der Bootstrap-Container ist für die Erstellung des IAM Roles Anywhere-Hostzertifikats und der privaten Zertifikatsschlüsseldateien auf der Instanz verantwortlich. Diese werden dann von den `verwendetaws_signing_helper`, um temporäre Anmeldeinformationen für die Authentifizierung mit Ihrem Amazon EKS-Cluster zu erhalten. Die an den Bootstrap-Container übergebenen Benutzerdaten haben die Form eines Befehlsaufrufs, der den Inhalt des zuvor erstellten Zertifikats und des privaten Schlüssels als Eingabe akzeptiert:

```
eks-hybrid-iam-ra-setup --certificate=<certificate> --key=<private-key>
```

## Schritt 2: Bereitstellen der Bottlerocket vSphere-VM mit Benutzerdaten

Nachdem Sie die TOML-Datei erstellt haben, übergeben Sie sie bei der Erstellung der vSphere-VM als Benutzerdaten. Beachten Sie, dass die Benutzerdaten konfiguriert werden müssen, bevor die VM zum ersten Mal eingeschaltet wird. Daher müssen Sie sie bei der Erstellung der Instanz angeben. Wenn Sie die VM im Voraus erstellen möchten, muss sich die VM im Status `PoweredOff` befinden, bis Sie die Benutzerdaten dafür konfiguriert haben. Wenn Sie beispielsweise die `govc` CLI verwenden:

### VM zum ersten Mal erstellen

```
govc vm.create \
 -on=true \
 -c=2 \
 -m=4096 \
 -net.adapter=<network-adapter> \
 -net=<network-name> \
 -e guestinfo.userdata.encoding="base64" \
 -e guestinfo.userdata="$(base64 -w0 settings.toml)" \
 -template=<template-name> \
 <vm-name>
```

### Benutzerdaten für eine bestehende VM aktualisieren

```
govc vm.create \

```

```
-on=false \
-c=2 \
-m=4096 \
-net.adapter=<network-adapter> \
-net=<network-name> \
-template=<template-name> \
<vm-name>
```

```
govc vm.change
-vm <vm-name> \
-e guestinfo.userdata="$(base64 -w0 settings.toml)" \
-e guestinfo.userdata.encoding="base64"
```

```
govc vm.power -on <vm-name>
```

In den obigen Abschnitten gibt die `-e guestinfo.userdata.encoding="base64"` Option an, dass die Benutzerdaten Base64-codiert sind. Die `-e guestinfo.userdata` Option übergibt den Base64-codierten Inhalt der `settings.toml` Datei als Benutzerdaten an die Bottlerocket-Instanz. Ersetzen Sie die Platzhalter durch Ihre spezifischen Werte, z. B. die Bottlerocket-OVA-Vorlage und Netzwerkdetails.

### Schritt 3: Überprüfen Sie die Verbindung mit dem Hybridknoten

Nachdem die Bottlerocket-Instance gestartet wurde, versucht sie, Ihrem Amazon EKS-Cluster beizutreten. Sie können die Verbindung in der Amazon EKS-Konsole überprüfen, indem Sie zur Registerkarte Compute für Ihren Cluster navigieren oder den folgenden Befehl ausführen:

```
kubectl get nodes
```

#### Important

Ihre Knoten erhalten dann den erwarteten Status `Not Ready`, der darauf zurückzuführen ist, dass auf Ihren Hybridknoten kein CNI läuft. Wenn Ihre Knoten dem Cluster nicht beigetreten sind, finden Sie weitere Informationen unter [the section called “Fehlerbehebung”](#).

### Schritt 4: Konfigurieren Sie ein CNI für Hybridknoten

Um Ihre Hybridknoten für die Ausführung von Anwendungen vorzubereiten, fahren Sie mit den Schritten unter [the section called “CNI konfigurieren”](#) fort.



## Aktualisieren Sie Hybridknoten für Ihren Cluster

Die Anleitung für das Upgrade von Hybridknoten ähnelt den selbstverwalteten Amazon EKS-Knoten, die in Amazon EC2 ausgeführt werden. Wir empfehlen Ihnen, neue Hybridknoten auf Ihrer Kubernetes-Zielversion zu erstellen, Ihre vorhandenen Anwendungen ordnungsgemäß auf die Hybridknoten der neuen Kubernetes-Version zu migrieren und die Hybridknoten auf der alten Kubernetes-Version aus Ihrem Cluster zu entfernen. Lesen Sie unbedingt die [Amazon EKS Best Practices](#) für Upgrades, bevor Sie ein Upgrade starten. Amazon EKS-Hybridknoten bieten dieselbe [Kubernetes-Versionsunterstützung](#) für Amazon EKS-Cluster mit Cloud-Knoten, einschließlich Standard- und erweiterter Unterstützung.

Amazon EKS-Hybridknoten folgen derselben [Richtlinie für Versionsverzerrungen](#) für Knoten wie Upstream-Kubernetes. Amazon EKS-Hybridknoten können nicht auf einer neueren Version als der Amazon EKS-Kontrollebene installiert sein, und Hybridknoten können bis zu drei Kubernetes-Nebenenversionen sein, die älter sind als die Nebenversion der Amazon EKS-Steuerungsebene.

Wenn Sie keine freien Kapazitäten haben, um neue Hybridknoten auf Ihrer Kubernetes-Zielversion für eine Upgrade-Strategie zur Umstellung der Migration zu erstellen, können Sie alternativ die Amazon EKS Hybrid Nodes CLI (nodeadm) verwenden, um die Kubernetes-Version Ihrer Hybridknoten vor Ort zu aktualisieren.

### Important

Wenn Sie Ihre Hybridknoten direkt mit `aktualisierennodeadm`, kommt es während des Vorgangs, bei dem die ältere Version der Kubernetes-Komponenten heruntergefahren und die Komponenten der neuen Kubernetes-Version installiert und gestartet werden, zu Ausfallzeiten für den Knoten.

## Voraussetzungen

Stellen Sie vor dem Upgrade sicher, dass Sie die folgenden Voraussetzungen erfüllt haben.

- Die Kubernetes-Zielversion für Ihr Hybrid-Knoten-Upgrade muss gleich oder kleiner als die Version der Amazon EKS-Kontrollebene sein.
- Wenn Sie eine Upgrade-Strategie für die Umstellung der Migration verfolgen, müssen die neuen Hybridknoten, die Sie auf Ihrer Kubernetes-Zielversion installieren, die Anforderungen erfüllen. [the section called “Voraussetzungen”](#) Dazu gehören IP-Adressen innerhalb des Remote Node Network CIDR, das Sie bei der Erstellung des Amazon EKS-Clusters übergeben haben.

- Sowohl für die Umstellung als auch für direkte Upgrades müssen die Hybridknoten Zugriff auf die [erforderlichen Domänen](#) haben, um die neuen Versionen der Abhängigkeiten der Hybridknoten abrufen zu können.
- Sie müssen kubect1 auf Ihrem lokalen Computer oder Ihrer Instance installiert haben, die Sie für die Interaktion mit Ihrem Amazon EKS Kubernetes API-Endpunkt verwenden.
- Die Version Ihres CNI muss die Kubernetes-Version unterstützen, auf die Sie ein Upgrade durchführen. Wenn dies nicht der Fall ist, aktualisieren Sie Ihre CNI-Version, bevor Sie Ihre Hybridknoten aktualisieren. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#).

### Upgrades für die Cutover-Migration (blau-grün)

Bei Cutover-Migrationsaktualisierungen handelt es sich um den Prozess der Erstellung neuer Hybridknoten auf neuen Hosts mit Ihrer Kubernetes-Zielversion, der ordnungsgemäßen Migration Ihrer vorhandenen Anwendungen auf die neuen Hybridknoten auf Ihrer Kubernetes-Zielversion und der Entfernung der Hybridknoten auf der alten Kubernetes-Version aus Ihrem Cluster. Diese Strategie wird auch als blau-grüne Migration bezeichnet.

1. Connect Ihre neuen Hosts als Hybridknoten, indem Sie die folgenden [the section called “Hybridknoten Connect”](#) Schritte befolgen. Verwenden Sie bei der Ausführung des `nodeadm install` Befehls Ihre Kubernetes-Zielversion.
2. Ermöglichen Sie die Kommunikation zwischen den neuen Hybridknoten auf der Ziel-Kubernetes-Version und Ihren Hybridknoten auf der alten Kubernetes-Version. Diese Konfiguration ermöglicht es Pods, miteinander zu kommunizieren, während Sie Ihren Workload auf die Hybridknoten auf der Kubernetes-Zielversion migrieren.
3. Bestätigen Sie, dass Ihre Hybridknoten auf Ihrer Kubernetes-Zielversion Ihrem Cluster erfolgreich beigetreten sind und den Status Bereit haben.
4. Verwenden Sie den folgenden Befehl, um jeden Knoten, den Sie entfernen möchten, als nicht planbar zu markieren. Dadurch wird verhindert, dass neue Pods auf den Knoten, die Sie ersetzen, geplant oder neu geplant werden. Weitere Informationen finden Sie unter [kubect1 cordon in der Kubernetes-Dokumentation](#). Ersetzen Sie es `NODE_NAME` durch den Namen der Hybridknoten in der alten Kubernetes-Version.

```
kubect1 cordon NODE_NAME
```

Sie können alle Knoten einer bestimmten Kubernetes-Version (in diesem Fall 1.28) mit dem folgenden Codeausschnitt identifizieren und absperren.

```
K8S_VERSION=1.28
for node in $(kubectl get nodes -o json | jq --arg K8S_VERSION
"$K8S_VERSION" -r '.items[] | select(.status.nodeInfo.kubeletVersion |
match("\($K8S_VERSION)")).metadata.name')
do
 echo "Cordoning $node"
 kubectl cordon $node
done
```

5. Wenn in Ihrer aktuellen Bereitstellung weniger als zwei CoreDNS-Replikate auf Ihren Hybridknoten ausgeführt werden, skalieren Sie die Bereitstellung auf mindestens zwei Replikate. Wir empfehlen, dass Sie mindestens zwei CoreDNS-Replikate auf Hybridknoten ausführen, um die Ausfallsicherheit während des normalen Betriebs zu gewährleisten.

```
kubectl scale deployments/coredns --replicas=2 -n kube-system
```

6. Entleeren Sie jeden der Hybridknoten auf der alten Kubernetes-Version, die Sie aus Ihrem Cluster entfernen möchten, mit dem folgenden Befehl. Weitere Informationen zum Entleeren von Knoten finden Sie unter [Safely Drain a Node](#) in der Kubernetes-Dokumentation. `NODE_NAME` Ersetzen Sie es durch den Namen der Hybridknoten in der alten Kubernetes-Version.

```
kubectl drain NODE_NAME --ignore-daemonsets --delete-emptydir-data
```

Sie können alle Knoten einer bestimmten Kubernetes-Version (in diesem Fall 1.28) mit dem folgenden Codeausschnitt identifizieren und löschen.

```
K8S_VERSION=1.28
for node in $(kubectl get nodes -o json | jq --arg K8S_VERSION
"$K8S_VERSION" -r '.items[] | select(.status.nodeInfo.kubeletVersion |
match("\($K8S_VERSION)")).metadata.name')
do
 echo "Draining $node"
 kubectl drain $node --ignore-daemonsets --delete-emptydir-data
done
```

7. Sie können es verwenden `nodeadm`, um die Artefakte der Hybridknoten zu stoppen und vom Host zu entfernen. Sie müssen die Ausführung `nodeadm` mit einem Benutzer ausführen, der über `root/`

`sudo` Berechtigungen verfügt. `nodeadm uninstall` Wird standardmäßig nicht fortgesetzt, wenn noch Pods auf dem Knoten vorhanden sind. Weitere Informationen finden Sie unter [the section called “Hybridknoten nodeadm”](#).

```
nodeadm uninstall
```

8. Nachdem die Artefakte der Hybridknoten gestoppt und deinstalliert wurden, entfernen Sie die Knotenressource aus Ihrem Cluster.

```
kubectl delete node node-name
```

Sie können alle Knoten einer bestimmten Kubernetes-Version (in diesem Fall 1.28) mit dem folgenden Codeausschnitt identifizieren und löschen.

```
K8S_VERSION=1.28
for node in $(kubectl get nodes -o json | jq --arg K8S_VERSION
"$K8S_VERSION" -r '.items[] | select(.status.nodeInfo.kubeletVersion |
match("\($K8S_VERSION)")).metadata.name')
do
 echo "Deleting $node"
 kubectl delete node $node
done
```

9. Je nachdem, für welches CNI Sie sich entschieden haben, können nach der Ausführung der obigen Schritte noch Artefakte auf Ihren Hybridknoten verbleiben. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#).

## Direkte Upgrades

Der direkte Upgrade-Prozess bezieht sich auf das Upgrade der Kubernetes-Version für Hybridknoten, ohne neue physische oder virtuelle Hosts und eine Umstellungsstrategie zu verwenden. `nodeadm upgrade` Der `nodeadm upgrade` Prozess fährt die vorhandenen älteren Kubernetes-Komponenten herunter, die auf dem Hybridknoten ausgeführt werden, deinstalliert die vorhandenen älteren Kubernetes-Komponenten, installiert die neuen Kubernetes-Zielkomponenten und startet die neuen Kubernetes-Zielkomponenten. Es wird dringend empfohlen, jeweils einen Knoten zu aktualisieren, um die Auswirkungen auf Anwendungen, die auf den Hybridknoten ausgeführt werden, zu minimieren. Die Dauer dieses Vorgangs hängt von Ihrer Netzwerkbandbreite und Latenz ab.

1. Verwenden Sie den folgenden Befehl, um den Knoten, den Sie aktualisieren, als nicht planbar zu markieren. Dadurch wird verhindert, dass neue Pods auf dem Knoten, den Sie aktualisieren, geplant oder verschoben werden. Weitere Informationen finden Sie unter [kubect1 cordon in der Kubernetes-Dokumentation](#). Ersetzen Sie es NODE\_NAME durch den Namen des Hybridknotens, den Sie aktualisieren

```
kubect1 cordon NODE_NAME
```

2. Entleeren Sie den Knoten, den Sie aktualisieren, mit dem folgenden Befehl. Weitere Informationen zum Entleeren von Knoten finden Sie unter [Sicheres Entleeren eines Knotens](#) in der Kubernetes-Dokumentation. NODE\_NAME Ersetzen Sie es durch den Namen des Hybridknotens, den Sie aktualisieren.

```
kubect1 drain NODE_NAME --ignore-daemonsets --delete-emptydir-data
```

3. Führen Sie es nodeadm upgrade auf dem Hybridknoten aus, den Sie aktualisieren. Sie müssen die Ausführung nodeadm mit einem Benutzer ausführen, der über root/sudo Rechte verfügt. Der Name des Knotens wird beim Upgrade sowohl für AWS SSM- als auch für AWS IAM Roles Anywhere-Anmeldeinformationsanbieter beibehalten. Sie können die Anbieter von Anmeldeinformationen während des Upgrade-Vorgangs nicht ändern. Konfigurationswerte [the section called “Hybridknoten nodeadm”](#) für finden Sie unter nodeConfig.yaml. K8S\_VERSION Ersetzen Sie es durch die Kubernetes-Zielversion, auf die Sie das Upgrade durchführen.

```
nodeadm upgrade K8S_VERSION -c file://nodeConfig.yaml
```

4. Geben Sie Folgendes ein, damit Pods nach dem Upgrade auf dem Knoten geplant werden können. NODE\_NAME Ersetzen Sie es durch den Namen des Knotens.

```
kubect1 uncordon NODE_NAME
```

5. Beobachten Sie den Status Ihrer Hybridknoten und warten Sie, bis Ihre Knoten heruntergefahren und mit der neuen Kubernetes-Version mit dem Status Bereit neu gestartet werden.

```
kubect1 get nodes -o wide -w
```

## Patchen Sie Sicherheitsupdates für Hybridknoten

In diesem Thema wird das Verfahren zum direkten Patchen von Sicherheitsupdates für bestimmte Pakete und Abhängigkeiten beschrieben, die auf Ihren Hybridknoten ausgeführt werden. Als bewährte Methode empfehlen wir Ihnen, Ihre Hybridknoten regelmäßig zu aktualisieren, um Sicherheitspatches CVEs zu erhalten.

Schritte zum Upgrade der Kubernetes-Version finden Sie unter [the section called “Aktualisieren Sie Hybridknoten”](#)

Ein Beispiel für Software, für die möglicherweise Sicherheitspatches erforderlich sind, ist `containerd`

### Containerd

`containerd` ist die standardmäßige Kubernetes-Container-Laufzeit und Kernabhängigkeit für EKS-Hybridknoten. Sie wird für die Verwaltung des Container-Lebenszyklus verwendet, einschließlich des Abrufs von Images und der Verwaltung der Containerausführung. Auf einem Hybridknoten können Sie die Installation `containerd` über die [Nodeadm-CLI](#) oder manuell durchführen. Je nach Betriebssystem Ihres Nodes erfolgt die Installation über das `containerd` vom Betriebssystem verteilte Paket oder das Docker-Paket. `nodeadm`

Wenn ein CVE-In veröffentlicht `containerd` wurde, haben Sie die folgenden Optionen, um auf Ihren Hybrid-Knoten `containerd` auf die gepatchte Version von zu aktualisieren.

Schritt 1: Überprüfen Sie, ob der Patch für die Paketmanager veröffentlicht wurde

Sie können anhand der entsprechenden Sicherheitsbulletins überprüfen, ob der `containerd` CVE-Patch für die jeweiligen Betriebssystem-Paketmanager veröffentlicht wurde:

- [Amazon Linux 2023](#)
- [RHEL](#)
- [Ubuntu 20.04](#)
- [Ubuntu 22.04](#)
- [Ubuntu 24.04](#)

Wenn Sie das Docker-Repo als Quelle für verwenden `containerd`, können Sie anhand der [Sicherheitsankündigungen von Docker](#) die Verfügbarkeit der gepatchten Version im Docker-Repo überprüfen.

## Schritt 2: Wählen Sie die Methode zur Installation des Patches

Es gibt drei Methoden, um Sicherheitsupdates direkt auf Knoten zu patchen und zu installieren. Welche Methode Sie verwenden können, hängt davon ab, ob der Patch vom Betriebssystem aus im Paketmanager verfügbar ist oder nicht:

1. Installieren Sie `Patchesnodeadm upgrade`, die in den Paketmanagern veröffentlicht wurden, siehe [Schritt 2 a.](#)
2. Installieren Sie Patches direkt mit den Paketmanagern, siehe [Schritt 2 b.](#)
3. Installieren Sie benutzerdefinierte Patches, die nicht in Paketmanagern veröffentlicht wurden. Beachten Sie, dass bei benutzerdefinierten Patches für `containerd` [Schritt 2 c](#) besondere Überlegungen zu beachten sind.

### Schritt 2 a: Patchen mit **nodeadm upgrade**

Nachdem Sie bestätigt haben, dass der `containerd` CVE-Patch in den OS- oder Docker-Repos (entweder Apt oder RPM) veröffentlicht wurde, können Sie den `nodeadm upgrade` Befehl verwenden, um auf die neueste Version von zu aktualisieren. `containerd` Da es sich nicht um ein Upgrade der Kubernetes-Version handelt, müssen Sie Ihre aktuelle Kubernetes-Version an den Upgrade-Befehl übergeben. `nodeadm`

```
nodeadm upgrade K8S_VERSION --config-source file:///root/nodeConfig.yaml
```

### Schritt 2 b: Patchen mit Paketmanagern des Betriebssystems

Alternativ können Sie das Update auch über den jeweiligen Paketmanager durchführen und damit das `containerd` Paket wie folgt aktualisieren.

#### Amazon Linux 2023

```
sudo yum update -y
sudo yum install -y containerd
```

#### RHEL

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo https://download.docker.com/linux/rhel/docker-
ce.repo
sudo yum update -y
```

```
sudo yum install -y containerd
```

## Ubuntu

```
sudo mkdir -p /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/
docker.asc
echo \
 "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/ubuntu \
 $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}") stable" | \
 sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update -y
sudo apt install -y --only-upgrade containerd.io
```

### Schritt 2 c: Der **Containerd** CVE-Patch wurde nicht in den Paketmanagern veröffentlicht

Wenn die gepatchte containerd Version nur auf andere Weise als im Paketmanager verfügbar ist, z. B. in GitHub Releases, können Sie sie containerd von der offiziellen GitHub Website aus installieren.

1. Wenn der Computer dem Cluster bereits als Hybridknoten beigetreten ist, müssen Sie den `nodeadm uninstall` Befehl ausführen.
2. Installieren Sie die offiziellen containerd Binärdateien. Sie können die Schritte verwenden, unter GitHub denen die [offiziellen Installationsschritte beschrieben](#) sind.
3. Führen Sie den `nodeadm install` Befehl mit dem `--containerd-source` Argument auf `ausnone`, wodurch die containerd Installation übersprungen wird. Sie können den Wert von `none` in der containerd Quelle für jedes Betriebssystem verwenden, das auf dem Knoten ausgeführt wird.

```
nodeadm install K8S_VERSION --credential-provider CREDS_PROVIDER --containerd-source
none
```

## Hybridknoten entfernen

In diesem Thema wird beschrieben, wie Sie Hybridknoten aus Ihrem Amazon EKS-Cluster löschen. [Sie müssen Ihre Hybridknoten mit einem Kubernetes-kompatiblen Tool Ihrer Wahl wie kubectl löschen.](#) Die Gebühren für Hybridknoten enden, wenn das Knotenobjekt aus dem Amazon EKS-



Cluster entfernt wird. Weitere Informationen zu den Preisen für Hybridknoten finden Sie unter [Amazon EKS-Preise](#).

 **Important**

Das Entfernen von Knoten beeinträchtigt die Workloads, die auf dem Knoten ausgeführt werden. Bevor Sie Hybridknoten löschen, empfehlen wir, den Knoten zunächst zu entleeren, um die Pods auf einen anderen aktiven Knoten zu verschieben. Weitere Informationen zum Entleeren von Knoten finden Sie unter [Sicheres Entleeren eines Knotens](#) in der Kubernetes-Dokumentation.

Führen Sie die folgenden kubectl-Schritte von Ihrem lokalen Computer oder Ihrer Instance aus, die Sie für die Interaktion mit dem Kubernetes-API-Endpunkt des Amazon EKS-Clusters verwenden. Wenn Sie eine bestimmte kubeconfig Datei verwenden, verwenden Sie das Flag. --kubeconfig

Schritt 1: Listen Sie Ihre Knoten auf

```
kubectl get nodes
```

Schritt 2: Entleeren Sie Ihren Knoten

Weitere Informationen zum Befehl finden Sie in der Kubernetes-Dokumentation unter [kubectl drain](#).  
`kubectl drain`

```
kubectl drain --ignore-daemonsets <node-name>
```

Schritt 3: Stoppen und deinstallieren Sie Hybrid-Knoten-Artefakte

Sie können die Amazon EKS Hybrid Nodes CLI (nodeadm) verwenden, um die Hybrid-Knoten-Artefakte zu stoppen und vom Host zu entfernen. Sie müssen nodeadm mit einem Benutzer arbeiten, der über root/sudo Rechte verfügt. `nodeadm uninstall` Wird standardmäßig nicht fortgesetzt, wenn noch Pods auf dem Knoten vorhanden sind. Wenn Sie AWS Systems Manager (SSM) als Ihren Anbieter für Anmeldeinformationen verwenden, wird der Host mit dem `nodeadm uninstall` Befehl als verwaltete AWS SSM-Instanz deregistriert. Weitere Informationen finden Sie unter [the section called "Hybridknoten nodeadm"](#).

```
nodeadm uninstall
```

## Schritt 4: Löschen Sie Ihren Knoten aus dem Cluster

Nachdem die Artefakte der Hybridknoten gestoppt und deinstalliert wurden, entfernen Sie die Knotenressource aus Ihrem Cluster.

```
kubectl delete node <node-name>
```

## Schritt 5: Suchen Sie nach verbleibenden Artefakten

Je nachdem, für welches CNI Sie sich entschieden haben, können nach der Ausführung der obigen Schritte noch Artefakte auf Ihren Hybridknoten verbleiben. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#).

## CNI, Add-Ons und Webhooks für Hybridknoten konfigurieren

Nachdem Sie einen Cluster für Hybridknoten konfiguriert haben, müssen Hybridknoten für Container Network Interfaces (CNI), Add-Ons, Webhooks und mögliche Proxyeinstellungen konfiguriert werden. Eine vollständige Liste der EKS- und Community-Add-Ons, die mit Hybridknoten kompatibel sind, finden Sie unter [the section called “Add-Ons konfigurieren”](#).

EKS Cluster Insights EKS bietet Insight-Checks auf Fehlkonfigurationen in Ihrem EKS-Hybridknoten-Setup, die die Funktionalität Ihres Clusters oder Ihrer Workloads beeinträchtigen könnten. Weitere Informationen zu Cluster-Erkenntnissen finden Sie unter [the section called “Cluster-Erkenntnisse”](#).

Im Folgenden sind die Add-Ons und andere Komponenten aufgeführt, die für Hybridknoten unterschiedlich konfiguriert sind:

- Container Networking Interface (CNI): Die Kernfunktionen von [Cilium](#) und [Calico](#) werden für die Verwendung mit Hybridknoten unterstützt. Sie können Ihr CNI auf Hybridknoten mit Tools Ihrer Wahl wie Helm verwalten. Das AWS VPC-CNI kann nicht mit Hybridknoten verwendet werden. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#).
- CoreDNS und **kube-proxy**: CoreDNS und kube-proxy werden automatisch installiert, wenn Hybridknoten dem EKS-Cluster beitreten. Diese Add-Ons können nach der Clustererstellung als EKS-Add-Ons verwaltet werden.
- Ingress und Load Balancing: Sie können den Load AWS Balancer Controller und den Application Load Balancer (ALB) oder den Network Load Balancer (NLB) mit dem Zieltyp `ip` für Workloads auf Hybridknoten verwenden, die mit Direct Connect oder VPN verbunden sind. AWS Site-to-Site Sie können alternativ einen Ingress-Controller oder einen Load Balancer Ihrer Wahl für Anwendungsdatenverkehr verwenden, der lokal in Ihrer lokalen Umgebung bleibt.

- **Metriken:** Sie können Amazon Managed Service für Prometheus (AMP) Scraper ohne Agenten, AWS Distro for Open Telemetry (ADOT) und den Amazon Observability Agent mit Hybridknoten verwenden. CloudWatch Um AMP-Scraper ohne Agenten für Pod-Metriken auf Hybridknoten zu verwenden, müssen Ihre Pods von der VPC aus zugänglich sein, die Sie für den EKS-Cluster verwenden.
- **Protokolle:** Sie können die Protokollierung der EKS-Kontrollebene für Cluster mit aktivierten Hybridknoten aktivieren. Sie können das ADOT EKS-Add-on und das Amazon CloudWatch Observability Agent EKS-Add-On für die Protokollierung von Hybridknoten und Pods verwenden.
- **Pod-Identitäten und IRSA:** Sie können EKS Pod Identities und IAM Roles for Service Accounts (IRSA) mit Anwendungen verwenden, die auf Hybridknoten ausgeführt werden, um einen detaillierten Zugriff für Ihre Pods zu ermöglichen, die auf Hybridknoten mit anderen Diensten ausgeführt werden. AWS
- **Webhooks:** Wenn Sie Webhooks ausführen, finden Sie unter Überlegungen und Schritte [the section called “Webhooks konfigurieren”](#) zum optionalen Ausführen von Webhooks auf Cloud-Knoten, falls Sie Ihre lokalen Pod-Netzwerke nicht routingfähig machen können.
- **Proxy:** Wenn Sie in Ihrer lokalen Umgebung einen Proxyserver für den Datenverkehr verwenden, der Ihr Rechenzentrum oder Ihre Edge-Umgebung verlässt, können Sie Ihre Hybridknoten und Ihren Cluster so konfigurieren, dass sie Ihren Proxyserver verwenden. Weitere Informationen finden Sie unter [the section called “Proxy konfigurieren”](#).

## Themen

- [Ein CNI für Hybridknoten konfigurieren](#)
- [Add-Ons für Hybridknoten konfigurieren](#)
- [Webhooks für Hybridknoten konfigurieren](#)
- [Proxy für Hybridknoten konfigurieren](#)

## Ein CNI für Hybridknoten konfigurieren

Cilium und Calico werden als Container Networking Interfaces (CNIs) für Amazon EKS-Hybridknoten unterstützt. Sie müssen ein CNI installieren, damit Hybridknoten bereit sind, Workloads zu bedienen. Hybridknoten werden mit Status angezeigt, Not Ready bis ein CNI ausgeführt wird. Sie können diese CNIs mit Tools Ihrer Wahl wie Helm verwalten. Das Amazon VPC CNI ist nicht mit Hybridknoten kompatibel und das VPC-CNI ist mit Anti-Affinität für das Label konfiguriert.

`eks.amazonaws.com/compute-type: hybrid`

## Kompatibilität der CNI-Version

Die Cilium-Version v1.16.x wird für EKS-Hybridknoten für jede in Amazon EKS unterstützte Kubernetes-Version unterstützt und empfohlen.

Die Calico-Version v3.29.x wird für EKS-Hybridknoten für jede in Amazon EKS unterstützte Kubernetes-Version unterstützt und empfohlen.

Informationen zu den von Amazon EKS unterstützten [Kubernetes-Versionen finden Sie unter Kubernetes-Versionsunterstützung](#). EKS-Hybridknoten bieten dieselbe Unterstützung für Kubernetes-Versionen wie Amazon EKS-Cluster mit Cloud-Knoten.

## Unterstützte Funktionen

AWS bietet technischen Support für die folgenden Funktionen von Cilium und Calico zur Verwendung mit Hybridknoten. Wenn Sie beabsichtigen, Funktionen außerhalb des AWS Support-Bereichs zu verwenden, empfehlen wir Ihnen, kommerziellen Support für das Plug-in in Anspruch zu nehmen oder über das interne Fachwissen zu verfügen, um Fehler zu beheben und Korrekturen für das CNI-Plug-in-Projekt vorzunehmen.

| Funktion                                                | Cilium                               | Calico                               |
|---------------------------------------------------------|--------------------------------------|--------------------------------------|
| Konformität mit dem Kubernetes-Netzwerk                 | Ja                                   | Ja                                   |
| Konnektivität zwischen der Kontrollebene und dem Knoten | Ja                                   | Ja                                   |
| Konnektivität zwischen Kontrollebene und Pod            | Ja                                   | Ja                                   |
| Verwaltung des Lebenszyklus                             | Installieren, aktualisieren, löschen | Installieren, aktualisieren, löschen |
| Netzwerkmodus                                           | VXLAN                                | VXLAN                                |
| IP-Adressverwaltung (IPAM)                              | Cluster-Bereich (Cilium IPAM)        | Calico IPAM                          |
| IP-Familie                                              | IPv4                                 | IPv4                                 |

| Funktion | Cilium                    | Calico |
|----------|---------------------------|--------|
| BGP      | Ja (Cilium Control Plane) | Ja     |

## Überlegungen zu Cilium

- [Standardmäßig ist Cilium so konfiguriert, dass es im Overlay-/Tunnelmodus mit VXLAN als Kapselungsmethode ausgeführt wird.](#) Dieser Modus hat die geringsten Anforderungen an das zugrunde liegende physische Netzwerk.
- Standardmäßig [maskiert Cilium die Quell-IP-Adresse](#) des gesamten Pod-Datenverkehrs, der den Cluster verlässt, für die IP-Adresse des Knotens. Dadurch ist es möglich, Cilium mit Hybridknoten auszuführen, unabhängig davon, ob Remote-Pod-Netzwerke auf dem Cluster konfiguriert sind oder nicht. Wenn Sie Masquerading deaktivieren, CIDRs muss Ihr Pod in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren Amazon EKS-Cluster mit Ihren Remote-Pod-Netzwerken konfigurieren.
- Wenn Sie Webhooks auf Ihren Hybridknoten ausführen, CIDRs muss Ihr Pod in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren Amazon EKS-Cluster mit Ihren Remote-Pod-Netzwerken konfigurieren. Wenn CIDRs Ihr Pod in Ihrem lokalen Netzwerk nicht routbar ist, empfehlen wir Ihnen, Webhooks auf Cloud-Knoten im selben Cluster auszuführen. Weitere Informationen finden [Sie unter Webhooks für Hybridknoten konfigurieren](#).
- Eine gängige Methode, Ihren Pod-CIDR in Ihrem lokalen Netzwerk routingfähig zu machen, besteht darin, Pod-Adressen mit BGP bekannt zu geben. Um BGP mit Cilium zu verwenden, müssen Sie dies in Ihrer Helm-Konfiguration festlegen. `bgpControlPlane.enabled: true` Weitere Informationen zur BGP-Unterstützung von Cilium finden Sie unter Cilium BGP [Control Plane in der Cilium-Dokumentation](#).
- Die standardmäßige IP-Adressverwaltung (IPAM) in Cilium heißt [Cluster Scope](#). Dabei weist der Cilium-Operator jedem Knoten auf der Grundlage des vom Benutzer konfigurierten Pods IP-Adressen zu. CIDRs Die Pods CIDRs sind mit dem `clusterPoolIPv4PodCIDRList` Helm-Wert konfiguriert, der dem Remote-Pod-Netzwerk entsprechen sollte, das CIDRs Sie für Ihren Amazon EKS-Cluster konfiguriert haben. Cilium weist jedem Knoten Segmente von `clusterPoolIPv4PodCIDRList` zu. Die Größe der Segmente pro Knoten wird mit dem Helm-Wert konfiguriert. `clusterPoolIPv4MaskSize` Weitere Informationen zu `clusterPoolIPv4PodCIDRList` und `clusterPoolIPv4MaskSize` finden Sie unter [Erweiterung des Cluster-Pools](#) in der Cilium-Dokumentation.

## Installieren Sie Cilium auf Hybridknoten

1. Stellen Sie sicher, dass Sie die Helm-CLI in Ihrer Befehlszeilenumgebung installiert haben. Installationsanweisungen finden Sie im [Setup-Helm](#).
2. Installieren Sie das Cilium Helm Repo.

```
helm repo add cilium https://helm.cilium.io/
```

3. Erstellen Sie eine YAML-Datei mit dem Namen `cilium-values.yaml`. Im folgenden Beispiel wird Cilium so konfiguriert, dass es nur auf Hybridknoten ausgeführt wird, indem die Affinität für das Label festgelegt wird. `eks.amazonaws.com/compute-type: hybrid`
  - Wenn Sie Ihren Amazon EKS-Cluster mit Remote-Pod-Netzwerken konfiguriert haben, konfigurieren Sie denselben Pod CIDRs für Ihre `clusterPoolIPv4PodCIDRList`. Beispiel, `10.100.0.0/24`. Ihr lokales Pod-CIDR darf sich nicht mit dem CIDR Ihres lokalen Knotens überschneiden, wenn Sie das CNI im Overlay-/Tunnelmodus ausführen.
  - Konfigurieren Sie `clusterPoolIPv4MaskSize` auf der Grundlage Ihrer erforderlichen Pods pro Knoten. Zum Beispiel 25 für eine Segmentgröße von /25 von 128 Pods pro Knoten.
  - Sie sollten Ihr `clusterPoolIPv4PodCIDRList` oder `clusterPoolIPv4MaskSize` nach der Bereitstellung von Cilium auf Ihrem Cluster nicht ändern. Weitere Informationen finden Sie unter [Erweiterung des Cluster-Pools in der](#) Cilium-Dokumentation.
  - Eine vollständige Liste der Helm-Werte für Cilium finden Sie in der [Helm-Referenz](#) in der Cilium-Dokumentation.

```
affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: In
 values:
 - hybrid
ipam:
 mode: cluster-pool
 operator:
 clusterPoolIPv4MaskSize: 25
 clusterPoolIPv4PodCIDRList:
 - POD_CIDR
loadBalancer:
```

```

serviceTopology: true
operator:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: In
 values:
 - hybrid
 unmanagedPodWatcher:
 restart: false
 envoy:
 enabled: false

```

#### 4. Installieren Sie Cilium auf Ihrem Cluster.

- `CILIUM_VERSION` Ersetzen Sie es durch eine Cilium-Version (zum Beispiel `v1.17.0`). Wir empfehlen, dass Sie die neueste Patch-Version für Ihre Cilium-Nebenversion ausführen. Die neueste Patch-Version für eine bestimmte Cilium-Kleinversion finden Sie im [Abschnitt Stable Releases](#) der Cilium-Dokumentation.
- Wenn Sie BGP für Ihre Bereitstellung aktivieren, fügen Sie das `--set bgpControlPlane.enabled=true` Flag im folgenden Befehl hinzu.
- Wenn Sie eine bestimmte kubeconfig-Datei verwenden, verwenden Sie das `--kubeconfig` Flag mit dem Befehl Helm install.

```

helm install cilium cilium/cilium \
 --version CILIUM_VERSION \
 --namespace kube-system \
 --values cilium-values.yaml

```

5. Mit den folgenden Befehlen können Sie bestätigen, dass Ihre Cilium-Installation erfolgreich war. Sie sollten die `cilium-operator` Bereitstellung und die `cilium-agent` Ausführung auf jedem Ihrer Hybridknoten sehen. Außerdem sollten Ihre Hybridknoten jetzt den Status `Ready` haben. Informationen zur Konfiguration von BGP für Cilium finden Sie im nächsten Schritt.

```
kubectl get pods -n kube-system
```

| NAME         | READY | STATUS  | RESTARTS | AGE |
|--------------|-------|---------|----------|-----|
| cilium-jjjn8 | 1/1   | Running | 0        | 11m |

|                                 |     |         |   |     |
|---------------------------------|-----|---------|---|-----|
| cilium-operator-d4f4d7fcb-sc5xn | 1/1 | Running | 0 | 11m |
|---------------------------------|-----|---------|---|-----|

```
kubectl get nodes
```

| NAME                 | STATUS | ROLES  | AGE | VERSION             |
|----------------------|--------|--------|-----|---------------------|
| mi-04a2cf999b7112233 | Ready  | <none> | 19m | v1.31.0-eks-a737599 |

6. Um BGP mit Cilium zu verwenden, um Ihre Pod-Adressen in Ihrem lokalen Netzwerk zu bewerben, müssen Sie Cilium mit installiert haben. `bgpControlPlane.enabled: true` Wenn Sie BGP für eine bestehende Cilium-Bereitstellung aktivieren, müssen Sie den Cilium-Operator neu starten, um die BGP-Konfiguration anzuwenden, falls BGP zuvor nicht aktiviert war. Sie können `true` in Ihren Helm-Werten `operator.rolloutPods` auf einstellen, um den Cilium-Operator im Rahmen des Helm-Installations-/Upgrade-Vorgangs neu zu starten.

Um BGP in Cilium zu konfigurieren, erstellen Sie zunächst eine Datei mit einem Namen und einer Definition. `cilium-bgp-cluster.yaml` CiliumBGPClusterConfig Möglicherweise müssen Sie die folgenden Informationen von Ihrem Netzwerkadministrator einholen.

- Konfigurieren Sie `localASN` mit der ASN für die Knoten, auf denen Cilium ausgeführt wird.
- Konfigurieren Sie `peerASN` mit der ASN für Ihren lokalen Router.
- Konfigurieren Sie die `peerAddress` mit der lokalen Router-IP, mit der jeder Knoten, auf dem Cilium ausgeführt wird, eine Verbindung herstellen kann.

```
apiVersion: cilium.io/v2alpha1
kind: CiliumBGPClusterConfig
metadata:
 name: cilium-bgp
spec:
 nodeSelector:
 matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: In
 values:
 - hybrid
 bgpInstances:
 - name: "rack0"
 localASN: NODES_ASN
 peers:
 - name: "onprem-router"
 peerASN: ONPREM_ROUTER_ASN
```



```
peerAddress: ONPREM_ROUTER_IP
peerConfigRef:
 name: "cilium-peer"
```

7. Wenden Sie die Cilium BGP-Cluster-Konfiguration auf Ihren Cluster an.

```
kubectl apply -f cilium-bgp-cluster.yaml
```

8. Die `CiliumBGPPeerConfig` Ressource definiert eine BGP-Peer-Konfiguration. Mehrere Peers können dieselbe Konfiguration verwenden und auf die gemeinsame `CiliumBGPPeerConfig` Ressource verweisen. Erstellen Sie eine Datei mit dem Namen `cilium-bgp-peer.yaml`, um die Peer-Konfiguration für Ihr lokales Netzwerk zu konfigurieren. Eine vollständige Liste der [Konfigurationsoptionen finden Sie in der BGP-Peer-Konfiguration](#) in der Cilium-Dokumentation.

```
apiVersion: cilium.io/v2alpha1
kind: CiliumBGPPeerConfig
metadata:
 name: cilium-peer
spec:
 timers:
 holdTimeSeconds: 30
 keepAliveTimeSeconds: 10
 gracefulRestart:
 enabled: true
 restartTimeSeconds: 120
 families:
 - afi: ipv4
 safi: unicast
 advertisements:
 matchLabels:
 advertise: "bgp"
```

9. Wenden Sie die Cilium BGP-Peer-Konfiguration auf Ihren Cluster an.

```
kubectl apply -f cilium-bgp-peer.yaml
```

10 Die `CiliumBGPAdvertisement` Ressource wird verwendet, um verschiedene Werbetypen und damit verbundene Attribute zu definieren. Erstellen Sie eine Datei mit dem Namen `cilium-bgp-advertisement.yaml` und konfigurieren Sie die `CiliumBGPAdvertisement` Ressource mit Ihren Einstellungen.

```
apiVersion: cilium.io/v2alpha1
```

```
kind: CiliumBGPAdvertisement
metadata:
 name: bgp-advertisements
 labels:
 advertise: bgp
spec:
 advertisements:
 - advertisementType: "PodCIDR"
 - advertisementType: "Service"
 service:
 addresses:
 - ClusterIP
 - ExternalIP
 - LoadBalancerIP
```

11. Wenden Sie die Konfiguration von Cilium BGP Advertisement auf Ihren Cluster an.

```
kubectl apply -f cilium-bgp-advertisement.yaml
```

Mit dem Befehl können Sie überprüfen, ob das BGP-Peering mit der [Cilium-CLI](#) funktioniert hat. `cilium bgp peers` Sie sollten in der Ausgabe die richtigen Werte für Ihre Umgebung und den Sitzungsstatus als `established` sehen. Weitere Informationen zur [Fehlerbehebung finden Sie im Leitfaden zur Fehlerbehebung und Bedienung](#) in der Cilium-Dokumentation.

Führen Sie ein Upgrade von Cilium auf Hybridknoten durch

Lesen Sie vor dem Upgrade Ihrer Cilium-Bereitstellung sorgfältig die [Cilium-Upgrade-Dokumentation und die Upgrade-Hinweise](#), um sich über die Änderungen in der Cilium-Zielversion zu informieren.

1. Stellen Sie sicher, dass Sie die `helm` CLI in Ihrer Befehlszeilenumgebung installiert haben. Installationsanweisungen finden Sie in der [Helm-Dokumentation](#).
2. Installieren Sie das Cilium Helm Repo.

```
helm repo add cilium https://helm.cilium.io/
```

3. Führen Sie den Cilium-Upgrade-Pre-Flight-Check durch. Ersetzen Sie `CILIUM_VERSION` durch Ihre Zielversion von Cilium. Wir empfehlen, dass Sie die neueste Patch-Version für Ihre Cilium-Nebenversion ausführen. Die neueste Patch-Version für eine bestimmte Cilium-Kleinversion finden Sie im [Abschnitt Stable Releases](#) der Cilium-Dokumentation.

```
helm install cilium-preflight cilium/cilium --version CILIUM_VERSION \
 --namespace=kube-system \
 --set preflight.enabled=true \
 --set agent=false \
 --set operator.enabled=false
```

4. Stellen Sie nach der Installation von `sichercilium-preflight.yaml`, dass die Anzahl der READY Pods der Anzahl der laufenden Cilium-Pods entspricht.

```
kubectl get ds -n kube-system | sed -n '1p;/cilium/p'
```

| NAME                    | SELECTOR | AGE   | DESIRED | CURRENT | READY | UP-TO-DATE | AVAILABLE | NODE   |
|-------------------------|----------|-------|---------|---------|-------|------------|-----------|--------|
| cilium                  |          | 1h20m | 2       | 2       | 2     | 2          | 2         | <none> |
| cilium-pre-flight-check |          | 7m15s | 2       | 2       | 2     | 2          | 2         | <none> |

5. Sobald die Anzahl der READY-Pods gleich ist, stellen Sie sicher, dass der Einsatz von Cilium vor dem Flug ebenfalls als READY 1/1 gekennzeichnet ist. Wenn READY 0/1 angezeigt wird, lesen Sie im Abschnitt [CNP-Validierung](#) nach und beheben Sie Probleme mit der Bereitstellung, bevor Sie mit dem Upgrade fortfahren.

```
kubectl get deployment -n kube-system cilium-pre-flight-check -w
```

| NAME                    | READY | UP-TO-DATE | AVAILABLE | AGE |
|-------------------------|-------|------------|-----------|-----|
| cilium-pre-flight-check | 1/1   | 1          | 0         | 12s |

6. Löschen Sie den Preflight

```
helm uninstall cilium-preflight --namespace kube-system
```

7. Während des normalen Clusterbetriebs sollten alle Cilium-Komponenten dieselbe Version ausführen. In den folgenden Schritten wird beschrieben, wie Sie alle Komponenten von einer stabilen Version auf eine spätere stabile Version aktualisieren. Wenn Sie von einer Nebenversion auf eine andere Nebenversion aktualisieren, empfehlen wir, dass Sie zuerst auf die neueste Patch-Version für die vorhandene Cilium-Nebenversion aktualisieren. Um Unterbrechungen zu

minimieren, stellen Sie die `upgradeCompatibility` Option auf die ursprüngliche Cilium-Version ein, die Sie in diesem Cluster installiert haben.

Bevor Sie den Befehl `helm upgrade` ausführen, sollten Sie die Werte für Ihre Bereitstellung in `cilium-values.yaml` oder `--set` Befehlszeilenoptionen für Ihre Einstellungen verwenden. Der Upgrade-Vorgang überschreibt das Cilium ConfigMap, daher ist es wichtig, dass Ihre Konfigurationswerte beim Upgrade übergeben werden. Wenn Sie BGP verwenden, empfehlen wir Ihnen, die `--set bgpControlPlane=true` Befehlszeilenoption zu verwenden, anstatt diese Informationen in Ihrer Wertedatei anzugeben.

```
helm upgrade cilium cilium/cilium --version CILIUM_VERSION \
 --namespace kube-system \
 --set upgradeCompatibility=1.X \
 -f cilium-values.yaml
```

8. (Optional) Wenn Sie Ihr Upgrade aufgrund von Problemen rückgängig machen müssen, führen Sie die folgenden Befehle aus.

```
helm history cilium --namespace kube-system
helm rollback cilium [REVISION] --namespace kube-system
```

## Löschen Sie Cilium von Hybridknoten

1. Führen Sie den folgenden Befehl aus, um alle Cilium-Komponenten aus Ihrem Cluster zu deinstallieren. Beachten Sie, dass die Deinstallation des CNI die Integrität von Knoten und Pods beeinträchtigen kann und daher nicht auf Produktionsclustern durchgeführt werden sollte.

```
helm uninstall cilium --namespace kube-system
```

Die von Cilium konfigurierten Schnittstellen und Routen werden standardmäßig nicht entfernt, wenn das CNI aus dem Cluster entfernt wird. Weitere Informationen finden Sie unter dem [GitHub Problem](#).

2. Um die Konfigurationsdateien und Ressourcen auf der Festplatte zu bereinigen, können Sie, wenn Sie die Standardkonfigurationsverzeichnisse verwenden, die Dateien wie im [cni-uninstall.shSkript](#) im Cilium-Repository unter gezeigt entfernen. GitHub
3. Um die benutzerdefinierten Cilium-Ressourcendefinitionen (CRDs) aus Ihrem Cluster zu entfernen, können Sie die folgenden Befehle ausführen.

```
kubectl get crds -oname | grep "cilium" | xargs kubectl delete
```

## Überlegungen zu Calico

- [Wir empfehlen, Calico im Overlay-/Tunnelmodus mit VXLAN als Kapselungsmethode auszuführen.](#) Dieser Modus hat die geringsten Anforderungen an das zugrunde liegende physische Netzwerk. Weitere Informationen zu den verschiedenen Calico-Netzwerkmodi finden Sie in [der Calico-Dokumentation unter Bestimmung der besten Netzwerkooption.](#)
- Wir empfehlen, dass Sie Calico mit `natOutgoing` set to ausführen. `true` Bei `natOutgoing` Einstellung auf `true` wird die Quell-IP-Adresse des gesamten Pod-Datenverkehrs, der den Cluster verlässt, in die IP-Adresse des Knotens übersetzt. Dadurch ist es möglich, Calico mit Amazon EKS-Clustern auszuführen, unabhängig davon, ob Remote-Pod-Netzwerke auf dem Cluster konfiguriert sind oder nicht. Wenn Sie die Option deaktivieren `natOutgoing`, CIDRs muss Ihr Pod in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren Amazon EKS-Cluster mit Ihren Remote-Pod-Netzwerken konfigurieren.
- Wenn Sie Webhooks auf Ihren Hybridknoten ausführen, CIDRs muss Ihr Pod in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren Amazon EKS-Cluster mit Ihren Remote-Pod-Netzwerken konfigurieren. Wenn CIDRs Ihr Pod in Ihrem lokalen Netzwerk nicht routbar ist, empfehlen wir Ihnen, Webhooks auf Cloud-Knoten im selben Cluster auszuführen. Weitere Informationen finden [Sie unter Webhooks für Hybridknoten konfigurieren.](#)
- Eine gängige Methode, Ihren Pod-CIDR in Ihrem lokalen Netzwerk routingfähig zu machen, besteht darin, Pod-Adressen mit BGP bekannt zu geben. Um BGP mit Calico zu verwenden, müssen Sie dies in Ihrer Helm-Konfiguration festlegen. `installation.calicoNetwork.bgp: Enabled` Weitere Informationen zur BGP-Unterstützung von Calico finden [Sie unter BGP-Peering konfigurieren in der Calico-Dokumentation.](#)
- Die Standard-IP-Adressverwaltung (IPAM) in Calico heißt [Calico IPAM. Dabei weist das calico-ipam Plugin jedem Knoten IP-Adressen](#) auf der Grundlage des vom Benutzer konfigurierten Pods zu. CIDRs Die Pods CIDRs sind mit dem `installation.calicoNetwork.ipPools.cidr` Helm-Wert konfiguriert, der dem Remote-Pod-Netzwerk entsprechen sollte, das CIDRs Sie für Ihren Amazon EKS-Cluster konfiguriert haben. Calico weist jedem Knoten Segmente von `ipPools.cidr` zu. Die Größe der Segmente pro Knoten wird mit dem Helm-Wert konfiguriert. `ipPools.blockSize` Weitere Informationen zu IPAM mit Calico finden [Sie unter Erste Schritte mit der IP-Adressverwaltung](#) in der Calico-Dokumentation.

## Installieren Sie Calico auf Hybridknoten

1. Stellen Sie sicher, dass Sie die Helm-CLI in Ihrer Befehlszeilenumgebung installiert haben. Installationsanweisungen finden Sie in der [Helm-Dokumentation](#).
2. Installieren Sie das Cilium Helm Repo.

```
helm repo add projectcalico https://docs.tigera.io/calico/charts
```

3. Erstellen Sie eine YAML-Datei mit dem Namen `calico-values.yaml`. Im folgenden Beispiel werden alle Calico-Komponenten so konfiguriert, dass sie nur auf Hybridknoten ausgeführt werden, indem die Affinität für das Label festgelegt wird. `eks.amazonaws.com/compute-type: hybrid`
  - Ersetzen Sie es `POD_CIDR` durch die CIDR-Bereiche für Ihre Pods. Wenn Sie Ihren Amazon EKS-Cluster mit Remote-Pod-Netzwerken konfiguriert haben, sollte `POD_CIDR` das, was Sie für Calico angeben, mit den Remote-Pod-Netzwerken identisch sein. Beispiel, `10.100.0.0/24`. Ihr lokales Pod-CIDR darf sich nicht mit dem CIDR Ihres lokalen Knotens überschneiden, wenn Sie das CNI im Overlay-/Tunnelmodus ausführen.
  - Ersetzen Sie es `CIDR_SIZE` durch die Größe des CIDR-Segments, das Sie jedem Knoten zuweisen möchten. Zum Beispiel 25 für eine Segmentgröße von /25 von 128 Pod-Adressen pro Knoten. Weitere Informationen zu CIDR `blockSize` und zum Ändern von finden Sie unter [Ändern der blockSize IP-Pool-Blockgröße](#) in der Calico-Dokumentation.
  - Im Beispiel unten `natOutgoing` ist aktiviert und `bgp` deaktiviert. Ändern Sie diese Werte basierend auf Ihrer Zielkonfiguration.

```
installation:
 enabled: true
 cni:
 type: Calico
 ipam:
 type: Calico
 calicoNetwork:
 bgp: Disabled
 ipPools:
 - cidr: POD_CIDR
 blockSize: CIDR_SIZE
 encapsulation: VXLAN
 natOutgoing: Enabled
 nodeSelector: eks.amazonaws.com/compute-type == "hybrid"
 controlPlaneReplicas: 1
```

```

controlPlaneNodeSelector:
 eks.amazonaws.com/compute-type: hybrid
calicoNodeDaemonSet:
 spec:
 template:
 spec:
 nodeSelector:
 eks.amazonaws.com/compute-type: hybrid
csiNodeDriverDaemonSet:
 spec:
 template:
 spec:
 nodeSelector:
 eks.amazonaws.com/compute-type: hybrid
calicoKubeControllersDeployment:
 spec:
 template:
 spec:
 nodeSelector:
 eks.amazonaws.com/compute-type: hybrid
typhaDeployment:
 spec:
 template:
 spec:
 nodeSelector:
 eks.amazonaws.com/compute-type: hybrid

```

#### 4. Installieren Sie Calico auf Ihrem Cluster.

- `CALICO_VERSION` Ersetzen Sie es durch eine Calico-Version (zum Beispiel `v3.29.0`). In den [Calico-Versionen](#) finden Sie die neueste Patch-Version für Ihre Calico-Nebenversion. Wir empfehlen, dass Sie die neueste Patch-Version für die Calico-Minor-Version ausführen.
- Wenn Sie eine bestimmte kubeconfig Datei verwenden, verwenden Sie das `--kubeconfig` Flag.

```

helm install calico projectcalico/tigera-operator \
 --version CALICO_VERSION \
 --namespace kube-system \
 -f calico-values.yaml

```

5. Mit den folgenden Befehlen können Sie überprüfen, ob Ihre Calico-Installation erfolgreich war. Sie sollten die `tigera-operator` Bereitstellung sehen, den `calico-node` Agenten, der auf jedem Ihrer Hybridknoten ausgeführt wird, den `calico-apiserver`, `csi-node-driver`, und

calico-kube-controllers bereitgestellt. Außerdem sollten Ihre Hybridknoten jetzt den Status habenReady. Wenn Sie dies verwendennatOutgoing: Disabled, können alle Calico-Komponenten erst erfolgreich gestartet werden, wenn Sie Ihre Pod-Adressen in Ihrem lokalen Netzwerk bekannt geben. Informationen zur Konfiguration von BGP für Calico finden Sie im nächsten Schritt.

```
kubectl get pods -A
```

| NAMESPACE        | NAME                                     | READY | STATUS  |   |
|------------------|------------------------------------------|-------|---------|---|
| RESTARTS         | AGE                                      |       |         |   |
| calico-apiserver | calico-apiserver-6c77bb6d46-2n8mq        | 1/1   | Running | 0 |
| 69s              |                                          |       |         |   |
| calico-system    | calico-kube-controllers-7c5f8556b5-7h267 | 1/1   | Running | 0 |
| 68s              |                                          |       |         |   |
| calico-system    | calico-node-s5nnk                        | 1/1   | Running | 0 |
| 68s              |                                          |       |         |   |
| calico-system    | calico-typha-6487cc9d8c-wc5jm            | 1/1   | Running | 0 |
| 69s              |                                          |       |         |   |
| calico-system    | csi-node-driver-cv42d                    | 2/2   | Running | 0 |
| 68s              |                                          |       |         |   |
| kube-system      | coredns-7bb495d866-2lc9v                 | 1/1   | Running | 0 |
| 6m27s            |                                          |       |         |   |
| kube-system      | coredns-7bb495d866-2t8ln                 | 1/1   | Running | 0 |
| 157m             |                                          |       |         |   |
| kube-system      | kube-proxy-lxzxh                         | 1/1   | Running | 0 |
| 18m              |                                          |       |         |   |
| kube-system      | tigera-operator-f8bc97d4c-28b4d          | 1/1   | Running | 0 |
| 90s              |                                          |       |         |   |

```
kubectl get nodes
```

| NAME                 | STATUS | ROLES  | AGE   | VERSION             |
|----------------------|--------|--------|-------|---------------------|
| mi-0c6ec2f6f79176565 | Ready  | <none> | 5h13m | v1.31.0-eks-a737599 |

- Wenn du Calico ohne BGP installiert hast, überspringe diesen Schritt. Um BGP zu konfigurieren, erstellen Sie eine Datei namens `calico-bgp.yaml` mit einer `BGPPeer` Konfiguration und einem. `BGPConfiguration` Es ist wichtig, zwischen `BGPPeer` und `BGPConfiguration` zu unterscheiden. Das `BGPPeer` ist der BGP-fähige Router oder die Remote-Ressource, mit der die Knoten in einem Calico-Cluster eine Verbindung herstellen.



Die `asNumber` in der `BGPPeer` Konfiguration ähnelt der `Cilium-Einstellung`. `peerASN`  
 Das `BGPConfiguration` wird auf jeden Calico-Knoten angewendet und das `asNumber`  
 für das `BGPConfiguration` entspricht der `Cilium-Einstellung`. `localASN` Ersetzen Sie  
`ONPREM_ROUTER_IP`, `ONPREM_ROUTER_ASN`, und `LOCAL_ASN` im folgenden Beispiel durch  
 die Werte für Ihre lokale Umgebung, die Sie möglicherweise von Ihrem Netzwerkadministrator  
 anfordern müssen. Diese `keepOriginalNextHop: true` Einstellung wird verwendet, um  
 sicherzustellen, dass jeder Knoten nur das Pod-Netzwerk-CIDR ankündigt, dessen Eigentümer er  
 ist.

```
apiVersion: projectcalico.org/v3
kind: BGPPeer
metadata:
 name: calico-hybrid-nodes
spec:
 peerIP: ONPREM_ROUTER_IP
 asNumber: ONPREM_ROUTER_ASN
 keepOriginalNextHop: true

apiVersion: projectcalico.org/v3
kind: BGPConfiguration
metadata:
 name: default
spec:
 nodeToNodeMeshEnabled: false
 asNumber: LOCAL_ASN
```

7. Wenden Sie die Datei auf Ihren Cluster an.

```
kubectl apply -f calico-bgp.yaml
```

8. Bestätigen Sie mit dem folgenden Befehl, dass die Calico-Pods ausgeführt werden.

```
kubectl get pods -n calico-system -w
```

| NAMESPACE        | NAME                                     | READY | STATUS  | RESTARTS | AGE             |
|------------------|------------------------------------------|-------|---------|----------|-----------------|
| calico-apiserver | calico-apiserver-598bf99b6c-2vltk        | 1/1   | Running | 0        | 3h24m           |
| calico-system    | calico-kube-controllers-75f84bbfd6-zwmnx | 1/1   | Running | 31       | (59m ago) 3h20m |

|                        |                                  |     |         |   |
|------------------------|----------------------------------|-----|---------|---|
| calico-system<br>5h17m | calico-node-9b2pg                | 1/1 | Running | 0 |
| calico-system<br>5h18m | calico-typha-7d55c76584-kxtnq    | 1/1 | Running | 0 |
| calico-system<br>5h18m | csi-node-driver-dmnmm            | 2/2 | Running | 0 |
| kube-system<br>6h23m   | coredns-7bb495d866-dtn4z         | 1/1 | Running | 0 |
| kube-system<br>6h19m   | coredns-7bb495d866-mk7j4         | 1/1 | Running | 0 |
| kube-system<br>6h12m   | kube-proxy-vms28                 | 1/1 | Running | 0 |
| kube-system<br>73m     | tigera-operator-55f9d9d565-jj9bg | 1/1 | Running | 0 |

Wenn Sie bei diesen Schritten auf Probleme gestoßen sind, lesen Sie die [Anleitung zur Fehlerbehebung](#) in der Calico-Dokumentation.

### Aktualisieren Sie Calico auf Hybridknoten

Bevor Sie Ihre Calico-Implementierung aktualisieren, sollten Sie die [Calico-Upgrade-Dokumentation](#) und die [Versionshinweise](#) sorgfältig lesen, um die Änderungen in der Calico-Zielversion zu verstehen. Die Upgrade-Schritte variieren je nachdem, ob Sie Helm, den Calico-Operator und den Typ des Datenspeichers verwenden. Bei den folgenden Schritten wird die Verwendung von Helm vorausgesetzt.

1. Laden Sie das Operator-Manifest für die Version von Calico herunter, auf die Sie aktualisieren. Ersetzen Sie es beispielsweise `v3.29.0` durch die Version, auf die Sie aktualisieren. Stellen Sie sicher, dass Sie das dem `v major.minor.patch` voranstellen.

```
kubectl apply --server-side --force-conflicts \
 -f https://raw.githubusercontent.com/projectcalico/calico/CALICO_VERSION/
 manifests/operator-crd.yaml
```

2. Führen Sie das Programm aus, um Ihr Calico-Deployment zu aktualisieren. `helm upgrade CALICO_VERSION` Ersetzen Sie es beispielsweise `v3.29.0` durch die Version, auf die Sie aktualisieren. Erstellen Sie die `calico-values.yaml` Datei aus den Konfigurationswerten, die Sie zur Installation von Calico verwendet haben.

```
helm upgrade calico projectcalico/tigera-operator \
```

```
--version CALICO_VERSION \
--namespace kube-system \
-f calico-values.yaml
```

## Löschen Sie Calico von Hybridknoten

1. Führen Sie den folgenden Befehl aus, um die Calico-Komponenten von Ihrem Cluster zu deinstallieren. Beachten Sie, dass die Deinstallation des CNI die Integrität von Knoten und Pods beeinträchtigen kann und nicht auf Produktionsclustern durchgeführt werden sollte. Wenn Sie Calico in einem anderen Namespace installiert haben, `kube-system` ändern Sie den Namespace im folgenden Befehl.

```
helm uninstall calico --namespace kube-system
```

Beachten Sie, dass die von Calico konfigurierten Schnittstellen und Routen standardmäßig nicht entfernt werden, wenn Sie das CNI aus dem Cluster entfernen.

2. Um die Konfigurationsdateien und Ressourcen auf der Festplatte zu bereinigen, entfernen Sie die Calico-Dateien aus den Verzeichnissen `/opt/cni` und `/etc/cni`
3. Führen Sie die folgenden Befehle aus, um Calico CRDs aus Ihrem Cluster zu entfernen.

```
kubectl get crds -oname | grep "calico" | xargs kubectl delete
```

```
kubectl get crds -oname | grep "tigera" | xargs kubectl delete
```

## Add-Ons für Hybridknoten konfigurieren

Auf dieser Seite werden Überlegungen zum Ausführen von AWS Add-Ons und Community-Add-Ons auf Amazon EKS-Hybridknoten beschrieben. Weitere Informationen zu Amazon EKS-Add-Ons und den Prozessen zum Erstellen, Aktualisieren und Entfernen von Add-Ons aus Ihrem Cluster finden Sie unter [the section called “Amazon-EKS-Add-ons”](#). Sofern auf dieser Seite nicht anders angegeben, sind die Verfahren zum Erstellen, Aktualisieren und Entfernen von Amazon EKS-Add-Ons für Amazon EKS-Cluster mit Hybridknoten identisch wie für Amazon EKS-Cluster mit Knoten, die in der AWS Cloud laufen. Nur die auf dieser Seite enthaltenen Add-Ons wurden auf ihre Kompatibilität mit Amazon EKS Hybrid Nodes überprüft.

Die folgenden AWS Add-Ons sind mit Amazon EKS Hybrid Nodes kompatibel.

| AWS Add-on                                | Kompatible Zusatzversionen                                                                                                                                  |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| kube-proxy                                | v1.25.14-eksbuild.2 und höher                                                                                                                               |
| CoreDNS                                   | v1.9.3-eksbuild.7 und höher                                                                                                                                 |
| AWS Distribution für (ADOT) OpenTelemetry | v0.102.1-eksbuild.2 und höher                                                                                                                               |
| CloudWatch Agent für Beobachtbarkeit      | v2.2.1-eksbuild.1 und höher                                                                                                                                 |
| EKS Pod Identity Agent                    | <ul style="list-style-type: none"> <li>v1.3.3-eksbuild.1 und höher, außer für Bottlerocket</li> <li>v1.3.7-eksbuild.2 und höher für Bottlerocket</li> </ul> |
| Agent zur Knotenüberwachung               | v1.2.0-eksbuild.1 und höher                                                                                                                                 |
| CSI-Snapshot-Controller                   | v8.1.0-eksbuild.1 und höher                                                                                                                                 |
| AWS Privater CA-Connector für Kubernetes  | v1.6.0-eksbuild.1 und höher                                                                                                                                 |

Die folgenden Community-Add-Ons sind mit Amazon EKS Hybrid Nodes kompatibel. Weitere Informationen zu Community-Add-Ons finden Sie unter [the section called “Community-Erweiterungen”](#).

| Community-Add-on           | Kompatible Zusatzversionen   |
|----------------------------|------------------------------|
| Kubernetes Metrics Server  | v0.7.2-eksbuild.1 und höher  |
| Cert-Manager               | v1.17.2-eksbuild.1 und höher |
| Prometheus-Knotenexporteur | v1.9.1-eksbuild.2 und höher  |
| kube-state-metrics         | v2.15.0-eksbuild.4 und höher |

Zusätzlich zu den Amazon EKS-Add-Ons in den obigen Tabellen sind der [Amazon Managed Service für Prometheus Collector](#) und der [Load AWS Balancer Controller](#) für [Anwendungseingang](#) (HTTP) und Load [Balancing](#) (TCP/UDP) mit Hybridknoten kompatibel.

Es gibt AWS Add-Ons und Community-Add-Ons, die nicht mit Amazon EKS Hybrid Nodes kompatibel sind. Die neuesten Versionen dieser Add-Ons verfügen über eine Anti-Affinitätsregel für das `eks.amazonaws.com/compute-type: hybrid` Standardlabel, das auf Hybridknoten angewendet wird. Dadurch wird verhindert, dass sie auf Hybridknoten ausgeführt werden, wenn sie in Ihren Clustern eingesetzt werden. Wenn Sie Cluster mit sowohl Hybridknoten als auch Knoten haben, die in der AWS Cloud ausgeführt werden, können Sie diese Add-Ons in Ihrem Cluster auf Knoten bereitstellen, die in der AWS Cloud ausgeführt werden. Das Amazon VPC CNI ist nicht mit Hybridknoten kompatibel, und Cilium und Calico werden als Container Networking Interfaces (CNIs) für Amazon EKS-Hybridknoten unterstützt. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#).

## AWS Add-Ons

In den folgenden Abschnitten werden die Unterschiede zwischen der Ausführung kompatibler AWS Add-Ons auf Hybridknoten im Vergleich zu anderen Amazon EKS-Compute-Typen beschrieben.

### kube-proxy und CoreDNS

EKS installiert Kube-Proxy und CoreDNS standardmäßig als selbstverwaltete Add-Ons, wenn Sie einen EKS-Cluster mit der AWS API und AWS SDKs, auch über die CLI, erstellen. AWS Sie können diese Add-Ons nach der Cluster-Erstellung mit Amazon EKS-Add-Ons überschreiben. Einzelheiten zu [the section called “kube-proxy”](#) und [the section called “CoreDNS”](#) finden Sie in der EKS-Dokumentation. Wenn Sie einen Cluster im gemischten Modus mit Hybridknoten und Knoten in der AWS Cloud ausführen, empfehlen wir, dass Sie mindestens ein CoreDNS-Replikat auf Hybridknoten und mindestens ein CoreDNS-Replikat auf Ihren Knoten in der Cloud haben. AWS Die Schritte zur Konfiguration finden Sie unter [the section called “CoreDNS-Replikate konfigurieren”](#).

### CloudWatch Agent für Beobachtbarkeit

[Der CloudWatch Observability-Agent-Operator verwendet Webhooks](#). Wenn Sie den Operator auf Hybridknoten ausführen, muss Ihr lokales Pod-CIDR in Ihrem lokalen Netzwerk routenfähig sein und Sie müssen Ihren EKS-Cluster mit Ihrem Remote-Pod-Netzwerk konfigurieren. Weitere Informationen finden Sie unter [Webhooks für Hybridknoten konfigurieren](#).

Metriken auf Knotenebene sind für Hybridknoten nicht verfügbar, da [CloudWatch Container Insights](#) von der Verfügbarkeit des [Instance Metadata Service](#) (IMDS) für Metriken auf Knotenebene abhängt. Metriken auf Cluster-, Workload-, Pod- und Container-Ebene sind für Hybridknoten verfügbar.

Nachdem Sie das Add-on mithilfe der unter [Installieren des CloudWatch Agenten mit Amazon CloudWatch Observability](#) beschriebenen Schritte installiert haben, muss das Zusatz-Manifest

aktualisiert werden, bevor der Agent erfolgreich auf Hybridknoten ausgeführt werden kann.

Bearbeiten Sie die `amazoncloudwatchagents` Ressource im Cluster, um die `RUN_WITH_IRSA` Umgebungsvariable hinzuzufügen, wie unten gezeigt.

```
kubectl edit amazoncloudwatchagents -n amazon-cloudwatch cloudwatch-agent
```

```
apiVersion: v1
items:
- apiVersion: cloudwatch.aws.amazon.com/v1alpha1
 kind: AmazonCloudWatchAgent
 metadata:
 ...
 name: cloudwatch-agent
 namespace: amazon-cloudwatch
 ...
 spec:
 ...
 env:
 - name: RUN_WITH_IRSA # <-- Add this
 value: "True" # <-- Add this
 - name: K8S_NODE_NAME
 valueFrom:
 fieldRef:
 fieldPath: spec.nodeName
 ...
```

## Amazon Managed Prometheus Managed Collector für Hybridknoten

Ein von Amazon Managed Service for Prometheus (AMP) verwalteter Collector besteht aus einem Scraper, der Metriken aus den Ressourcen in einem Amazon EKS-Cluster erkennt und sammelt. AMP verwaltet den Scraper für Sie, sodass Sie keine Instanzen, Agenten oder Scraper selbst verwalten müssen.

Sie können AMP Managed Collectors ohne zusätzliche Konfiguration verwenden, die spezifisch für Hybridknoten ist. Die metrischen Endpunkte für Ihre Anwendungen auf den Hybridknoten müssen jedoch von der VPC aus erreichbar sein, einschließlich der Routen von der VPC zum Remote-Pod-Netzwerk CIDRs und der offenen Ports in Ihrer lokalen Firewall. Darüber hinaus muss Ihr Cluster über einen [privaten](#) Cluster-Endpunktzugriff verfügen.

Folgen Sie den Schritten [unter Verwenden eines AWS verwalteten Collectors](#) im Amazon Managed Service for Prometheus Benutzerhandbuch.

## AWS Distribution für OpenTelemetry (ADOT)

Sie können das Add-on AWS Distro for OpenTelemetry (ADOT) verwenden, um Metriken, Protokolle und Ablaufverfolgungsdaten von Ihren Anwendungen zu sammeln, die auf Hybridknoten ausgeführt werden. ADOT verwendet [Zugangswebhooks, um die Anfragen für benutzerdefinierte Collector-Ressourcen](#) zu mutieren und zu validieren. Wenn Sie den ADOT-Operator auf Hybridknoten ausführen, muss Ihr lokales Pod-CIDR in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren EKS-Cluster mit Ihrem Remote-Pod-Netzwerk konfigurieren. Weitere Informationen finden Sie unter Webhooks für Hybridknoten [konfigurieren](#).

Folgen Sie den Schritten unter [Erste Schritte mit AWS Distro zur OpenTelemetry Verwendung von EKS-Add-Ons](#) in der Dokumentation von AWS Distro. OpenTelemetry

## AWS Load Balancer Balancer-Controller

Sie können den [Load AWS Balancer Controller](#) und den Application Load Balancer (ALB) oder den Network Load Balancer (NLB) mit dem Zieltyp ip für Workloads auf Hybridknoten verwenden, die mit Direct Connect oder VPN verbunden sind. AWS Site-to-Site Die IP-Ziele, die mit dem ALB oder NLB verwendet werden, müssen von dort aus routbar sein. Der AWS Load Balancer Balancer-Controller verwendet auch [Webhooks](#). Wenn Sie den Load AWS Balancer Controller-Operator auf Hybridknoten ausführen, muss Ihr lokales Pod-CIDR in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren EKS-Cluster mit Ihrem Remote-Pod-Netzwerk konfigurieren. Weitere Informationen finden Sie unter Webhooks für Hybridknoten [konfigurieren](#).

Um den Load AWS Balancer Controller zu installieren, folgen Sie den Schritten unter [the section called “Mit Helm installieren”](#) oder [the section called “Mit Manifesten installieren”](#).

Für den Dateneingang mit ALB müssen Sie die folgenden Anmerkungen angeben. Detaillierte Anweisungen finden Sie unter [the section called “Application Load Balancing”](#).

```
alb.ingress.kubernetes.io/target-type: ip
```

Für den Lastenausgleich mit NLB müssen Sie die folgenden Anmerkungen angeben. Detaillierte Anweisungen finden Sie unter [the section called “Netzwerk-Load-Balancer”](#).

```
service.beta.kubernetes.io/aws-load-balancer-type: "external"
service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: "ip"
```

## EKS Pod Identity Agent

### Note

Um das EKS Pod Identity Agent-Add-On erfolgreich auf Hybridknoten bereitzustellen, auf denen Bottlerocket ausgeführt wird, stellen Sie sicher, dass Ihre Bottlerocket-Version mindestens v1.39.0 ist. Der Pod Identity Agent wird auf früheren Bottlerocket-Versionen in Hybridknotenumgebungen nicht unterstützt.

Der ursprüngliche Amazon EKS Pod Identity Agent DaemonSet ist auf die Verfügbarkeit von EC2 IMDS auf dem Knoten angewiesen, um die erforderlichen AWS Anmeldeinformationen zu erhalten. Da IMDS ab Version 1.3.3-eksbuild.1 auf Hybridknoten nicht verfügbar ist, stellt das Pod Identity Agent-Add-on optional einen bereit, der die erforderlichen Anmeldeinformationen bereitstellt. DaemonSet Hybridknoten, auf denen Bottlerocket ausgeführt wird, benötigen eine andere Methode zum Mounten der Anmeldeinformationen. Ab Version 1.3.7-eksbuild.2 stellt das Pod Identity Agent-Add-on optional eine bereit, die speziell auf Bottlerocket-Hybridknoten abzielt. DaemonSet In den folgenden Abschnitten wird DaemonSets der Prozess zur Aktivierung der optionalen Option beschrieben.

### Ubuntu/RHEL/AL2023

1. Um den Pod Identity-Agenten auf Ubuntu/RHEL/AI 2023 Hybridknoten zu verwenden, legen Sie `enableCredentialsFile: true` im Hybrid-Abschnitt der nodeadm Konfiguration wie unten gezeigt fest:

```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 hybrid:
 enableCredentialsFile: true # <-- Add this
```

Dadurch wird eine Anmeldeinformationsdatei erstellt, die auf dem darunter `/eks-hybrid/.aws/credentials` liegenden Knoten konfiguriert wird und von `eks-pod-identity-agent` Pods verwendet wird. nodeadm Diese Anmeldeinformationsdatei enthält temporäre AWS Anmeldeinformationen, die regelmäßig aktualisiert werden.

2. Nachdem Sie die nodeadm Konfiguration auf jedem Knoten aktualisiert haben, führen Sie den folgenden nodeadm `init` Befehl mit Ihrem aus, `nodeConfig.yaml` um Ihre Hybridknoten



mit Ihrem Amazon EKS-Cluster zu verbinden. Wenn Ihre Knoten dem Cluster schon einmal beigetreten sind, führen Sie den `init` Befehl trotzdem erneut aus.

```
nodeadm init -c file:///nodeConfig.yaml
```

3. Installieren Sie `eks-pod-identity-agent` mit aktivierter Unterstützung für Hybridknoten, entweder über die AWS CLI oder AWS Management Console.
  - a. AWS CLI: Führen Sie auf dem Computer, den Sie zur Verwaltung des Clusters verwenden, den folgenden Befehl aus, um die Installation `eks-pod-identity-agent` mit aktivierter Unterstützung für Hybridknoten zu installieren. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks create-addon \
 --cluster-name my-cluster \
 --addon-name eks-pod-identity-agent \
 --configuration-values '{"daemonsets":{"hybrid":{"create": true}}}'
```

- b. AWS Management Console: Wenn Sie das Pod Identity Agent-Add-on über die AWS Konsole installieren, fügen Sie der optionalen Konfiguration Folgendes hinzu, um DaemonSet das Add-on für Hybridknoten bereitzustellen.

```
{"daemonsets":{"hybrid":{"create": true}}}
```

## Bottlerocket

1. Um den Pod Identity-Agenten auf Bottlerocket-Hybridknoten zu verwenden, fügen Sie das `--enable-credentials-file=true` Flag zu dem Befehl hinzu, der für die Benutzerdaten des Bottlerocket-Bootstrap-Containers verwendet wird, wie unter beschrieben. [the section called "Connect Hybridknoten mit Bottlerocket"](#)
  - a. Wenn Sie den SSM-Anmeldeinformationsanbieter verwenden, sollte Ihr Befehl wie folgt aussehen:

```
eks-hybrid-ssm-setup --activation-id=<activation-id> --activation-
code=<activation-code> --region=<region> --enable-credentials-file=true
```

- b. Wenn Sie den Anmeldeinformationsanbieter von IAM Roles Anywhere verwenden, sollte Ihr Befehl wie folgt aussehen:

```
eks-hybrid-iam-ra-setup --certificate=<certificate> --key=<private-key> --enable-credentials-file=true
```

Dadurch wird das Bootstrap-Skript so konfiguriert, dass es auf dem darunter liegenden Knoten eine Anmeldeinformationsdatei erstellt/`var/eks-hybrid/.aws/credentials`, die von Pods verwendet wird. `eks-pod-identity-agent` Diese Anmeldeinformationsdatei enthält temporäre AWS Anmeldeinformationen, die regelmäßig aktualisiert werden.

2. Installieren Sie `eks-pod-identity-agent` mit aktivierter Unterstützung für Bottlerocket-Hybridknoten, entweder über die AWS CLI oder. AWS Management Console

- a. AWS CLI: Führen Sie auf dem Computer, den Sie zur Verwaltung des Clusters verwenden, den folgenden Befehl aus, um die Installation `eks-pod-identity-agent` mit aktivierter Unterstützung für Bottlerocket-Hybridknoten zu installieren. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks create-addon \
 --cluster-name my-cluster \
 --addon-name eks-pod-identity-agent \
 --configuration-values '{"daemonsets":{"hybrid-bottlerocket":{"create":true}}}'
```

- b. AWS Management Console: Wenn Sie das Pod Identity Agent-Add-On über die AWS Konsole installieren, fügen Sie der optionalen Konfiguration Folgendes hinzu, um die auf Bottlerocket-Hybridknoten DaemonSet abzielenden Pakete bereitzustellen.

```
{"daemonsets":{"hybrid-bottlerocket":{"create": true}}}
```

## CSI-Snapshot-Controller

Ab Version `v8.1.0-eksbuild.2` wendet das [CSI-Snapshot-Controller-Add-on](#) eine Soft-Anti-Affinitätsregel für Hybridknoten an und bevorzugt es, deployment dass der Controller EC2 in derselben AWS Region wie die Amazon EKS-Steuerungsebene ausgeführt wird. Die gemeinsame Platzierung deployment in derselben AWS Region wie die Amazon EKS-Steuerebene verbessert die Latenz.

## Community-Erweiterungen

In den folgenden Abschnitten werden die Unterschiede zwischen der Ausführung kompatibler Community-Add-Ons auf Hybridknoten im Vergleich zu anderen Amazon EKS-Compute-Typen beschrieben.

### Kubernetes Metrics Server

Die Steuerungsebene muss die Pod-IP des Metrics Servers (oder die Knoten-IP, wenn HostNetwork aktiviert ist) erreichen. Sofern Sie Metrics Server nicht im HostNetwork-Modus ausführen, müssen Sie daher bei der Erstellung Ihres Amazon EKS-Clusters ein Remote-Pod-Netzwerk konfigurieren und Ihre Pod-IP-Adressen routingfähig machen. Die Implementierung des Border Gateway Protocol (BGP) mit dem CNI ist eine gängige Methode, um Ihre Pod-IP-Adressen routingfähig zu machen.

### Cert-Manager

`cert-manager` [verwendet Webhooks](#). Wenn Sie `cert-manager` auf Hybridknoten laufen, muss Ihr lokales Pod-CIDR in Ihrem lokalen Netzwerk routingfähig sein und Sie müssen Ihren EKS-Cluster mit Ihrem Remote-Pod-Netzwerk konfigurieren. Weitere Informationen finden Sie unter [Webhooks für Hybridknoten konfigurieren](#).

## Webhooks für Hybridknoten konfigurieren

Auf dieser Seite werden Überlegungen zum Ausführen von Webhooks mit Hybridknoten beschrieben. Webhooks werden in Kubernetes-Anwendungen und Open-Source-Projekten wie dem Load AWS Balancer Controller und dem CloudWatch Observability Agent verwendet, um Mutations- und Validierungsfunktionen zur Laufzeit auszuführen.

### Routbare Pod-Netzwerke

Wenn Sie in der Lage sind, Ihren lokalen Pod-CIDR in Ihrem lokalen Netzwerk routingfähig zu machen, können Sie Webhooks auf Hybridknoten ausführen. Es gibt verschiedene Techniken, mit denen Sie Ihren lokalen Pod-CIDR in Ihrem lokalen Netzwerk routingfähig machen können, darunter Border Gateway Protocol (BGP), statische Routen oder andere benutzerdefinierte Routing-Lösungen. BGP ist die empfohlene Lösung, da sie skalierbarer und einfacher zu verwalten ist als alternative Lösungen, die eine benutzerdefinierte oder manuelle Routenkonfiguration erfordern. AWS unterstützt die BGP-Funktionen von Cilium und Calico für Werbe-Pods CIDRs. Weitere Informationen finden Sie unter [the section called “CNI konfigurieren”](#) und [the section called “Routbarer Remote-Pod CIDRs”](#).

Pod-Netzwerke, die nicht routbar sind

Wenn Sie Ihren lokalen Pod-CIDR in Ihrem lokalen Netzwerk nicht routingfähig machen können und Webhooks ausführen müssen, empfehlen wir, dass Sie alle Webhooks auf Cloud-Knoten im selben EKS-Cluster wie Ihre Hybridknoten ausführen.

## Überlegungen zu Clustern im gemischten Modus

Cluster im gemischten Modus sind als EKS-Cluster definiert, bei denen sowohl Hybridknoten als auch Knoten in der AWS Cloud ausgeführt werden. Beachten Sie bei der Ausführung eines Clusters im gemischten Modus die folgenden Empfehlungen:

- Führen Sie das VPC-CNI auf Knoten in der AWS Cloud und entweder Cilium oder Calico auf Hybridknoten aus. Cilium und Calico werden nicht unterstützt, AWS wenn sie auf Knoten in der Cloud ausgeführt werden. AWS
- Konfigurieren Sie Webhooks so, dass sie auf Knoten in der Cloud ausgeführt werden. AWS Weitere Informationen [the section called “Konfigurieren Sie Webhooks für Add-Ons”](#) zur Konfiguration der Webhooks für AWS und Community-Add-Ons finden Sie unter.
- Wenn für Ihre Anwendungen Pods erforderlich sind, die auf Knoten in der AWS Cloud ausgeführt werden, um direkt mit Pods zu kommunizieren, die auf Hybridknoten ausgeführt werden („Ost-West-Kommunikation“), und Sie das VPC-CNI auf Knoten in der AWS Cloud und Cilium oder Calico auf Hybridknoten verwenden, muss Ihr lokales Pod-CIDR in Ihrem lokalen Netzwerk routbar sein.
- Führen Sie mindestens ein CoreDNS-Replikat auf Knoten in der AWS Cloud und mindestens ein CoreDNS-Replikat auf Hybridknoten aus.
- Konfigurieren Sie die Dienstdatenverkehrsverteilung so, dass der Dienstverkehr lokal in der Zone bleibt, aus der er stammt. Weitere Informationen zur Verteilung des Dienstverkehrs finden Sie unter [the section called “Konfigurieren Sie die Verteilung des Servicedatenverkehrs”](#).
- Wenn Sie AWS Application Load Balancers (ALB) oder Network Load Balancers (NLB) für Workload-Verkehr auf Hybridknoten verwenden, müssen die IP-Ziele, die mit dem ALB oder NLB verwendet werden, routbar sein. AWS
- Das Metrics Server-Add-on erfordert Konnektivität von der EKS-Steuerebene zur Pod-IP-Adresse des Metrics Servers. Wenn Sie das Metrics Server-Add-on auf Hybridknoten ausführen, muss Ihr lokales Pod-CIDR in Ihrem lokalen Netzwerk routingfähig sein.
- Um Metriken für Hybridknoten mithilfe von Amazon Managed Service for Prometheus (AMP) Managed Collectors zu sammeln, muss Ihr lokaler Pod-CIDR in Ihrem lokalen Netzwerk routingfähig sein. Oder Sie können den AMP Managed Collector für die Metriken und Ressourcen

der EKS-Kontrollebene, die in der AWS Cloud ausgeführt werden, und das AWS Add-on Distro for OpenTelemetry (ADOT) verwenden, um Metriken für Hybridknoten zu sammeln.

## Cluster im gemischten Modus konfigurieren

Um die mutierenden und validierenden Webhooks zu sehen, die auf Ihrem Cluster ausgeführt werden, können Sie den Ressourcentyp Erweiterungen im Bereich Ressourcen der EKS-Konsole für Ihren Cluster anzeigen oder Sie können die folgenden Befehle verwenden. EKS meldet auch Webhook-Metriken im Cluster-Observability-Dashboard, weitere Informationen finden Sie unter [the section called “Beobachtungs-Dashboard”](#)

```
kubectl get mutatingwebhookconfigurations
```

```
kubectl get validatingwebhookconfigurations
```

## Konfigurieren Sie die Verteilung des Servicedatenverkehrs

Wenn Sie Cluster im gemischten Modus ausführen, empfehlen wir, [Service Traffic Distribution](#) zu verwenden, um den Dienstverkehr lokal in der Zone zu halten, aus der er stammt. Service Traffic Distribution (verfügbar für Kubernetes-Versionen 1.31 und höher in EKS) ist die empfohlene Lösung gegenüber [Topology Aware Routing](#), da sie vorhersehbarer ist. Mit Service Traffic Distribution erhalten fehlerfreie Endpunkte in der Zone den gesamten Datenverkehr für diese Zone. Bei topologiebewusstem Routing muss jeder Dienst mehrere Bedingungen in dieser Zone erfüllen, um das benutzerdefinierte Routing anwenden zu können. Andernfalls wird der Verkehr gleichmäßig an alle Endpunkte weitergeleitet.

Wenn Sie Cilium als Ihr CNI verwenden, müssen Sie das CNI mit der `enable-service-topology` Einstellung auf ausführen, um Service Traffic Distribution `true` zu aktivieren. Sie können diese Konfiguration mit dem Helm-Installationsflag übergeben `--set loadBalancer.serviceTopology=true` oder eine bestehende Installation mit dem Cilium-CLI-Befehl `cilium config set enable-service-topology true` aktualisieren. Der Cilium-Agent, der auf jedem Knoten ausgeführt wird, muss nach der Aktualisierung der Konfiguration für eine bestehende Installation neu gestartet werden.

Ein Beispiel für die Konfiguration von Service Traffic Distribution für den CoreDNS-Dienst finden Sie im folgenden Abschnitt. Wir empfehlen, dass Sie dasselbe für alle Services in Ihrem Cluster aktivieren, um unbeabsichtigten Umgebungsverkehr zu vermeiden.

## CoreDNS-Replikate konfigurieren

Wenn Sie Cluster im gemischten Modus ausführen, empfehlen wir, dass Sie mindestens ein CoreDNS-Replikat auf Hybridknoten und mindestens ein CoreDNS-Replikat auf Knoten in der Cloud haben. AWS

1. Fügen Sie beispielsweise für jeden Ihrer Hybridknoten ein Topologiezonen-Label hinzu.  
topology.kubernetes.io/zone: onprem Sie können das Label auch in der nodeadm init Phase festlegen, indem Sie das Label in Ihrer nodeadm Konfiguration angeben, siehe [the section called “Node Config zum Anpassen von Kubelet \(optional\)”](#). Beachten Sie, dass auf Knoten, die in der AWS Cloud laufen, automatisch ein Topologiezonenlabel zugewiesen wird, das der Availability Zone (AZ) des Knotens entspricht.

```
kubectl label node hybrid-node-name topology.kubernetes.io/zone=zone
```

2. Fügen podAntiAffinity Sie der CoreDNS-Bereitstellung mit dem Topologiezonenschlüssel hinzu. Oder Sie können die CoreDNS-Bereitstellung während der Installation mit EKS-Add-Ons konfigurieren.

```
kubectl edit deployment coredns -n kube-system
```

```
spec:
 template:
 spec:
 affinity:
 ...
 podAntiAffinity:
 preferredDuringSchedulingIgnoredDuringExecution:
 - podAffinityTerm:
 labelSelector:
 matchExpressions:
 - key: k8s-app
 operator: In
 values:
 - kube-dns
 topologyKey: kubernetes.io/hostname
 weight: 100
 - podAffinityTerm:
 labelSelector:
 matchExpressions:
```

```

 - key: k8s-app
 operator: In
 values:
 - kube-dns
 topologyKey: topology.kubernetes.io/zone
 weight: 50
 ...

```

3. Fügen Sie die Einstellung `trafficDistribution: PreferClose` zur kube-dns Dienstkonfiguration hinzu, um die Verteilung des Dienstverkehrs zu aktivieren.

```

kubectl patch svc kube-dns -n kube-system --type=merge -p '{
 "spec": {
 "trafficDistribution": "PreferClose"
 }
}'

```

4. Sie können überprüfen, ob Service Traffic Distribution aktiviert ist, indem Sie sich die Endpunkt-Slices für den kube-dns Service ansehen. Ihre Endpunkt-Slices müssen die Zonenbeschriftungen `hints` für Ihre Topologie aufweisen, wodurch bestätigt wird, dass Service Traffic Distribution aktiviert ist. Wenn Sie die nicht `hints` für jede Endpunktadresse sehen, ist Service Traffic Distribution nicht aktiviert.

```

kubectl get endpointslice -A | grep "kube-dns"

```

```

kubectl get endpointslice [replaceable]`kube-dns-` -n kube-system -o yaml

```

```

addressType: IPv4
apiVersion: discovery.k8s.io/v1
endpoints:
- addresses:
 - <your-hybrid-node-pod-ip>
 hints:
 forZones:
 - name: onprem
 nodeName: <your-hybrid-node-name>
 zone: onprem
- addresses:
 - <your-cloud-node-pod-ip>
 hints:
 forZones:

```

```
- name: us-west-2a
nodeName: <your-cloud-node-name>
zone: us-west-2a
```

## Konfigurieren Sie Webhooks für Add-Ons

Die folgenden Add-Ons verwenden Webhooks und werden für die Verwendung mit Hybridknoten unterstützt.

- AWS Load Balancer Balancer-Controller
- CloudWatch Agent für Beobachtbarkeit
- AWS Distribution für OpenTelemetry (ADOT)
- `cert-manager`

In den folgenden Abschnitten finden Sie Informationen zur Konfiguration der Webhooks, die von diesen Add-Ons für die Ausführung auf Knoten in der Cloud verwendet werden. AWS

### AWS Load Balancer Balancer-Controller

Um den Load AWS Balancer Controller in einem Cluster-Setup im gemischten Modus zu verwenden, müssen Sie den Controller auf Knoten in der AWS Cloud ausführen. Fügen Sie dazu Ihrer Helm-Wertekonfiguration Folgendes hinzu oder geben Sie die Werte mithilfe der EKS-Add-On-Konfiguration an.

```
affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
```

### CloudWatch Observability-Agent

Das CloudWatch Observability Agent-Add-on verfügt über einen Kubernetes-Operator, der Webhooks verwendet. Um den Operator auf Knoten in der AWS Cloud in einem Cluster-Setup im gemischten Modus auszuführen, bearbeiten Sie die CloudWatch Observability Agent-Operatorkonfiguration. Sie



können die Operatoraffinität während der Installation mit Helm- und EKS-Add-Ons nicht konfigurieren (siehe [containers-roadmap](#) issue #2431).

```
kubectl edit -n amazon-cloudwatch deployment amazon-cloudwatch-observability-
controller-manager
```

```
spec:
 ...
 template:
 ...
 spec:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
```

## AWS Distribution für (ADOT) OpenTelemetry

Das Add-on AWS Distro for OpenTelemetry (ADOT) verfügt über einen Kubernetes-Operator, der Webhooks verwendet. Um den Operator auf Knoten in der AWS Cloud in einem Cluster-Setup im gemischten Modus auszuführen, fügen Sie Ihrer Helm-Wertekonfiguration Folgendes hinzu oder geben Sie die Werte mithilfe der EKS-Add-On-Konfiguration an.

```
affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
```

Wenn Ihr Pod-CIDR in Ihrem lokalen Netzwerk nicht routbar ist, muss der ADOT-Collector auf Hybridknoten ausgeführt werden, um die Metriken von Ihren Hybridknoten und den darauf laufenden Workloads zu extrahieren. Bearbeiten Sie dazu die benutzerdefinierte Ressourcendefinition (CRD).

```
kubectl -n opentelemetry-operator-system edit opentelemetrycollectors.opentelemetry.io
adot-col-prom-metrics
```

```
spec:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: In
 values:
 - hybrid
```

Sie können den ADOT-Collector so konfigurieren, dass er nur Metriken von Hybridknoten und Ressourcen, die auf Hybridknoten ausgeführt werden, scannt, indem Sie `scrape_configs` in der ADOT Collector-CRD-Konfiguration jeweils Folgendes `relabel_configs` hinzufügen.

```
relabel_configs:
 - action: keep
 regex: hybrid
 source_labels:
 - __meta_kubernetes_node_label_eks_aws_com_compute_type
```

`cert-manager` Für die Installation des ADOT-Add-Ons müssen die TLS-Zertifikate, die vom ADOT-Operator Webhook verwendet werden, installiert werden. `cert-manager` führt auch Webhooks aus und Sie können es so konfigurieren, dass es auf Knoten in der AWS Cloud mit der folgenden Konfiguration für Helm-Werte ausgeführt wird.

```
affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
webhook:
 affinity:
 nodeAffinity:
```

```

 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
cainjector:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
startupapicheck:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid

```

## cert-manager

Das cert-manager Add-on führt Webhooks aus und Sie können es so konfigurieren, dass es auf Knoten in der AWS Cloud mit der folgenden Helm-Wertekonfiguration ausgeführt wird.

```

affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
webhook:

```

```
affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
cainjector:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
startupapicheck:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - hybrid
```

## Proxy für Hybridknoten konfigurieren

Wenn Sie in Ihrer lokalen Umgebung einen Proxyserver für den Datenverkehr verwenden, der Ihr Rechenzentrum oder Ihre Edge-Umgebung verlässt, müssen Sie Ihre Knoten und Ihren Cluster für die Verwendung Ihres Proxyservers separat konfigurieren.

### Cluster

In Ihrem Cluster müssen Sie die Verwendung Ihres Proxyservers konfigurieren `kube-proxy`. Sie müssen `kube-proxy` nach der Erstellung Ihres Amazon EKS-Clusters die Konfiguration vornehmen.

## Knoten

Auf Ihren Knoten müssen Sie das Betriebssystem, `containerd` und den Amazon SSM-Agenten für die Verwendung Ihres Proxyserver konfigurieren. Sie können diese Änderungen während des Erstellungsprozesses für Ihre Betriebssystem-Images oder vor der Ausführung `nodeadm init` auf jedem Hybridknoten vornehmen.

### Konfiguration auf Knotenebene

Sie müssen die folgenden Konfigurationen entweder in Ihren Betriebssystem-Images oder vor der Ausführung `nodeadm init` auf jedem Hybridknoten anwenden.

#### **containerd**Proxy-Konfiguration

`containerd` ist die Standard-Container-Verwaltungslaufzeit für Kubernetes. Wenn Sie einen Proxy für den Internetzugang verwenden, müssen Sie ihn `containerd` so konfigurieren, dass er die von Kubernetes und Amazon EKS benötigten Container-Images abrufen kann.

Erstellen Sie auf jedem im `/etc/systemd/system/containerd.service.d` Verzeichnis `http-proxy.conf` aufgerufenen Hybridknoten eine Datei mit dem folgenden Inhalt. Ersetzen Sie `proxy-domain` und `port` durch die Werte für Ihre Umgebung.

```
[Service]
Environment="HTTP_PROXY=http://proxy-domain:port"
Environment="HTTPS_PROXY=http://proxy-domain:port"
Environment="NO_PROXY=localhost"
```

#### **containerd**Konfiguration anhand von Benutzerdaten

Das `containerd.service.d` Verzeichnis muss für diese Datei erstellt werden. Sie müssen Systemd neu laden, um die Konfigurationsdatei ohne Neustart abzurufen. In AL2 023 wird der Dienst wahrscheinlich bereits laufen, wenn Ihr Skript ausgeführt wird, sodass Sie ihn ebenfalls neu starten müssen.

```
mkdir -p /etc/systemd/system/containerd.service.d
echo '[Service]' > /etc/systemd/system/containerd.service.d/http-proxy.conf
echo 'Environment="HTTP_PROXY=http://proxy-domain:port"' >> /etc/systemd/system/
containerd.service.d/http-proxy.conf
echo 'Environment="HTTPS_PROXY=http://proxy-domain:port"' >> /etc/systemd/system/
containerd.service.d/http-proxy.conf
```

```
echo 'Environment="NO_PROXY=localhost"' >> /etc/systemd/system/containerd.service.d/
http-proxy.conf
systemctl daemon-reload
systemctl restart containerd
```

## kubeletProxy-Konfiguration

kubelet ist der Kubernetes-Knotenagent, der auf jedem Kubernetes-Knoten ausgeführt wird und für die Verwaltung des Nodes und der darauf laufenden Pods verantwortlich ist. Wenn Sie einen Proxy in Ihrer lokalen Umgebung verwenden, müssen Sie ihn kubelet so konfigurieren, dass er mit den öffentlichen oder privaten Endpunkten Ihres Amazon EKS-Clusters kommunizieren kann.

Erstellen Sie auf jedem im `/etc/systemd/system/kubelet.service.d/` Verzeichnis `http-proxy.conf` aufgerufenen Hybridknoten eine Datei mit dem folgenden Inhalt. Ersetzen Sie `proxy-domain` und `port` durch die Werte für Ihre Umgebung.

```
[Service]
Environment="HTTP_PROXY=http://proxy-domain:port"
Environment="HTTPS_PROXY=http://proxy-domain:port"
Environment="NO_PROXY=localhost"
```

## kubeletKonfiguration anhand von Benutzerdaten

Das `kubelet.service.d` Verzeichnis muss für diese Datei erstellt werden. Sie müssen Systemd neu laden, um die Konfigurationsdatei ohne Neustart abzurufen. In AL2 023 wird der Dienst wahrscheinlich bereits laufen, wenn Ihr Skript ausgeführt wird, sodass Sie ihn ebenfalls neu starten müssen.

```
mkdir -p /etc/systemd/system/kubelet.service.d
echo '[Service]' > /etc/systemd/system/kubelet.service.d/http-proxy.conf
echo 'Environment="HTTP_PROXY=http://proxy-domain:port"' >> /etc/systemd/system/
kubelet.service.d/http-proxy.conf
echo 'Environment="HTTPS_PROXY=http://proxy-domain:port"' >> /etc/systemd/system/
kubelet.service.d/http-proxy.conf
echo 'Environment="NO_PROXY=localhost"' >> /etc/systemd/system/kubelet.service.d/http-
proxy.conf
systemctl daemon-reload
systemctl restart kubelet
```

## ssmProxy-Konfiguration

ssm ist einer der Anbieter von Anmeldeinformationen, mit denen ein Hybridknoten initialisiert werden kann. ssm ist verantwortlich für die Authentifizierung AWS und Generierung temporärer Anmeldeinformationen, die verwendet werden. kubelet Wenn Sie einen Proxy in Ihrer lokalen Umgebung verwenden und ihn ssm als Ihren Anmeldeinformationsanbieter auf dem Knoten verwenden, müssen Sie ihn ssm so konfigurieren, dass er mit Amazon SSM-Serviceendpunkten kommunizieren kann.

Erstellen Sie je nach Betriebssystem auf jedem Hybridknoten, der `http-proxy.conf` im folgenden Pfad aufgerufen wird, eine Datei

- Ubuntu - `/etc/systemd/system/snap.amazon-ssm-agent.amazon-ssm-agent.service.d/http-proxy.conf`
- Amazon Linux 2023 und Red Hat Enterprise Linux - `/etc/systemd/system/amazon-ssm-agent.service.d/http-proxy.conf`

Füllen Sie die Datei mit dem folgenden Inhalt. Ersetzen Sie `proxy-domain` und `port` durch die Werte für Ihre Umgebung.

```
[Service]
Environment="HTTP_PROXY=http://proxy-domain:port"
Environment="HTTPS_PROXY=http://proxy-domain:port"
Environment="NO_PROXY=localhost"
```

## ssmKonfiguration anhand von Benutzerdaten

Das ssm Systemd-Dienstdateiverzeichnis muss für diese Datei erstellt werden. Der Verzeichnispfad hängt vom Betriebssystem ab, das auf dem Knoten verwendet wird.

- Ubuntu - `/etc/systemd/system/snap.amazon-ssm-agent.amazon-ssm-agent.service.d`
- Amazon Linux 2023 und Red Hat Enterprise Linux - `/etc/systemd/system/amazon-ssm-agent.service.d`

Ersetzen Sie den Dienstenamen `systemd` im nachfolgenden Restart-Befehl, je nachdem, welches Betriebssystem auf dem Knoten verwendet wird

- Ubuntu - `snap .amazon-ssm-agent .amazon-ssm-agent`
- Amazon Linux 2023 und Red Hat Enterprise Linux - `amazon-ssm-agent`

```
mkdir -p systemd-service-file-directory
echo '[Service]' > [.replaceable]#systemd-service-file-directory/http-proxy.conf
echo 'Environment="HTTP_PROXY=http://[.replaceable]#proxy-domain:port"' >> systemd-
service-file-directory/http-proxy.conf
echo 'Environment="HTTPS_PROXY=http://[.replaceable]#proxy-domain:port"' >>
[.replaceable]#systemd-service-file-directory/http-proxy.conf
echo 'Environment="NO_PROXY=localhost"' >> [.replaceable]#systemd-service-file-
directory/http-proxy.conf
systemctl daemon-reload
systemctl restart [.replaceable]#systemd-service-name
```

## Proxy-Konfiguration des Betriebssystems

Wenn Sie einen Proxy für den Internetzugang verwenden, müssen Sie Ihr Betriebssystem so konfigurieren, dass es die Abhängigkeiten der Hybridknoten aus dem Paketmanager Ihres Betriebssystems abrufen kann.

### Ubuntu

1. Konfigurieren Sie `snap` die Konfiguration für die Verwendung Ihres Proxys mit den folgenden Befehlen:

```
sudo snap set system proxy.https=http://proxy-domain:port
sudo snap set system proxy.http=http://proxy-domain:port
```

2. Um den Proxy für zu aktivieren `apt`, erstellen Sie eine Datei namens `apt.conf` in dem `/etc/apt/` Verzeichnis. Ersetzen Sie `proxy-domain` und `port` durch die Werte für Ihre Umgebung.

```
Acquire::http::Proxy "http://proxy-domain:port";
Acquire::https::Proxy "http://proxy-domain:port";
```

### Amazon Linux 2023

1. Konfigurieren Sie für `dnf` die Verwendung Ihres Proxys. Erstellen Sie eine Datei `/etc/dnf/dnf.conf` mit den Proxy-Domain- und Port-Werten für Ihre Umgebung.



```
proxy=http://proxy-domain:port
```

## Red Hat Enterprise Linux

1. Konfigurieren Sie für yum die Verwendung Ihres Proxys. Erstellen Sie eine Datei `/etc/yum.conf` mit den Proxy-Domain- und Port-Werten für Ihre Umgebung.

```
proxy=http://proxy-domain:port
```

## Proxykonfiguration von IAM Roles Anywhere

Der IAM Roles Anywhere-Anmeldeinformationsanbieterdienst ist für die Aktualisierung der Anmeldeinformationen verantwortlich, wenn IAM Roles Anywhere mit dem `enableCredentialsFile` Flag verwendet wird (siehe). [the section called “EKS Pod Identity Agent”](#) Wenn Sie in Ihrer lokalen Umgebung einen Proxy verwenden, müssen Sie den Dienst so konfigurieren, dass er mit IAM Roles Anywhere-Endpunkten kommunizieren kann.

Erstellen Sie eine Datei namens `http-proxy.conf` in dem `/etc/systemd/system/aws_signing_helper_update.service.d/` Verzeichnis mit dem folgenden Inhalt. Ersetzen Sie `proxy-domain` und `port` durch die Werte für Ihre Umgebung.

```
[Service]
Environment="HTTP_PROXY=http://proxy-domain:port"
Environment="HTTPS_PROXY=http://proxy-domain:port"
Environment="NO_PROXY=localhost"
```

## Cluster-weite Konfiguration

Die Konfigurationen in diesem Abschnitt müssen nach der Erstellung Ihres Amazon EKS-Clusters und vor der Ausführung `nodeadm init` auf jedem Hybridknoten angewendet werden.

### Kube-Proxy-Proxy-Konfiguration

Amazon EKS wird automatisch `kube-proxy` auf jedem Hybridknoten installiert `DaemonSet`, wenn Ihre Hybridknoten dem Cluster beitreten. `kube-proxy` ermöglicht das Routing zwischen Services,

die von Pods auf Amazon EKS-Clustern unterstützt werden. Um jeden Host zu konfigurieren, kube-proxy ist eine DNS-Auflösung für Ihren Amazon EKS-Cluster-Endpunkt erforderlich.

1. Bearbeiten Sie das kube-proxy DaemonSet mit dem folgenden Befehl

```
kubectl -n kube-system edit ds kube-proxy
```

Dadurch wird die kube-proxy DaemonSet Definition in Ihrem konfigurierten Editor geöffnet.

2. Fügen Sie die Umgebungsvariablen für HTTP\_PROXY und hinzuHTTPS\_PROXY. Beachten Sie, dass die NODE\_NAME Umgebungsvariable bereits in Ihrer Konfiguration vorhanden sein sollte. Ersetzen Sie proxy-domain und port durch Werte für Ihre Umgebung.

```
containers:
 - command:
 - kube-proxy
 - --v=2
 - --config=/var/lib/kube-proxy-config/config - --hostname-override=$(NODE_NAME)
 env:
 - name: HTTP_PROXY
 value: http://proxy-domain:port
 - name: HTTPS_PROXY
 value: http://proxy-domain:port
 - name: NODE_NAME
 valueFrom:
 fieldRef:
 apiVersion: v1
 fieldPath: spec.nodeName
```

## Konzepte für Hybridknoten

Mit Amazon EKS Hybrid Nodes verbinden Sie physische oder virtuelle Maschinen, die in lokalen oder Edge-Umgebungen ausgeführt werden, mit Amazon EKS-Clustern, die in der AWS Cloud ausgeführt werden. Dieser Ansatz bietet viele Vorteile, führt aber auch neue Netzwerkkonzepte und Architekturen für diejenigen ein, die mit der Ausführung von Kubernetes-Clustern in einer einzigen Netzwerkumgebung vertraut sind.

In den folgenden Abschnitten werden die Kubernetes- und Netzwerkkonzepte für EKS-Hybridknoten eingehend behandelt und detailliert beschrieben, wie der Datenverkehr durch die Hybridarchitektur fließt. Diese Abschnitte setzen voraus, dass Sie mit grundlegenden Kubernetes-Netzwerkkennntnissen

vertraut sind, z. B. mit den Konzepten von Pods, Knoten, Diensten, Kubernetes-Steuerebene, Kubelet und Kube-Proxy.

Wir empfehlen, diese Seiten der Reihe nach zu lesen, beginnend mit dem, dann dem und schließlich dem [the section called “Netzwerkkonzepte”](#). [the section called “Kubernetes-Konzepte”](#) [the section called “Verkehrsflüsse”](#)

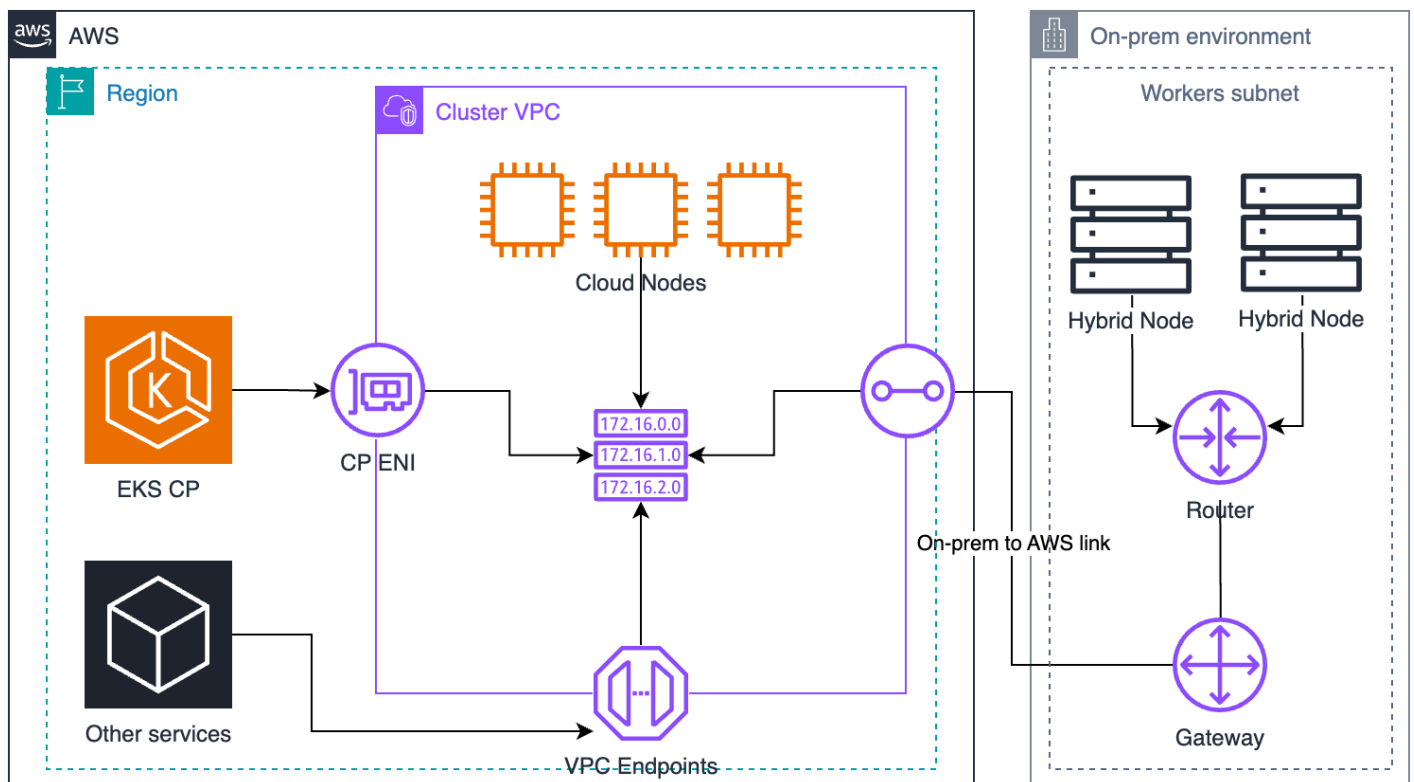
## Themen

- [Netzwerkkonzepte für Hybridknoten](#)
- [Kubernetes-Konzepte für Hybridknoten](#)
- [Netzwerkverkehrsflüsse für Hybridknoten](#)

## Netzwerkkonzepte für Hybridknoten

In diesem Abschnitt werden die wichtigsten Netzwerkkonzepte und die Einschränkungen beschrieben, die Sie beim Entwurf Ihrer Netzwerktopologie für EKS-Hybridknoten berücksichtigen müssen.

### Netzwerkkonzepte für EKS-Hybridknoten



## VPC als Netzwerk-Hub

Der gesamte Datenverkehr, der die Cloud-Grenze überschreitet, fließt durch Ihre VPC. Dazu gehört der Verkehr zwischen der EKS-Steuerebene oder den Pods, die in diesen ausgeführt werden AWS , und Hybridknoten oder Pods, die auf ihnen ausgeführt werden. Sie können sich die VPC Ihres Clusters als Netzwerkhub zwischen Ihren Hybridknoten und dem Rest des Clusters vorstellen. Diese Architektur gibt Ihnen die volle Kontrolle über den Datenverkehr und sein Routing, aber Sie sind auch dafür verantwortlich, Routen, Sicherheitsgruppen und Firewalls für die VPC korrekt zu konfigurieren.

## EKS-Steuerebene zur VPC

Die EKS-Steuerebene verbindet Elastic Network Interfaces (ENIs) mit Ihrer VPC. Diese ENIs verarbeiten den Verkehr zum und vom EKS-API-Server. Sie steuern die Platzierung der EKS-Steuerungsebene ENIs bei der Konfiguration Ihres Clusters, da EKS eine Verbindung ENIs zu den Subnetzen herstellt, die Sie bei der Clustererstellung übergeben.

EKS ordnet Sicherheitsgruppen den Gruppen zu ENIs , die EKS Ihren Subnetzen anhängt. Diese Sicherheitsgruppen ermöglichen den Verkehr zur und von der EKS-Steuerebene über die. ENIs Dies ist wichtig für EKS-Hybridknoten, da Sie den Datenverkehr von den Hybridknoten und den darauf laufenden Pods zur EKS-Steuerebene zulassen müssen ENIs.

## Netzwerke mit Remote-Knoten

Die Remote-Knoten-Netzwerke, insbesondere der Remote-Knoten CIDRs, sind die Bereiche, die den Maschinen IPs zugewiesen sind, die Sie als Hybridknoten verwenden. Wenn Sie Hybridknoten bereitstellen, befinden sie sich in Ihrem lokalen Rechenzentrum oder Edge-Standort, bei dem es sich um eine andere Netzwerkdomäne als die EKS-Steuerebene und die VPC handelt. Jeder Hybridknoten hat eine IP-Adresse oder Adressen von einem Remote-Knoten-CIDR, der sich von den Subnetzen in Ihrer VPC unterscheidet.

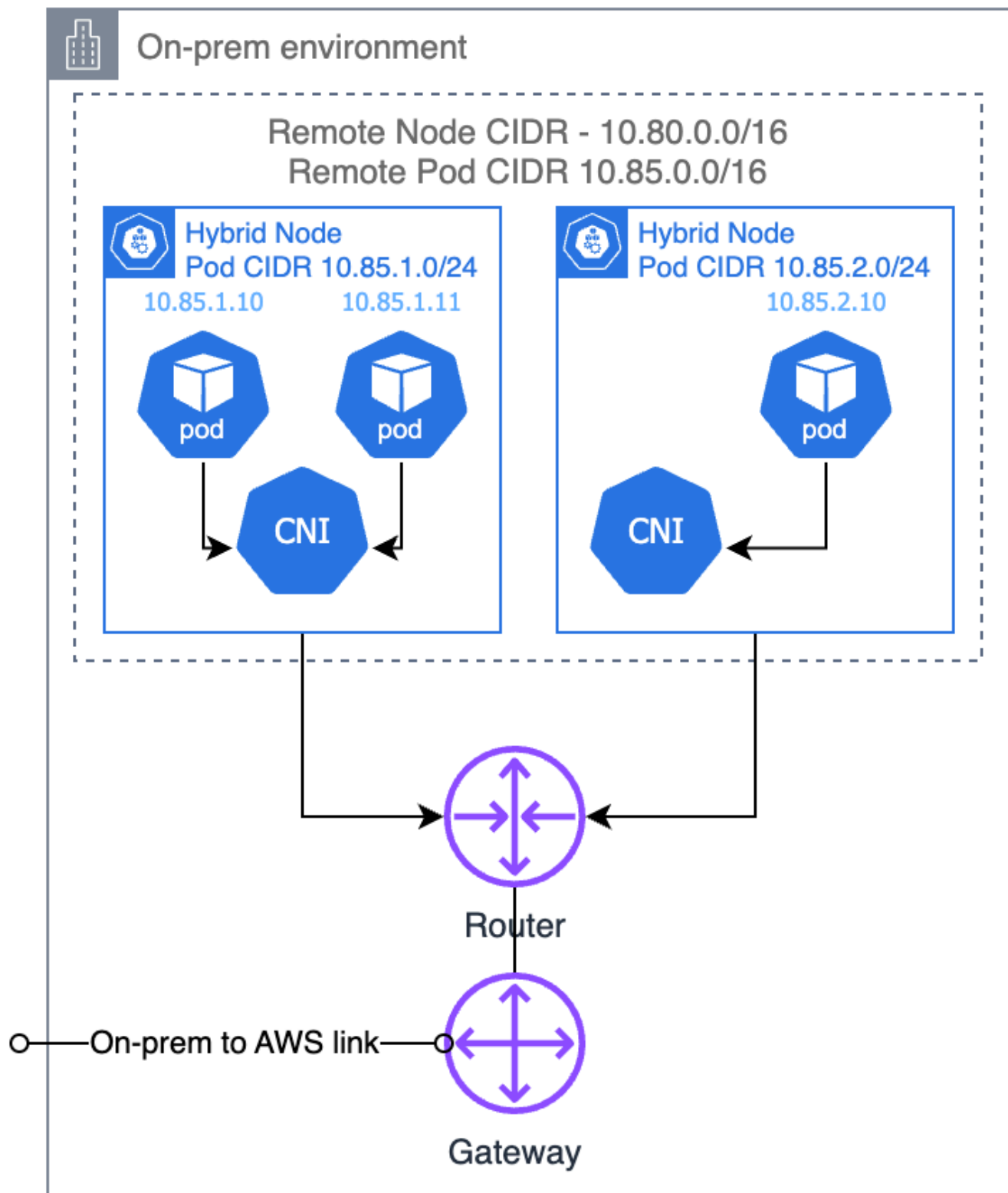
Sie konfigurieren den EKS-Cluster mit diesen Remote-Knoten, CIDRs sodass EKS den gesamten für die Hybridknoten bestimmten Datenverkehr IPs über Ihre Cluster-VPC weiterleiten kann, z. B. Anfragen an die Kubelet-API.

## Remote-Pod-Netzwerke

Die Remote-Pod-Netzwerke sind die Bereiche, die den Pods IPs zugewiesen sind, die auf den Hybridknoten ausgeführt werden. Im Allgemeinen konfigurieren Sie Ihr CNI mit diesen Bereichen, und die IP-Adressverwaltungsfunktion (IPAM) des CNI sorgt dafür, dass jedem Hybridknoten ein Teil

dieser Bereiche zugewiesen wird. Wenn Sie einen Pod erstellen, weist das CNI dem Pod eine IP aus dem Slice zu, der dem Knoten zugewiesen ist, für den der Pod geplant wurde.

Sie konfigurieren den EKS-Cluster mit diesen Remote-Pods, CIDRs sodass die EKS-Steuerebene weiß, dass sie den gesamten Datenverkehr, der für die Pods bestimmt ist, die auf den Hybridknoten ausgeführt werden, über die VPC Ihres Clusters weiterleitet, z. B. die Kommunikation mit Webhooks.



Lokal zur VPC

Das lokale Netzwerk, das Sie für Hybridknoten verwenden, muss zu der VPC weitergeleitet werden, die Sie für Ihren EKS-Cluster verwenden. Es stehen mehrere [Network-to-Amazon VPC-Konnektivitätsoptionen zur Verfügung, um Ihr lokales Netzwerk mit einer VPC](#) zu verbinden. Sie können auch Ihre eigene VPN-Lösung verwenden.

Es ist wichtig, dass Sie das Routing auf der AWS Cloud-Seite in der VPC und in Ihrem lokalen Netzwerk korrekt konfigurieren, sodass beide Netzwerke den richtigen Datenverkehr über die Verbindung für die beiden Netzwerke weiterleiten.

In der VPC muss der gesamte Datenverkehr, der zu den Remote-Knoten- und Remote-Pod-Netzwerken fließt, über die Verbindung zu Ihrem lokalen Netzwerk (als „Gateway“ bezeichnet) geleitet werden. Wenn einige Ihrer Subnetze unterschiedliche Routing-Tabellen haben, müssen Sie jede Routing-Tabelle mit den Routen für Ihre Hybridknoten und die darauf ausgeführten Pods konfigurieren. Dies gilt für die Subnetze, an die die EKS-Steuerebene ENIs angeschlossen ist, und für Subnetze, die EC2 Knoten oder Pods enthalten, die mit Hybridknoten kommunizieren müssen.

In Ihrem lokalen Netzwerk müssen Sie Ihr Netzwerk so konfigurieren, dass der Verkehr zur und von der VPC Ihres EKS-Clusters und den anderen für Hybridknoten erforderlichen AWS Diensten zugelassen wird. Der Datenverkehr für den EKS-Cluster durchquert das Gateway in beide Richtungen.

## Netzwerkeinschränkungen

### Vollständig geroutetes Netzwerk

Die Haupteinschränkung besteht darin, dass die EKS-Steuerebene und alle Knoten, Cloud- oder Hybridknoten, ein vollständig geroutetes Netzwerk bilden müssen. Das bedeutet, dass alle Knoten in der Lage sein müssen, einander auf Ebene drei über ihre IP-Adresse zu erreichen.

Die EKS-Kontrollebene und die Cloud-Knoten sind bereits voneinander erreichbar, da sie sich in einem flachen Netzwerk (der VPC) befinden. Die Hybridknoten befinden sich jedoch in einer anderen Netzwerkdomäne. Aus diesem Grund müssen Sie zusätzliches Routing in der VPC und in Ihrem lokalen Netzwerk konfigurieren, um den Verkehr zwischen den Hybridknoten und dem Rest des Clusters weiterzuleiten. Wenn die Hybridknoten voneinander und von der VPC aus erreichbar sind, können sich Ihre Hybridknoten in einem einzigen flachen Netzwerk oder in mehreren segmentierten Netzwerken befinden.

### Routbarer Remote-Pod CIDRs

Damit die EKS-Steuerebene mit Pods kommunizieren kann, die auf Hybridknoten ausgeführt werden (z. B. Webhooks oder der Metrics Server), oder für Pods, die auf Cloud-Knoten laufen,

mit Pods kommunizieren können, die auf Hybridknoten ausgeführt werden (Workload-Ost-West-Kommunikation), muss Ihr Remote-Pod-CIDR von der VPC aus routbar sein. Das bedeutet, dass die VPC in der Lage sein muss, den Datenverkehr zum Pod CIDRs über das Gateway zu Ihrem lokalen Netzwerk weiterzuleiten, und dass Ihr lokales Netzwerk in der Lage sein muss, den Datenverkehr für einen Pod an den richtigen Knoten weiterzuleiten.

Es ist wichtig, den Unterschied zwischen den Pod-Routing-Anforderungen in der VPC und den lokalen Anforderungen zu beachten. Die VPC muss nur wissen, dass der gesamte Datenverkehr, der zu einem Remote-Pod fließt, das Gateway passieren sollte. Wenn Sie nur einen Remote-Pod-CIDR haben, benötigen Sie nur eine Route.

Diese Anforderung gilt für alle Hops in Ihrem lokalen Netzwerk bis hin zum lokalen Router im selben Subnetz wie Ihre Hybridknoten. Dies ist der einzige Router, der den Pod-CIDR-Slice kennen muss, der jedem Knoten zugewiesen ist, um sicherzustellen, dass der Datenverkehr für einen bestimmten Pod an den Knoten weitergeleitet wird, für den der Pod geplant wurde.

Sie können diese Routen für den lokalen Pod CIDRs von Ihrem lokalen Router an die VPC-Routentabellen weitergeben, dies ist jedoch nicht erforderlich. Wenn sich Ihr lokaler Pod häufig CIDRs ändert und Ihre VPC-Routing-Tabellen aktualisiert werden müssen, um den sich ändernden Pod widerzuspiegeln CIDRs, empfehlen wir, den lokalen Pod an die VPC-Routing-Tabellen CIDRs weiterzugeben. Dies ist jedoch ungewöhnlich.

Beachten Sie, dass die Einschränkung, Ihren lokalen Pod routingfähig zu machen, optional ist. CIDRs Wenn Sie keine Webhooks auf Ihren Hybridknoten ausführen oder Pods auf Cloud-Knoten nicht mit Pods auf Hybridknoten kommunizieren lassen müssen, müssen Sie das Routing für den Pod in CIDRs Ihrem lokalen Netzwerk nicht konfigurieren.

Warum muss der lokale Pod mit CIDRs Hybridknoten routingfähig sein?

Wenn Sie EKS mit dem VPC-CNI für Ihre Cloud-Knoten verwenden, weist das VPC-CNI den Pods IPs direkt von der VPC zu. Das bedeutet, dass kein spezielles Routing erforderlich ist, da sowohl Cloud-Pods als auch die EKS-Steuerebene den Pod direkt erreichen können. IPs

Bei der Ausführung vor Ort (und mit anderen CNIs in der Cloud) werden die Pods normalerweise in einem isolierten Overlay-Netzwerk ausgeführt, und das CNI kümmert sich um die Übertragung des Datenverkehrs zwischen den Pods. Dies erfolgt üblicherweise durch Kapselung: Das CNI wandelt den Datenverkehr in pod-to-pod Datenverkehr um und kümmert sich dabei um die Kapselung und Entkapselung an beiden Enden. node-to-node Auf diese Weise ist keine zusätzliche Konfiguration auf den Knoten und Routern erforderlich.



Die Vernetzung mit Hybridknoten ist einzigartig, da sie eine Kombination aus beiden Topologien darstellt — die EKS-Kontrollebene und die Cloud-Knoten (mit dem VPC-CNI) erwarten ein flaches Netzwerk mit Knoten und Pods, während sich die Pods, die auf Hybridknoten laufen, in einem Overlay-Netzwerk befinden, das VXLAN zur Kapselung verwendet (standardmäßig in Cilium). Pods, die auf Hybridknoten ausgeführt werden, können die EKS-Steuerebene erreichen und Pods, die auf Cloud-Knoten ausgeführt werden, vorausgesetzt, das lokale Netzwerk kann zur VPC weiterleiten. Ohne Routing für den Pod CIDRs im lokalen Netzwerk wird jedoch jeglicher Datenverkehr, der zu einer lokalen Pod-IP zurückkehrt, irgendwann unterbrochen, wenn das Netzwerk nicht weiß, wie es das Overlay-Netzwerk erreichen und zu den richtigen Knoten weiterleiten kann.

## Kubernetes-Konzepte für Hybridknoten

Auf dieser Seite werden die wichtigsten Kubernetes-Konzepte beschrieben, die der EKS-Hybrid-Nodes-Systemarchitektur zugrunde liegen.

### EKS-Steuerebene in der VPC

Die IPs der EKS-Steuerungsebene ENIs werden im `kubernetes Endpoints` Objekt im `default Namespace` gespeichert. Wenn EKS neue erstellt ENIs oder ältere entfernt, aktualisiert EKS dieses Objekt, sodass die Liste der Objekte immer up-to-date angezeigt IPs wird.

Sie können diese Endpunkte über den `kubernetes Service` verwenden, auch im `default Namespace`. Diesem Dienst wird vom `ClusterIP` Typ her immer die erste IP des Dienstes CIDR des Clusters zugewiesen. Für den Dienst CIDR wird `172.16.0.0/16` beispielsweise die Dienst-IP lauten. `172.16.0.1`

Im Allgemeinen greifen Pods (unabhängig davon, ob sie in der Cloud oder in Hybridknoten ausgeführt werden) auf diese Weise auf den EKS-Kubernetes-API-Server zu. Pods verwenden die Dienst-IP als Ziel-IP, die in die tatsächliche IPs IP-Adresse einer der EKS-Steuerungsebenen übersetzt wird. ENIs Die wichtigste Ausnahme ist `kube-proxy`, dass damit die Übersetzung eingerichtet wird.

### Endpunkt des EKS-API-Servers

Die `kubernetes Service-IP` ist nicht die einzige Möglichkeit, auf den EKS-API-Server zuzugreifen. EKS erstellt auch einen Route53-DNS-Namen, wenn Sie Ihren Cluster erstellen. Dies ist das `endpoint` Feld Ihres EKS-Clusters, wenn Sie die `DescribeCluster` EKS-API-Aktion aufrufen.

```
{
 "cluster": {
 "endpoint": "https://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.gr7.us-
west-2.eks.amazonaws.com",
```

```
 "name": "my-cluster",
 "status": "ACTIVE"
 }
}
```

In einem Cluster mit öffentlichem Endpunktzugriff oder öffentlichem und privatem Endpunktzugriff lösen Ihre Hybridknoten diesen DNS-Namen standardmäßig in eine öffentliche IP auf, die über das Internet routbar ist. In einem privaten Endpunktzugriffscluster wird der DNS-Name in den privaten Namen IPs der EKS-Steuerebene aufgelöst. ENIs

So `kube-proxy` greifen die `kubelet` und auf den Kubernetes-API-Server zu. Wenn Sie möchten, dass Ihr gesamter Kubernetes-Cluster-Traffic über die VPC fließt, müssen Sie entweder Ihren Cluster im privaten Zugriffsmodus konfigurieren oder Ihren lokalen DNS-Server so ändern, dass der EKS-Cluster-Endpunkt in den privaten IPs Bereich der EKS-Steuerebene aufgelöst wird. ENIs

## **kubelet**-Endpunkt

Dadurch werden `kubelet` mehrere REST-Endpunkte verfügbar gemacht, sodass andere Teile des Systems mit jedem Knoten interagieren und Informationen von diesen sammeln können. In den meisten Clustern kommt der Großteil des Datenverkehrs zum `kubelet` Server von der Steuerungsebene, aber bestimmte Monitoring-Agenten können auch mit ihr interagieren.

Über diese Schnittstelle `kubelet` verarbeitet der verschiedene Anfragen: das Abrufen von Logs (`kubectl logs`), das Ausführen von Befehlen innerhalb von Containern (`kubectl exec`) und die Portweiterleitung von Traffic (`kubectl port-forward`). Jede dieser Anfragen interagiert über mit der zugrundeliegenden Container-Laufzeitkubel, was Clusteradministratoren und Entwicklern als nahtlos erscheint.

Der häufigste Nutzer dieser API ist der Kubernetes-API-Server. Wenn Sie einen der zuvor genannten `kubectl` Befehle verwenden, `kubectl` sendet er eine API-Anfrage an den API-Server, der dann die API des Knotens aufruft, auf dem der Pod ausgeführt wird. `kubelet` Dies ist der Hauptgrund, warum die Knoten-IP von der EKS-Steuerebene aus erreichbar sein muss und warum Sie, selbst wenn Ihre Pods laufen, nicht auf ihre Protokolle zugreifen können oder `exec` wenn die Knotenroute falsch konfiguriert ist.

## Knoten IPs

Wenn die EKS-Steuerebene mit einem Knoten kommuniziert, verwendet sie eine der Adressen, die im Node Objektstatus (`status.addresses`) gemeldet wurden.

Bei EKS-Cloud-Knoten ist es üblich, dass das Kubelet bei der Knotenregistrierung die private IP der EC2 Instanz als `InternalIP` angibt. Diese IP wird dann vom Cloud Controller Manager (CCM) validiert, um sicherzustellen, dass sie zur EC2 Instanz gehört. Darüber hinaus fügt der CCM in der Regel die öffentlichen IPs (`ExternalIP`) und DNS-Namen (`InternalDNS` und `ExternalDNS`) der Instanz zum Knotenstatus hinzu.

Es gibt jedoch kein CCM für Hybridknoten. Wenn Sie einen Hybridknoten mit der EKS-Hybrid-Nodes-CLI (`nodeadm`) registrieren, wird das Kubelet so konfiguriert, dass es die IP Ihres Computers direkt im Status des Knotens meldet, ohne das CCM.

```
apiVersion: v1
kind: Node
metadata:
 name: my-node-1
spec:
 providerID: eks-hybrid:///us-west-2/my-cluster/my-node-1
status:
 addresses:
 - address: 10.1.1.236
 type: InternalIP
 - address: my-node-1
 type: Hostname
```

Wenn Ihr Computer über mehrere verfügbare IPs verfügt, wählt das Kubelet nach seiner eigenen Logik eine davon aus. Sie können die ausgewählte IP mit dem `--node-ip` Flag steuern, das Sie in der `nodeadm` Konfiguration übergeben können. `spec.kubelet.flags` Nur die im Node Objekt gemeldete IP benötigt eine Route von der VPC. Ihre Maschinen können andere IP-Adressen haben, die von der Cloud aus nicht erreichbar sind.

## kube-proxy

`kube-proxy` ist verantwortlich für die Implementierung der Serviceabstraktion auf der Netzwerkebene jedes Knotens. Es fungiert als Netzwerk-Proxy und Load Balancer für den Datenverkehr, der für Kubernetes Services bestimmt ist. Indem der Kubernetes-API-Server kontinuierlich auf Änderungen im Zusammenhang mit Diensten und Endpunkten überwacht wird, werden die Netzwerkregeln des zugrunde liegenden Hosts `kube-proxy` dynamisch aktualisiert, um sicherzustellen, dass der Datenverkehr ordnungsgemäß geleitet wird.

`kube-proxy` programmiert im `iptables` Modus mehrere `netfilter` Ketten, um den Dienstdatenverkehr zu verarbeiten. Die Regeln bilden die folgende Hierarchie:

1. KUBE-SERVICES-Kette: Der Einstiegspunkt für den gesamten Dienstverkehr. Es gibt Regeln, die für jeden Dienst ClusterIP und jeden Port gelten.
2. KUBE-SVC-XXX Ketten: Dienstspezifische Ketten haben Lastenausgleichsregeln für jeden Dienst.
3. KUBE-SEP-XXX Ketten: Endpunktspezifische Ketten haben die tatsächlichen Regeln. DNAT

Lassen Sie uns untersuchen, was mit einem Dienst `test-server` im `default` Namespace passiert: \* Service ClusterIP: 172.16.31.14 \* Service Port: 80 \* Backing-Pods: 10.2.0.110, und 10.2.1.39 10.2.2.254

Wenn wir die iptables Regeln überprüfen (mit): `iptables-save | grep -A10 KUBE-SERVICES`

1. In der KUBE-SERVICES-Kette finden wir eine Regel, die dem Dienst entspricht:

```
-A KUBE-SERVICES -d 172.16.31.14/32 -p tcp -m comment --comment "default/test-server cluster IP" -m tcp --dport 80 -j KUBE-SVC-XYZABC123456
```

- Diese Regel entspricht Paketen, die für 172.16.31.14:80 bestimmt sind
  - Der Kommentar gibt an, wofür diese Regel gilt: `default/test-server cluster IP`
  - Passende Pakete werden in die KUBE-SVC-XYZABC123456 Kette gesprungen
2. Die XYZABC123456 KUBE-SVC-Kette verfügt über Wahrscheinlichkeitsregeln für den Lastenausgleich:

```
-A KUBE-SVC-XYZABC123456 -m statistic --mode random --probability 0.33333333349 -j KUBE-SEP-POD1XYZABC
-A KUBE-SVC-XYZABC123456 -m statistic --mode random --probability 0.50000000000 -j KUBE-SEP-POD2XYZABC
-A KUBE-SVC-XYZABC123456 -j KUBE-SEP-POD3XYZABC
```

- Erste Regel: 33,3% ige Chance, zu springen KUBE-SEP-POD1XYZABC
  - Zweite Regel: 50% ige Wahrscheinlichkeit, dass der verbleibende Traffic (33,3% des Gesamtverkehrs) zu einem KUBE-SEP-POD2XYZABC
  - Letzte Regel: Der gesamte verbleibende Verkehr (33,3% des Gesamtverkehrs) springt zu KUBE-SEP-POD3XYZABC
3. Die einzelnen KUBE-SEP-XXX-Ketten führen die DNAT (Destination NAT) durch:

```
-A KUBE-SEP-POD1XYZABC -p tcp -m tcp -j DNAT --to-destination 10.2.0.110:80
```

```
-A KUBE-SEP-POD2XYZABC -p tcp -m tcp -j DNAT --to-destination 10.2.1.39:80
-A KUBE-SEP-POD3XYZABC -p tcp -m tcp -j DNAT --to-destination 10.2.2.254:80
```

- Diese DNAT-Regeln schreiben die Ziel-IP und den Zielport neu, um den Verkehr an bestimmte Pods weiterzuleiten.
- Jede Regel verarbeitet etwa 33,3% des Datenverkehrs und sorgt so für einen gleichmäßigen Lastenausgleich zwischen 10.2.0.110, und 10.2.1.39 10.2.2.254

Diese mehrstufige Kettenstruktur ermöglicht eine kube-proxy effiziente Implementierung des Dienstlastenausgleichs und der Umleitung durch Paketmanipulation auf Kernelebene, ohne dass ein Proxyprozess im Datenpfad erforderlich ist.

### Auswirkungen auf den Kubernetes-Betrieb

Ein defekter kube-proxy Knoten verhindert, dass dieser Knoten den Dienstverkehr ordnungsgemäß weiterleitet, was zu Timeouts oder fehlgeschlagenen Verbindungen für Pods führt, die auf Clusterdienste angewiesen sind. Dies kann besonders störend sein, wenn ein Knoten zum ersten Mal registriert wird. Das CNI muss mit dem Kubernetes-API-Server kommunizieren, um Informationen wie die Pod-CIDR des Nodes zu erhalten, bevor es ein Pod-Netzwerk konfigurieren kann. Dazu verwendet es die Service-IP. Wenn jedoch der kube-proxy Start nicht möglich war oder die richtigen iptables Regeln nicht festgelegt wurden, werden die Anfragen, die an die Kubernetes Service-IP gesendet werden, nicht in die tatsächlichen Anforderungen IPs der EKS-Steuerebene übersetzt. Infolgedessen gerät das CNI in eine Absturzschleife und keiner der Pods kann ordnungsgemäß ausgeführt werden.

Wir wissen, dass Pods die Kubernetes Service-IP verwenden, um mit dem Kubernetes-API-Server zu kommunizieren, kube-proxy müssen aber zuerst iptables Regeln festlegen, damit das funktioniert.

### Wie kube-proxy kommuniziert man mit dem API-Server?

Der kube-proxy muss so konfiguriert sein, dass er den tatsächlichen IP/s Kubernetes-API-Server oder einen DNS-Namen verwendet, der in sie aufgelöst wird. Im Fall von EKS konfiguriert EKS die Standardeinstellung so, dass kube-proxy sie auf den Route53-DNS-Namen verweist, den EKS beim Erstellen des Clusters erstellt. Sie können diesen Wert im Namespace sehen. kube-proxy ConfigMap kube-system Der Inhalt ConfigMap ist einkubeconfig, der in den kube-proxy Pod injiziert wird. Suchen Sie also nach dem `clusters0.cluster.server` Feld. Dieser Wert entspricht dem `endpoint` Feld Ihres EKS-Clusters (wenn Sie die `DescribeCluster` EKS-API aufrufen).

```

apiVersion: v1
data:
 kubeconfig: |-
 kind: Config
 apiVersion: v1
 clusters:
 - cluster:
 certificate-authority: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
 server: https://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.gr7.us-
west-2.eks.amazonaws.com
 name: default
 contexts:
 - context:
 cluster: default
 namespace: default
 user: default
 name: default
 current-context: default
 users:
 - name: default
 user:
 tokenFile: /var/run/secrets/kubernetes.io/serviceaccount/token
kind: ConfigMap
metadata:
 name: kube-proxy
 namespace: kube-system

```

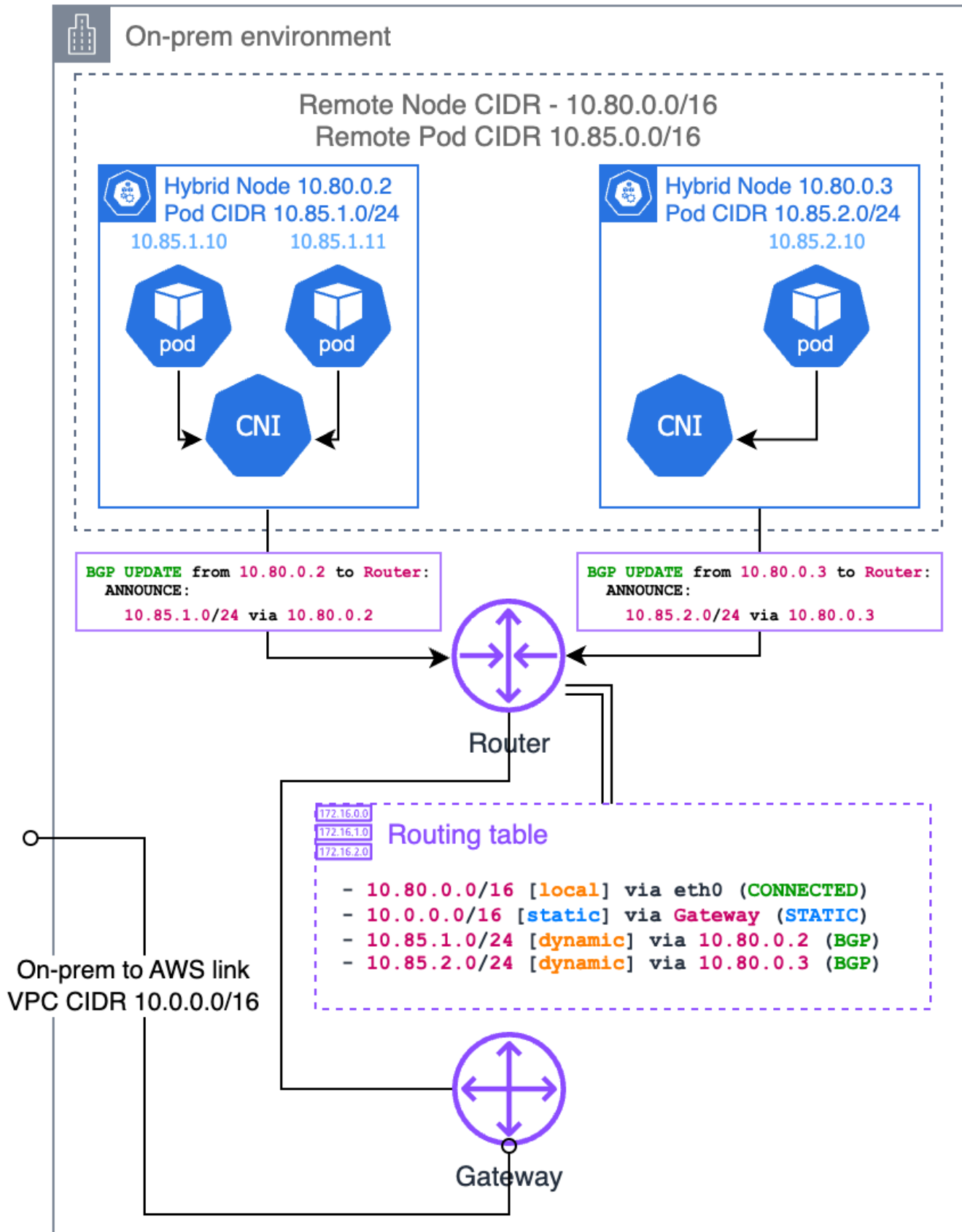
## Routbarer Remote-Pod CIDRs

[the section called “Netzwerkkonzepte”](#) Auf der Seite werden die Anforderungen für die Ausführung von Webhooks auf Hybridknoten oder für die Kommunikation von Pods, die auf Cloud-Knoten ausgeführt werden, mit Pods beschrieben, die auf Hybridknoten ausgeführt werden. Die wichtigste Anforderung besteht darin, dass der lokale Router wissen muss, welcher Knoten für eine bestimmte Pod-IP verantwortlich ist. Es gibt mehrere Möglichkeiten, dies zu erreichen, darunter das Border Gateway Protocol (BGP), statische Routen und das Address Resolution Protocol (ARP) -Proxy. Diese werden in den folgenden Abschnitten behandelt.

## Border Gateway Protocol (BGP)

Wenn Ihr CNI es unterstützt (wie Cilium und Calico), können Sie den BGP-Modus Ihres CNI verwenden, um Routen zu Ihrem Pod CIDRs pro Node von Ihren Nodes zu Ihrem lokalen Router zu übertragen. Wenn Sie den BGP-Modus des CNI verwenden, fungiert Ihr CNI als virtueller Router,

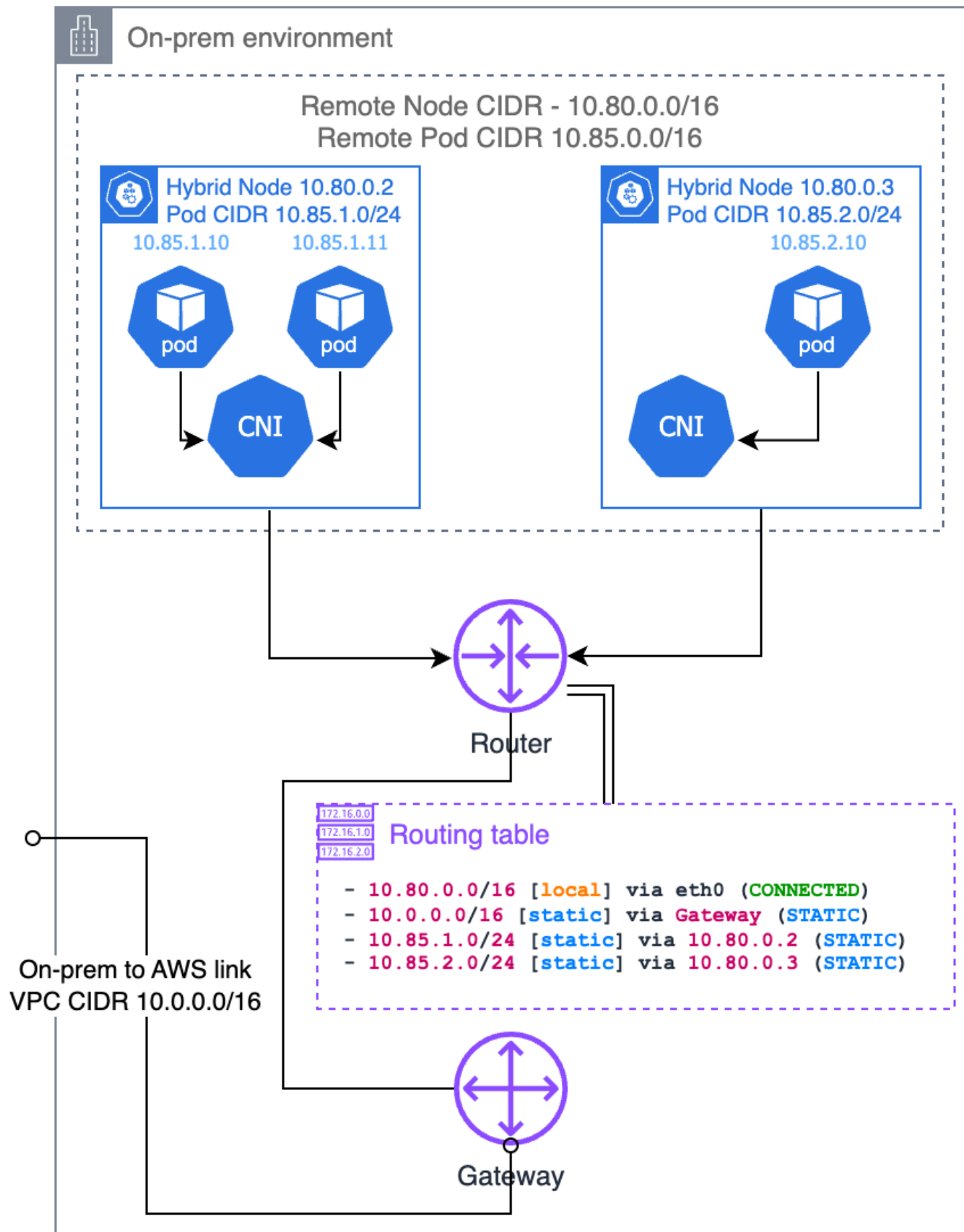
sodass Ihr lokaler Router davon ausgeht, dass der Pod-CIDR zu einem anderen Subnetz gehört und Ihr Knoten das Gateway zu diesem Subnetz ist.





## Statische Routen

Oder Sie können statische Routen in Ihrem lokalen Router konfigurieren. Dies ist die einfachste Methode, den lokalen Pod-CIDR an Ihre VPC weiterzuleiten, aber sie ist auch die fehleranfälligste und am schwierigsten zu warten. Sie müssen sicherstellen, dass die Routen immer zu den vorhandenen Knoten und up-to-date dem ihnen zugewiesenen Pod führen. CIDRs Wenn die Anzahl Ihrer Knoten gering und die Infrastruktur statisch ist, ist dies eine praktikable Option und macht die BGP-Unterstützung in Ihrem Router überflüssig. Wenn Sie sich dafür entscheiden, empfehlen wir, Ihr CNI mit dem Pod-CIDR-Slice zu konfigurieren, den Sie jedem Knoten zuweisen möchten, anstatt dessen IPAM entscheiden zu lassen.



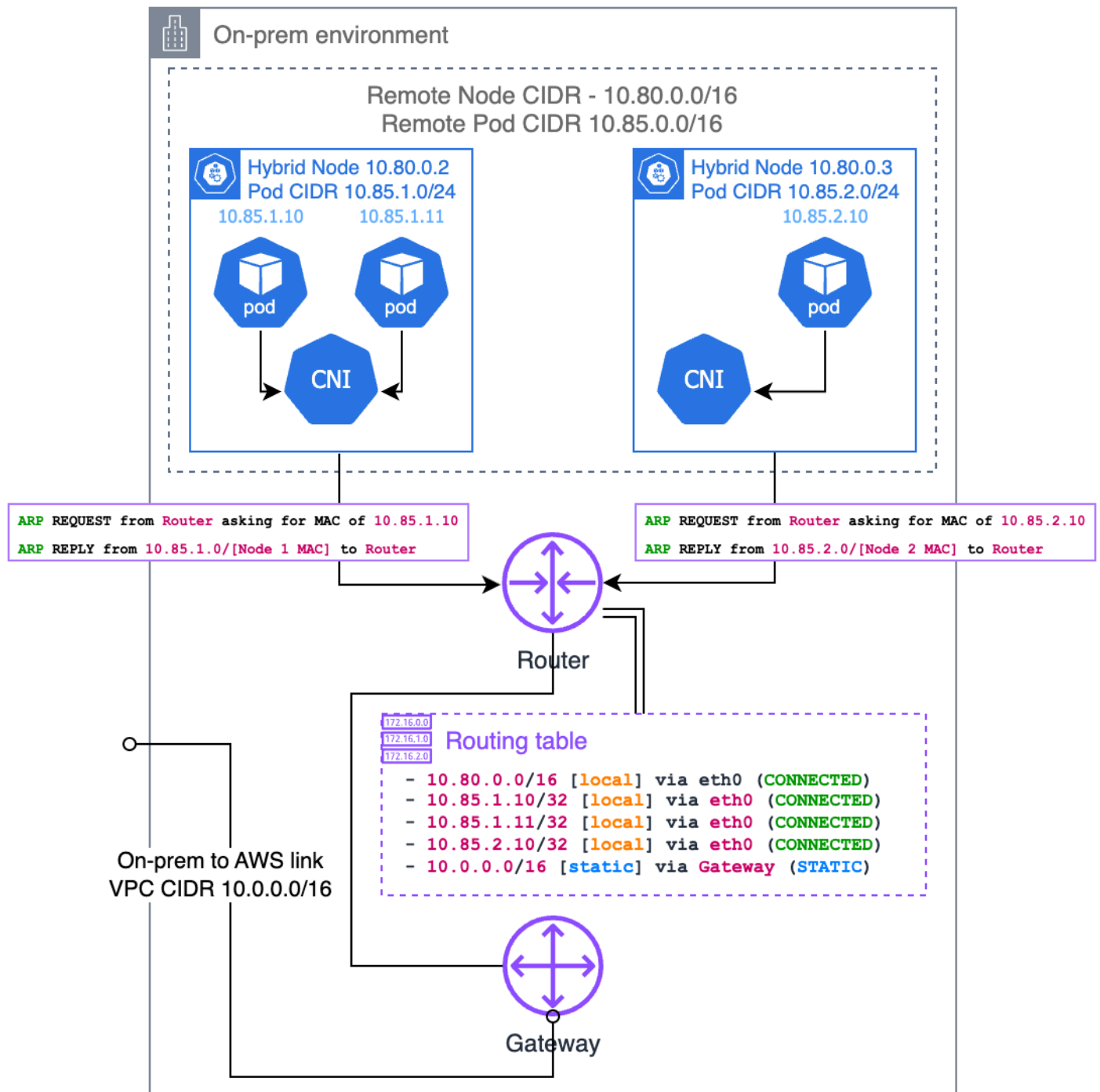
## Proxying mit dem Address Resolution Protocol (ARP)

ARP-Proxy ist ein weiterer Ansatz, um Pods vor Ort IPs routingfähig zu machen. Dies ist besonders nützlich, wenn sich Ihre Hybridknoten im selben Layer-2-Netzwerk wie Ihr lokaler Router befinden. Wenn ARP-Proxying aktiviert ist, reagiert ein Knoten auf ARP-Anfragen für Pods, die IPs er hostet, obwohl diese zu einem anderen Subnetz gehören. IPs

Wenn ein Gerät in Ihrem lokalen Netzwerk versucht, eine Pod-IP zu erreichen, sendet es zunächst eine ARP-Anfrage mit der Frage „Wer hat diese IP?“. Der Hybridknoten, der diesen Pod hostet, antwortet mit seiner eigenen MAC-Adresse und sagt: „Ich kann den Verkehr für diese IP verwalten.“ Dadurch entsteht ein direkter Pfad zwischen Geräten in Ihrem lokalen Netzwerk und den Pods, ohne dass eine Router-Konfiguration erforderlich ist.

Damit dies funktioniert, muss Ihr CNI die Proxy-ARP-Funktionalität unterstützen. Cilium verfügt über eine integrierte Unterstützung für Proxy-ARP, die Sie über die Konfiguration aktivieren können. Die wichtigste Überlegung ist, dass sich der Pod-CIDR nicht mit anderen Netzwerken in Ihrer Umgebung überschneiden darf, da dies zu Routing-Konflikten führen kann.

Dieser Ansatz hat mehrere Vorteile: \* Sie müssen Ihren Router nicht mit BGP konfigurieren oder statische Routen beibehalten. \* Funktioniert gut in Umgebungen, in denen Sie keine Kontrolle über Ihre Router-Konfiguration haben



## Pod-to-Pod Verkapselung

Verwenden Sie in lokalen Umgebungen in CNIs der Regel Kapselungsprotokolle, um Overlay-Netzwerke zu erstellen, die auf dem physischen Netzwerk betrieben werden können, ohne dass dieses neu konfiguriert werden muss. In diesem Abschnitt wird erklärt, wie diese Kapselung funktioniert. Beachten Sie, dass einige Details je nach verwendetem CNI variieren können.

Bei der Kapselung werden die ursprünglichen Pod-Netzwerkpakete in ein anderes Netzwerkpaket eingeschlossen, das über das zugrunde liegende physische Netzwerk weitergeleitet werden kann. Auf diese Weise können Pods zwischen Knoten kommunizieren, auf denen dasselbe CNI ausgeführt wird, ohne dass das physische Netzwerk wissen muss, wie diese Pods weitergeleitet werden sollen.

### CIDRs

Das am häufigsten mit Kubernetes verwendete Kapselungsprotokoll ist Virtual Extensible LAN (VXLAN), obwohl je nach Ihrem CNI auch andere (z. B. Geneve) verfügbar sind.

### VXLAN-Kapselung

VXLAN kapselt Layer-2-Ethernet-Frames in UDP-Paketen. Wenn ein Pod Datenverkehr an einen anderen Pod auf einem anderen Knoten sendet, führt das CNI Folgendes aus:

1. Das CNI fängt Pakete von Pod A ab
2. Das CNI verpackt das Originalpaket in einen VXLAN-Header
3. Dieses verpackte Paket wird dann über den regulären Netzwerkstapel des Knotens an den Zielknoten gesendet
4. Das CNI auf dem Zielknoten entpackt das Paket und übermittelt es an Pod B

Folgendes passiert mit der Paketstruktur während der VXLAN-Kapselung:

Ursprüngliches Paket: Pod-to-Pod

```
+-----+-----+-----+-----+
Ethernet Header	IP Header	TCP/UDP	Payload
Src: Pod A MAC	Src: Pod A IP	Src Port	
Dst: Pod B MAC	Dst: Pod B IP	Dst Port	
+-----+-----+-----+-----+
```

Nach der VXLAN-Kapselung:

```
+-----+-----+-----+-----+
+-----+
| Outer Ethernet | Outer IP | Outer UDP | VXLAN | Original Pod-to-Pod
| | | | |
| Src: Node A MAC | Src: Node A | Src: Random | VNI: xx | Packet (unchanged
| | | | |
| Dst: Node B MAC | Dst: Node B | Dst: 4789 | | from above)
| | | | |
```

```
+-----+-----+-----+-----+
+-----+
```

Der VXLAN Network Identifier (VNI) unterscheidet zwischen verschiedenen Overlay-Netzwerken.

## Szenarien für die Pod-Kommunikation

### Pods auf demselben Hybridknoten

Wenn Pods auf demselben Hybridknoten kommunizieren, ist normalerweise keine Kapselung erforderlich. Das CNI richtet lokale Routen ein, die den Verkehr zwischen Pods über die internen virtuellen Schnittstellen des Knotens leiten:

```
Pod A -> veth0 -> node's bridge/routing table -> veth1 -> Pod B
```

Das Paket verlässt den Knoten nie und muss nicht gekapselt werden.

### Pods auf verschiedenen Hybridknoten

Die Kommunikation zwischen Pods auf verschiedenen Hybridknoten erfordert eine Kapselung:

```
Pod A -> CNI -> [VXLAN encapsulation] -> Node A network -> router or gateway -> Node B
network -> [VXLAN decapsulation] -> CNI -> Pod B
```

Dadurch kann der Pod-Verkehr die physische Netzwerkinfrastruktur durchqueren, ohne dass das physische Netzwerk das Pod-IP-Routing verstehen muss.

## Netzwerkverkehrsflüsse für Hybridknoten

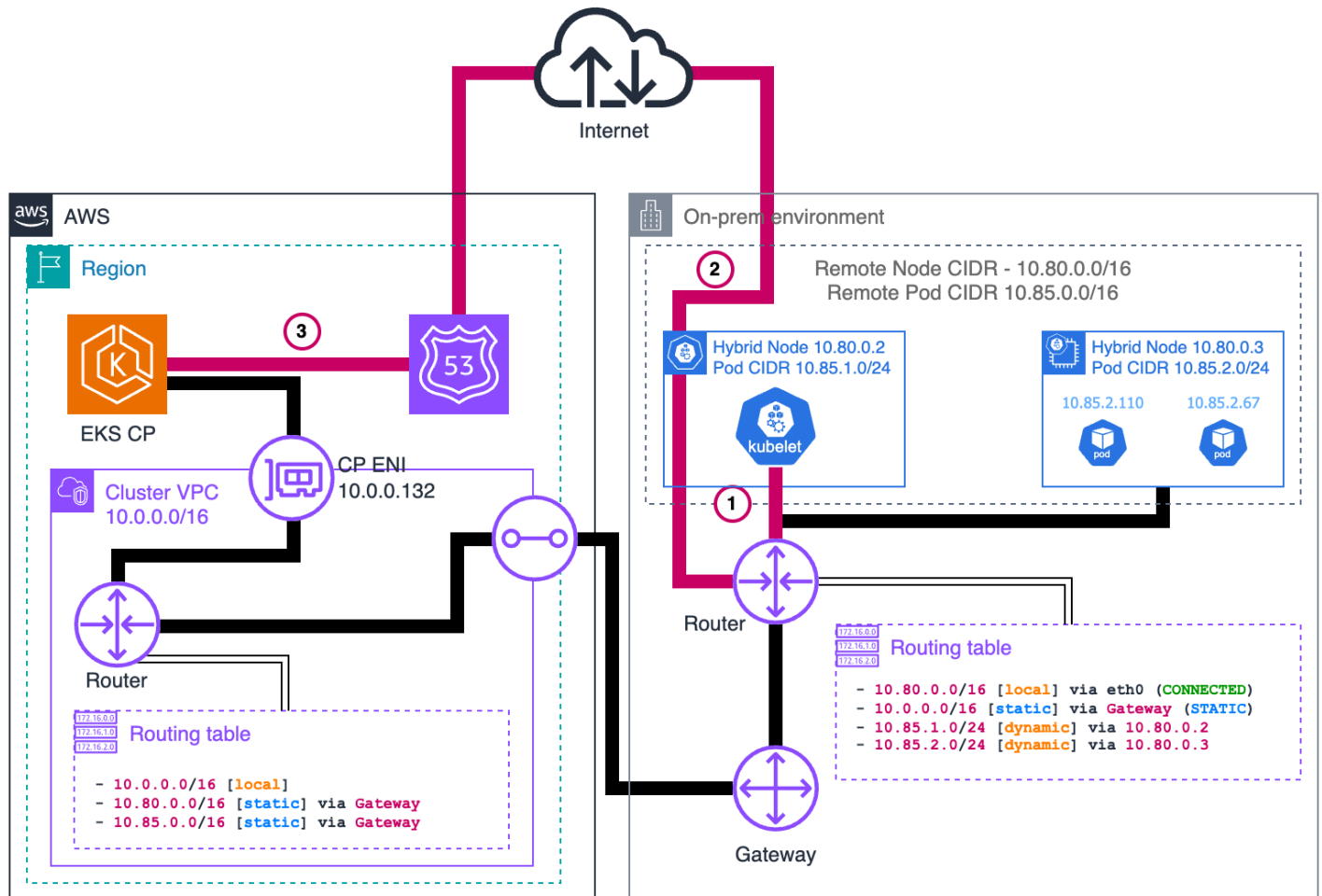
Auf dieser Seite werden die Netzwerkverkehrsflüsse für EKS-Hybridknoten anhand von Diagrammen beschrieben, die die end-to-end Netzwerkpfade für die verschiedenen Verkehrstypen zeigen.

Die folgenden Verkehrsflüsse werden behandelt:

- [the section called “Vom Hybridknoten kubelet zur EKS-Steuerebene”](#)
- [the section called “EKS-Steuerebene zum Hybridknoten \(Server\) kubelet”](#)
- [the section called “Pods, die auf Hybridknoten zur EKS-Steuerebene laufen”](#)
- [the section called “EKS-Steuerebene für Pods, die auf einem Hybridknoten laufen \(Webhooks\)”](#)

- [the section called “Pod-to-Pod läuft auf Hybridknoten”](#)
- [the section called “Von Pods auf Cloud-Knoten zu Pods auf Hybridknoten \(Ost-West-Verkehr\)”](#)

Vom Hybridknoten **kubelet** zur EKS-Steuerebene



## Anforderung

### 1**kubelet**. Initiiert eine Anfrage

Wenn der Knoten **kubelet** auf einem Hybridknoten mit der EKS-Steuerebene kommunizieren muss (z. B. um den Knotenstatus zu melden oder die Pod-Spezifikationen abzurufen), verwendet er die bei der Knotenregistrierung bereitgestellte kubeconfig Datei. Dies kubeconfig hat die API-Serverendpunkt-URL (den Route53-DNS-Namen) und nicht direkte IP-Adressen.

Der **kubelet** führt eine DNS-Suche nach dem Endpunkt durch (z. B. <https://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.gr7.us-west-2.eks.amazonaws.com>). In einem

Public-Access-Cluster wird dies in eine öffentliche IP-Adresse (z. B. 54.239.118.52) aufgelöst, die zu dem EKS-Dienst gehört, in AWS dem ausgeführt wird. `kubelet` Anschließend wird eine sichere HTTPS-Anfrage an diesen Endpunkt erstellt. Das erste Paket sieht so aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.80.0.2	Src: 52390 (random)	
Dst: 54.239.118.52	Dst: 443	
+-----+-----+-----+
```

## 2. Lokales Router-Routing

Da die Ziel-IP eine öffentliche IP-Adresse und nicht Teil des lokalen Netzwerks ist, sendet `kubelet` dieses Paket an sein Standard-Gateway (den lokalen Router). Der Router untersucht die Ziel-IP und stellt fest, dass es sich um eine öffentliche IP-Adresse handelt.

Bei öffentlichem Verkehr leitet der Router das Paket in der Regel an ein Internet-Gateway oder einen Grenzrouter weiter, der den ausgehenden Verkehr ins Internet abwickelt. Dies ist in der Abbildung nicht enthalten und hängt davon ab, wie Ihr lokales Netzwerk eingerichtet ist. Das Paket durchquert Ihre lokale Netzwerkinfrastruktur und erreicht schließlich das Netzwerk Ihres Internetdienstanbieters.

## 3. Lieferung an die EKS-Steuerebene

Das Paket wird über das öffentliche Internet und die Transitnetze übertragen, bis es AWS das Netzwerk erreicht. AWS Das Netzwerk leitet das Paket an den EKS-Dienstendpunkt in der entsprechenden Region weiter. Wenn das Paket den EKS-Dienst erreicht, wird es an die eigentliche EKS-Steuerebene für Ihren Cluster weitergeleitet.

Dieses Routing durch das öffentliche Internet unterscheidet sich von dem privaten VPC-gerouteten Pfad, den wir in anderen Verkehrsströmen sehen werden. Der Hauptunterschied besteht darin, dass bei Verwendung des öffentlichen Zugriffsmodus der Datenverkehr vom lokalen Standort `kubelet` (allerdings nicht von Pods) zur EKS-Steuerebene nicht über Ihre VPC läuft, sondern die globale Internetinfrastruktur verwendet wird.

### Antwort

Nachdem die EKS-Steuerebene die `kubelet` Anfrage verarbeitet hat, sendet sie eine Antwort zurück:

## 3. Die EKS-Steuerebene sendet eine Antwort



Die EKS-Steuerebene erstellt ein Antwortpaket. Dieses Paket hat die öffentliche IP als Quelle und die IP des Hybridknotens als Ziel:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 54.239.118.52	Src: 443	
Dst: 10.80.0.2	Dst: 52390	
+-----+-----+-----+
```

## 2. Internet-Routing

Das Antwortpaket wird über das Internet zurückgeleitet und folgt dabei dem von den Internetdiensteanbietern festgelegten Routingpfad, bis es Ihren lokalen Netzwerk-Edge-Router erreicht.

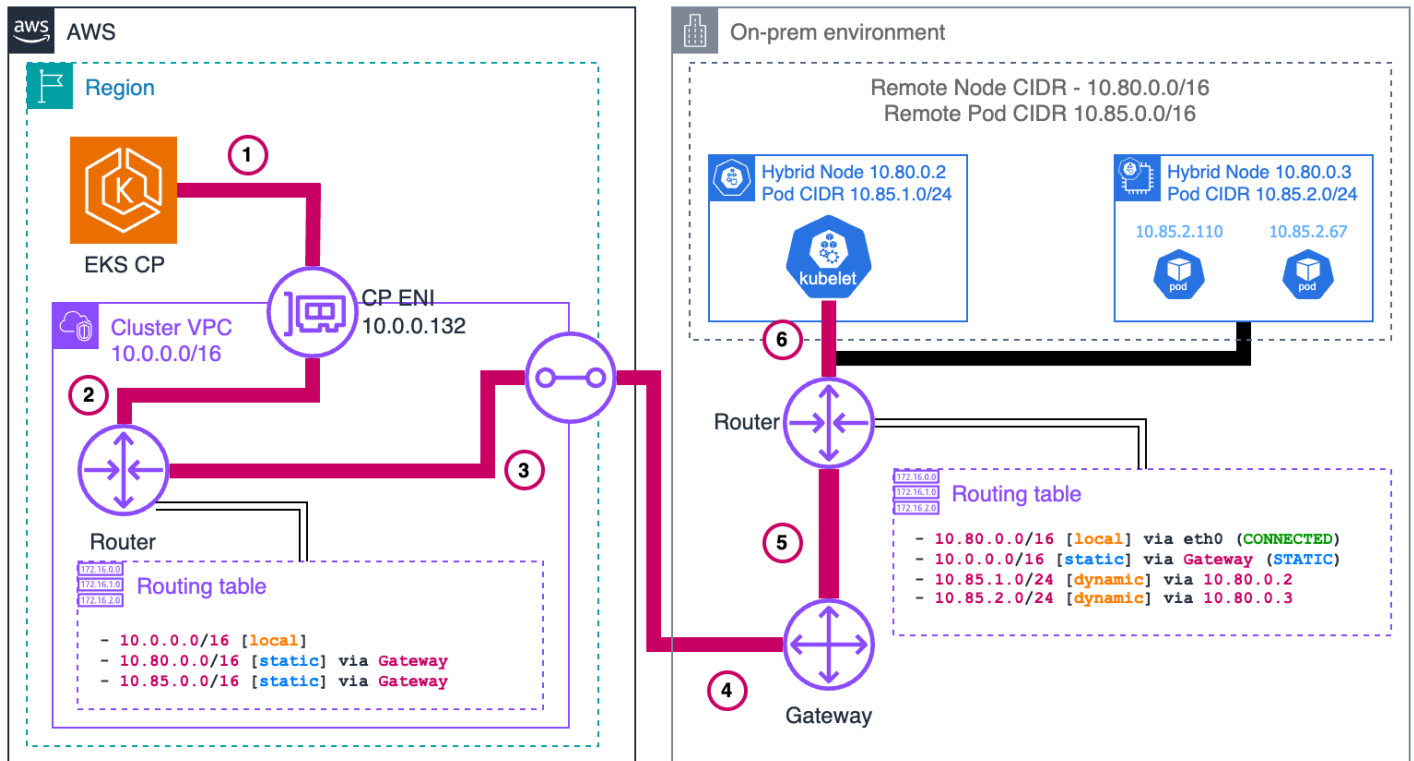
### 1. Lokale Zustellung

Ihr lokaler Router empfängt das Paket und erkennt, dass die Ziel-IP (10.80.0.2) zu Ihrem lokalen Netzwerk gehört. Er leitet das Paket über Ihre lokale Netzwerkinfrastruktur weiter, bis es den Ziel-Hybridknoten erreicht, wo `kubelet` er die Antwort empfängt und verarbeitet.

Der Hybridknoten **kube-proxy** zur EKS-Steuerebene

Wenn Sie den öffentlichen Endpunktzugriff für den Cluster aktivieren, verwendet der Rückverkehr das öffentliche Internet. Dieser Verkehr stammt vom Hybridknoten zur EKS-Steuerebene und folgt demselben Pfad wie der Verkehr von der `kubelet` zur EKS-Steuerebene. `kube-proxy`

## EKS-Steuerebene zum Hybridknoten (Server) **kubelet**



### Anforderung

#### 1. Der EKS Kubernetes API-Server initiiert eine Anfrage

Der EKS Kubernetes API-Server ruft die IP-Adresse des Knotens (10.80.0.2) aus dem Status des Knotenobjekts ab. Anschließend leitet er diese Anfrage über seine ENI in der VPC weiter, da die Ziel-IP zum konfigurierten Remote-Knoten CIDR () 10.80.0.0/16 gehört. Das erste Paket sieht wie folgt aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.0.0.132	Src: 67493 (random)	
Dst: 10.80.0.2	Dst: 10250	
+-----+-----+-----+
```

#### 2. VPC-Netzwerkverarbeitung

Das Paket verlässt die ENI und gelangt in die VPC-Netzwerkschicht, wo es zur weiteren Weiterleitung an das Gateway des Subnetzes weitergeleitet wird.

#### 3. Suche nach VPC-Routentabellen

Die VPC-Routentabelle für das Subnetz, das die EKS-Steuerebene ENI enthält, hat eine spezifische Route (die zweite im Diagramm) für den Remote-Knoten CIDR. Basierend auf dieser Routing-Regel wird das Paket an das Gateway weitergeleitet. VPC-to-onprem

#### 4. Grenzüberschreitender Transit

Das Gateway überträgt das Paket über die Cloud-Grenze über Ihre bestehende Verbindung (z. B. Direct Connect oder VPN) an Ihr lokales Netzwerk.

#### 5. Netzwerkempfang vor Ort

Das Paket kommt an Ihrem lokalen lokalen Router an, der den Verkehr für das Subnetz verarbeitet, in dem sich Ihre Hybridknoten befinden.

#### 6. Endgültige Lieferung

Der lokale Router erkennt, dass die Ziel-IP-Adresse (10.80.0.2) zu seinem direkt verbundenen Netzwerk gehört, und leitet das Paket direkt an den Ziel-Hybridknoten weiter, wo der die Anfrage `kubelet` empfängt und verarbeitet.

#### Antwort

Nachdem der Hybridknoten die Anfrage `kubelet` verarbeitet hat, sendet er eine Antwort zurück, die demselben Pfad in umgekehrter Reihenfolge folgt:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.80.0.2	Src: 10250	
Dst: 10.0.0.132	Dst: 67493	
+-----+-----+-----+
```

#### 6. **kubelet** Sendet Antwort

Der `kubelet` auf dem Hybridknoten befindliche Knoten (10.80.0.2) erstellt ein Antwortpaket mit der ursprünglichen Quell-IP als Ziel. Das Ziel gehört nicht zum lokalen Netzwerk und wird daher an das Standard-Gateway des Hosts gesendet, den lokalen Router.

#### 5. Lokales Router-Routing

Der Router stellt fest, dass die Ziel-IP (10.0.0.132) zu ihr gehört 10.0.0.0/16, deren Route auf das Gateway verweist, mit dem eine Verbindung hergestellt wird AWS.

#### 4. Grenzüberschreitende Rückkehr

Das Paket wird über dieselbe lokale Verbindung zur VPC-Verbindung (wie Direct Connect oder VPN) zurückgeleitet und überquert dabei die Cloud-Grenze in umgekehrter Richtung.

#### 3. VPC-Routing

Wenn das Paket in der VPC ankommt, identifizieren die Routentabellen, dass die Ziel-IP zu einer VPC-CIDR gehört. Die Paketrouten innerhalb der VPC.

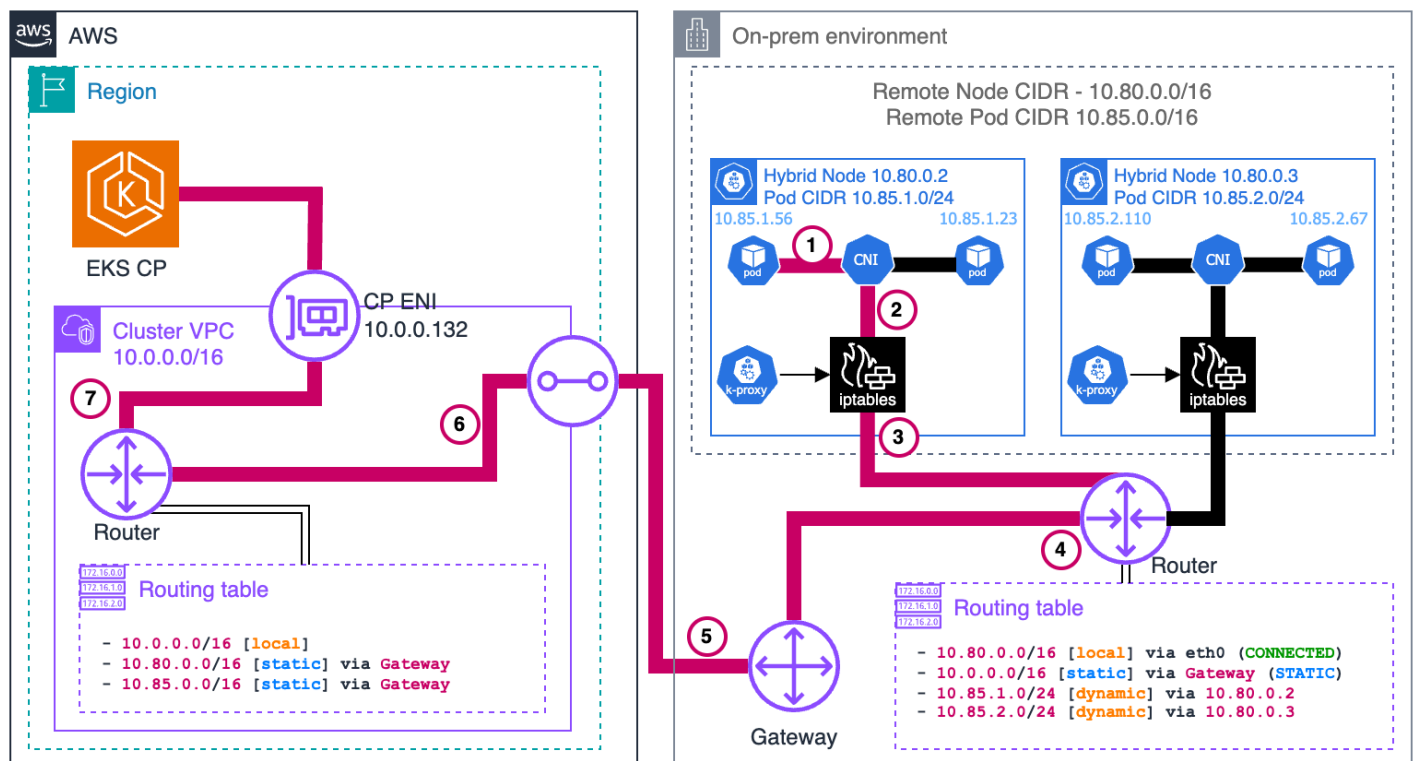
#### 2. VPC-Netzwerkbereitstellung

Die VPC-Netzwerkschicht leitet das Paket mit der EKS-Steuerebene ENI () an das Subnetz weiter.  
10.0.0.132

#### 1. ENI-Empfang

Das Paket erreicht die EKS-Steuerebene ENI, die an den Kubernetes-API-Server angeschlossen ist, und schließt damit den Roundtrip ab.

Pods, die auf Hybridknoten zur EKS-Steuerebene laufen



## Ohne CNI NAT

### Anforderung

Pods kommunizieren in der Regel über den Dienst mit dem Kubernetes-API-Server. `kubernetes` Die Service-IP ist die erste IP des Dienstes CIDR des Clusters. Diese Konvention ermöglicht es Pods, die ausgeführt werden müssen, bevor CoreDNS verfügbar ist, den API-Server zu erreichen, z. B. den CNI. Anfragen verlassen den Pod mit der Service-IP als Ziel. Wenn der Dienst beispielsweise CIDR ist `172.16.0.0/16`, ist auch die Service-IP. `172.16.0.1`

### 1. Pod initiiert Anfrage

Der Pod sendet von einem zufälligen Quellport aus eine Anfrage an die `kubernetes` Service-IP (`172.16.0.1`) auf dem API-Serverport (443). Das Paket sieht wie folgt aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.85.1.56	Src: 67493 (random)	
Dst: 172.16.0.1	Dst: 443	
+-----+-----+-----+
```

### 2. CNI-Verarbeitung

Das CNI erkennt, dass die Ziel-IP zu keinem Pod-CIDR gehört, das es verwaltet. Da ausgehendes NAT deaktiviert ist, leitet das CNI das Paket an den Host-Netzwerkstapel weiter, ohne es zu ändern.

### 3. Knoten-Netzwerkverarbeitung

Das Paket gelangt in den Netzwerkstapel des Knotens, wo `netfilter` Hooks die von `kube-proxy` festgelegten `iptables` Regeln auslösen. Es gelten mehrere Regeln in der folgenden Reihenfolge:

1. Das Paket trifft zuerst auf die `KUBE-SERVICES` Kette, die Regeln enthält, die der ClusterIP und dem Port jedes Dienstes entsprechen.
2. Die Vergleichsregel springt zur `KUBE-SVC-XXX` Kette für den `kubernetes` Dienst (Pakete, für die sie bestimmt sind `172.16.0.1:443`), die Regeln für den Lastenausgleich enthält.
3. Die Lastenausgleichsregel wählt nach dem Zufallsprinzip eine der `KUBE-SEP-XXX` Ketten für die Steuerungsebene ENI IPs (`10.0.0.132` oder `10.0.1.23`) aus.
4. Die ausgewählte `KUBE-SEP-XXX` Kette enthält die tatsächliche Regel, die die Ziel-IP von der Dienst-IP zur ausgewählten IP ändert. Dies wird als Destination Network Address Translation (DNAT) bezeichnet.

Nachdem diese Regeln angewendet wurden und davon ausgegangen wird, dass die IP der ausgewählten EKS-Kontrollebene ENI ist `10.0.0.132`, sieht das Paket wie folgt aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.85.1.56	Src: 67493 (random)	
Dst: 10.0.0.132	Dst: 443	
+-----+-----+-----+
```

Der Knoten leitet das Paket an sein Standard-Gateway weiter, da sich die Ziel-IP nicht im lokalen Netzwerk befindet.

#### 4. Lokales Router-Routing

Der lokale Router stellt fest, dass die Ziel-IP (`10.0.0.132`) zur VPC CIDR (`10.0.0.0/16`) gehört, und leitet sie an das Gateway weiter, mit dem eine Verbindung hergestellt wird. AWS

#### 5. Grenzüberschreitender Transit

Das Paket wird über Ihre bestehende Verbindung (wie Direct Connect oder VPN) über die Cloud-Grenze zur VPC übertragen.

#### 6. VPC-Netzwerkbereitstellung

Die VPC-Netzwerkschicht leitet das Paket an das richtige Subnetz weiter, in dem sich die EKS-Steuerebene ENI (`10.0.0.132`) befindet.

#### 7. ENI-Empfang

Das Paket erreicht die EKS-Steuerebene ENI, die an den Kubernetes-API-Server angeschlossen ist.

#### Antwort

Nachdem die EKS-Steuerebene die Anfrage verarbeitet hat, sendet sie eine Antwort zurück an den Pod:

#### 7. API-Server sendet Antwort

Der EKS Kubernetes API-Server erstellt ein Antwortpaket mit der ursprünglichen Quell-IP als Ziel. Das Paket sieht so aus:

```
+-----+-----+-----+
```

| IP Header       | TCP Header | Payload |
|-----------------|------------|---------|
| Src: 10.0.0.132 | Src: 443   |         |
| Dst: 10.85.1.56 | Dst: 67493 |         |

Da die Ziel-IP zum konfigurierten Remote-Pod CIDR (10.85.0.0/16) gehört, sendet er sie über seine ENI in der VPC mit dem Router des Subnetzes als nächsten Hop.

## 6. VPC-Routing

Die VPC-Routentabelle enthält einen Eintrag für den Remote-Pod CIDR (10.85.0.0/16), der diesen Datenverkehr an das Gateway weiterleitet. VPC-to-onprem

## 5. Grenzüberschreitender Transit

Das Gateway überträgt das Paket über die Cloud-Grenze über Ihre bestehende Verbindung (z. B. Direct Connect oder VPN) an Ihr lokales Netzwerk.

## 4. Netzwerkempfang vor Ort

Das Paket kommt an Ihrem lokalen lokalen Router an.

## 3. Lieferung an den Knoten

Die Tabelle des Routers hat einen Eintrag für 10.85.1.0/24 with 10.80.0.2 als nächsten Hop, der das Paket an unseren Knoten zustellt.

## 2. Knoten-Netzwerkverarbeitung

Während das Paket vom Netzwerkstapel des Knotens verarbeitet wird, ordnet `conntrack` (ein Teil von `netfilter`) das Paket der Verbindung zu, die der Pod ursprünglich herstellt. Da DNAT ursprünglich angewendet wurde, `conntrack` kehrt es die DNAT um, indem die Quell-IP von der ENI-IP der EKS-Kontrollebene auf die Service-IP umgeschrieben wird: `kubernetes`

| IP Header       | TCP Header | Payload |
|-----------------|------------|---------|
| Src: 172.16.0.1 | Src: 443   |         |
| Dst: 10.85.1.56 | Dst: 67493 |         |

## 1. CNI-Verarbeitung

Das CNI erkennt, dass die Ziel-IP zu einem Pod in seinem Netzwerk gehört, und übermittelt das Paket an den richtigen Pod-Netzwerk-Namespaces.

Dieser Ablauf zeigt, warum Remote Pod von der VPC bis zu dem spezifischen Knoten, der jeden Pod hostet, ordnungsgemäß routbar sein CIDRs muss. Der gesamte Rückpfad hängt vom ordnungsgemäßen Routing des Pods sowohl IPs in der Cloud als auch in lokalen Netzwerken ab.

## Mit CNI NAT

Dieser Ablauf ist dem ohne CNI NAT sehr ähnlich, weist jedoch einen wesentlichen Unterschied auf: Das CNI wendet Quell-NAT (SNAT) auf das Paket an, bevor es an den Netzwerkstapel des Knotens gesendet wird. Dadurch wird die Quell-IP des Pakets in die IP des Knotens geändert, sodass das Paket ohne zusätzliche Routing-Konfiguration zum Knoten zurückgeleitet werden kann.

## Anforderung

### 1. Der Pod initiiert die Anfrage

Der Pod sendet von einem zufälligen Quellport eine Anfrage an die kubernetes Service-IP (172.16.0.1) auf dem EKS Kubernetes API-Serverport (443). Das Paket sieht wie folgt aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.85.1.56	Src: 67493 (random)	
Dst: 172.16.0.1	Dst: 443	
+-----+-----+-----+
```

### 2. CNI-Verarbeitung

Das CNI erkennt, dass die Ziel-IP zu keinem Pod-CIDR gehört, das es verwaltet. Da ausgehendes NAT aktiviert ist, wendet das CNI SNAT auf das Paket an und ändert die Quell-IP in die IP des Knotens, bevor sie an den Netzwerkstapel des Knotens weitergegeben wird:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.80.0.2	Src: 67493 (random)	
Dst: 172.16.0.1	Dst: 443	
+-----+-----+-----+
```

Hinweis: CNI und iptables werden im Beispiel aus Gründen der Übersichtlichkeit als separate Blöcke dargestellt. In der Praxis ist es jedoch möglich, dass einige NAT CNIs verwenden iptables.



### 3. Knoten-Netzwerkverarbeitung

Hier kube-proxy verhalten sich die von festgelegten iptables Regeln genauso wie im vorherigen Beispiel, indem sie den Lastenausgleich zwischen dem Paket und einer der EKS-Steuerungsebenen durchführen ENIs. Das Paket sieht jetzt so aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.80.0.2	Src: 67493 (random)	
Dst: 10.0.0.132	Dst: 443	
+-----+-----+-----+
```

Der Knoten leitet das Paket an sein Standard-Gateway weiter, da sich die Ziel-IP nicht im lokalen Netzwerk befindet.

### 4. Lokales Router-Routing

Der lokale Router stellt fest, dass die Ziel-IP (10.0.0.132) zur VPC CIDR (10.0.0.0/16) gehört, und leitet sie an das Gateway weiter, mit dem eine Verbindung hergestellt wird. AWS

### 5. Grenzüberschreitender Transit

Das Paket wird über Ihre bestehende Verbindung (wie Direct Connect oder VPN) über die Cloud-Grenze zur VPC übertragen.

### 6. VPC-Netzwerkbereitstellung

Die VPC-Netzwerkschicht leitet das Paket an das richtige Subnetz weiter, in dem sich die EKS-Steuerungsebene ENI (10.0.0.132) befindet.

### 7. ENI-Empfang

Das Paket erreicht die EKS-Steuerungsebene ENI, die an den Kubernetes-API-Server angeschlossen ist.

### Antwort

Nachdem die EKS-Steuerungsebene die Anfrage verarbeitet hat, sendet sie eine Antwort zurück an den Pod:

### 7. API-Server sendet Antwort

Der EKS Kubernetes API-Server erstellt ein Antwortpaket mit der ursprünglichen Quell-IP als Ziel. Das Paket sieht so aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.0.0.132	Src: 443	
Dst: 10.80.0.2	Dst: 67493	
+-----+-----+-----+
```

Da die Ziel-IP zum konfigurierten Remote-Knoten CIDR (10.80.0.0/16) gehört, sendet er sie über seine ENI in der VPC mit dem Router des Subnetzes als nächsten Hop.

## 6. VPC-Routing

Die VPC-Routentabelle enthält einen Eintrag für den Remote-Knoten CIDR (10.80.0.0/16), der diesen Verkehr an das Gateway weiterleitet. VPC-to-onprem

## 5. Grenzüberschreitender Transit

Das Gateway überträgt das Paket über die Cloud-Grenze über Ihre bestehende Verbindung (z. B. Direct Connect oder VPN) an Ihr lokales Netzwerk.

## 4. Netzwerkempfang vor Ort

Das Paket kommt an Ihrem lokalen lokalen Router an.

## 3. Lieferung an den Knoten

Der lokale Router erkennt, dass die Ziel-IP-Adresse (10.80.0.2) zu seinem direkt verbundenen Netzwerk gehört, und leitet das Paket direkt an den Ziel-Hybridknoten weiter.

## 2. Knoten-Netzwerkverarbeitung

Da das Paket vom Netzwerkstapel des Knotens verarbeitet wird, ordnet `conntrack` (ein Teil von `netfilter`) das Paket der Verbindung zu, die der Pod ursprünglich eingerichtet hat. Da DNAT ursprünglich angewendet wurde, wird dies rückgängig gemacht, indem die Quell-IP von der ENI-IP der EKS-Steuerebene in die Dienst-IP umgeschrieben wird: `kubernetes`

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 172.16.0.1	Src: 443	
Dst: 10.80.0.2	Dst: 67493	
+-----+-----+-----+
```

+-----+-----+-----+

## 1. CNI-Verarbeitung

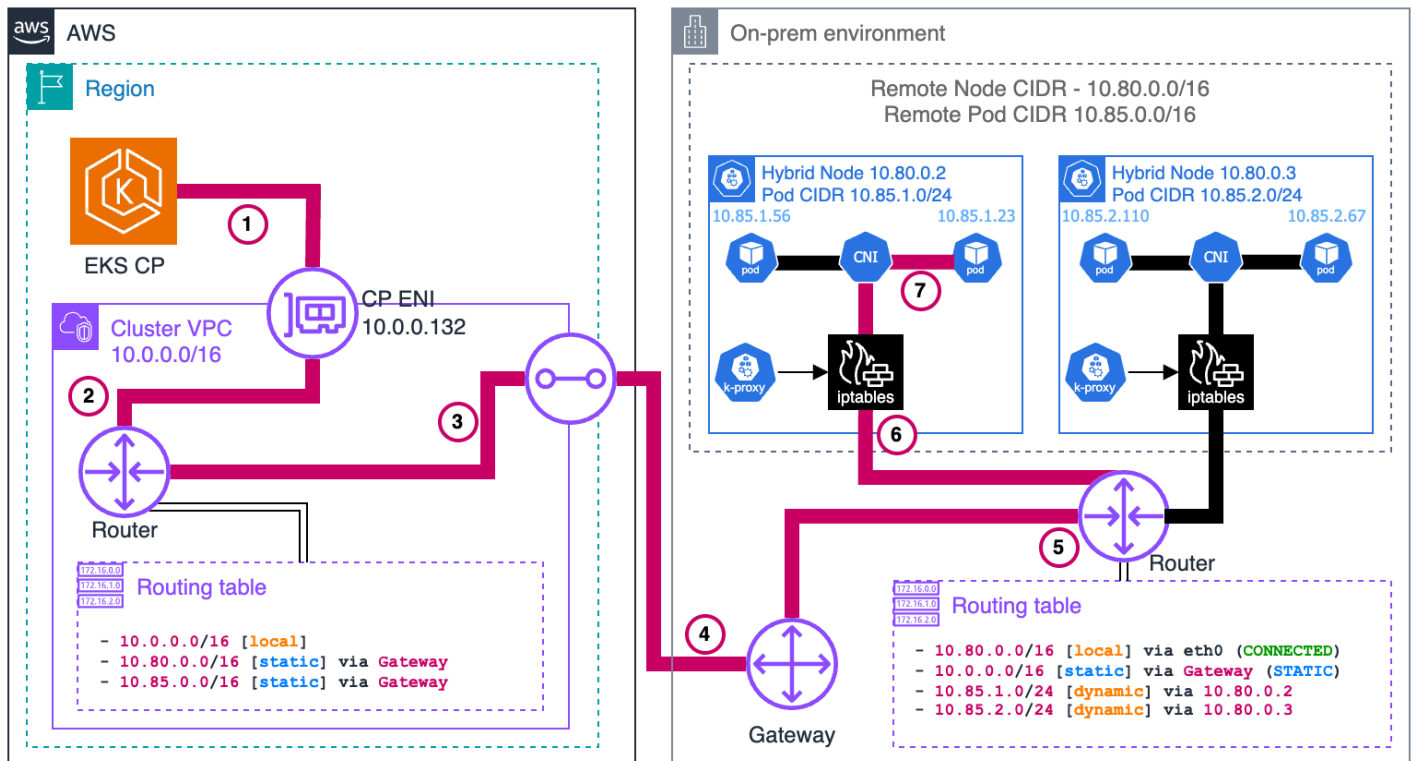
Das CNI identifiziert, dass dieses Paket zu einer Verbindung gehört, für die es zuvor SNAT angewendet hat. Es kehrt den SNAT um und ändert die Ziel-IP wieder auf die IP des Pods:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 172.16.0.1	Src: 443	
Dst: 10.85.1.56	Dst: 67493	
+-----+-----+-----+
```

Das CNI erkennt, dass die Ziel-IP zu einem Pod in seinem Netzwerk gehört, und übermittelt das Paket an den richtigen Pod-Netzwerk-Namespaces.

Dieser Ablauf zeigt, wie CNI NAT-ing die Konfiguration vereinfachen kann, indem Pakete an den Knoten zurückgeleitet werden können, ohne dass zusätzliches Routing für den Pod erforderlich ist. CIDRs

EKS-Steuerebene für Pods, die auf einem Hybridknoten laufen (Webhooks)



Dieses Verkehrsmuster tritt am häufigsten bei Webhooks auf, bei denen die EKS-Steuerebene direkt Verbindungen zu Webhook-Servern initiieren muss, die in Pods auf Hybridknoten ausgeführt werden. Beispiele hierfür sind die Validierung und Mutation von Zugangswebhooks, die vom API-Server während der Ressourcenvalidierung oder bei Mutationsprozessen aufgerufen werden.

## Anforderung

### 1. Der EKS Kubernetes API-Server initiiert eine Anfrage

Wenn ein Webhook im Cluster konfiguriert ist und ein relevanter API-Vorgang ihn auslöst, muss der EKS Kubernetes API-Server eine direkte Verbindung zum Webhook-Server-Pod herstellen. Der API-Server sucht zunächst die IP-Adresse des Pods anhand der Service- oder Endpunktresource, die dem Webhook zugeordnet ist.

Unter der Annahme, dass der Webhook-Pod auf einem Hybridknoten mit IP ausgeführt wird `10.85.1.23`, erstellt der EKS Kubernetes API-Server eine HTTPS-Anfrage an den Webhook-Endpunkt. Das erste Paket wird über die EKS-Steuerebene ENI in Ihrer VPC gesendet, da die Ziel-IP zum konfigurierten Remote-Pod CIDR (`() 10.85.1.23 10.85.0.0/16`) gehört. Das Paket sieht wie folgt aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.0.0.132	Src: 41892 (random)	
Dst: 10.85.1.23	Dst: 8443	
+-----+-----+-----+
```

### 2. VPC-Netzwerkverarbeitung

Das Paket verlässt die EKS-Steuerebene ENI und tritt in die VPC-Netzwerkschicht ein, wobei der Router des Subnetzes der nächste Hop ist.

### 3. Suche nach VPC-Routentabellen

Die VPC-Routentabelle für das Subnetz, das die EKS-Steuerebene ENI enthält, enthält eine spezifische Route für den Remote-Pod CIDR (`() 10.85.0.0/16`). Diese Routing-Regel leitet das Paket an das VPC-to-onprem Gateway weiter (z. B. ein Virtual Private Gateway für Direct Connect- oder VPN-Verbindungen):

| Destination  | Target                  |
|--------------|-------------------------|
| 10.85.0.0/16 | Virtual Private Gateway |

|              |                                |
|--------------|--------------------------------|
| 10.0.0.0/16  | local                          |
| 10.85.0.0/16 | vgw-id (VPC-to-onprem gateway) |

#### 4. Grenzüberschreitender Transit

Das Gateway überträgt das Paket über die Cloud-Grenze über Ihre bestehende Verbindung (z. B. Direct Connect oder VPN) an Ihr lokales Netzwerk. Das Paket behält beim Durchqueren dieser Verbindung seine ursprünglichen Quell- und Ziel-IP-Adressen bei.

#### 5. Netzwerkempfang vor Ort

Das Paket kommt an Ihrem lokalen lokalen Router an. Der Router ermittelt anhand seiner Routingtabelle, wie die Adresse 10.85.1.23 erreicht werden kann. Damit dies funktioniert, muss Ihr lokales Netzwerk über Routen für den Pod verfügen, die den Datenverkehr an den entsprechenden CIDRs Hybridknoten weiterleiten.

In diesem Fall enthält die Routing-Tabelle des Routers einen Eintrag, der angibt, dass das 10.85.1.0/24 Subnetz über den Hybridknoten mit IP erreichbar ist: 10.80.0.2

| Destination  | Next Hop  |
|--------------|-----------|
| 10.85.1.0/24 | 10.80.0.2 |

#### 6. Lieferung an den Knoten

Basierend auf dem Eintrag in der Routingtabelle leitet der Router das Paket an den Hybridknoten weiter (10.80.0.2). Wenn das Paket am Knoten ankommt, sieht es genauso aus wie zu dem Zeitpunkt, als der EKS Kubernetes API-Server es gesendet hat, wobei die Ziel-IP immer noch die IP des Pods ist.

#### 7. CNI-Verarbeitung

Der Netzwerkstapel des Knotens empfängt das Paket und leitet es zur Verarbeitung an das CNI weiter, da es sich bei der Ziel-IP nicht um die eigene IP des Knotens handelt. Das CNI erkennt, dass die Ziel-IP zu einem Pod gehört, der lokal auf diesem Knoten läuft, und leitet das Paket über die entsprechenden virtuellen Schnittstellen an den richtigen Pod weiter:

Original packet -> node routing -> CNI -> Pod's network namespace

Der Webhook-Server im Pod empfängt die Anfrage und verarbeitet sie.

## Antwort

Nachdem der Webhook-Pod die Anfrage verarbeitet hat, sendet er eine Antwort zurück, die demselben Pfad in umgekehrter Reihenfolge folgt:

### 7. Pod sendet Antwort

Der Webhook-Pod erstellt ein Antwortpaket mit seiner eigenen IP als Quelle und dem ursprünglichen Anforderer (der EKS-Steuerebene ENI) als Ziel:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.85.1.23	Src: 8443	
Dst: 10.0.0.132	Dst: 41892	
+-----+-----+-----+
```

Das CNI identifiziert, dass dieses Paket an ein externes Netzwerk (keinen lokalen Pod) gesendet wird, und leitet das Paket an den Netzwerkstapel des Knotens weiter, wobei die ursprüngliche Quell-IP erhalten bleibt.

### 6. Verarbeitung von Knotennetzwerken

Der Knoten stellt fest, dass sich die Ziel-IP (10.0.0.132) nicht im lokalen Netzwerk befindet, und leitet das Paket an sein Standard-Gateway (den lokalen Router) weiter.

### 5. Lokales Router-Routing

Der lokale Router konsultiert seine Routingtabelle und stellt fest, dass die Ziel-IP (10.0.0.132) zur VPC CIDR () gehört. 10.0.0.0/16 Er leitet das Paket an das Gateway weiter, mit dem eine Verbindung hergestellt wird. AWS

### 4. Grenzüberschreitender Transit

Das Paket wird über dieselbe lokale Verbindung zur VPC-Verbindung zurückgeleitet und überschreitet die Cloud-Grenze in umgekehrter Richtung.

### 3. VPC-Routing

Wenn das Paket in der VPC ankommt, identifizieren die Routing-Tabellen, dass die Ziel-IP zu einem Subnetz innerhalb der VPC gehört. Das Paket wird innerhalb der VPC entsprechend geroutet.

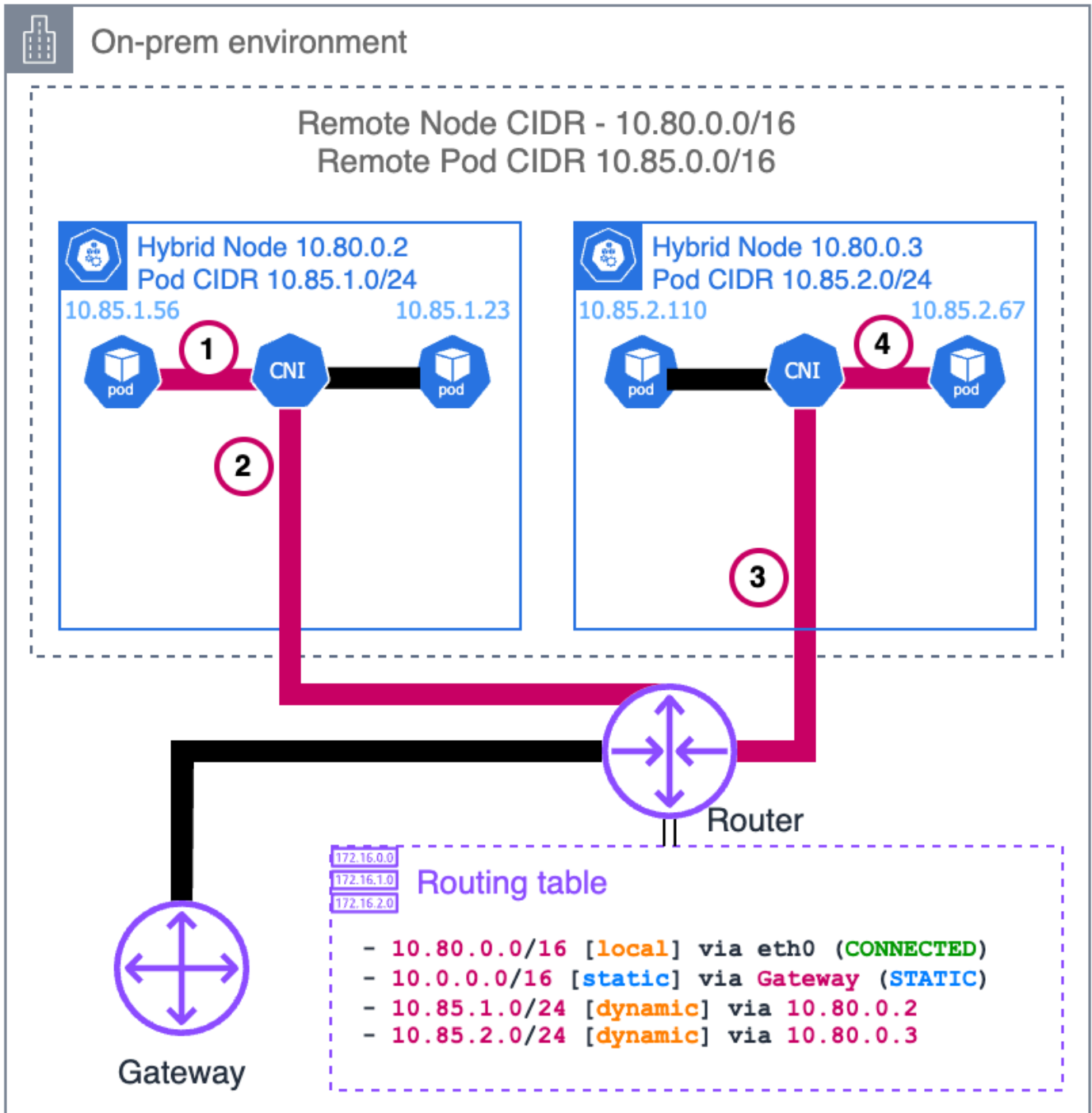
## 2. und 1. EKS-Steuerebene ENI Empfang

Das Paket erreicht das ENI, das an den EKS-Kubernetes-API-Server angeschlossen ist, wodurch der Roundtrip abgeschlossen ist. Der API-Server empfängt die Webhook-Antwort und setzt die Verarbeitung der ursprünglichen API-Anfrage auf der Grundlage dieser Antwort fort.

Dieser Verkehrsfluss zeigt, warum der Remote-Pod ordnungsgemäß konfiguriert und geroutet werden muss:

- Die VPC muss über Routen für den Remote-Pod verfügen, die auf das lokale Gateway CIDRs verweisen
- Ihr lokales Netzwerk muss über Routen für Pods verfügen CIDRs , die den Datenverkehr zu den spezifischen Knoten weiterleiten, auf denen diese Pods gehostet werden
- Ohne diese Routing-Konfiguration wären Webhooks und andere ähnliche Dienste, die in Pods auf Hybridknoten ausgeführt werden, von der EKS-Steuerebene aus nicht erreichbar.

## Pod-to-Pod läuft auf Hybridknoten



In diesem Abschnitt wird erklärt, wie Pods, die auf verschiedenen Hybridknoten ausgeführt werden, miteinander kommunizieren. In diesem Beispiel wird davon ausgegangen, dass Ihr CNI VXLAN für



die Kapselung verwendet, was bei Cilium CNIs oder Calico üblich ist. Der Gesamtprozess ist bei anderen Kapselungsprotokollen wie Geneve oder ähnlich. IP-in-IP

## Anforderung

### 1. Pod A initiiert die Kommunikation

Pod A (10.85.1.56) auf Knoten 1 möchte Traffic an Pod B (10.85.2.67) auf Knoten 2 senden. Das erste Paket sieht wie folgt aus:

```
+-----+-----+-----+-----+
Ethernet Header	IP Header	TCP/UDP	Payload
Src: Pod A MAC	Src: 10.85.1.56	Src: 43721	
Dst: Gateway MAC	Dst: 10.85.2.67	Dst: 8080	
+-----+-----+-----+-----+
```

### 2. CNI fängt das Paket ab und verarbeitet es

Wenn das Paket von Pod A seinen Netzwerk-Namespace verlässt, fängt das CNI es ab. Das CNI konsultiert seine Routingtabelle und stellt fest: - Die Ziel-IP (10.85.2.67) gehört zum Pod-CIDR. - Diese IP befindet sich nicht auf dem lokalen Knoten, sondern gehört zu Knoten 2 (10.80.0.3). - Das Paket muss mit VXLAN gekapselt werden.

Die Entscheidung für die Kapselung ist entscheidend, da das zugrunde liegende physische Netzwerk nicht weiß, wie es den Pod CIDRs direkt weiterleitet — es weiß nur, wie der Verkehr zwischen den Knoten weitergeleitet wird. IPs

Das CNI kapselt das gesamte Originalpaket in einem VXLAN-Frame. Dadurch wird effektiv ein „Paket innerhalb eines Pakets“ mit neuen Headern erstellt:

```
+-----+-----+-----+-----+
+-----+
| Outer Ethernet | Outer IP | Outer UDP | VXLAN | Original Pod-to-Pod
| | | | |
| Src: Node1 MAC | Src: 10.80.0.2 | Src: Random | VNI: 42 | Packet (unchanged
| | | | |
| Dst: Router MAC | Dst: 10.80.0.3 | Dst: 8472 | | from above)
| | | | |
+-----+-----+-----+-----+
+-----+
```

Wichtige Punkte zu dieser Kapselung: - Das äußere Paket wird von Knoten 1 (10.80.0.2) an Knoten 2 (10.80.0.3) adressiert - UDP-Port 8472 ist der VXLAN-Port, den Cilium standardmäßig verwendet - Der VXLAN Network Identifier (VNI) identifiziert, zu welchem Overlay-Netzwerk dieses Paket gehört - Das gesamte Originalpaket (mit der IP von Pod A als Quelle und der IP von Pod B als Ziel) wird im Inneren intakt aufbewahrt

Das gekapselte Paket tritt nun in den regulären Netzwerkstapel von Knoten 1 ein und wird auf die gleiche Weise wie jedes andere Paket verarbeitet:

1. Knoten-Netzwerkverarbeitung: Der Netzwerkstapel von Knoten 1 leitet das Paket auf der Grundlage seines Ziels weiter () 10.80.0.3
2. Lokale Netzwerkzustellung:
  - Wenn sich beide Knoten im selben Layer-2-Netzwerk befinden, wird das Paket direkt an Knoten 2 gesendet
  - Wenn sie sich in unterschiedlichen Subnetzen befinden, wird das Paket zuerst an den lokalen Router weitergeleitet
3. Router-Behandlung: Der Router leitet das Paket auf der Grundlage seiner Routing-Tabelle weiter und übermittelt es an Knoten 2

### 3. Verarbeitung des Empfangsknotens

Wenn das gekapselte Paket bei Knoten 2 ankommt ()10.80.0.3:

1. Der Netzwerkstapel des Knotens empfängt es und identifiziert es als VXLAN-Paket (UDP-Port 4789)
2. Das Paket wird zur Verarbeitung an die VXLAN-Schnittstelle des CNI weitergeleitet

### 4. VXLAN-Entkapselung

Das CNI auf Knoten 2 verarbeitet das VXLAN-Paket:

1. Es entfernt die äußeren Header (Ethernet, IP, UDP und VXLAN)
2. Es extrahiert das ursprüngliche innere Paket
3. Das Paket hat jetzt wieder seine ursprüngliche Form:

```
+-----+-----+-----+-----+-----+
```

|                  |                 |            |         |   |
|------------------|-----------------|------------|---------|---|
| Ethernet Header  | IP Header       | TCP/UDP    | Payload |   |
| Src: Pod A MAC   | Src: 10.85.1.56 | Src: 43721 |         |   |
| Dst: Gateway MAC | Dst: 10.85.2.67 | Dst: 8080  |         |   |
| +-----+          | +-----+         | +-----+    | +-----+ | + |

Das CNI auf Knoten 2 untersucht die Ziel-IP (10.85.2.67) und:

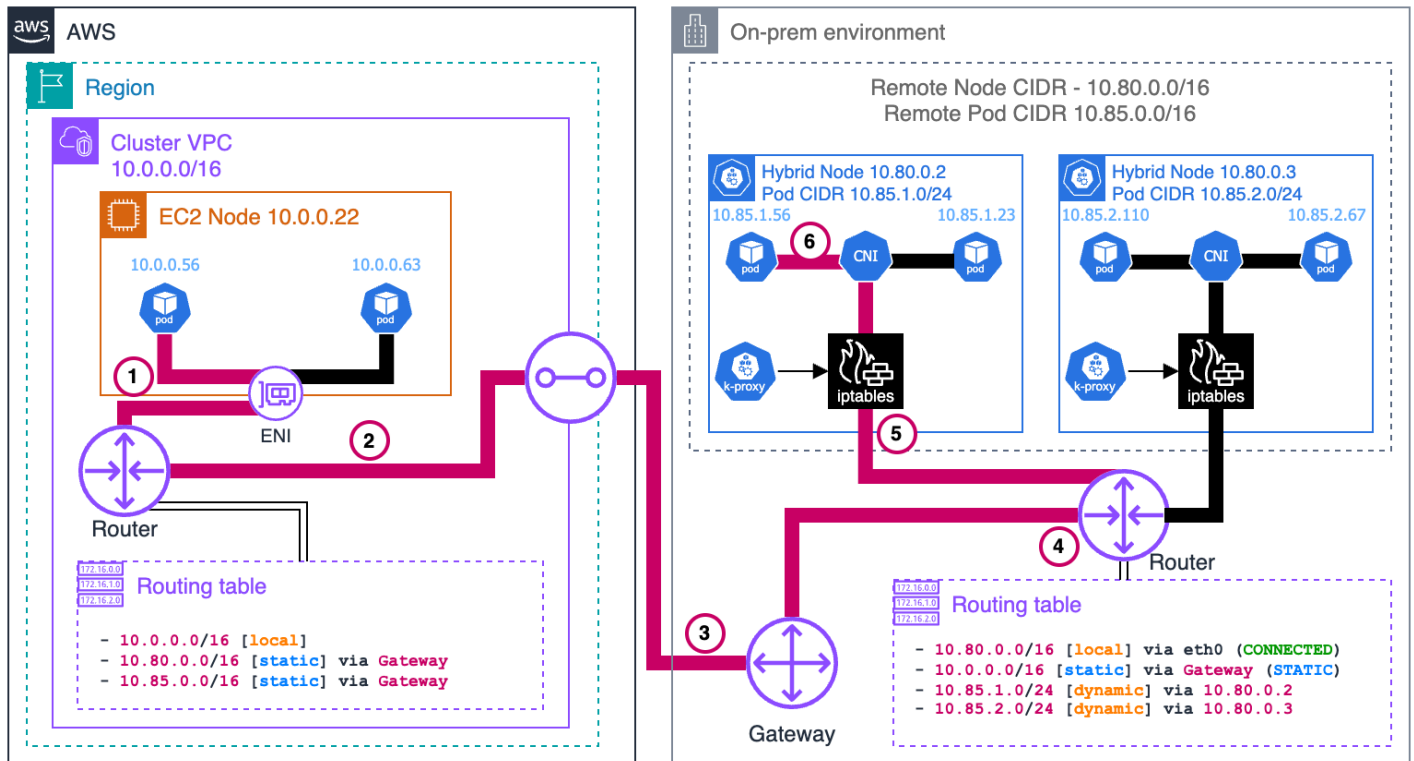
1. Identifiziert, dass diese IP zu einem lokalen Pod gehört
2. Leitet das Paket über die entsprechenden virtuellen Schnittstellen weiter
3. Liefert das Paket an den Netzwerk-Namespace von Pod B

## Antwort

Wenn Pod B auf Pod A reagiert, läuft der gesamte Vorgang umgekehrt ab:

4. Pod B sendet ein Paket an Pod A (10.85.1.56)
5. Das CNI von Knoten 2 kapselt es mit VXLAN und setzt das Ziel auf Knoten 1 () 10.80.0.2
6. Das gekapselte Paket wird an Knoten 1 übermittelt
7. Das CNI von Knoten 1 entkapselt es und übermittelt die ursprüngliche Antwort an Pod A

## Von Pods auf Cloud-Knoten zu Pods auf Hybridknoten (Ost-West-Verkehr)



### Anforderung

#### 1. Pod A initiiert die Kommunikation

Pod A (10.0.0.56) auf dem EC2 Knoten möchte Traffic an Pod B (10.85.1.56) auf dem Hybridknoten senden. Das erste Paket sieht so aus:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.0.0.56	Src: 52390 (random)	
Dst: 10.85.1.56	Dst: 8080	
+-----+-----+-----+
```

Mit der VPC CNI hat Pod A eine IP von der VPC CIDR und ist direkt mit einer ENI auf der Instance verbunden. EC2 Der Netzwerk-Namespace des Pods ist mit dem VPC-Netzwerk verbunden, sodass das Paket direkt in die VPC-Routing-Infrastruktur gelangt.

#### 2. VPC-Routing

Die VPC-Routentabelle enthält eine spezifische Route für den Remote Pod CIDR (10.85.0.0/16), die diesen Verkehr an das Gateway weiterleitet: VPC-to-onprem

| Destination  | Target                         |
|--------------|--------------------------------|
| 10.0.0.0/16  | local                          |
| 10.85.0.0/16 | vgw-id (VPC-to-onprem gateway) |

Basierend auf dieser Routing-Regel wird das Paket an das Gateway weitergeleitet, das eine Verbindung zu Ihrem lokalen Netzwerk herstellt.

### 3. Grenzüberschreitender Transit

Das Gateway überträgt das Paket über die Cloud-Grenze über Ihre bestehende Verbindung (z. B. Direct Connect oder VPN) an Ihr lokales Netzwerk. Das Paket behält während dieser Übertragung seine ursprünglichen Quell- und Ziel-IP-Adressen bei.

### 4. Netzwerkempfang vor Ort

Das Paket kommt an Ihrem lokalen lokalen Router an. Der Router verwendet seine Routingtabelle, um den nächsten Hop für das Erreichen der 10.85.1.56-Adresse zu ermitteln. Ihr lokaler Router muss über Routen für den Pod verfügen, die den Datenverkehr an den entsprechenden CIDRs Hybridknoten weiterleiten.

Die Tabelle des Routers enthält einen Eintrag, der angibt, dass das 10.85.1.0/24 Subnetz über den Hybridknoten mit IP erreichbar ist: 10.80.0.2

| Destination  | Next Hop  |
|--------------|-----------|
| 10.85.1.0/24 | 10.80.0.2 |

### 5. Verarbeitung von Knotennetzwerken

Der Router leitet das Paket an den Hybridknoten weiter (10.80.0.2). Wenn das Paket am Knoten ankommt, hat es immer noch die IP von Pod A als Quelle und die IP von Pod B als Ziel.

### 6. CNI-Verarbeitung

Der Netzwerkstapel des Knotens empfängt das Paket und leitet es zur Verarbeitung an das CNI weiter, da es sich bei der Ziel-IP nicht um seine eigene handelt. Das CNI erkennt, dass die Ziel-IP zu einem Pod gehört, der lokal auf diesem Knoten läuft, und leitet das Paket über die entsprechenden virtuellen Schnittstellen an den richtigen Pod weiter:

Original packet -> node routing -> CNI -> Pod B's network namespace

Pod B empfängt das Paket und verarbeitet es nach Bedarf.

Antwort

6. Pod B sendet Antwort

Pod B erstellt ein Antwortpaket mit seiner eigenen IP als Quelle und der IP von Pod A als Ziel:

```
+-----+-----+-----+
IP Header	TCP Header	Payload
Src: 10.85.1.56	Src: 8080	
Dst: 10.0.0.56	Dst: 52390	
+-----+-----+-----+
```

Das CNI identifiziert, dass dieses Paket für ein externes Netzwerk bestimmt ist, und leitet es an den Netzwerkstapel des Knotens weiter.

5. Verarbeitung von Knotennetzwerken

Der Knoten stellt fest, dass die Ziel-IP (10.0.0.56) nicht zum lokalen Netzwerk gehört, und leitet das Paket an sein Standard-Gateway (den lokalen Router) weiter.

4. Lokales Router-Routing

Der lokale Router konsultiert seine Routingtabelle und stellt fest, dass die Ziel-IP (10.0.0.56) zur VPC CIDR () gehört. 10.0.0.0/16 Er leitet das Paket an das Gateway weiter, mit dem eine Verbindung hergestellt wird. AWS

3. Grenzüberschreitender Transit

Das Paket wird über dieselbe lokale Verbindung zur VPC-Verbindung zurückgeleitet und überschreitet die Cloud-Grenze in umgekehrter Richtung.

2. VPC-Routing

Wenn das Paket in der VPC ankommt, erkennt das Routingsystem, dass die Ziel-IP zu einem Subnetz innerhalb der VPC gehört. Das Paket wird durch das VPC-Netzwerk an die EC2 Instance weitergeleitet, die Pod A hostet.

1. Pod A erhält Antwort

Das Paket kommt bei der EC2 Instance an und wird über das angehängte ENI direkt an Pod A übermittelt. Da das VPC-CNI kein Overlay-Netzwerk für Pods in der VPC verwendet, ist keine zusätzliche Entkapselung erforderlich — das Paket kommt mit intakten ursprünglichen Headern an.

Dieser Ost-West-Verkehrsfluss zeigt, warum der Remote-Pod ordnungsgemäß konfiguriert und aus beiden Richtungen routbar CIDRs sein muss:

- Die VPC muss über Routen für den Remote-Pod verfügen, die auf das lokale Gateway CIDRs verweisen
- Ihr lokales Netzwerk muss über Routen für Pods verfügen CIDRs , die den Datenverkehr zu den spezifischen Knoten weiterleiten, auf denen diese Pods gehostet werden.

## nodeadmReferenz für Hybridknoten

Die Amazon EKS Hybrid Nodes CLI (nodeadm) vereinfacht die Installation, Konfiguration, Registrierung und Deinstallation der Hybridknoten-Komponenten. Sie können Images nodeadm in Ihr Betriebssystem aufnehmen, um das Bootstrap von Hybridknoten zu automatisieren. [the section called “Bereiten Sie das Betriebssystem vor”](#) Weitere Informationen finden Sie unter.

Die nodeadm Version für Hybridknoten unterscheidet sich von der nodeadm Version, die für das Bootstrapping von EC2 Amazon-Instances als Knoten in Amazon EKS-Clustern verwendet wird. Folgen Sie der Dokumentation und den Referenzen für die entsprechende nodeadm Version. Diese Dokumentationsseite bezieht sich auf die nodeadm Hybridknoten-Version.

Der Quellcode für die Hybridknoten nodeadm ist im <https://github.com/aws/GitHub eks-hybrid-Repository> veröffentlicht.

### Important

Sie müssen nodeadm mit einem Benutzer arbeiten, der über Root-/Sudo-Rechte verfügt.

## Herunterladen von **nodeadm**

Die Hybridknoten-Version von nodeadm wird in Amazon S3 gehostet, das von Amazon CloudFront bereitgestellt wird. Um nodeadm auf jedem lokalen Host zu installieren, können Sie den folgenden Befehl von Ihren lokalen Hosts aus ausführen.

Für x86\_64-Hosts

```
curl -OL 'https://hybrid-assets.eks.amazonaws.com/releases/latest/bin/linux/amd64/
nodeadm'
```

## Für ARM-Hosts

```
curl -OL 'https://hybrid-assets.eks.amazonaws.com/releases/latest/bin/linux/arm64/
nodeadm'
```

Fügen Sie der heruntergeladenen Binärdatei auf jedem Host die Berechtigung für eine ausführbare Datei hinzu.

```
chmod +x nodeadm
```

## nodeadm install

Der `nodeadm install` Befehl wird verwendet, um die Artefakte und Abhängigkeiten zu installieren, die für den Betrieb und die Verbindung von Hybridknoten zu einem Amazon EKS-Cluster erforderlich sind. Der `nodeadm install` Befehl kann einzeln auf jedem Hybridknoten oder während der Image-Build-Pipelines ausgeführt werden, um die Abhängigkeiten der Hybridknoten in Betriebssystem-Images vorzuinstallieren.

## Usage

```
nodeadm install [KUBERNETES_VERSION] [flags]
```

## Positionelle Argumente

(Erforderlich) `KUBERNETES_VERSION` Die zu installierende Major.Minor-Version von EKS Kubernetes, zum Beispiel `1.32`

## Flags

| Name                                                   | Erforderlich | Beschreibung                                                                                                                                                                          |
|--------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-p,</code><br><code>--credential-provider</code> | TRUE         | Zu installierender Anmeldeinformationsanbieter. Unterstützte Werte sind <code>iam-ra</code> und <code>ssm</code> . Weitere Informationen finden Sie unter <a href="#">the section</a> |



| Name                           | Erforderlich | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |              | <a href="#">called “Bereiten Sie die Anmeldeinformationen vor”</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -s,<br><br>--containerd-source | FALSE        | <p>Quelle für containerd . nodeadm unterstützt die Installation containerd über die Betriebssystemdistribution, Docker-Pakete und das Überspringen containerd der Installation.</p> <p>Werte</p> <p>distro- Dies ist der Standardwert. nodeadm installiert das vom Node-Betriebssystem verteilte containerd Paket. distro ist kein unterstützter Wert für Red Hat Enterprise Linux (RHEL) -Betriebssysteme.</p> <p>docker- installiert nodeadm ein von containerd Docker erstelltes und verteiltes Paket. docker ist kein unterstützter Wert für Amazon Linux 2023</p> <p>none- installiert nodeadm das containerd Paket nicht. Sie müssen es manuell installieren, containerd bevor Sie es ausführen nodeadm init.</p> |

| Name             | Erforderlich | Beschreibung                                                                                                                                                                                      |
|------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r,<br>--region  | FALSE        | Gibt die AWS Region an, in die Artefakte wie der SSM-Agent heruntergeladen werden sollen. Standardeinstellung: us-west-2 .                                                                        |
| -t,<br>--timeout | FALSE        | Maximale Dauer des Installationsbefehls. Die Eingabe folgt dem Format für die Dauer. Zum Beispiel 1h23m. Das Standard-Download-Timeout für den Installationsbefehl ist auf 20 Minuten festgelegt. |
| -h, --help       | FALSE        | Zeigt eine Hilfmeldung mit den verfügbaren Parametern für Flaggen, Unterbefehle und Positionswerte an.                                                                                            |

## Beispiele

Installieren Sie die Kubernetes-Version 1.32 mit AWS Systems Manager (SSM) als Anmeldeinformationsanbieter

```
nodeadm install 1.32 --credential-provider ssm
```

Installieren Sie die Kubernetes-Version 1.32 mit AWS Systems Manager (SSM) als Anmeldeinformationsanbieter und Docker als Container-Quelle mit einem Download-Timeout von 20 Minuten.

```
nodeadm install 1.32 --credential-provider ssm --containerd-source docker --timeout 20m
```

Installieren Sie die Kubernetes-Version mit IAM Roles Anywhere als Anmeldeinformationsanbieter 1.32 AWS

```
nodeadm install 1.32 --credential-provider iam-ra
```

## nodeadm config check

Der `nodeadm config check` Befehl überprüft die angegebene Knotenkonfiguration auf Fehler. Dieser Befehl kann verwendet werden, um die Richtigkeit einer Hybridknoten-Konfigurationsdatei zu überprüfen und zu validieren.

### Usage

```
nodeadm config check [flags]
```

### Flags

| Name                                             | Erforderlich | Beschreibung                                                                                            |
|--------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------|
| <code>-c,</code><br><code>--config-source</code> | TRUE         | Quelle der Nodeadm-Konfiguration. Bei Hybridknoten sollte die Eingabe einem URI mit Dateischema folgen. |
| <code>-h, --help</code>                          | FALSE        | Zeigt eine Hilfmeldung mit den verfügbaren Parametern für Flaggen, Unterbefehle und Positionswerte an.  |

### Beispiele

```
nodeadm config check -c file://nodeConfig.yaml
```

## nodeadm init

Der `nodeadm init` Befehl startet und verbindet den Hybridknoten mit dem konfigurierten Amazon EKS-Cluster. Einzelheiten [the section called “Knotenkonfiguration für IAM-Rollen Anywhere”](#) zur Konfiguration der `nodeConfig.yaml` Datei finden Sie unter [the section called “Knotenkonfiguration für SSM-Hybrid-Aktivierungen”](#) oder.

## Usage

```
nodeadm init [flags]
```

## Flags

| Name                                             | Erforderlich | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-c,</code><br><code>--config-source</code> | TRUE         | Quelle der nodeadm Konfiguration. Bei Hybridknoten sollte die Eingabe einem URI mit Dateischema folgen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>-s,</code><br><code>--skip</code>          | FALSE        | <p>Phaseninit, die übersprungen werden sollen. Es wird nicht empfohlen, eine der Phasen zu überspringen, es sei denn, dies hilft, ein Problem zu beheben.</p> <p>Werte</p> <p><code>install-validation</code> überspringt die Überprüfung, ob der vorherige Installationsbefehl erfolgreich ausgeführt wurde.</p> <p><code>cni-validation</code> überspringt die Überprüfung, ob entweder die VXLAN-Ports von Cilium oder Calico CNI geöffnet sind, wenn die Firewall auf dem Knoten aktiviert ist</p> <p><code>node-ip-validation</code> überspringt die Überprüfung</p> |

| Name       | Erforderlich | Beschreibung                                                                                       |
|------------|--------------|----------------------------------------------------------------------------------------------------|
|            |              | ng, ob die Knoten-IP innerhalb eines CIDR in den Netzwerken der Remote-Knoten liegt                |
| -h, --help | FALSE        | Zeigt eine Hilfmeldung mit verfügbaren Parametern für Flaggen, Unterbefehle und Positionswerte an. |

## Beispiele

```
nodeadm init -c file://nodeConfig.yaml
```

## nodeadm upgrade

Der `nodeadm upgrade` Befehl aktualisiert alle installierten Artefakte auf die neueste Version und bootet den Knoten, um die aktualisierten Artefakte zu konfigurieren und dem EKS-Cluster beizutreten. AWS Beim Upgrade handelt es sich um einen Befehl, der die Workloads, die auf dem Knoten ausgeführt werden, unterbricht. Bitte verschieben Sie Ihre Workloads auf einen anderen Knoten, bevor Sie das Upgrade ausführen.

## Usage

```
nodeadm upgrade [KUBERNETES_VERSION] [flags]
```

## Positionelle Argumente

(Erforderlich) `KUBERNETES_VERSION` Die zu installierende Major.Minor-Version von EKS Kubernetes, zum Beispiel 1.32

## Flags

| Name                   | Erforderlich | Beschreibung                                             |
|------------------------|--------------|----------------------------------------------------------|
| -c,<br>--config-source | TRUE         | nodeadmQuelle der Konfiguration. Bei Hybridknoten sollte |

| Name                                       | Erforderlich | Beschreibung                                                                                                                                                                                      |
|--------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            |              | die Eingabe einem URI mit Dateischema folgen.                                                                                                                                                     |
| <code>-t,</code><br><code>--timeout</code> | FALSE        | Timeout für das Herunterladen von Artefakten. Die Eingabe folgt dem Format für die Dauer. Zum Beispiel 1h23m. Das Standard-Download-Timeout für den Upgrade-Befehl ist auf 10 Minuten festgelegt. |

| Name                                    | Erforderlich | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-s,</code><br><code>--skip</code> | FALSE        | <p>Upgrade-Phasen müssen übersprungen werden. Es wird nicht empfohlen, eine der Phasen zu überspringen, es sei denn, dies hilft, ein Problem zu beheben.</p> <p>Werte</p> <p><code>pod-validation</code> überspringt die Überprüfung, ob alle Pods auf dem Knoten laufen, mit Ausnahme von Daemon-Sets und statischen Pods.</p> <p><code>node-validation</code> überspringt die Überprüfung, ob der Knoten gesperrt wurde.</p> <p><code>init-validation</code> überspringt die Überprüfung, ob der Knoten erfolgreich initialisiert wurde, bevor das Upgrade ausgeführt wird.</p> |
| <code>-h, --help</code>                 | FALSE        | Zeigt eine Hilfmeldung mit verfügbaren Parametern für Flaggen, Unterbefehle und Positionswerte an.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Beispiele

```
nodeadm upgrade 1.32 -c file:///nodeConfig.yaml
```

```
nodeadm upgrade 1.32 -c file:///nodeConfig.yaml --timeout 20m
```

## nodeadm uninstall

Der `nodeadm uninstall` Befehl stoppt und entfernt die Artefakte, die `nodeadm` währenddessen installiert wurden `nodeadm install`, einschließlich Kubelet und containerd. Beachten Sie, dass der Deinstallationsbefehl Ihre Hybridknoten nicht entleert oder aus Ihrem Cluster löscht. Sie müssen die Vorgänge „Entleeren“ und „Löschen“ getrennt ausführen. [the section called “Löschen Sie Hybridknoten”](#) Weitere Informationen finden Sie unter. `nodeadm uninstall` Wird standardmäßig nicht fortgesetzt, wenn noch Pods auf dem Knoten vorhanden sind. Ebenso werden CNI-Abhängigkeiten oder Abhängigkeiten anderer Kubernetes-Add-Ons, die Sie auf Ihrem Cluster ausführen, `nodeadm uninstall` nicht entfernt. Informationen zum vollständigen Entfernen der CNI-Installation von Ihrem Host finden Sie in den Anweisungen unter. [the section called “CNI konfigurieren”](#) Wenn Sie AWS SSM-Hybrid-Aktivierungen als Anbieter für lokale Anmeldeinformationen verwenden, werden Ihre Hosts mit dem `nodeadm uninstall` Befehl als SSM-verwaltete Instanzen deregistriert. AWS

### Usage

```
nodeadm uninstall [flags]
```

### Flags

| Name                                    | Erforderlich | Beschreibung                                                                                                                                                                                                                                                           |
|-----------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-s,</code><br><code>--skip</code> | FALSE        | Upgrade-Phasen müssen übersprungen werden. Es wird nicht empfohlen, eine der Phasen zu überspringen, es sei denn, dies hilft, ein Problem zu beheben.<br><br>Werte<br><br><code>pod-validation</code> überspringt die Überprüfung, ob alle Pods auf dem Knoten laufen, |



| Name                                    | Erforderlich | Beschreibung                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         |              | mit Ausnahme von Daemon-Sets und statischen Pods.<br><br><code>node-validation</code> überspringt die Überprüfung, ob der Knoten gesperrt wurde.<br><br><code>init-validation</code> überspringt die Überprüfung, ob der Knoten erfolgreich initialisiert wurde, bevor die Deinstallation ausgeführt wird. |
| <code>-h,</code><br><code>--help</code> | FALSE        | Zeigt eine Hilfmeldung mit den verfügbaren Parametern für Flaggen, Unterbefehle und Positionswerte an.                                                                                                                                                                                                     |

## Beispiele

```
nodeadm uninstall
```

```
nodeadm uninstall --skip node-validation,pod-validation
```

## nodeadm debug

Der `nodeadm debug` Befehl kann zur Fehlerbehebung bei fehlerhaften oder falsch konfigurierten Hybridknoten verwendet werden. Es bestätigt, dass die folgenden Anforderungen erfüllt sind.

- Der Knoten hat Netzwerkzugriff auf die zum Abrufen der AWS APIs Anmeldeinformationen erforderlichen
- Der Knoten ist in der Lage, AWS Anmeldeinformationen für die konfigurierte IAM-Rolle für Hybridknoten abzurufen.

- Der Knoten hat Netzwerkzugriff auf den EKS Kubernetes API-Endpunkt und die Gültigkeit des EKS Kubernetes API-Endpunktzertifikats,
- Der Knoten kann sich beim EKS-Cluster authentifizieren, seine Identität im Cluster ist gültig und der Knoten hat über die für den EKS-Cluster konfigurierte VPC Zugriff auf den EKS-Cluster.

Wenn Fehler gefunden werden, schlägt die Ausgabe des Befehls Schritte zur Fehlerbehebung vor. Bei bestimmten Validierungsschritten werden untergeordnete Prozesse angezeigt. Wenn diese fehlschlagen, wird die Ausgabe in einem stderr-Abschnitt unter dem Validierungsfehler angezeigt.

## Usage

```
nodeadm debug [flags]
```

## Flags

| Name                             | Erforderlich | Beschreibung                                                                                               |
|----------------------------------|--------------|------------------------------------------------------------------------------------------------------------|
| <code>-c, --config-source</code> | TRUE         | Quelle der Konfiguration.<br>nodeadm Bei Hybridknoten sollte die Eingabe einem URI mit Dateischema folgen. |
| <code>--no-color</code>          | FALSE        | Deaktiviert die Farbausgabe. Nützlich für die Automatisierung.                                             |
| <code>-h, --help</code>          | FALSE        | Zeigt eine Hilfmeldung mit verfügbaren Parametern für Flaggen, Unterbefehle und Positionswerte an.         |

## Beispiele

```
nodeadm debug -c file://nodeConfig.yaml
```

## Speicherorte von Nodeadm-Dateien

### nodeadm installieren

Bei der Ausführung werden `nodeadm install` die folgenden Dateien und Dateispeicherorte konfiguriert.

| Artefakt                              | Pfad                                                                                                                                                  |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| IAM-Rollen Anywhere CLI               | <code>/_signing_helper usr/local/bin/aws</code>                                                                                                       |
| Kubelet-Binärdatei                    | <code>/usr/bin/kubelet</code>                                                                                                                         |
| Kubectl-Binärdatei                    | <code>usr/local/bin/kubectl</code>                                                                                                                    |
| Anbieter von ECR-Anmeldeinformationen | <code>/-Anmeldeinformationsanbieter etc/eks/image-credential-provider/ecr</code>                                                                      |
| AWS IAM-Authentifikator               | <code>/-iam-Authentifikator usr/local/bin/aws</code>                                                                                                  |
| SSM-Setup-CLI                         | <code>/-setup-cli opt/ssm/ssm</code>                                                                                                                  |
| SSM-Agent                             | <p>Auf Ubuntu <code>/-ssm-agent snap/amazon-ssm-agent/current/amazon</code></p> <p>Auf RHEL &amp; AL2 023 <code>/-ssm-agent usr/bin/amazon</code></p> |
| In Containern                         | <p>Auf Ubuntu &amp; AL2 023 <code>/usr/bin/containerd</code></p> <p>Auf RHEL <code>/bin/containerd</code></p>                                         |
| Iptables                              | <p>Auf Ubuntu &amp; AL2 023 <code>/usr/sbin/iptables</code></p> <p>Auf RHEL <code>/sbin/iptables</code></p>                                           |
| CNI-Plug-ins                          | <code>/opt/cni/bin</code>                                                                                                                             |
| installierter Artefakt-Tracker        | <code>/opt/nodeadm/tracker</code>                                                                                                                     |

## nodeadm init

Bei der Ausführung werden `nodeadm init` die folgenden Dateien und Dateispeicherorte konfiguriert.

| Name                                                                       | Pfad                                                  |
|----------------------------------------------------------------------------|-------------------------------------------------------|
| Kubelet kubeconfig                                                         | /var/lib/kubelet/kubeconfig                           |
| Kubelet-Konfiguration                                                      | /.json etc/kubernetes/kubelet/config                  |
| Kubelet-Systemeinheit                                                      | /etc/systemd/system/kubelet.dienst                    |
| Konfiguration des Anbieters von Image-Anmeldeinformationen                 | /etc/eks/image-credential-provider/config.json        |
| Kubelet-Env-Datei                                                          | /etc/eks/kubelet/environment                          |
| Kubelet-Zertifikate                                                        | /etc/kubernetes/pki/ca.crt                            |
| Container-Konfiguration                                                    | /.toml etc/containerd/config                          |
| Konfiguration der containerten Kernelmodule                                | /.conf etc/modules-load.d/containerd                  |
| AWS Konfigurationsdatei                                                    | /etc/aws/hybrid/config                                |
| AWS Anmeldeinformationsdatei (wenn Anmeldeinformationsdatei aktiviert ist) | /eks-hybrid/.aws/credentials                          |
| AWS Helper-Systemeinheit signieren                                         | /etc/systemd/system/aws_signing_helper_update.service |
| Sysctl-Conf-Datei                                                          | /etc/sysctl.d/99-nodeadm.conf                         |
| CA-Zertifikate                                                             | /-certificates.crt etc/ssl/certs/ca                   |
| Gpg-Schlüsseldatei                                                         | /.asc etc/apt/keyrings/docker                         |
| Docker-Repo-Quelldatei                                                     | /.liste etc/apt/sources.list.d/docker                 |

## Knotenkonfiguration für SSM-Hybrid-Aktivierungen

Im Folgenden finden Sie ein Beispiel für die `nodeConfig.yaml` Verwendung von AWS SSM-Hybrid-Aktivierungen für Anmeldeinformationen für Hybridknoten.

```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: # Name of the EKS cluster
 region: # AWS Region where the EKS cluster resides
 hybrid:
 ssm:
 activationCode: # SSM hybrid activation code
 activationId: # SSM hybrid activation id
```

## Knotenkonfiguration für IAM-Rollen Anywhere

Im Folgenden finden Sie ein Beispiel `nodeConfig.yaml` für Anmeldeinformationen für AWS IAM Roles Anywhere für Hybridknoten.

Wenn `nodeName` Sie AWS IAM Roles Anywhere als Ihren lokalen Anbieter für Anmeldeinformationen verwenden, müssen die in Ihrer `nodeadm` Konfiguration verwendeten Berechtigungen mit den Berechtigungen übereinstimmen, die Sie für Ihre IAM-Rolle für Hybrid Nodes festgelegt haben. Wenn Ihre Berechtigungen für die IAM-Rolle Hybrid Nodes beispielsweise nur zulassen, dass AWS IAM Roles Anywhere die Rolle übernimmt, wenn der Name der Rollensitzung dem CN des Host-Zertifikats entspricht, muss der `nodeName` in Ihrer `nodeadm` Konfiguration dem CN Ihrer Zertifikate entsprechen. Das `nodeName`, was Sie verwenden, darf nicht länger als 64 Zeichen sein. Weitere Informationen finden Sie unter [the section called “Bereiten Sie die Anmeldeinformationen vor”](#).

```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: # Name of the EKS cluster
 region: # AWS Region where the EKS cluster resides
 hybrid:
 iamRolesAnywhere:
 nodeName: # Name of the node
 trustAnchorArn: # ARN of the IAM Roles Anywhere trust anchor
 profileArn: # ARN of the IAM Roles Anywhere profile
```

```

roleArn: # ARN of the Hybrid Nodes IAM role
certificatePath: # Path to the certificate file to authenticate with the IAM
Roles Anywhere trust anchor
privateKeyPath: # Path to the private key file for the certificate

```

## Node Config zum Anpassen von Kubelet (optional)

Sie können die Kubelet-Konfiguration und die Flags in Ihrer Konfiguration übergeben. `nodeadm` Im folgenden Beispiel erfahren Sie, wie Sie ein zusätzliches Knotenlabel `abc.amazonaws.com/test-label` und eine zusätzliche Konfiguration für die Einstellung `shutdownGracePeriod` auf 30 Sekunden hinzufügen.

```

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: # Name of the EKS cluster
 region: # AWS Region where the EKS cluster resides
 kubelet:
 config: # Map of kubelet config and values
 shutdownGracePeriod: 30s
 flags: # List of kubelet flags
 - --node-labels=abc.company.com/test-label=true
 hybrid:
 ssm:
 activationCode: # SSM hybrid activation code
 activationId: # SSM hybrid activation id

```

## Node Config zum Anpassen von containerd (optional)

Sie können eine benutzerdefinierte `containerd` in Ihrer `nodeadm` Konfiguration übergeben. Die Container-Konfiguration für `nodeadm` akzeptiert Inline-TOML. Im folgenden Beispiel erfahren Sie, wie Sie `containerd` so konfigurieren, dass das Löschen entpackter Bildebenen im `containerd` Content Store deaktiviert wird.

```

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: # Name of the EKS cluster
 region: # AWS Region where the EKS cluster resides

```

```

containerd:
 config: | # Inline TOML containerd additional configuration
 [plugins."io.containerd.grpc.v1.cri".containerd]
 discard_unpacked_layers = false
 hybrid:
 ssm:
 activationCode: # SSM hybrid activation code
 activationId: # SSM hybrid activation id

```

Sie können auch die Containerd-Konfiguration verwenden, um die SELinux Unterstützung zu aktivieren. Wenn diese Option auf containerd aktiviert ist, stellen Sie sicher, dass Pods, die auf dem Knoten geplant sind, den richtigen SecurityContext haben und selinuxOptions aktiviert sind. Weitere Informationen zur Konfiguration eines Sicherheitskontextes finden Sie in der [Kubernetes-Dokumentation](#).

#### Note

Red Hat Enterprise Linux (RHEL) 8 und RHEL 9 sind standardmäßig SELinux aktiviert und auf dem Host auf Strict gesetzt. Amazon Linux 2023 ist standardmäßig SELinux aktiviert und auf den permissiven Modus eingestellt. Wenn auf dem Host auf den permissiven Modus gesetzt SELinux ist, blockiert die Aktivierung auf containerd keine Anfragen, sondern protokolliert sie entsprechend der SELinux Konfiguration auf dem Host.

```

apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
 cluster:
 name: # Name of the EKS cluster
 region: # AWS Region where the EKS cluster resides
 containerd:
 config: | # Inline TOML containerd additional configuration
 [plugins."io.containerd.grpc.v1.cri"]
 enable_selinux = true
 hybrid:
 ssm:
 activationCode: # SSM hybrid activation code
 activationId: # SSM hybrid activation id

```

## Fehlerbehebung bei Hybridknoten

In diesem Thema werden einige häufig auftretende Fehler behandelt, die bei der Verwendung von Amazon EKS-Hybridknoten auftreten können, und deren Behebung. Weitere Informationen zur Fehlerbehebung finden Sie unter [Fehlerbehebung](#) und dem [Knowledge Center-Tag für Amazon EKS](#) auf AWS re:POST. Wenn Sie das Problem nicht lösen können, wenden Sie sich an den AWS Support.

Fehlerbehebung bei Knoten mit **nodeadm debug** Sie können den `nodeadm debug` Befehl von Ihren Hybridknoten aus ausführen, um zu überprüfen, ob die Netzwerk- und Anmeldeinformationen erfüllt sind. Weitere Informationen zu dem `nodeadm debug` Befehl finden Sie unter [the section called "Hybridknoten nodeadm"](#).

Erkennen Sie Probleme mit Ihren Hybridknoten mit Cluster-Einblicken Amazon EKS-Cluster-Insights umfasst Insight-Checks, mit denen häufig auftretende Probleme bei der Konfiguration von EKS-Hybridknoten in Ihrem Cluster erkannt werden. Sie können die Ergebnisse aller Insight-Checks über die AWS Management Console, AWS CLI und die anzeigen AWS SDKs. Weitere Informationen zu Cluster-Insights finden Sie unter [the section called "Cluster-Erkenntnisse"](#).

## Fehlerbehebung bei der Installation von Hybridknoten

Die folgenden Themen zur Fehlerbehebung beziehen sich auf die Installation der Abhängigkeiten von Hybridknoten auf Hosts mit dem `nodeadm install` Befehl.

### **nodeadm**Befehl ist fehlgeschlagen **must run as root**

Der `nodeadm install` Befehl muss mit einem Benutzer ausgeführt werden, der über `sudo` Root-Rechte oder Rechte auf Ihrem Host verfügt. Wenn Sie `nodeadm install` mit einem Benutzer ausführen, der weder über Root noch über `sudo` Rechte verfügt, wird in der `nodeadm` Ausgabe der folgende Fehler angezeigt.

```
"msg":"Command failed","error":"must run as root"
```

Es konnte keine Verbindung zu Abhängigkeiten hergestellt werden

Der `nodeadm install` Befehl installiert die für Hybridknoten erforderlichen Abhängigkeiten. Zu den Abhängigkeiten der Hybridknoten gehören `containerd`, `kubelet`, `kubect1`, und AWS SSM- oder AWS IAM Roles Anywhere-Komponenten. Sie benötigen Zugriff von Ihrem aktuellen Standort aus, um diese Abhängigkeiten herunterladen `nodeadm install` zu können. Weitere Informationen



zur Liste der Speicherorte, auf die Sie zugreifen können müssen, finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#). Wenn Sie keinen Zugriff haben, werden in der `nodeadm install` Ausgabe Fehler ähnlich den folgenden angezeigt.

```
"msg":"Command failed","error":"failed reading file from url: ...: max retries achieved for http request"
```

### Der Paketmanager konnte nicht aktualisiert werden

Der `nodeadm install` Befehl wird `apt update` `yum update` oder `dnf update` vor der Installation der Abhängigkeiten der Hybridknoten ausgeführt. Wenn dieser Schritt nicht erfolgreich ist, werden möglicherweise Fehler ähnlich den folgenden angezeigt. Um das Problem zu beheben, können Sie `apt update` oder `yum update` oder `dnf update` vor der Ausführung ausführen `nodeadm install` oder versuchen, die Ausführung erneut `nodeadm install` durchzuführen.

```
failed to run update using package manager
```

### Timeout oder Kontext-Frist überschritten

Wenn Sie bei der Ausführung in verschiedenen Phasen des Installationsvorgangs Probleme mit Fehlern feststellen `nodeadm install`, die darauf hindeuten, dass ein Timeout oder eine Kontextfrist überschritten wurde, haben Sie möglicherweise eine langsame Verbindung, wodurch verhindert wird, dass die Abhängigkeiten der Hybridknoten installiert werden, bevor die Timeouts eingehalten werden. Um diese Probleme zu umgehen, können Sie versuchen, das `--timeout` Flag in zu verwenden, `nodeadm` um die Dauer der Timeouts für das Herunterladen der Abhängigkeiten zu verlängern.

```
nodeadm install K8S_VERSION --credential-provider CRED_PROVIDER --timeout 20m0s
```

## Fehlerbehebung beim Verbinden von Hybridknoten

Die Themen zur Fehlerbehebung in diesem Abschnitt beziehen sich auf den Prozess der Verbindung von Hybridknoten mit EKS-Clustern mithilfe des `nodeadm init` Befehls.

### Betriebsfehler oder nicht unterstütztes Schema

Wenn Sie bei der Ausführung `nodeadm init` Fehler im Zusammenhang mit `operation error` oder `unsupported scheme` sehen, überprüfen Sie `nodeConfig.yaml`, ob das Dokument richtig

formatiert und an übergeben wurde. `nodeadm` Weitere Informationen zum Format und zu den Optionen für finden Sie `nodeConfig.yaml` unter [the section called “Hybridknoten nodeadm”](#).

```
"msg":"Command failed","error":"operation error ec2imds: GetRegion, request canceled, context deadline exceeded"
```

Für die IAM-Rolle „Hybrid Nodes“ fehlen die Berechtigungen für die **eks:DescribeCluster** Aktion.

`nodeadm` Versucht bei der Ausführung `nodeadm init`, Informationen über Ihren EKS-Cluster zu sammeln, indem `Describe Cluster` aufgerufen wird. Wenn Ihre IAM-Rolle Hybrid Nodes nicht über die Berechtigung für die `eks:DescribeCluster` Aktion verfügt. Weitere Informationen zu den erforderlichen Berechtigungen für die IAM-Rolle Hybrid Nodes finden Sie unter. [the section called “Bereiten Sie die Anmeldeinformationen vor”](#)

```
"msg":"Command failed","error":"operation error EKS: DescribeCluster, https response error StatusCode: 403 ... AccessDeniedException"
```

Die Knoten-IP befindet sich nicht im CIDR des Remote-Knoten-Netzwerks

Bei der Ausführung kann ein Fehler auftreten `nodeadm init`, wenn sich die IP-Adresse des Knotens nicht im angegebenen Remote-Knoten-Netzwerk CIDRs befindet. Der Fehler wird dem folgenden Beispiel ähneln:

```
node IP 10.18.0.1 is not in any of the remote network CIDR blocks [10.0.0.0/16 192.168.0.0/16]
```

Dieses Beispiel zeigt einen Knoten mit IP 10.18.0.1, der versucht, einem Cluster mit dem Remote-Netzwerk CIDRs 10.0.0.0/16 und 192.168.0.0/16 beizutreten. Der Fehler tritt auf, weil 10.18.0.1 in keinem der Bereiche liegt.

Vergewissern Sie sich, dass Sie Ihre Konfiguration so konfiguriert haben `RemoteNodeNetworks`, dass alle Knoten-IP-Adressen enthalten sind. Weitere Informationen zur Netzwerkkonfiguration finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#).

- Führen Sie den folgenden Befehl in der Region aus, in der sich Ihr Cluster befindet, um Ihre `RemoteNodeNetwork` Konfigurationen zu überprüfen. Stellen Sie sicher, dass die in der Ausgabe aufgeführten CIDR-Blöcke den IP-Bereich Ihres Knotens enthalten und mit den in der Fehlermeldung aufgeführten CIDR-Blöcken identisch sind. Wenn sie nicht

übereinstimmen, überprüfen Sie, ob der Clustername und die Region in Ihrem gewünschten Cluster `nodeConfig.yaml` übereinstimmen.

```
aws eks describe-cluster --name CLUSTER_NAME --region REGION_NAME --query
cluster.remoteNetworkConfig.remoteNodeNetworks
```

- Stellen Sie sicher, dass Sie mit dem vorgesehenen Knoten arbeiten:
  - Vergewissern Sie sich, dass Sie sich auf dem richtigen Knoten befinden, indem Sie überprüfen, ob dessen Hostname und IP-Adresse mit denen übereinstimmen, die Sie beim Cluster registrieren möchten.
  - Vergewissern Sie sich, dass sich dieser Knoten im richtigen lokalen Netzwerk befindet (dem, dessen CIDR-Bereich `RemoteNodeNetwork` bei der Clustereinrichtung registriert wurde).

Wenn Ihre Knoten-IP immer noch nicht Ihren Erwartungen entspricht, überprüfen Sie Folgendes:

- Wenn Sie IAM Roles Anywhere verwenden, führt `kubelet` eine DNS-Suche in IAM Roles Anywhere durch `nodeName` und verwendet eine dem Knotennamen zugeordnete IP, falls verfügbar. Wenn Sie DNS-Einträge für Ihre Knoten verwalten, stellen Sie sicher, dass diese Einträge auf IPs Ihr Remote-Knotennetzwerk verweisen. CIDRs
- Wenn Ihr Knoten über mehrere Netzwerkschnittstellen verfügt, wählen Sie `kubelet` möglicherweise standardmäßig eine Schnittstelle mit einer IP-Adresse außerhalb Ihres Remote-Knoten-Netzwerks CIDRs aus. Um eine andere Schnittstelle zu verwenden, geben Sie deren IP-Adresse mithilfe des `--node-ip` `kubelet` Kennzeichens in Ihrem `nodeConfig.yaml`. Weitere Informationen finden Sie unter [the section called "Hybridknoten nodeadm"](#). Sie können die Netzwerkschnittstellen und IP-Adressen Ihres Knotens anzeigen, indem Sie den folgenden Befehl auf Ihrem Knoten ausführen:

```
ip addr show
```

Hybridknoten werden im EKS-Cluster nicht angezeigt

Wenn Sie den Vorgang ausgeführt haben `nodeadm init` und der Vorgang abgeschlossen wurde, Ihre Hybridknoten jedoch nicht in Ihrem Cluster erscheinen, liegt möglicherweise ein Problem mit der Netzwerkverbindung zwischen Ihren Hybridknoten und der EKS-Steuerebene vor, Sie haben möglicherweise nicht die erforderlichen Sicherheitsgruppenberechtigungen konfiguriert, oder

Sie haben möglicherweise nicht die erforderliche Zuordnung Ihrer Hybrid Nodes IAM-Rolle zur Rollenbasierten Zugriffskontrolle von Kubernetes (RBAC). Sie können den Debugging-Vorgang starten, indem Sie den Status kubelet und die kubelet Protokolle mit den folgenden Befehlen überprüfen. Führen Sie die folgenden Befehle von den Hybridknoten aus, die Ihrem Cluster nicht beitreten konnten.

```
systemctl status kubelet
```

```
journalctl -u kubelet -f
```

### Kommunikation mit dem Cluster nicht möglich

Wenn Ihr Hybridknoten nicht mit der Cluster-Steuerebene kommunizieren konnte, werden Ihnen möglicherweise Protokolle angezeigt, die den folgenden ähneln.

```
"Failed to ensure lease exists, will retry" err="Get ..."
```

```
"Unable to register node with API server" err="Post ..."
```

```
Failed to contact API server when waiting for CSINode publishing ... dial tcp <ip address>: i/o timeout
```

Wenn Sie diese Meldungen sehen, überprüfen Sie Folgendes, um sicherzustellen, dass der Hybridknoten die unter aufgeführten Anforderungen erfüllt [the section called “Bereiten Sie das Netzwerk vor”](#).

- Vergewissern Sie sich, dass die an den EKS-Cluster übergebene VPC Routen zu Ihrem Transit Gateway (TGW) oder Virtual Private Gateway (VGW) für Ihren lokalen Knoten und optional Ihren Pod hat. CIDRs
- Vergewissern Sie sich, dass Sie über eine zusätzliche Sicherheitsgruppe für Ihren EKS-Cluster verfügen, die Regeln für eingehenden Datenverkehr für Ihren lokalen Knoten und optional für den Pod enthält. CIDRs CIDRs
- Vergewissern Sie sich, dass Ihr lokaler Router so konfiguriert ist, dass er Datenverkehr zur und von der EKS-Steuerebene zulässt.

### Nicht autorisiert

Wenn Ihr Hybridknoten mit der EKS-Steuerebene kommunizieren, sich aber nicht registrieren konnte, werden Ihnen möglicherweise Protokolle angezeigt, die den folgenden ähneln. Beachten Sie, dass der Hauptunterschied in den folgenden Protokollmeldungen der Unauthorized Fehler ist. Dies signalisiert, dass der Knoten seine Aufgaben nicht ausführen konnte, da er nicht über die erforderlichen Berechtigungen verfügt.

```
"Failed to ensure lease exists, will retry" err="Unauthorized"
```

```
"Unable to register node with API server" err="Unauthorized"
```

```
Failed to contact API server when waiting for CSINode publishing: Unauthorized
```

Wenn Sie diese Meldungen sehen, überprüfen Sie Folgendes, um sicherzustellen, dass er die Anforderungen für Hybridknoten erfüllt (siehe [the section called “Bereiten Sie die Anmeldeinformationen vor”](#) und) [the section called “Bereiten Sie den Clusterzugriff vor”](#).

- Vergewissern Sie sich, dass die Identität der Hybridknoten Ihrer erwarteten IAM-Rolle für Hybridknoten entspricht. Dies kann durch Ausführen von Ihren Hybridknoten `sudo aws sts get-caller-identity` aus erfolgen.
- Vergewissern Sie sich, dass Ihre IAM-Rolle für Hybrid Nodes über die erforderlichen Berechtigungen verfügt.
- Vergewissern Sie sich, dass Sie in Ihrem Cluster einen EKS-Zugriffseintrag für Ihre Hybrid Nodes IAM-Rolle haben, oder vergewissern Sie sich, dass Sie `aws-auth ConfigMap` einen Eintrag für Ihre Hybrid Nodes IAM-Rolle haben. Wenn Sie EKS-Zugriffseinträge verwenden, vergewissern Sie sich, dass Ihr Zugriffseintrag für Ihre IAM-Rolle für Hybrid Nodes den `HYBRID_LINUX` Zugriffstyp hat. Wenn Sie den verwenden, stellen Sie sicher `aws-auth ConfigMap`, dass Ihr Eintrag für die IAM-Rolle Hybrid Nodes die unter beschriebenen Anforderungen und Formatierungen erfüllt. [the section called “Bereiten Sie den Clusterzugriff vor”](#)

Hybridknoten sind beim EKS-Cluster registriert, zeigen aber den Status **Not Ready**

Wenn sich Ihre Hybridknoten erfolgreich bei Ihrem EKS-Cluster registriert haben, die Hybridknoten jedoch den Status anzeigen `Not Ready`, müssen Sie zunächst den Status Ihres Container Networking Interface (CNI) überprüfen. Wenn Sie kein CNI installiert haben, wird davon ausgegangen, dass Ihre Hybridknoten den Status haben. `Not Ready` Sobald ein CNI installiert ist und erfolgreich ausgeführt wird, werden die Knoten auf den Status aktualisiert. `Ready` Wenn Sie

versucht haben, ein CNI zu installieren, es aber nicht erfolgreich ausgeführt wird, finden Sie weitere Informationen [the section called “CNI-Fehlerbehebung bei Hybridknoten”](#) auf dieser Seite.

Anfragen zum Signieren von Zertifikaten (CSRs) bleiben hängen. Ausstehend

Wenn Sie nach dem Verbinden der Hybridknoten mit Ihrem EKS-Cluster feststellen, dass noch ausstehende Knoten CSRs für Ihre Hybridknoten vorliegen, erfüllen Ihre Hybridknoten nicht die Anforderungen für die automatische Genehmigung. CSRs für Hybridknoten werden automatisch genehmigt und ausgestellt, wenn die CSRs vier Hybridknoten von einem Knoten mit `eks.amazonaws.com/compute-type: hybrid` Bezeichnung erstellt wurden und der CSR die folgenden alternativen Subject Names (SANs) hat: mindestens ein DNS-SAN, das dem Knotennamen und der IP entspricht, SANs gehört zum Netzwerk CIDRs des Remote-Knotens.

Das Hybridprofil ist bereits vorhanden

Wenn Sie Ihre `nodeadm` Konfiguration geändert haben und versuchen, den Knoten mit der neuen Konfiguration erneut zu registrieren, wird möglicherweise eine Fehlermeldung angezeigt, die besagt, dass das Hybridprofil bereits existiert, sein Inhalt sich jedoch geändert hat. Anstatt die Ausführung `nodeadm init` zwischen den Konfigurationsänderungen durchzuführen, führen Sie den Befehl aus, `nodeadm uninstall` gefolgt von einem und `nodeadm install nodeadm init`. Dadurch wird gewährleistet, dass die Änderungen in der Konfiguration ordnungsgemäß bereinigt werden.

```
"msg":"Command failed","error":"hybrid profile already exists at /etc/aws/hybrid/config but its contents do not align with the expected configuration"
```

Der Hybridknoten konnte die private API nicht auflösen

Wenn Sie nach der Ausführung einen Fehler in den `kubelet` Protokollen sehen `nodeadm init`, der darauf hinweist, dass keine Verbindung zum EKS Kubernetes API-Server hergestellt werden konnte, weil dies der Fall ist `no such host`, müssen Sie möglicherweise Ihren DNS-Eintrag für den EKS Kubernetes API-Endpunkt in Ihrem lokalen Netzwerk oder auf Host-Ebene ändern. Weitere Informationen finden Sie [in der AWS Route53-Dokumentation unter Weiterleiten eingehender DNS-Abfragen an Ihre VPC](#).

```
Failed to contact API server when waiting for CSINode publishing: Get ... no such host
```

Hybridknoten können in der EKS-Konsole nicht angezeigt werden

Wenn Sie Ihre Hybridknoten registriert haben, sie aber nicht in der EKS-Konsole anzeigen können, überprüfen Sie die Berechtigungen des IAM-Prinzipals, den Sie zum Anzeigen der Konsole

verwenden. Der von Ihnen verwendete IAM-Prinzipal muss über bestimmte IAM- und Kubernetes-Mindestberechtigungen verfügen, um Ressourcen in der Konsole anzeigen zu können. Weitere Informationen finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

## Fehlerbehebung beim Ausführen von Hybridknoten

Wenn Ihre Hybridknoten bei Ihrem EKS-Cluster registriert wurden, einen Status Ready hatten und dann in den Status übergegangen sind `Not Ready`, gibt es eine Vielzahl von Problemen, die zu dem fehlerhaften Status beigetragen haben könnten, z. B. wenn dem Knoten nicht genügend Ressourcen für CPU, Arbeitsspeicher oder verfügbaren Festplattenspeicher fehlen oder der Knoten von der EKS-Steuerebene getrennt ist. Sie können die folgenden Schritte verwenden, um Probleme mit Ihren Knoten zu beheben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an den AWS Support.

Führen Sie die Ausführung `nodeadm debug` von Ihren Hybridknoten aus, um zu überprüfen, ob die Netzwerk- und Anmeldeinformationsanforderungen erfüllt sind. Weitere Informationen zu diesem `nodeadm debug` Befehl finden Sie unter [the section called “Hybridknoten nodeadm”](#).

Rufen Sie den Knotenstatus ab

```
kubectl get nodes -o wide
```

Überprüfen Sie die Bedingungen und Ereignisse des Knotens

```
kubectl describe node NODE_NAME
```

Pod-Status abrufen

```
kubectl get pods -A -o wide
```

Überprüfe die Bedingungen und Ereignisse des Pods

```
kubectl describe pod POD_NAME
```

Überprüfe die Pod-Logs

```
kubectl logs POD_NAME
```

## Überprüfe die **kubect1** Logs

```
systemctl status kubelet
```

```
journalctl -u kubelet -f
```

Tests zur Verfügbarkeit von Pods schlagen fehl oder Webhooks funktionieren nicht

Wenn Anwendungen, Add-Ons oder Webhooks, die auf Ihren Hybridknoten ausgeführt werden, nicht ordnungsgemäß gestartet werden, haben Sie möglicherweise Netzwerkprobleme, die die Kommunikation mit den Pods blockieren. Damit die EKS-Steuerebene Webhooks kontaktieren kann, die auf Hybridknoten ausgeführt werden, müssen Sie Ihren EKS-Cluster mit einem Remote-Pod-Netzwerk konfigurieren und Routen für Ihren lokalen Pod-CIDR in Ihrer VPC-Routingtabelle haben, wobei das Ziel Ihr Transit Gateway (TGW), Virtual Private Gateway (VPW) oder ein anderes Gateway ist, das Sie verwenden, um Ihre VPC mit Ihrem lokalen Netzwerk zu verbinden. Weitere Informationen zu den Netzwerkanforderungen für Hybridknoten finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#). Sie müssen diesen Datenverkehr außerdem in Ihrer lokalen Firewall zulassen und sicherstellen, dass Ihr Router ordnungsgemäß zu Ihren Pods weiterleiten kann. Weitere Informationen zu den Anforderungen [the section called “Webhooks konfigurieren”](#) für die Ausführung von Webhooks auf Hybridknoten finden Sie unter.

Im Folgenden wird eine häufig vorkommende Pod-Log-Meldung für dieses Szenario angezeigt, wobei die IP-Adresse die Cluster-IP für den Kubernetes-Dienst ist.

```
dial tcp <ip-address>:443: connect: no route to host
```

## **kubect1 logs**oder Befehle funktionieren **kubect1 exec** nicht

Wenn bei `kubect1 logs kubect1 exec` Oder-Befehlen ein Timeout auftritt, während andere `kubect1` Befehle erfolgreich sind, liegt das Problem wahrscheinlich an der Remote-Netzwerkconfiguration. Diese Befehle stellen über den Cluster eine Verbindung zum `kubelet` Endpunkt auf dem Knoten her. Weitere Informationen finden Sie unter [the section called “kubelet-Endpunkt”](#).

Stellen Sie sicher, dass Ihr Knoten IPs und Ihr IPs Pod in das für Ihren Cluster CIDRs konfigurierte Remote-Knoten-Netzwerk und das Remote-Pod-Netzwerk gehören. Verwenden Sie die folgenden Befehle, um IP-Zuweisungen zu überprüfen.



```
kubectl get nodes -o wide
```

```
kubectl get pods -A -o wide
```

Vergleichen Sie diese IPs mit Ihrem konfigurierten Remote-Netzwerk CIDRs , um sicherzustellen, dass das Routing korrekt ist. Informationen zu den Anforderungen an die Netzwerkkonfiguration finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#).

## CNI-Fehlerbehebung bei Hybridknoten

Wenn Sie Probleme beim ersten Start von Cilium oder Calico mit Hybridknoten haben, ist dies meistens auf Netzwerkprobleme zwischen Hybridknoten oder den auf Hybridknoten laufenden CNI-Pods und der EKS-Steuerebene zurückzuführen. Stellen Sie sicher, dass Ihre Umgebung die Anforderungen unter Netzwerk für Hybridknoten vorbereiten erfüllt. Es ist nützlich, das Problem in einzelne Teile zu zerlegen.

### EKS-Cluster-Konfiguration

Sind die RemotePodNetwork Konfigurationen RemoteNodeNetwork und korrekt?

### VPC-Konfiguration

Gibt es Routen für das RemoteNodeNetwork und RemotePodNetwork in der VPC-Routingtabelle mit dem Ziel des Transit Gateway oder Virtual Private Gateways?

### Sicherheitsgruppenkonfiguration

Gibt es Regeln für eingehenden und ausgehenden Datenverkehr? RemoteNodeNetwork  
RemotePodNetwork

### Lokales Netzwerk

Gibt es Routen und Zugänge zur und von der EKS-Steuerebene sowie zu und von den Hybridknoten und den Pods, die auf Hybridknoten ausgeführt werden?

### CNI-Konfiguration

Stimmt bei Verwendung eines Overlay-Netzwerks die IP-Pool-Konfiguration für das CNI mit der für den EKS-Cluster RemotePodNetwork konfigurierten Konfiguration überein, wenn Webhooks verwendet werden?

Der Hybridknoten hat den Status, dass kein CNI **Ready** installiert ist

Wenn Ihre Hybridknoten den Status anzeigen Ready, Sie aber kein CNI auf Ihrem Cluster installiert haben, ist es möglich, dass auf Ihren Hybridknoten alte CNI-Artefakte vorhanden sind. Wenn Sie Cilium und Calico mit Tools wie Helm deinstallieren, werden die Festplattenressourcen standardmäßig nicht von Ihren physischen oder virtuellen Maschinen entfernt. Darüber hinaus sind die benutzerdefinierten Ressourcendefinitionen (CRDs) für diese CNIs möglicherweise noch aus einer alten Installation auf Ihrem Cluster vorhanden. Weitere Informationen finden Sie in den Abschnitten [Delete Cilium](#) und [Delete Calico](#) von [the section called "CNI konfigurieren"](#).

## Fehlerbehebung bei Cilium

Wenn Sie Probleme beim Ausführen von Cilium auf Hybridknoten haben, lesen Sie [die Schritte zur Fehlerbehebung in der](#) Cilium-Dokumentation. In den folgenden Abschnitten werden Probleme behandelt, die möglicherweise nur bei der Bereitstellung von Cilium auf Hybridknoten auftreten.

### Cilium startet nicht

Wenn die Cilium-Agenten, die auf den einzelnen Hybridknoten ausgeführt werden, nicht starten, überprüfen Sie die Protokolle der Cilium-Agent-Pods auf Fehler. Der Cilium-Agent benötigt zum Starten eine Verbindung zum EKS-Kubernetes-API-Endpunkt. Der Start des Cilium-Agenten schlägt fehl, wenn diese Konnektivität nicht korrekt konfiguriert ist. In diesem Fall werden Ihnen in den Pod-Protokollen des Cilium-Agenten Protokollmeldungen ähnlich den folgenden angezeigt.

```
msg="Unable to contact k8s api-server"
level=fatal msg="failed to start: Get \"https://<k8s-cluster-ip>:443/api/v1/namespaces/
kube-system\": dial tcp <k8s-cluster-ip>:443: i/o timeout"
```

Der Cilium-Agent wird im Host-Netzwerk ausgeführt. Ihr EKS-Cluster muss RemoteNodeNetwork für die Cilium-Konnektivität konfiguriert sein. Vergewissern Sie sich, dass Sie eine zusätzliche Sicherheitsgruppe für Ihren EKS-Cluster mit einer eingehenden Regel für Ihren RemoteNodeNetwork haben, dass Sie Routen in Ihrer VPC für Ihren RemoteNodeNetwork haben und dass Ihr lokales Netzwerk korrekt konfiguriert ist RemoteNodeNetwork, um Konnektivität mit der EKS-Steuerebene zu ermöglichen.

Wenn der Cilium-Operator läuft und einige Ihrer Cilium-Agenten laufen, aber nicht alle, stellen Sie sicher, dass Sie über einen verfügbaren Pod verfügen, den Sie allen Knoten in Ihrem Cluster IPs zuweisen können. Sie konfigurieren die Größe Ihres zuweisbaren Pods, CIDRs wenn Sie den Clusterpool IPAM mit in Ihrer Cilium-Konfiguration verwenden. `clusterPoolIPv4PodCIDRList` Die CIDR-Größe pro Knoten wird mit der Einstellung in Ihrer Cilium-Konfiguration konfiguriert.

`clusterPoolIPv4MaskSize` Weitere Informationen finden Sie in [der Cilium-Dokumentation unter Erweiterung des Cluster-Pools](#).

## Cilium BGP funktioniert nicht

Wenn Sie Cilium BGP Control Plane verwenden, um Ihre Pod- oder Serviceadressen in Ihrem lokalen Netzwerk bekannt zu geben, können Sie die folgenden Cilium-CLI-Befehle verwenden, um zu überprüfen, ob BGP die Routen zu Ihren Ressourcen ankündigt. Schritte zur Installation der Cilium-CLI finden [Sie unter Installieren der Cilium-CLI in der Cilium-Dokumentation](#).

Wenn BGP ordnungsgemäß funktioniert, sollten Sie Ihre Hybridknoten mit dem Sitzungsstatus `established` in der Ausgabe versehen. Möglicherweise müssen Sie mit Ihrem Netzwerkteam zusammenarbeiten, um die richtigen Werte für das lokale AS, das Peer-AS und die Peer-Adresse Ihrer Umgebung zu ermitteln.

```
cilium bgp peers
```

```
cilium bgp routes
```

Wenn Sie Cilium BGP verwenden, um die IPs Dienste mit Typ `LoadBalancer` zu bewerben, müssen Sie sowohl auf Ihrem `CiliumLoadBalancerIPPool` als auch auf dem Service dieselbe Bezeichnung haben, die in der Auswahl Ihres Dienstes verwendet werden sollte. `CiliumBGPAdvertisement` Es folgt ein Beispiel. Hinweis: Wenn Sie Cilium BGP verwenden, um die Dienste mit Typ `LoadBalancer` zu bewerben, können die BGP-Routen während IPs des Neustarts des Cilium-Agenten unterbrochen werden. Weitere Informationen finden Sie in der Cilium-Dokumentation unter [Ausfallszenarien](#).

## Service

```
kind: Service
apiVersion: v1
metadata:
 name: guestbook
 labels:
 app: guestbook
spec:
 ports:
 - port: 3000
 targetPort: http-server
 selector:
```

```
app: guestbook
type: LoadBalancer
```

## CiliumLoadBalancerIPPool

```
apiVersion: cilium.io/v2alpha1
kind: CiliumLoadBalancerIPPool
metadata:
 name: guestbook-pool
 labels:
 app: guestbook
spec:
 blocks:
 - cidr: <CIDR to advertise>
 serviceSelector:
 matchExpressions:
 - { key: app, operator: In, values: [guestbook] }
```

## CiliumBGPAdvertisement

```
apiVersion: cilium.io/v2alpha1
kind: CiliumBGPAdvertisement
metadata:
 name: bgp-advertisements-guestbook
 labels:
 advertise: bgp
spec:
 advertisements:
 - advertisementType: "Service"
 service:
 addresses:
 - ExternalIP
 - LoadBalancerIP
 selector:
 matchExpressions:
 - { key: app, operator: In, values: [guestbook] }
```

## Calico-Fehlerbehebung

Wenn Sie Probleme beim Ausführen von Calico auf Hybridknoten haben, lesen Sie [die Schritte zur Fehlerbehebung in der](#) Calico-Dokumentation. In den folgenden Abschnitten werden Probleme behandelt, die möglicherweise nur bei der Bereitstellung von Calico auf Hybridknoten auftreten.

Die folgende Tabelle fasst die Calico-Komponenten zusammen und gibt an, ob sie standardmäßig im Knoten- oder Pod-Netzwerk ausgeführt werden. Wenn Sie Calico so konfiguriert haben, dass NAT für ausgehenden Pod-Verkehr verwendet wird, muss Ihr lokales Netzwerk so konfiguriert sein, dass der Verkehr an Ihren lokalen Node CIDR weitergeleitet wird, und Ihre VPC-Routing-Tabellen müssen mit einer Route für Ihren lokalen Node CIDR mit Ihrem Transit Gateway (TGW) oder Virtual Private Gateway (VGW) als Ziel konfiguriert sein. Wenn Sie Calico nicht so konfigurieren, dass NAT für ausgehenden Pod-Verkehr verwendet wird, muss Ihr lokales Netzwerk so konfiguriert sein, dass es den Verkehr zu Ihrem lokalen Pod-CIDR weiterleitet, und Ihre VPC-Routing-Tabellen müssen mit einer Route für Ihren lokalen Pod-CIDR mit Ihrem Transit Gateway (TGW) oder Virtual Private Gateway (VGW) als Ziel konfiguriert werden.

| Komponente                       | Netzwerk |
|----------------------------------|----------|
| Calico API-Server                | Knoten   |
| Calico Controller für Kubernetes | Pod      |
| Calico-Knotenagent               | Knoten   |
| Calico typha                     | Knoten   |
| Calico CSI-Knotentreiber         | Pod      |
| Calico-Betreiber                 | Knoten   |

Calico-Ressourcen sind geplant oder werden auf gesperrten Knoten ausgeführt

Die Calico-Ressourcen, die nicht als A ausgeführt werden, DaemonSet verfügen standardmäßig über flexible Toleranzen, sodass sie auf gesperrten Knoten geplant werden können, die noch nicht für die Planung oder Ausführung von Pods bereit sind. Sie können die Toleranzen für Ressourcen, die nicht zu DaemonSet Calico gehören, verschärfen, indem Sie Ihre Betreiberinstallation dahingehend ändern, dass sie Folgendes beinhaltet.

```
installation:
 ...
 controlPlaneTolerations:
 - effect: NoExecute
 key: node.kubernetes.io/unreachable
 operator: Exists
```

```
tolerationSeconds: 300
- effect: NoExecute
 key: node.kubernetes.io/not-ready
 operator: Exists
 tolerationSeconds: 300
calicoKubeControllersDeployment:
 spec:
 template:
 spec:
 tolerations:
 - effect: NoExecute
 key: node.kubernetes.io/unreachable
 operator: Exists
 tolerationSeconds: 300
 - effect: NoExecute
 key: node.kubernetes.io/not-ready
 operator: Exists
 tolerationSeconds: 300
typhaDeployment:
 spec:
 template:
 spec:
 tolerations:
 - effect: NoExecute
 key: node.kubernetes.io/unreachable
 operator: Exists
 tolerationSeconds: 300
 - effect: NoExecute
 key: node.kubernetes.io/not-ready
 operator: Exists
 tolerationSeconds: 300
```

## Fehlerbehebung bei Anmeldedaten

Sowohl bei AWS SSM-Hybrid-Aktivierungen als auch bei AWS IAM Roles Anywhere können Sie überprüfen, ob die Anmeldeinformationen für die IAM-Rolle Hybrid Nodes auf Ihren Hybridknoten korrekt konfiguriert sind, indem Sie den folgenden Befehl von Ihren Hybridknoten aus ausführen. Vergewissern Sie sich, dass der Knotenname und der Name der IAM-Rolle der Hybridknoten Ihren Erwartungen entsprechen.

```
sudo aws sts get-caller-identity
```

```
{
 "UserId": "ABCDEFGHJKLM12345678910:<node-name>",
 "Account": "<aws-account-id>",
 "Arn": "arn:aws:sts:<aws-account-id>:assumed-role/<hybrid-nodes-iam-role>/<node-name>"
}
```

## AWS Problembehebung bei Systems Manager (SSM)

Wenn Sie AWS SSM-Hybrid-Aktivierungen für Ihre Anmeldeinformationen für Hybridknoten verwenden, beachten Sie die folgenden SSM-Verzeichnisse und -Artefakte, die auf Ihren Hybridknoten von installiert werden. `nodeadm` Weitere Informationen zum SSM-Agenten finden Sie unter [Arbeiten mit dem SSM-Agenten](#) im AWS Systems Manager Manager-Benutzerhandbuch.

| Beschreibung         | Ort                                                                                                                           |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| SSM-Agent            | Ubuntu — <code>/snap/amazon-ssm-agent/current/amazon-ssm-agent</code> RHEL & 023 — AL2 <code>/usr/bin/amazon-ssm-agent</code> |
| SSM-Agent-Protokolle | <code>/var/log/amazon/ssm</code>                                                                                              |
| AWS Referenzen       | <code>/root/.aws/credentials</code>                                                                                           |
| SSM-Setup-CLI        | <code>/opt/ssm/ssm-setup-cli</code>                                                                                           |

### Den SSM-Agenten neu starten

Einige Probleme können durch einen Neustart des SSM-Agenten behoben werden. Sie können die folgenden Befehle verwenden, um ihn neu zu starten.

#### AL20.23 und andere Betriebssysteme

```
systemctl restart amazon-ssm-agent
```

#### Ubuntu

```
systemctl restart snap.amazon-ssm-agent.amazon-ssm-agent
```

## Überprüfen Sie die Konnektivität zu SSM-Endpunkten

Stellen Sie sicher, dass Sie von Ihren Hybridknoten aus eine Verbindung zu den SSM-Endpunkten herstellen können. Eine Liste der SSM-Endpunkte finden Sie unter [AWS Systems Manager Manager-Endpunkte](#) und Kontingente. Ersetzen Sie `us-west-2` den Befehl unten durch die AWS Region für Ihre AWS SSM-Hybrid-Aktivierung.

```
ping ssm.us-west-2.amazonaws.com
```

## Den Verbindungsstatus registrierter SSM-Instanzen anzeigen

Sie können den Verbindungsstatus der Instances, die mit SSM-Hybrid-Aktivierungen registriert sind, mit dem folgenden AWS CLI-Befehl überprüfen. Ersetzen Sie die Maschinen-ID durch die Maschinen-ID Ihrer Instanz.

```
aws ssm get-connection-status --target mi-012345678abcdefgh
```

## SSM-Setup-CLI-Prüfsumme stimmt nicht überein

`nodeadm install` Wenn Sie bei der Ausführung ein Problem mit der Nichtübereinstimmung der `ssm-setup-cli` Prüfsumme feststellen, sollten Sie sicherstellen, dass auf Ihrem Host keine älteren SSM-Installationen vorhanden sind. Wenn auf Ihrem Host ältere SSM-Installationen vorhanden sind, entfernen Sie diese und führen Sie sie erneut `nodeadm install` aus, um das Problem zu beheben.

```
Failed to perform agent-installation/on-prem registration: error while verifying
installed ssm-setup-cli checksum: checksum mismatch with latest ssm-setup-cli.
```

## SSM **InvalidActivation**

Wenn Sie einen Fehler bei der Registrierung Ihrer Instance bei AWS SSM sehen, überprüfen Sie, ob die `regionactivationCode`, und `activationId` in Ihrem richtig `nodeConfig.yaml` sind. Die AWS Region für Ihren EKS-Cluster muss mit der Region Ihrer SSM-Hybrid-Aktivierung übereinstimmen. Wenn diese Werte falsch konfiguriert sind, wird möglicherweise ein Fehler ähnlich dem folgenden angezeigt.

```
ERROR Registration failed due to error registering the instance with AWS SSM.
InvalidActivation
```



**SSMExpiredTokenException:** Das in der Anfrage enthaltene Sicherheitstoken ist abgelaufen

Wenn der SSM-Agent die Anmeldeinformationen nicht aktualisieren kann, wird möglicherweise eine `ExpiredTokenException` angezeigt. Wenn Sie in diesem Szenario von Ihren Hybridknoten aus eine Verbindung zu den SSM-Endpunkten herstellen können, müssen Sie möglicherweise den SSM-Agent neu starten, um eine Aktualisierung der Anmeldeinformationen zu erzwingen.

```
"msg":"Command failed","error":"operation error SSM: DescribeInstanceInformation, https response error StatusCode: 400, RequestID: eee03a9e-f7cc-470a-9647-73d47e4cf0be, api error ExpiredTokenException: The security token included in the request is expired"
```

**SSM-Fehler beim Ausführen des Befehls `register machine`**

Wenn bei der Registrierung des Computers bei SSM ein Fehler auftritt, müssen Sie den Computer möglicherweise erneut ausführen, `nodeadm install` um sicherzustellen, dass alle SSM-Abhängigkeiten ordnungsgemäß installiert sind.

```
"error":"running register machine command: , error: fork/exec /opt/aws/ssm-setup-cli: no such file or directory"
```

**SSM `ActivationExpired`**

Wenn Sie bei der Ausführung `nodeadm init` aufgrund einer abgelaufenen Aktivierung einen Fehler bei der Registrierung der Instance bei SSM sehen, müssen Sie eine neue SSM-Hybrid-Aktivierung erstellen, Ihre `nodeConfig.yaml` mit dem Ende Ihrer neuen SSM-Hybrid-Aktivierung aktualisieren und `activationCode` und `activationId` erneut ausführen. `nodeadm init`

```
"msg":"Command failed","error":"SSM activation expired. Please use a valid activation"
```

```
ERROR Registration failed due to error registering the instance with AWS SSM.
ActivationExpired
```

**SSM konnte die zwischengespeicherten Anmeldeinformationen nicht aktualisieren**

Wenn Sie feststellen, dass die zwischengespeicherten Anmeldeinformationen nicht aktualisiert werden können, wurde die `/root/.aws/credentials` Datei möglicherweise auf Ihrem Host gelöscht. Überprüfen Sie zunächst Ihre SSM-Hybrid-Aktivierung und stellen Sie sicher, dass sie aktiv ist und dass Ihre Hybridknoten korrekt konfiguriert sind, um die Aktivierung zu verwenden. Überprüfen

Sie die SSM-Agent-Protokolle unter `/var/log/amazon/ssm` und führen Sie den `nodeadm init` Befehl erneut aus, sobald Sie das Problem auf der SSM-Seite behoben haben.

```
"Command failed","error":"operation error SSM: DescribeInstanceInformation, get identity: get credentials: failed to refresh cached credentials"
```

## Bereinigen Sie SSM

Um den SSM-Agenten von Ihrem Host zu entfernen, können Sie die folgenden Befehle ausführen.

```
dnf remove -y amazon-ssm-agent
sudo apt remove --purge amazon-ssm-agent
snap remove amazon-ssm-agent
rm -rf /var/lib/amazon/ssm/Vault/Store/RegistrationKey
```

## AWS Fehlerbehebung bei IAM Roles Anywhere

Wenn Sie AWS IAM Roles Anywhere für Ihre Anmeldeinformationen für Hybridknoten verwenden, beachten Sie die folgenden Verzeichnisse und Artefakte, die auf Ihren Hybridknoten von installiert werden. `nodeadm` Weitere Informationen zur Problembehandlung bei IAM Roles Anywhere finden Sie unter [Problembehandlung bei Identität und Zugriff auf AWS IAM Roles Anywhere](#) im AWS IAM Roles Anywhere-Benutzerhandbuch.

| Beschreibung                                 | Ort                                            |
|----------------------------------------------|------------------------------------------------|
| IAM-Rollen Anywhere CLI                      | <code>/usr/local/bin/aws_signing_helper</code> |
| Speicherort und Name des Standardzertifikats | <code>/etc/iam/pki/server.pem</code>           |
| Standardspeicherort und Name des Schlüssels  | <code>/etc/iam/pki/server.key</code>           |

IAM Roles Anywhere konnte die zwischengespeicherten Anmeldeinformationen nicht aktualisieren

Wenn Sie feststellen, dass die Aktualisierung der zwischengespeicherten Anmeldeinformationen fehlschlägt, überprüfen Sie den Inhalt von `/etc/aws/hybrid/config` und stellen Sie sicher, dass IAM Roles Anywhere in Ihrer Konfiguration korrekt konfiguriert wurde. `nodeadm` Vergewissern Sie sich, dass das existiert `/etc/iam/pki`. Jeder Knoten muss über ein eindeutiges Zertifikat und einen eindeutigen Schlüssel verfügen. Wenn Sie IAM Roles Anywhere als Anmeldeinformationsanbieter

verwenden, nodeadm verwendet dies standardmäßig `/etc/iam/pki/server.pem` für den Speicherort und den Namen des Zertifikats sowie `/etc/iam/pki/server.key` für den privaten Schlüssel. Möglicherweise müssen Sie die Verzeichnisse erstellen, bevor Sie die Zertifikate und Schlüssel in den Verzeichnissen mit platzieren können. `sudo mkdir -p /etc/iam/pki` Sie können den Inhalt Ihres Zertifikats mit dem folgenden Befehl überprüfen.

```
openssl x509 -text -noout -in server.pem
```

```
open /etc/iam/pki/server.pem: no such file or directory
could not parse PEM data
Command failed {"error": "... get identity: get credentials: failed to refresh cached
credentials, process provider error: error in credential_process: exit status 1"}
```

### IAM Roles Anywhere ist zur Ausführung nicht autorisiert **sts:AssumeRole**

Wenn Sie in den kubelet Protokollen das Problem „Zugriff verweigert“ für den `sts:AssumeRole` Vorgang bei der Verwendung von IAM Roles Anywhere sehen, überprüfen Sie die Vertrauensrichtlinie Ihrer IAM-Rolle für Hybrid Nodes, um sicherzustellen, dass der IAM Roles Anywhere-Dienstprinzipal die IAM-Rolle für Hybrid Nodes übernehmen darf. Vergewissern Sie sich außerdem, dass der Trust Anchor ARN in Ihrer IAM-Rollenvertrauensrichtlinie für Hybrid Nodes ordnungsgemäß konfiguriert ist und dass Ihre Hybrid Nodes IAM-Rolle zu Ihrem IAM Roles Anywhere-Profil hinzugefügt wurde.

```
could not get token: AccessDenied: User: ... is not authorized to perform:
sts:AssumeRole on resource: ...
```

### IAM Roles Anywhere ist nicht zur Einstellung autorisiert **roleSessionName**

Wenn Sie in den kubelet Protokollen ein Problem mit der Einstellung von „Zugriff verweigert“ sehen, vergewissern Sie sich `roleSessionName`, dass Sie für Ihr IAM `acceptRoleSessionName` Roles Anywhere-Profil die Einstellung auf „true“ gesetzt haben.

```
AccessDeniedException: Not authorized to set roleSessionName
```

## Fehlerbehebung beim Betriebssystem

### RHEL

#### Fehler bei der Registrierung des Berechtigungs- oder Abonnement-Managers

Falls Sie das Programm ausführen `nodeadm install` und bei der Installation der Abhängigkeiten der Hybridknoten aufgrund von Problemen mit der Berechtigungsregistrierung ein Fehler auftritt, stellen Sie sicher, dass Sie Ihren RedHat-Benutzernamen und Ihr Passwort auf Ihrem Host korrekt eingerichtet haben.

```
This system is not registered with an entitlement server
```

## Ubuntu

### GLIBC wurde nicht gefunden

Wenn Sie Ubuntu für Ihr Betriebssystem und IAM Roles Anywhere für Ihren Anmeldeinformationsanbieter mit Hybridknoten verwenden und feststellen, dass ein Problem mit GLIBC nicht gefunden wurde, können Sie diese Abhängigkeit manuell installieren, um das Problem zu beheben.

```
GLIBC_2.32 not found (required by /usr/local/bin/aws_signing_helper)
```

Führen Sie die folgenden Befehle aus, um die Abhängigkeit zu installieren:

```
ldd --version
sudo apt update && apt install libc6
sudo apt install glibc-source
```

## Bottlerocket

Wenn Sie den Bottlerocket-Admin-Container aktiviert haben, können Sie mit SSH auf ihn zugreifen, um erweiterte Debugging- und Fehlerbehebungsmaßnahmen mit erhöhten Rechten durchzuführen. Die folgenden Abschnitte enthalten Befehle, die im Kontext des Bottlerocket-Hosts ausgeführt werden müssen. Sobald Sie sich im Admin-Container befinden, können Sie ausführen, `sheltie` um eine vollständige Root-Shell im Bottlerocket-Host zu erhalten.

```
sheltie
```

Sie können die Befehle in den folgenden Abschnitten auch von der Admin-Container-Shell aus ausführen, indem Sie jedem Befehl ein Präfix voranstellen. `sudo chroot /.bottlerocket/rootfs`

```
sudo chroot /.bottlerocket/rootfs <command>
```

## Logdog für die Protokollsammlung verwenden

Bottlerocket bietet das logdog Tool zum effizienten Sammeln von Protokollen und Systeminformationen zur Fehlerbehebung.

```
logdog
```

Das logdog Hilfsprogramm sammelt Logs von verschiedenen Orten auf einem Bottlerocket-Host und kombiniert sie zu einem Tarball. Standardmäßig wird der Tarball unter `/var/log/support/bottlerocket-logs.tar.gz` erstellt und ist von den Host-Containern `/var/log/support/bottlerocket-logs.tar.gz` aus zugänglich.

Mit journalctl auf Systemprotokolle zugreifen

Mit den folgenden Befehlen können Sie den Status der verschiedenen Systemdienste wie kubeletcontainerd, usw. überprüfen und deren Protokolle einsehen. Die -f Flagge folgt den Protokollen in Echtzeit.

Um den kubelet Dienststatus zu überprüfen und kubelet Protokolle abzurufen, können Sie Folgendes ausführen:

```
systemctl status kubelet
journalctl -u kubelet -f
```

Um den containerd Dienststatus zu überprüfen und die Protokolle für die orchestrierte containerd Instanz abzurufen, können Sie Folgendes ausführen:

```
systemctl status containerd
journalctl -u containerd -f
```

Um den host-containerd Dienststatus zu überprüfen und die Protokolle für die containerd Host-Instanz abzurufen, können Sie Folgendes ausführen:

```
systemctl status host-containerd
journalctl -u host-containerd -f
```

Um die Protokolle für die Bootstrap-Container und Host-Container abzurufen, können Sie Folgendes ausführen:

```
journalctl _COMM=host-ctr -f
```

# Verwenden Sie Anwendungsdatenspeicher für Ihren Cluster

Sie können mit Amazon EKS eine Reihe von AWS Speicherservices für die Speicheranforderungen Ihrer Anwendungen nutzen. Durch eine Vielzahl von AWS unterstützten Container Storage Interface (CSI) -Treibern können Sie Amazon EBS, Amazon S3, Amazon EFS, Amazon FSx und Amazon File Cache problemlos für die Speicheranforderungen Ihrer auf Amazon EKS ausgeführten Anwendungen verwenden.

In diesem Kapitel werden Speicheroptionen für Amazon EKS-Cluster behandelt.

## Themen

- [Verwenden Sie Kubernetes-Volumenspeicher mit Amazon EBS](#)
- [Verwenden Sie elastischen Dateisystemspeicher mit Amazon EFS](#)
- [Verwenden Sie leistungsstarken App-Speicher mit Amazon FSx for Lustre](#)
- [Verwenden Sie leistungsstarken App-Speicher mit FSx für NetApp ONTAP](#)
- [Datenspeicher mit Amazon FSx für OpenZFS verwenden](#)
- [Minimierung der Latenz mit Amazon File Cache](#)
- [Greifen Sie mit dem Mountpoint for Amazon S3 CSI-Treiber auf Amazon S3-Objekte zu](#)
- [Snapshot-Funktionalität für CSI-Volumes aktivieren](#)

## Verwenden Sie Kubernetes-Volumenspeicher mit Amazon EBS

### Note

Neu: Der automatische Modus von Amazon EKS automatisiert Routineaufgaben für Blockspeicher. Weitere Informationen erhalten Sie unter [the section called “Stellen Sie einen statusbehafteten Work”](#).

Der [Container Storage Interface \(CSI\) -Treiber für Amazon Elastic Block Store \(Amazon EBS\)](#) verwaltet den Lebenszyklus von Amazon EBS-Volumes als Speicher für die von Ihnen erstellten Kubernetes-Volumes. [Der Amazon EBS CSI-Treiber erstellt Amazon EBS-Volumes für diese Typen von Kubernetes-Volumes: generische ephemere Volumes und persistente Volumes.](#)

## Überlegungen

- Sie müssen den Amazon EBS CSI-Controller nicht auf EKS-Auto-Mode-Clustern installieren.
- Sie können Amazon EBS-Volumes nicht auf Fargate Pods mounten.
- Sie können den Amazon EBS CSI-Controller auf Fargate-Knoten ausführen, aber der Amazon EBS CSI-Knoten DaemonSet kann nur auf Amazon-Instances ausgeführt werden. EC2
- Amazon EBS-Volumes und der Amazon EBS CSI-Treiber sind nicht mit Amazon EKS-Hybridknoten kompatibel.
- Support wird für die neueste Add-On-Version und eine frühere Version bereitgestellt. In der neuesten Version gefundene Fehler oder Sicherheitslücken werden in einer neuen Nebenversion auf die vorherige Version zurückportiert.
- Für den automatischen Modus von EKS müssen Speicherklassen `ebs.csi.eks.amazonaws.com` als Provisioner verwendet werden. Der standardmäßige Amazon EBS CSI Driver (`ebs.csi.aws.com`) verwaltet seine eigenen Volumes separat. Um vorhandene Volumes mit dem automatischen EKS-Modus zu verwenden, migrieren Sie sie mithilfe von Volume-Snapshots zu einer Speicherklasse, die den Auto Mode-Provisioner verwendet.

### Important

Um die Snapshot-Funktionalität des Amazon EBS CSI-Treibers nutzen zu können, müssen Sie zuerst den CSI-Snapshot-Controller installieren. Weitere Informationen finden Sie unter [the section called “CSI-Snapshot-Controller”](#).

## Voraussetzungen

- Einen vorhandenen -Cluster. Führen Sie den folgenden Befehl aus, um die erforderliche Plattformversion anzuzeigen.

```
aws eks describe-addon-versions --addon-name aws-ebs-csi-driver
```

- Der EBS-CSI-Treiber benötigt AWS IAM-Berechtigungen.
  - AWS schlägt vor, EKS Pod Identities zu verwenden. Weitere Informationen finden Sie unter [the section called “Übersicht über die Einrichtung von EKS-Pod-Identitäten”](#).



- Informationen zu IAM-Rollen für Dienstkonten finden Sie unter [the section called “IAM OIDC-Anbieter”](#)

## Schritt 1: Erstellen einer IAM-Rolle

Das Amazon EBS CSI-Plugin benötigt IAM-Berechtigungen, um in Ihrem Namen Anrufe tätigen AWS APIs zu können. Wenn Sie diese Schritte nicht ausführen, `kubectl describe pvc` wird beim Versuch, das Add-on zu installieren und es auszuführen, eine `failed to provision volume with StorageClass could not create volume in EC2: UnauthorizedOperation` Fehlermeldung angezeigt. Weitere Informationen finden Sie unter [Treiberberechtigung einrichten](#) auf GitHub.

### Note

Pods haben Zugriff auf die Berechtigungen, die der IAM-Rolle zugewiesen sind, sofern Sie den Zugriff auf IMDS nicht blockieren. Weitere Informationen finden Sie unter [the section called “Bewährte Methoden”](#).

Das folgende Verfahren zeigt Ihnen, wie Sie eine IAM-Rolle erstellen und ihr die AWS verwaltete Richtlinie zuordnen. Um dieses Verfahren zu implementieren, können Sie eines der folgenden Tools verwenden:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)
- [the section called “AWS CLI”](#)

### Note

Die spezifischen Schritte in diesem Verfahren sind für die Verwendung des Treibers als Amazon-EKS-Add-on geschrieben. Es sind verschiedene Schritte erforderlich, um den Treiber als selbstverwaltetes Add-on zu verwenden. Weitere Informationen finden Sie unter [Fahrerberechtigungen einrichten](#) für GitHub.

## eksctl

1. Erstellen Sie eine IAM-Rolle und fügen Sie eine Richtlinie hinzu. AWS verwaltet eine AWS verwaltete Richtlinie oder Sie können Ihre eigene benutzerdefinierte Richtlinie erstellen. Sie können eine IAM-Rolle erstellen und die AWS verwaltete Richtlinie mit dem folgenden Befehl anhängen. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Der Befehl stellt einen AWS CloudFormation Stack bereit, der eine IAM-Rolle erstellt und ihr die IAM-Richtlinie anhängt.

```
eksctl create iamserviceaccount \
 --name ebs-csi-controller-sa \
 --namespace kube-system \
 --cluster my-cluster \
 --role-name AmazonEKS_EBS_CSI_DriverRole \
 --role-only \
 --attach-policy-arn arn:aws:iam::aws:policy/service-role/
AmazonEBSCSIDriverPolicy \
 --approve
```

2. [Sie können diesen Schritt überspringen, wenn Sie keinen benutzerdefinierten KMS-Schlüssel verwenden.](#) Wenn Sie eine für die Verschlüsselung auf Ihren Amazon EBS-Volumes verwenden, passen Sie die IAM-Rolle nach Bedarf an. Führen Sie beispielsweise folgende Schritte aus:
  - a. Kopieren Sie den folgenden Code und fügen Sie diesen in eine neue `kms-key-for-encryption-on-ebs.json`-Datei ein. Ersetzen Sie *custom-key-arn* durch den benutzerdefinierten [KMS-Schlüssel-ARN](#).

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kms:CreateGrant",
 "kms:ListGrants",
 "kms:RevokeGrant"
],
 "Resource": ["custom-key-arn"],
 "Condition": {
 "Bool": {
 "kms:GrantIsForAWSResource": "true"
 }
 }
 }
]
}
```

```
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": ["custom-key-arn"]
 }
]
}
```

- b. Erstellen Sie die Richtlinie. Sie können *KMS\_Key\_For\_Encryption\_On\_EBS\_Policy* in einen anderen Namen ändern. In diesem Fall ändern Sie sie auch in den späteren Schritten.

```
aws iam create-policy \
 --policy-name KMS_Key_For_Encryption_On_EBS_Policy \
 --policy-document file://kms-key-for-encryption-on-ebs.json
```

- c. Hängen Sie die IAM-Richtlinie mit dem folgenden Befehl an die Rolle an. Ersetzen Sie *111122223333* durch Ihre Konto-ID.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::111122223333:policy/KMS_Key_For_Encryption_On_EBS_Policy \
 --role-name AmazonEKS_EBS_CSI_DriverRole
```

## AWS Management Console

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
  - a. Wählen Sie im Abschnitt Trusted entity type (Typ der vertrauenswürdigen Entität) die Option Web identity (Web-Identität) aus.

- b. Wählen Sie für Identity provider (Identitätsanbieter) die Option OpenID Connect provider URL (OpenID-Connect-Anbieter-URL) für Ihren Cluster aus (wie unter Overview (Übersicht) in Amazon EKS gezeigt).
  - c. Wählen Sie für Audience (Zielgruppe) `sts.amazonaws.com`.
  - d. Wählen Sie Weiter aus.
5. Gehen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) wie folgt vor:
  - a. Geben Sie im Feld Filter policies (Filterrichtlinien) `AmazonEBS CSI Driver Policy` ein.
  - b. Aktivieren Sie das Kontrollkästchen links neben der `AmazonEBS CSI Driver Policy`, die bei der Suche zurückgegeben wurde.
  - c. Wählen Sie Weiter aus.
6. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
  - a. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. *`AmazonEKS_EBS_CSI_DriverRole`*.
  - b. Fügen Sie der Rolle unter Tags hinzufügen (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Markieren von IAM-Ressourcen](#) im IAM-Benutzerhandbuch.
  - c. Wählen Sie Create role (Rolle erstellen) aus.
7. Nachdem die Rolle erstellt wurde, wählen Sie die Rolle in der Konsole aus, um sie zur Bearbeitung zu öffnen.
8. Wählen Sie die Registerkarte Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
9. Suchen Sie die Zeile, die der folgenden Zeile ähnelt:

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud":
 "sts.amazonaws.com"
```

Fügen Sie am Ende der vorherigen Zeile ein Komma hinzu und fügen Sie anschließend die folgende Zeile nach der vorherigen Zeile hinzu. Ersetzen Sie *region-code* durch die AWS Region, in der sich Ihr Cluster befindet. *EXAMPLED539D4633E53DE1B71EXAMPLE* Ersetzen Sie es durch die OIDC-Anbieter-ID Ihres Clusters.

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub":
 "system:serviceaccount:kube-system:ebs-csi-controller-sa"
```

10. Wählen Sie Update Policy (Richtlinie aktualisieren) aus, um den Vorgang abzuschließen.
11. Wenn Sie einen benutzerdefinierten [KMS-Schlüssel](#) für die Verschlüsselung auf Ihren Amazon-EBS-Volumes verwenden, passen Sie die IAM-Rolle nach Bedarf an. Führen Sie beispielsweise folgende Schritte aus:
- Wählen Sie im linken Navigationsbereich die Option Policies aus.
  - Wählen Sie auf der Seite Policies (Richtlinien) die Option Create a policy (Richtlinie erstellen).
  - Wählen Sie auf der Seite Create policy (Richtlinie erstellen) die Registerkarte JSON aus.
  - Kopieren Sie den folgenden Code in den Editor und ersetzen Sie *custom-key-arn* durch den benutzerdefinierten [KMS-Schlüssel-ARN](#):

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kms:CreateGrant",
 "kms:ListGrants",
 "kms:RevokeGrant"
],
 "Resource": ["custom-key-arn"],
 "Condition": {
 "Bool": {
 "kms:GrantIsForAWSResource": "true"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": ["custom-key-arn"]
 }
]
}
```

- e. Wählen Sie Next: Markierungen (Weiter: Markierungen).
- f. Wählen Sie auf der Seite Add Tags (optional) (Tags hinzufügen (optional)) die Option Next: Review (Weiter: Prüfen).
- g. Geben Sie unter Name einen eindeutigen Namen für Ihre Richtlinie ein (z. B. *KMS\_Key\_For\_Encryption\_On\_EBS\_Policy*).
- h. Wählen Sie Create Policy (Richtlinie erstellen) aus.
- i. Wählen Sie im linken Navigationsbereich Roles aus.
- j. Wählen Sie das *AmazonEKS\_EBS\_CSI\_DriverRole* in der Konsole aus, um es zur Bearbeitung zu öffnen.
- k. Wählen Sie in der Dropdown-Liste Add permissions (Berechtigungen hinzufügen) Attach policies (Richtlinien hinzufügen) aus.
- l. Geben Sie im Feld Filter policies (Filterrichtlinien) *KMS\_Key\_For\_Encryption\_On\_EBS\_Policy* ein.
- m. Aktivieren Sie das Kontrollkästchen links neben der *KMS\_Key\_For\_Encryption\_On\_EBS\_Policy*, die bei der Suche zurückgegeben wurde.
- n. Wählen Sie Attach Policies (Richtlinien hinzufügen).

## AWS CLI

1. Sehen Sie sich die OIDC-Provider-URL Ihres Clusters an. Ersetzen Sie *my-cluster* durch Ihren Clusternamen. Wenn die Ausgabe des Befehls None ist, überprüfen Sie die Voraussetzungen.

```
aws eks describe-cluster --name my-cluster --query "cluster.identity.oidc.issuer" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
https://oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE
```

2. Erstellen Sie die IAM-Rolle und gewähren Sie ihr die AssumeRoleWithWebIdentity-Aktion.
  - a. Kopieren Sie den folgenden Inhalt in eine Datei mit dem Namen `aws-ebs-csi-driver-trust-policy.json`. Ersetzen Sie *111122223333* durch Ihre Konto-ID. Ersetzen Sie *EXAMPLED539D4633E53DE1B71EXAMPLE* und *region-code* mit den im vorherigen Schritt zurückgegebenen Werten.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Federated": "arn:aws:iam::111122223333:oidc-provider/
oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
 },
 "Action": "sts:AssumeRoleWithWebIdentity",
 "Condition": {
 "StringEquals": {
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:efs-csi-
controller-sa"
 }
 }
 }
]
}
```

- b. Erstellen Sie die -Rolle. Sie können *AmazonEKS\_EBS\_CSI\_DriverRole* in einen anderen Namen ändern. Wenn Sie es ändern, ändern Sie es in späteren Schritten.

```
aws iam create-role \
 --role-name AmazonEKS_EBS_CSI_DriverRole \
 --assume-role-policy-document file://aws-efs-csi-driver-trust-policy.json"
```

3. Hängen Sie eine Richtlinie an. AWS verwaltet eine AWS verwaltete Richtlinie oder Sie können Ihre eigene benutzerdefinierte Richtlinie erstellen. Hängen Sie die AWS verwaltete Richtlinie mit dem folgenden Befehl an die Rolle an.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBS_CSI_DriverPolicy \
 --role-name AmazonEKS_EBS_CSI_DriverRole
```

4. Wenn Sie einen benutzerdefinierten [KMS-Schlüssel](#) für die Verschlüsselung auf Ihren Amazon-EBS-Volumes verwenden, passen Sie die IAM-Rolle nach Bedarf an. Führen Sie beispielsweise folgende Schritte aus:

- a. Kopieren Sie den folgenden Code und fügen Sie diesen in eine neue `kms-key-for-encryption-on-ebs.json`-Datei ein. Ersetzen Sie *custom-key-arn* durch den benutzerdefinierten [KMS-Schlüssel-ARN](#).

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kms:CreateGrant",
 "kms:ListGrants",
 "kms:RevokeGrant"
],
 "Resource": ["custom-key-arn"],
 "Condition": {
 "Bool": {
 "kms:GrantIsForAWSResource": "true"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": ["custom-key-arn"]
 }
]
}
```

- b. Erstellen Sie die Richtlinie. Sie können *KMS\_Key\_For\_Encryption\_On\_EBS\_Policy* in einen anderen Namen ändern. In diesem Fall ändern Sie sie auch in den späteren Schritten.

```
aws iam create-policy \
 --policy-name KMS_Key_For_Encryption_On_EBS_Policy \
 --policy-document file://kms-key-for-encryption-on-ebs.json
```



- c. Hängen Sie die IAM-Richtlinie mit dem folgenden Befehl an die Rolle an. Ersetzen Sie **111122223333** durch Ihre Konto-ID.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::111122223333:policy/
 KMS_Key_For_Encryption_On_EBS_Policy \
 --role-name AmazonEKS_EBS_CSI_DriverRole
```

Nachdem Sie die IAM-Rolle des Amazon EBS CSI-Treibers erstellt haben, können Sie mit dem nächsten Abschnitt fortfahren. Wenn Sie das Add-on mit dieser IAM-Rolle bereitstellen, erstellt es ein benanntes Dienstkonto und ist für dessen Verwendung konfiguriert. `ebs-csi-controller-sa` Das Dienstkonto ist an ein Kubernetes-Konto gebunden, dem `clusterrole` die erforderlichen Kubernetes-Berechtigungen zugewiesen wurden.

## Schritt 2: Holen Sie sich den Amazon EBS CSI-Treiber

Wir empfehlen, den Amazon EBS CSI-Treiber über das Amazon EKS-Add-on zu installieren, um die Sicherheit zu verbessern und den Arbeitsaufwand zu reduzieren. Wenn Sie ein Amazon-EKS-Add-on zu Ihrem Cluster hinzufügen möchten, lesen Sie [the section called “Erstellen Sie ein Add-on”](#). Weitere Informationen zu Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

### Important

Bevor Sie den Amazon EBS-Treiber als Amazon EKS-Add-on hinzufügen, stellen Sie sicher, dass Sie keine selbstverwaltete Version des Treibers auf Ihrem Cluster installiert haben. Falls ja, siehe [Deinstallation eines selbstverwalteten Amazon-EBS-CSI-Treibers](#) in GitHub.

Wenn Sie alternativ eine selbstverwaltete Installation des Amazon EBS CSI-Treibers wünschen, finden Sie weitere Informationen unter [Installation](#) auf GitHub.

## Schritt 3: Stellen Sie eine Beispielanwendung bereit

Sie können eine Vielzahl von Beispiel-Apps bereitstellen und diese nach Bedarf ändern. Weitere Informationen finden Sie unter [Kubernetes-Beispiele](#) unter GitHub.

# Verwenden Sie elastischen Dateisystemspeicher mit Amazon EFS

[Amazon Elastic File System](#) (Amazon EFS) bietet vollständig elastischen Serverless-Dateispeicher, sodass Sie Dateidaten gemeinsam nutzen können, ohne Speicherkapazität und Leistung bereitstellen oder verwalten zu müssen. Der [Amazon EFS Container Storage Interface \(CSI\) -Treiber](#) bietet eine CSI-Schnittstelle, über die Kubernetes-Cluster ausgeführt werden, AWS um den Lebenszyklus von Amazon EFS-Dateisystemen zu verwalten. In diesem Thema erfahren Sie, wie Sie den Amazon-EFS-CSI-Treiber für Ihren Amazon-EKS-Cluster bereitstellen.

## Überlegungen

- Der Amazon EFS CSI-Treiber ist nicht mit Windows-basierten Container-Images kompatibel.
- Sie können keine [dynamische Bereitstellung](#) für persistente Volumes mit Fargate-Knoten verwenden, aber Sie können [statische](#) Bereitstellung verwenden.
- Für die [dynamische Bereitstellung](#) ist der Treiber [1.2](#) oder höher erforderlich. Sie können die [statische Bereitstellung](#) für persistente Volumes verwenden, indem Sie die Version 1.1 des Treibers auf jeder unterstützten Amazon EKS-Cluster-Version verwenden (siehe [the section called "Kubernetes-Versionen"](#)).
- Version [1.3.2](#) oder höher dieses Treibers unterstützt die Arm64-Architektur, einschließlich Amazon EC2 Graviton-basierter Instances.
- Version [1.4.2](#) oder höher dieses Treibers unterstützt die Verwendung von FIPS zum Mounten von Dateisystemen.
- Beachten Sie die Ressourcenkontingente für Amazon EFS. Beispielsweise gibt es ein Kontingent von 1000 Access Points, die für jedes Amazon EFS-Dateisystem erstellt werden können. Weitere Informationen finden Sie unter [Amazon-EFS-Ressourcenkontingente, die Sie nicht ändern können](#).
- Ab Version [2.0.0](#) wurde dieser Treiber nicht mehr für TLS-Verbindungen verwendet, sondern nur noch `stunnel efs-proxy` für TLS-Verbindungen verwendet. Wenn er verwendet `efs-proxy` wird, öffnet er eine Anzahl von Threads, die einem plus der Anzahl der Kerne für den Knoten entspricht, auf dem er läuft.
- Der Amazon EFS CSI-Treiber ist nicht mit Amazon EKS-Hybridknoten kompatibel.

## Voraussetzungen

- Der Amazon EFS CSI-Treiber benötigt AWS Identity and Access Management (IAM) - Berechtigungen.

- AWS schlägt vor, EKS Pod Identities zu verwenden. Weitere Informationen finden Sie unter [the section called “Übersicht über die Einrichtung von EKS-Pod-Identitäten”](#).
- Informationen zu IAM-Rollen für Dienstkonten und zum Einrichten eines IAM OpenID Connect (OIDC) -Anbieters für Ihren Cluster finden Sie unter [the section called “IAM OIDC-Anbieter”](#)
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie yumapt-get, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Das kubectl-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie kubectl-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von kubectl finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).

#### Note

Ein Pod, der auf Fargate läuft, mountet automatisch ein Amazon EFS-Dateisystem, ohne dass manuelle Schritte zur Treiberinstallation erforderlich sind.

## Schritt 1: Erstellen einer IAM-Rolle

Der Amazon-EFS-CSI-Treiber benötigt IAM-Berechtigungen, um mit Ihrem Dateisystem zu interagieren. Erstellen Sie eine IAM-Rolle und fügen Sie ihr die erforderliche AWS verwaltete Richtlinie hinzu. Um dieses Verfahren zu implementieren, können Sie eines der folgenden Tools verwenden:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

- [the section called “AWS CLI”](#)

### Note

Die spezifischen Schritte in diesem Verfahren sind für die Verwendung des Treibers als Amazon-EKS-Add-on geschrieben. Ausführliche Informationen zu selbstverwalteten Installationen finden Sie auf GitHub unter [Set up driver permission](#).

## eksctl

Wenn Sie Pod Identities verwenden

Führen Sie die folgenden Befehle aus, um eine IAM-Rolle und eine Pod-Identity-Zuordnung zu erstellen. `eksctl` Ersetzen Sie `my-cluster` mit Ihrem Clusternamen. Sie können es auch durch einen anderen Namen `AmazonEKS_EFS_CSI_DriverRole` ersetzen.

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
eksctl create podidentityassociation \
 --service-account-name efs-csi-controller-sa \
 --namespace kube-system \
 --cluster $cluster_name \
 --role-name $role_name \
 --permission-policy-arns arn:aws:iam::aws:policy/service-role/
AmazonEFSCSIDriverPolicy
```

Wenn Sie IAM-Rollen für Dienstkonten verwenden

Führen Sie die folgenden Befehle aus, um eine IAM-Rolle mit zu erstellen. `eksctl` Ersetzen Sie `my-cluster` mit Ihrem Clusternamen. Sie können es auch durch einen anderen Namen `AmazonEKS_EFS_CSI_DriverRole` ersetzen.

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
eksctl create iamserviceaccount \
 --name efs-csi-controller-sa \
 --namespace kube-system \
 --cluster $cluster_name \
```

```

--role-name $role_name \
--role-only \
--attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy
\
--approve
TRUST_POLICY=$(aws iam get-role --output json --role-name $role_name --query
'Role.AssumeRolePolicyDocument' | \
sed -e 's/efs-csi-controller-sa/efs-csi-*/' -e 's/StringEquals/StringLike/')
aws iam update-assume-role-policy --role-name $role_name --policy-document
"$TRUST_POLICY"

```

## AWS Management Console

Führen Sie den folgenden Befehl aus, um eine IAM-Rolle mit AWS Management Console zu erstellen.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
  - a. Wenn Sie EKS Pod Identities verwenden:
    - i. Wählen Sie im Abschnitt Vertrauenswürdiger Entitätstyp die Option AWS Service aus.
    - ii. Wählen Sie in der Dropdownliste Dienst oder Anwendungsfall die Option EKS aus.
    - iii. Wählen Sie im Abschnitt „Anwendungsfall“ die Option EKS — Pod Identity aus.
    - iv. Wählen Sie Weiter aus.
  - b. Wenn Sie IAM-Rollen für Dienstkonten verwenden:
    - i. Wählen Sie im Abschnitt Trusted entity type (Typ der vertrauenswürdigen Entität) die Option Web identity (Web-Identität) aus.
    - ii. Wählen Sie für Identity provider (Identitätsanbieter) die Option OpenID Connect provider URL (OpenID-Connect-Anbieter-URL) für Ihren Cluster aus (wie unter Overview (Übersicht) in Amazon EKS gezeigt).
    - iii. Wählen Sie für Audience (Zielgruppe) sts.amazonaws.com.
    - iv. Wählen Sie Weiter aus.
5. Gehen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) wie folgt vor:
  - a. Geben Sie im Feld Filter policies (Filterrichtlinien) AmazonEFSCSIDriverPolicy ein.

- b. Aktivieren Sie das Kontrollkästchen links neben der `AmazonEFSCSIDriverPolicy`, die bei der Suche zurückgegeben wurde.
  - c. Wählen Sie Weiter aus.
6. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
  - a. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. `AmazonEKS_EFS_CSI_DriverRole`.
  - b. Fügen Sie der Rolle unter Tags hinzufügen (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Markieren von IAM-Ressourcen](#) im IAM-Benutzerhandbuch.
  - c. Wählen Sie Rolle erstellen aus.
7. Nachdem die Rolle erstellt wurde:
  - a. Wenn Sie EKS Pod Identities verwenden:
    - i. Öffnen Sie die [Amazon-EKS-Konsole](#).
    - ii. Wählen Sie im linken Navigationsbereich Clusters und dann den Namen des Clusters aus, für den Sie die EKS Pod Identity-Zuordnung konfigurieren möchten.
    - iii. Wählen Sie die Registerkarte Zugriff aus.
    - iv. Wählen Sie unter Pod Identity-Zuordnungen die Option Create aus.
    - v. Wählen Sie das Drop-down-Menü für die IAM-Rolle und wählen Sie Ihre neu erstellte Rolle aus.
    - vi. Wählen Sie das Feld Kubernetes-Namespace und geben Sie es ein. `kube-system`
    - vii. Wählen Sie das Feld Kubernetes-Dienstkonto und geben Sie es ein. `efs-csi-controller-sa`
    - viii. Wählen Sie Erstellen aus.
    - ix. Weitere Informationen zum Erstellen von Pod Identity-Verknüpfungen finden Sie unter [the section called "Erstellen Sie eine Pod Identity-Zuordnung \(Konsole\)AWS"](#)
  - b. Wenn Sie IAM-Rollen für Dienstkonto verwenden:
    - i. Wählen Sie die Rolle aus, um sie zur Bearbeitung zu öffnen.
    - ii. Wählen Sie die Registerkarte Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
    - iii. Suchen Sie die Zeile, die der folgenden Zeile ähnelt:

```
"oidc.eks.region-code.amazonaws.com/id/<EXAMPLED539D4633E53DE1B71EXAMPLE>:aud":
"sts.amazonaws.com"
```

Fügen Sie die folgende Zeile über der vorherigen Zeile hinzu. <region-code> Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. <EXAMPLED539D4633E53DE1B71EXAMPLE> Ersetzen Sie es durch die OIDC-Anbieter-ID Ihres Clusters.

```
"oidc.eks.<region-code>.amazonaws.com/id/
<EXAMPLED539D4633E53DE1B71EXAMPLE>:sub": "system:serviceaccount:kube-system:efs-
csi-*",
```

- iv. Ändern Sie den Condition-Operator von "StringEquals" zu "StringLike".
- v. Wählen Sie Update Policy (Richtlinie aktualisieren) aus, um den Vorgang abzuschließen.

## AWS CLI

Führen Sie die folgenden Befehle aus, um eine IAM-Rolle mit AWS CLI zu erstellen.

Wenn Sie Pod-Identitäten verwenden

1. Erstellen Sie die IAM-Rolle, die dem Dienst die AssumeRole und TagSession -Aktionen gewährt. pods.eks.amazonaws.com
  - a. Kopieren Sie den folgenden Inhalt in eine Datei namens aws-efs-csi-driver-trust-policy-pod-identity.json.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "AllowEksAuthToAssumeRoleForPodIdentity",
 "Effect": "Allow",
 "Principal": {
 "Service": "pods.eks.amazonaws.com"
 },
 "Action": [
 "sts:AssumeRole",
 "sts:TagSession"
]
 }
]
}
```

```
 }
]
}
```

- b. Erstellen Sie die -Rolle. Ersetzen Sie `my-cluster` mit Ihrem Clusternamen. Sie können den Namen auch `AmazonEKS_EFS_CSI_DriverRole` durch einen anderen Namen ersetzen.

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
aws iam create-role \
 --role-name $role_name \
 --assume-role-policy-document file://"aws-efs-csi-driver-trust-policy-pod-identity.json"
```

2. Fügen Sie der Rolle mit dem folgenden Befehl die erforderliche AWS verwaltete Richtlinie hinzu.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
 --role-name $role_name
```

3. Führen Sie den folgenden Befehl aus, um die Pod Identity-Zuordnung zu erstellen. `arn:aws:iam::<111122223333>:role/my-role` Ersetzen Sie diese durch die Rolle, die Sie in den vorherigen Schritten erstellt haben.

```
aws eks create-pod-identity-association --cluster-name $cluster_name --role-arn {arn-aws}iam::<111122223333>:role/my-role --namespace kube-system --service-account efs-csi-controller-sa
```

4. Weitere Informationen zum Erstellen von Pod Identity-Zuordnungen finden Sie unter [the section called “Erstellen Sie eine Pod Identity-Zuordnung \(Konsole\)AWS”](#).

Wenn Sie IAM-Rollen für Dienstkonto verwenden

1. Sehen Sie sich die OIDC-Provider-URL Ihres Clusters an. Ersetzen Sie `my-cluster` mit Ihrem Clusternamen. Sie können sie auch durch einen anderen Namen `AmazonEKS_EFS_CSI_DriverRole` ersetzen.

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
```



```
aws eks describe-cluster --name $cluster_name --query "cluster.identity.oidc.issuer"
--output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
https://oidc.eks.<region-code>.amazonaws.com/id/<EXAMPLED539D4633E53DE1B71EXAMPLE>
```

Wenn die Ausgabe des Befehls None ist, überprüfen Sie die Voraussetzungen.

## 2. Erstellen Sie die IAM-Rolle, die die Aktion AssumeRoleWithWebIdentity erlaubt.

- a. Kopieren Sie den folgenden Inhalt in eine Datei namens `aws-efs-csi-driver-trust-policy.json`. Ersetzen Sie `<111122223333>` durch Ihre Konto-ID. Ersetzen Sie `<EXAMPLED539D4633E53DE1B71EXAMPLE>` und `<region-code>` mit den im vorherigen Schritt zurückgegebenen Werten.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Federated": "arn:aws:iam::<111122223333>:oidc-provider/oidc.eks.<region-code>.amazonaws.com/id/<EXAMPLED539D4633E53DE1B71EXAMPLE>"
 },
 "Action": "sts:AssumeRoleWithWebIdentity",
 "Condition": {
 "StringLike": {
 "oidc.eks.region-code.amazonaws.com/id/<EXAMPLED539D4633E53DE1B71EXAMPLE>:sub": "system:serviceaccount:kube-system:efs-csi-*",
 "oidc.eks.region-code.amazonaws.com/id/<EXAMPLED539D4633E53DE1B71EXAMPLE>:aud": "sts.amazonaws.com"
 }
 }
 }
]
}
```

- b. Erstellen Sie die -Rolle.

```
aws iam create-role \
--role-name $role_name \
```

```
--assume-role-policy-document file://"aws-efs-csi-driver-trust-policy.json"
```

3. Fügen Sie der Rolle mit dem folgenden Befehl die erforderliche AWS verwaltete Richtlinie hinzu.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
 --role-name $role_name
```

## Schritt 2: Holen Sie sich den Amazon EFS CSI-Treiber

Wir empfehlen, den Amazon-EFS-CSI-Treiber über das Amazon-EKS-Add-on zu installieren. Wenn Sie ein Amazon-EKS-Add-on zu Ihrem Cluster hinzufügen möchten, lesen Sie [the section called “Erstellen Sie ein Add-on”](#). Weitere Informationen zu Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#). Wenn Sie das Amazon EKS-Add-on nicht verwenden können, empfehlen wir Ihnen, ein Problem mit der Begründung, warum Sie das nicht können, an das [GitHub Container-Roadmap-Repository](#) zu senden.

### Important

Bevor Sie den Amazon EFS-Treiber als Amazon EKS-Add-on hinzufügen, stellen Sie sicher, dass Sie keine selbstverwaltete Version des Treibers auf Ihrem Cluster installiert haben. Falls ja, finden Sie weitere Informationen unter [Deinstallieren des Amazon EFS CSI-Treibers](#) auf GitHub.

Wenn Sie alternativ eine selbstverwaltete Installation des Amazon-EFS-CSI-Treibers wünschen, finden Sie Informationen unter [Installation](#) in GitHub.

## Schritt 3: Erstellen eines Amazon EFS-Dateisystems

Informationen zum Erstellen eines Amazon-EFS-Dateisystems finden Sie unter [Erstellen eines Amazon-EFS-Dateisystems für Amazon EKS](#) in GitHub.

## Schritt 4: Stellen Sie eine Beispielanwendung bereit

Sie können eine Vielzahl von Beispiel-Apps bereitstellen und diese nach Bedarf ändern. Weitere Informationen finden Sie unter [Beispiele](#) unter GitHub.

# Verwenden Sie leistungsstarken App-Speicher mit Amazon FSx for Lustre

Der [Amazon FSx for Lustre Container Storage Interface \(CSI\) -Treiber](#) bietet eine CSI-Schnittstelle, mit der Amazon EKS-Cluster den Lebenszyklus von Amazon FSx for Lustre-Dateisystemen verwalten können. Weitere Informationen finden Sie im [Amazon FSx for Lustre-Benutzerhandbuch](#).

Einzelheiten dazu, wie Sie den Amazon FSx for Lustre CSI-Treiber in Ihrem Amazon EKS-Cluster bereitstellen und überprüfen, ob er funktioniert, finden Sie unter [the section called “Stellen Sie den Treiber bereit”](#).

## Stellen Sie den FSx for Lustre-Treiber bereit

In diesem Thema erfahren Sie, wie Sie den [FSx for Lustre CSI-Treiber](#) in Ihrem Amazon EKS-Cluster bereitstellen und überprüfen, ob er funktioniert. Wir empfehlen die neueste Version des Treibers zu verwenden. Die verfügbaren Versionen finden Sie in der [Kompatibilitätsmatrix der CSI-Spezifikation](#) unter GitHub.

### Note

Der Treiber wird auf Fargate- oder Amazon EKS-Hybridknoten nicht unterstützt.

Eine ausführliche Beschreibung der verfügbaren Parameter und vollständige Beispiele, die die Funktionen des Treibers demonstrieren, finden Sie im Treiberprojekt [FSx for Lustre Container Storage Interface \(CSI\)](#) unter GitHub

## Voraussetzungen

- Einen vorhandenen -Cluster.
- Das Amazon FSx CSI Driver EKS-Add-On benötigt den EKS Pod Identity-Agenten für die Authentifizierung. Ohne diese Komponente schlägt das Add-on mit dem Fehler fehl `Amazon EKS Pod Identity agent is not installed in the cluster` und verhindert Volume-Operationen. Installieren Sie den Pod Identity-Agenten vor oder nach der Bereitstellung des FSx CSI-Treiber-Add-ons. Weitere Informationen finden Sie unter [the section called “Richten Sie den Agenten ein”](#).
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um

Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit `aws configure`](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).

- Version 0.210.0 oder höher des `eksctl`-Befehlszeilen-Tools, das auf Ihrem Computer oder in der AWS CloudShell installiert ist. Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).

## Schritt 1: Erstellen einer IAM-Rolle

Das Amazon FSx CSI-Plugin benötigt IAM-Berechtigungen, um in Ihrem Namen Anrufe tätigen AWS APIs zu können.

### Note

Pods haben Zugriff auf die Berechtigungen, die der IAM-Rolle zugewiesen sind, sofern Sie den Zugriff auf IMDS nicht blockieren. Weitere Informationen finden Sie unter [the section called “Bewährte Methoden”](#).

Das folgende Verfahren zeigt Ihnen, wie Sie eine IAM-Rolle erstellen und ihr die AWS verwaltete Richtlinie zuordnen.

1. Erstellen Sie eine IAM-Rolle und fügen Sie die AWS verwaltete Richtlinie mit dem folgenden Befehl an. `my-cluster` Ersetzen Sie durch den Namen des Clusters, den Sie verwenden möchten. Der Befehl stellt einen AWS CloudFormation Stack bereit, der eine IAM-Rolle erstellt und ihr die IAM-Richtlinie anhängt.

```
eksctl create iamserviceaccount \
 --name fsx-csi-controller-sa \
 --namespace kube-system \
 --cluster my-cluster \
 --role-name AmazonEKS_FSx_CSI_DriverRole \
 --role-only \
 --attach-policy-arn arn:aws:iam::aws:policy/AmazonFSxFullAccess \
 --approve
```

Während der Erstellung des Dienstkontos werden mehrere Ausgabezeilen angezeigt. Die letzten Ausgabezeilen ähneln den folgenden.

```
[#] 1 task: {
 2 sequential sub-tasks: {
 create IAM role for serviceaccount "kube-system/fsx-csi-controller-sa",
 create serviceaccount "kube-system/fsx-csi-controller-sa",
 } }
[#] building iamserviceaccount stack "eksctl-my-cluster-addon-iamserviceaccount-kube-system-fsx-csi-controller-sa"
[#] deploying stack "eksctl-my-cluster-addon-iamserviceaccount-kube-system-fsx-csi-controller-sa"
[#] waiting for CloudFormation stack "eksctl-my-cluster-addon-iamserviceaccount-kube-system-fsx-csi-controller-sa"
[#] created serviceaccount "kube-system/fsx-csi-controller-sa"
```

Notieren Sie sich den Namen des AWS CloudFormation Stacks, der bereitgestellt wurde. In der vorigen Beispielausgabe lautet der Name des Stacks `eksctl-my-cluster-addon-iamserviceaccount-kube-system-fsx-csi-controller-sa`.

Nachdem Sie die IAM-Rolle des Amazon FSx CSI-Treibers erstellt haben, können Sie mit dem nächsten Abschnitt fortfahren. Wenn Sie das Add-on mit dieser IAM-Rolle bereitstellen, erstellt es ein benanntes Dienstkonto und ist für dessen Verwendung konfiguriert. `fsx-csi-controller-sa` Das Dienstkonto ist an ein Kubernetes-Konto gebunden, dem `clusterrole` die erforderlichen Kubernetes-Berechtigungen zugewiesen wurden.

## Schritt 2: Installieren Sie den Amazon FSx CSI-Treiber

Wir empfehlen, den Amazon FSx CSI-Treiber über das Amazon EKS-Add-on zu installieren, um die Sicherheit zu verbessern und den Arbeitsaufwand zu reduzieren. Wenn Sie ein Amazon-EKS-Add-on

zu Ihrem Cluster hinzufügen möchten, lesen Sie [the section called “Erstellen Sie ein Add-on”](#). Weitere Informationen zu Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

### Important

Bereits vorhandene Amazon FSx CSI-Treiberinstallationen im Cluster können zu Fehlern bei der Installation von Add-Ons führen. Wenn Sie versuchen, die Amazon EKS-Add-On-Version zu installieren, während ein FSx Nicht-EKS-CSI-Treiber vorhanden ist, schlägt die Installation aufgrund von Ressourcenkonflikten fehl. Verwenden Sie die OVERWRITE Markierung während der Installation, um dieses Problem zu beheben.

```
aws eks create-addon --addon-name aws-fsx-csi-driver --cluster-name my-cluster
--resolve-conflicts OVERWRITE
```

Wenn Sie alternativ eine selbstverwaltete Installation des Amazon FSx CSI-Treibers wünschen, finden Sie weitere Informationen unter [Installation](#) auf GitHub.

## Schritt 3: Stellen Sie eine Speicherklasse, einen Anspruch auf ein persistentes Volume und eine Beispiel-App bereit

Bei diesem Verfahren wird das [GitHub Treiber-Repository FSx für Lustre Container Storage Interface \(CSI\)](#) verwendet, um ein dynamisch bereitgestelltes FSx Volume für Lustre zu nutzen.

1. Beachten Sie die Sicherheitsgruppe für Ihren Cluster. Sie können es im AWS Management Console Abschnitt Netzwerk oder mit dem folgenden AWS CLI-Befehl sehen. my-cluster Ersetzen Sie es durch den Namen des Clusters, den Sie verwenden möchten.

```
aws eks describe-cluster --name my-cluster --query
cluster.resourcesVpcConfig.clusterSecurityGroupId
```

2. Erstellen Sie eine Sicherheitsgruppe für Ihr FSx Amazon-Dateisystem gemäß den Kriterien, die im [Amazon FSx for Lustre-Benutzerhandbuch unter Amazon VPC-Sicherheitsgruppen](#) aufgeführt sind. Als VPC wählen Sie die VPC Ihres Clusters aus, die im Abschnitt Networking (Netzwerk) gezeigt wird. Unter „the security groups associated with your Lustre clients“ (die mit Ihren Lustre-Clients verknüpften Sicherheitsgruppen) wählen Sie Ihre Cluster-Sicherheitsgruppe aus. Wenn Sie keine Regeln für ausgehenden Datenverkehr festlegen, können Sie den All traffic (gesamten Datenverkehr) erlauben.

### 3. Laden Sie das Speicherklassen-Manifest mit dem folgenden Befehl herunter.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-fsx-csi-driver/master/examples/kubernetes/dynamic_provisioning/specs/storageclass.yaml
```

### 4. Bearbeiten Sie den Parameterabschnitt in der Datei `storageclass.yaml`. Ersetzen Sie jeden Beispielwert durch Ihre eigenen Werte.

```
parameters:
 subnetId: subnet-0eabfaa81fb22bcaf
 securityGroupIds: sg-068000ccf82dfba88
 deploymentType: PERSISTENT_1
 automaticBackupRetentionDays: "1"
 dailyAutomaticBackupStartTime: "00:00"
 copyTagsToBackups: "true"
 perUnitStorageThroughput: "200"
 dataCompressionType: "NONE"
 weeklyMaintenanceStartTime: "7:09:00"
 fileSystemTypeVersion: "2.12"
```

- **subnetId**— Die Subnetz-ID, in der das Amazon FSx for Lustre-Dateisystem erstellt werden soll. Amazon FSx for Lustre wird nicht in allen Availability Zones unterstützt. Öffnen Sie die Amazon FSx for Lustre-Konsole unter, <https://console.aws.amazon.com/fsx/>um zu bestätigen, dass sich das Subnetz, das Sie verwenden möchten, in einer unterstützten Availability Zone befindet. Das Subnetz kann Ihre Knoten enthalten oder ein anderes Subnetz oder eine andere VPC sein:
  - Sie können nach den Knoten-Subnetzen in der suchen, AWS Management Console indem Sie die Knotengruppe im Abschnitt Compute auswählen.
  - Wenn das von Ihnen angegebene Subnetz nicht dasselbe Subnetz ist, in dem Sie Knoten haben, VPCs müssen Sie [verbunden](#) sein und sicherstellen, dass die erforderlichen Ports in Ihren Sicherheitsgruppen geöffnet sind.
- **securityGroupIds**— Die ID der Sicherheitsgruppe, die Sie für das Dateisystem erstellt haben.
- **deploymentType**(optional) — Der Bereitstellungstyp des Dateisystems. Gültige Werte sind SCRATCH\_1, SCRATCH\_2, PERSISTENT\_1 und PERSISTENT\_2. Weitere Informationen zu Bereitstellungstypen finden Sie unter [Erstellen Sie Ihr Amazon FSx for Lustre-Dateisystem](#).
- andere Parameter (optional) — Informationen zu den anderen Parametern finden Sie unter [Bearbeiten StorageClass](#) am GitHub.

## 5. Erstellen Sie das Speicherklassen-Manifest.

```
kubectl apply -f storageclass.yaml
```

Eine Beispielausgabe sieht wie folgt aus.

```
storageclass.storage.k8s.io/fsx-sc created
```

## 6. Laden Sie das Manifest für den dauerhaften Volume-Anspruch herunter.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-fsx-csi-driver/master/examples/kubernetes/dynamic_provisioning/specs/claim.yaml
```

## 7. (Optional) Bearbeiten Sie die claim.yaml-Datei. Ändern Sie 1200Gi in einen der folgenden Inkrementwerte, basierend auf Ihren Speicheranforderungen und dem deploymentType, den Sie in einem vorherigen Schritt ausgewählt haben.

```
storage: 1200Gi
```

- SCRATCH\_2 und PERSISTENT – 1.2 TiB, 2.4 TiB oder Schritte von 2,4 TiB über 2,4 TiB.
- SCRATCH\_1 – 1.2 TiB, 2.4 TiB, 3.6 TiB oder Schritte von 3,6 TiB über 3,6 TiB.

## 8. Erstellen Sie den dauerhaften Volume-Anspruch.

```
kubectl apply -f claim.yaml
```

Eine Beispielausgabe sieht wie folgt aus.

```
persistentvolumeclaim/fsx-claim created
```

## 9. Vergewissern Sie sich, dass das Dateisystem bereitgestellt wurde.

```
kubectl describe pvc
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name: fsx-claim
Namespace: default
StorageClass: fsx-sc
Status: Bound
```



[...]

 Note

Der Status kann für 5-10 Minuten als Pending angezeigt werden, bevor er zu Bound wechselt. Fahren Sie erst mit dem nächsten Schritt fort, wenn dies der Status Fall istBound. Wenn der Status länger als 10 Minuten Pending anzeigt, verwenden Sie die Warnmeldungen in den Events als Referenz zur Behebung von Problemen.

10.Stellen Sie die Beispielanwendung bereit.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/aws-fsx-csi-driver/master/examples/kubernetes/dynamic_provisioning/specs/pod.yaml
```

11.Stellen Sie sicher, dass die Beispielanwendung ausgeführt wird.

```
kubectl get pods
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME    | READY | STATUS  | RESTARTS | AGE |
|---------|-------|---------|----------|-----|
| fsx-app | 1/1   | Running | 0        | 8s  |

12.Überprüfen Sie, ob das Dateisystem ordnungsgemäß von der Anwendung aufgespielt wurde.

```
kubectl exec -ti fsx-app -- df -h
```

Eine Beispielausgabe sieht wie folgt aus.

| Filesystem              | Size | Used | Avail | Use% | Mounted on                  |
|-------------------------|------|------|-------|------|-----------------------------|
| overlay                 | 80G  | 4.0G | 77G   | 5%   | /                           |
| tmpfs                   | 64M  | 0    | 64M   | 0%   | /dev                        |
| tmpfs                   | 3.8G | 0    | 3.8G  | 0%   | /sys/fs/cgroup              |
| 192.0.2.0@tcp:/abcdef01 | 1.1T | 7.8M | 1.1T  | 1%   | /data                       |
| /dev/nvme0n1p1          | 80G  | 4.0G | 77G   | 5%   | /etc/hosts                  |
| shm                     | 64M  | 0    | 64M   | 0%   | /dev/shm                    |
| tmpfs                   | 6.9G | 12K  | 6.9G  | 1%   | /run/secrets/kubernetes.io/ |
| serviceaccount          |      |      |       |      |                             |
| tmpfs                   | 3.8G | 0    | 3.8G  | 0%   | /proc/acpi                  |

```
tmpfs 3.8G 0 3.8G 0% /sys/firmware
```

13 Stellen Sie sicher, dass die Beispiel-App Daten in das FSx for Lustre-Dateisystem geschrieben hat.

```
kubectl exec -it fsx-app -- ls /data
```

Eine Beispielausgabe sieht wie folgt aus.

```
out.txt
```

Diese Beispielausgabe zeigt, dass die Beispiel-App erfolgreich die `out.txt`-Datei in das Dateisystem geschrieben hat.

#### Note

Stellen Sie vor dem Löschen des Clusters sicher, dass Sie das FSx for Lustre-Dateisystem löschen. Weitere Informationen finden Sie unter [Ressourcen bereinigen](#) im FSx for Lustre-Benutzerhandbuch.

## Leistungssteigerung für FSx für Lustre

Wenn Sie FSx for Lustre mit Amazon EKS verwenden, können Sie die Leistung optimieren, indem Sie Lustre-Tunings während der Knoteninitialisierung anwenden. Der empfohlene Ansatz besteht darin, Benutzerdaten der Startvorlage zu verwenden, um eine konsistente Konfiguration auf allen Knoten sicherzustellen.

Zu diesen Optimierungen gehören:

- Netzwerk- und RPC-Optimierungen
- Verwaltung von Lustre-Modulen
- LRU-Tunings (Lock Resource Unit)
- Einstellungen für die Client-Cache-Steuerung
- RPC-Steuerelemente für OST und MDC

Ausführliche Anweisungen zur Implementierung dieser Leistungsoptimierungen finden Sie unter:

- Informationen zur Leistungsoptimierung für Standardknoten (ohne EFA) finden Sie unter [the section called “Optimieren \(ohne EFA\)”](#) ein vollständiges Skript, das zu den Benutzerdaten Ihrer Startvorlage hinzugefügt werden kann.
- Informationen zur Leistungsoptimierung für EFA-fähige Knoten finden Sie unter. [the section called “Optimieren \(EFA\)”](#)

## Optimieren Sie die Leistung von Amazon FSx for Lustre auf Knoten (EFA)

In diesem Thema wird beschrieben, wie Sie das Elastic Fabric Adapter (EFA) -Tuning mit Amazon EKS und Amazon FSx for Lustre einrichten.

### Note

- Informationen zur Erstellung und Bereitstellung des CSI-Treibers FSx für Lustre finden Sie unter. [the section called “Stellen Sie den Treiber bereit”](#)
- Informationen zur Optimierung von Standardknoten ohne EFA finden Sie unter. [the section called “Optimieren \(ohne EFA\)”](#)

## Schritt 1. EKS-Cluster erstellen

Erstellen Sie einen Cluster mit der bereitgestellten Konfigurationsdatei:

```
Create cluster using efa-cluster.yaml
eksctl create cluster -f efa-cluster.yaml
```

Beispielefa-cluster.yaml:

```
#efa-cluster.yaml

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: csi-fsx
 region: us-east-1
 version: "1.30"

iam:
```

```

withOIDC: true

availabilityZones: ["us-east-1a", "us-east-1d"]

managedNodeGroups:
 - name: my-efa-ng
 instanceType: c6gn.16xlarge
 minSize: 1
 desiredCapacity: 1
 maxSize: 1
 availabilityZones: ["us-east-1b"]
 volumeSize: 300
 privateNetworking: true
 amiFamily: Ubuntu2204
 efaEnabled: true
 preBootstrapCommands:
 - |
 #!/bin/bash
 eth_intf="$(/sbin/ip -br -4 a sh | grep $(hostname -i)/ | awk '{print $1}')"
 efa_version=$(modinfo efa | awk '/^version:/ {print $2}' | sed 's/[^0-9.]/g')
 min_efa_version="2.12.1"

 if [["$(printf '%s\n' "$min_efa_version" "$efa_version" | sort -V | head -
n1)" != "$min_efa_version"]]; then
 sudo curl -O https://efa-installer.amazonaws.com/aws-efa-
installer-1.37.0.tar.gz
 tar -xf aws-efa-installer-1.37.0.tar.gz && cd aws-efa-installer
 echo "Installing EFA driver"
 sudo apt-get update && apt-get upgrade -y
 sudo apt install -y pciutils environment-modules libnl-3-dev libnl-
route-3-200 libnl-route-3-dev dkms
 sudo ./efa_installer.sh -y
 modinfo efa
 else
 echo "Using EFA driver version $efa_version"
 fi

 echo "Installing Lustre client"
 sudo wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-
ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-
key.gpg > /dev/null
 sudo echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg]
https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu jammy main" > /etc/apt/
sources.list.d/fsxlustreclientrepo.list

```

```

sudo apt update | tail
sudo apt install -y lustre-client-modules-$(uname -r) amazon-ec2-utils | tail
modinfo lustre

echo "Loading Lustre/EFA modules..."
sudo /sbin/modprobe lnet
sudo /sbin/modprobe kefalnd ipif_name="$eth_intf"
sudo /sbin/modprobe ksocklnd
sudo lnetctl lnet configure

echo "Configuring TCP interface..."
sudo lnetctl net del --net tcp 2> /dev/null
sudo lnetctl net add --net tcp --if $eth_intf

For P5 instance type which supports 32 network cards,
by default add 8 EFA interfaces selecting every 4th device (1 per PCI bus)
echo "Configuring EFA interface(s)..."
instance_type="$(ec2-metadata --instance-type | awk '{ print $2 }')"
num_efa_devices="$(ls -1 /sys/class/infiniband | wc -l)"
echo "Found $num_efa_devices available EFA device(s)"

if [["$instance_type" == "p5.48xlarge" || "$instance_type" ==
"p5e.48xlarge"]]; then
 for intf in $(ls -1 /sys/class/infiniband | awk 'NR % 4 == 1'); do
 sudo lnetctl net add --net efa --if $intf --peer-credits 32
 done
else
 # Other instances: Configure 2 EFA interfaces by default if the instance
supports multiple network cards,
 # or 1 interface for single network card instances
 # Can be modified to add more interfaces if instance type supports it
 sudo lnetctl net add --net efa --if $(ls -1 /sys/class/infiniband | head -
n1) --peer-credits 32
 if [[$num_efa_devices -gt 1]]; then
 sudo lnetctl net add --net efa --if $(ls -1 /sys/class/infiniband | tail
-n1) --peer-credits 32
 fi
fi

echo "Setting discovery and UDSP rule"
sudo lnetctl set discovery 1
sudo lnetctl udsp add --src efa --priority 0
sudo /sbin/modprobe lustre

```

```
sudo lnctl net show
echo "Added $(sudo lnctl net show | grep -c '@efa') EFA interface(s)"
```

## Schritt 2. Knotengruppen erstellen

Erstellen Sie eine EFA-fähige Knotengruppe:

```
Create node group using efa-ng.yaml
eksctl create nodegroup -f efa-ng.yaml
```

### Important

=== Passen Sie diese Werte im Abschnitt für Ihre Umgebung an. # 5. Mount FSx filesystem

```
FSX_DNS="<your-fsx-filesystem-dns>" # Needs to be adjusted.
MOUNT_NAME="<your-mount-name>" # Needs to be adjusted.
MOUNT_POINT="</your/mount/point>" # Needs to be adjusted.
```

===

Beispiel: efa-ng.yaml

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: final-efa
 region: us-east-1

managedNodeGroups:
 - name: ng-1
 instanceType: c6gn.16xlarge
 minSize: 1
 desiredCapacity: 1
 maxSize: 1
 availabilityZones: ["us-east-1a"]
 volumeSize: 300
 privateNetworking: true
 amiFamily: Ubuntu2204
```

```
efaEnabled: true
preBootstrapCommands:
- |
 #!/bin/bash
 exec 1> >(logger -s -t $(basename $0)) 2>&1
```

```
#####
Configuration Section
#
#####

File System Configuration
FSX_DNS="" # Needs to be adjusted.
MOUNT_NAME="" # Needs to be adjusted.
MOUNT_POINT="/your/mount/point" # Needs to be adjusted.

Lustre Tuning Parameters
LUSTRE_LRU_MAX_AGE=600000
LUSTRE_MAX_CACHED_MB=64
LUSTRE_OST_MAX_RPC=32
LUSTRE_MDC_MAX_RPC=64
LUSTRE_MDC_MOD_RPC=50

File paths
FUNCTIONS_SCRIPT="/usr/local/bin/lustre_functions.sh"
TUNINGS_SCRIPT="/usr/local/bin/apply_lustre_tunings.sh"
SERVICE_FILE="/etc/systemd/system/lustre-tunings.service"

#EFA
MIN_EFA_VERSION="2.12.1"

Function to check if a command was successful
check_success() {
 if [$? -eq 0]; then
 echo "SUCCESS: $1"
 else
 echo "FAILED: $1"
 return 1
 fi
}

echo "*****Starting FSx for Lustre configuration*****"
```

```

1. Install Lustre client
if grep -q '^ID=ubuntu' /etc/os-release; then
 echo "Detected Ubuntu, proceeding with Lustre setup..."
 # Add Lustre repository
 sudo wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/
fsx-ubuntu-public-key.asc | sudo gpg --dearmor | sudo tee /usr/share/keyrings/fsx-
ubuntu-public-key.gpg > /dev/null

 echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg]
https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu jammy main" | sudo tee /etc/
apt/sources.list.d/fsxlustreclientrepo.list

 sudo apt-get update
 sudo apt-get install -y lustre-client-modules-$(uname -r)
 sudo apt-get install -y lustre-client
else
 echo "Not Ubuntu, exiting"
 exit 1
fi

check_success "Install Lustre client"

Ensure Lustre tools are in the PATH
export PATH=$PATH:/usr/sbin

2. Apply network and RPC tunings
echo "*****Applying network and RPC tunings*****"
if ! grep -q "options ptlrpc ptlrpcd_per_cpt_max" /etc/modprobe.d/
modprobe.conf; then
 echo "options ptlrpc ptlrpcd_per_cpt_max=64" | sudo tee -a /etc/modprobe.d/
modprobe.conf
 check_success "Set ptlrpcd_per_cpt_max"
else
 echo "ptlrpcd_per_cpt_max already set in modprobe.conf"
fi

if ! grep -q "options ksocklnd credits" /etc/modprobe.d/modprobe.conf; then
 echo "options ksocklnd credits=2560" | sudo tee -a /etc/modprobe.d/
modprobe.conf
 check_success "Set ksocklnd credits"
else
 echo "ksocklnd credits already set in modprobe.conf"
fi

```



```
3. Load Lustre modules
manage_lustre_modules() {
 echo "Checking for existing Lustre modules..."
 if lsmod | grep -q lustre; then
 echo "Existing Lustre modules found."

 # Check for mounted Lustre filesystems
 echo "Checking for mounted Lustre filesystems..."
 if mount | grep -q "type lustre"; then
 echo "Found mounted Lustre filesystems. Attempting to unmount..."
 mounted_fs=$(mount | grep "type lustre" | awk '{print $3}')
 for fs in $mounted_fs; do
 echo "Unmounting $fs"
 sudo umount $fs
 check_success "Unmount filesystem $fs"
 done
 else
 echo "No Lustre filesystems mounted."
 fi

 # After unmounting, try to remove modules
 echo "Attempting to remove Lustre modules..."
 sudo lustre_rmmod
 if [$? -eq 0]; then
 echo "SUCCESS: Removed existing Lustre modules"
 else
 echo "WARNING: Could not remove Lustre modules. They may still be
in use."

 echo "Please check for any remaining Lustre processes or mounts."
 return 1
 fi
 else
 echo "No existing Lustre modules found."
 fi

 echo "Loading Lustre modules..."
 sudo modprobe lustre
 check_success "Load Lustre modules" || exit 1

 echo "Checking loaded Lustre modules:"
 lsmod | grep lustre
}
```

```

Managing Lustre kernel modules
echo "*****Managing Lustre kernel modules*****"
manage_lustre_modules

4. Initializing Lustre networking
echo "*****Initializing Lustre networking*****"
sudo lctl network up
check_success "Initialize Lustre networking" || exit 1

4.5 EFA Setup and Configuration
setup_efa() {
 echo "*****Starting EFA Setup*****"

 # Get interface and version information
 eth_intf="$(/sbin/ip -br -4 a sh | grep $(hostname -i)/ | awk '{print
$1}')"
 efa_version=$(modinfo efa | awk '/^version:/ {print $2}' | sed 's/^[^0-9.]//
g')
 min_efa_version=$MIN_EFA_VERSION

 # Install or verify EFA driver
 if [["$(printf '%s\n' "$min_efa_version" "$efa_version" | sort -V | head -
n1)" != "$min_efa_version"]]; then
 echo "Installing EFA driver..."
 sudo curl -O https://efa-installer.amazonaws.com/aws-efa-
installer-1.37.0.tar.gz
 tar -xf aws-efa-installer-1.37.0.tar.gz && cd aws-efa-installer

 # Install dependencies
 sudo apt-get update && apt-get upgrade -y
 sudo apt install -y pciutils environment-modules libnl-3-dev libnl-
route-3-200 libnl-route-3-dev dkms

 # Install EFA
 sudo ./efa_installer.sh -y
 modinfo efa
 else
 echo "Using existing EFA driver version $efa_version"
 fi
}

configure_efa_network() {
 echo "*****Configuring EFA Network*****"

```

```

Load required modules
echo "Loading network modules..."
sudo /sbin/modprobe lnet
sudo /sbin/modprobe kefalnd ipif_name="$eth_intf"
sudo /sbin/modprobe ksocklnd

Initialize LNet
echo "Initializing LNet..."
sudo lnetctl lnet configure

Configure TCP interface
echo "Configuring TCP interface..."
sudo lnetctl net del --net tcp 2> /dev/null
sudo lnetctl net add --net tcp --if $eth_intf

For P5 instance type which supports 32 network cards,
by default add 8 EFA interfaces selecting every 4th device (1 per PCI
bus)

echo "Configuring EFA interface(s)..."
instance_type="$(ec2-metadata --instance-type | awk '{ print $2 }')"
num_efa_devices="$(ls -1 /sys/class/infiniband | wc -l)"
echo "Found $num_efa_devices available EFA device(s)"

if [["$instance_type" == "p5.48xlarge" || "$instance_type" ==
"p5e.48xlarge"]]; then
 # P5 instance configuration
 for intf in $(ls -1 /sys/class/infiniband | awk 'NR % 4 == 1'); do
 sudo lnetctl net add --net efa --if $intf --peer-credits 32
 done
else
 # Standard configuration
 # Other instances: Configure 2 EFA interfaces by default if the
instance supports multiple network cards,
 # or 1 interface for single network card instances
 # Can be modified to add more interfaces if instance type supports it
 sudo lnetctl net add --net efa --if $(ls -1 /sys/class/infiniband |
head -n1) --peer-credits 32
 if [[$num_efa_devices -gt 1]]; then
 sudo lnetctl net add --net efa --if $(ls -1 /sys/class/infiniband |
tail -n1) --peer-credits 32
 fi
fi

Configure discovery and UDSP

```

```

 echo "Setting up discovery and UDSP rules..."
 sudo lnctl set discovery 1
 sudo lnctl udsp add --src efa --priority 0
 sudo /sbin/modprobe lustre

 # Verify configuration
 echo "Verifying EFA network configuration..."
 sudo lnctl net show
 echo "Added $(sudo lnctl net show | grep -c '@efa') EFA interface(s)"
}

Main execution
setup_efa
configure_efa_network

5. Mount FSx filesystem
if [! -z "$FSX_DNS"] && [! -z "$MOUNT_NAME"]; then
 echo "*****Creating mount point*****"
 sudo mkdir -p $MOUNT_POINT
 check_success "Create mount point"

 echo "Mounting FSx filesystem..."
 sudo mount -t lustre ${FSX_DNS}@tcp:${MOUNT_NAME} ${MOUNT_POINT}
 check_success "Mount FSx filesystem"
else
 echo "Skipping FSx mount as DNS or mount name is not provided"
fi

6. Applying Lustre performance tunings
echo "*****Applying Lustre performance tunings*****"

Get number of CPUs
NUM_CPUS=$(nproc)

Calculate LRU size (100 * number of CPUs)
LRU_SIZE=$((100 * NUM_CPUS))

#Apply LRU tunings
echo "Apply LRU tunings"
sudo lctl set_param ldlm.namespaces.*.lru_max_age=${LUSTRE_LRU_MAX_AGE}
check_success "Set lru_max_age"
sudo lctl set_param ldlm.namespaces.*.lru_size=$LRU_SIZE
check_success "Set lru_size"

```

```

Client Cache Control
sudo lctl set_param llite.*.max_cached_mb=${LUSTRE_MAX_CACHED_MB}
check_success "Set max_cached_mb"

RPC Controls
sudo lctl set_param osc.*OST*.max_rpcs_in_flight=${LUSTRE_OST_MAX_RPC}
check_success "Set OST max_rpcs_in_flight"

sudo lctl set_param mdc.*.max_rpcs_in_flight=${LUSTRE_MDC_MAX_RPC}
check_success "Set MDC max_rpcs_in_flight"

sudo lctl set_param mdc.*.max_mod_rpcs_in_flight=${LUSTRE_MDC_MOD_RPC}
check_success "Set MDC max_mod_rpcs_in_flight"

7. Verify all tunings
echo "*****Verifying all tunings*****"

Function to verify parameter value
verify_param() {
 local param=$1
 local expected=$2
 local actual=$3

 if ["$actual" == "$expected"]; then
 echo "SUCCESS: $param is correctly set to $expected"
 else
 echo "WARNING: $param is set to $actual (expected $expected)"
 fi
}

echo "Verifying all parameters:"

LRU tunings
actual_lru_max_age=$(lctl get_param -n ldlm.namespaces.*.lru_max_age | head -1)
verify_param "lru_max_age" "600000" "$actual_lru_max_age"

actual_lru_size=$(lctl get_param -n ldlm.namespaces.*.lru_size | head -1)
verify_param "lru_size" "$LRU_SIZE" "$actual_lru_size"

Client Cache
actual_max_cached_mb=$(lctl get_param -n llite.*.max_cached_mb | grep
"max_cached_mb:" | awk '{print $2}')
verify_param "max_cached_mb" "64" "$actual_max_cached_mb"

```

```

RPC Controls
actual_ost_rpcs=$(lctl get_param -n osc.*OST*.max_rpcs_in_flight | head -1)
verify_param "OST max_rpcs_in_flight" "32" "$actual_ost_rpcs"

actual_mdc_rpcs=$(lctl get_param -n mdc.*.max_rpcs_in_flight | head -1)
verify_param "MDC max_rpcs_in_flight" "64" "$actual_mdc_rpcs"

actual_mdc_mod_rpcs=$(lctl get_param -n mdc.*.max_mod_rpcs_in_flight | head -1)
verify_param "MDC max_mod_rpcs_in_flight" "50" "$actual_mdc_mod_rpcs"

Network and RPC configurations from modprobe.conf
actual_ptlrpc=$(grep "ptlrpc ptlrpcd_per_cpt_max" /etc/modprobe.d/modprobe.conf
| awk '{print $3}')
verify_param "ptlrpcd_per_cpt_max" "ptlrpcd_per_cpt_max=64" "$actual_ptlrpc"

actual_ksocklnd=$(grep "ksocklnd credits" /etc/modprobe.d/modprobe.conf | awk
'{print $3}')
verify_param "ksocklnd credits" "credits=2560" "$actual_ksocklnd"

8. Setup persistence
setup_persistence() {
 # Create functions file
 cat << EOF > $FUNCTIONS_SCRIPT
#!/bin/bash

apply_lustre_tunings() {
 local NUM_CPUS=$(nproc)
 local LRU_SIZE=$((100 * NUM_CPUS))

 echo "Applying Lustre performance tunings..."
 lctl set_param ldlm.namespaces.*.lru_max_age=$LUSTRE_LRU_MAX_AGE
 lctl set_param ldlm.namespaces.*.lru_size=$LRU_SIZE
 lctl set_param llite.*.max_cached_mb=$LUSTRE_MAX_CACHED_MB
 lctl set_param osc.*OST*.max_rpcs_in_flight=$LUSTRE_OST_MAX_RPC
 lctl set_param mdc.*.max_rpcs_in_flight=$LUSTRE_MDC_MAX_RPC
 lctl set_param mdc.*.max_mod_rpcs_in_flight=$LUSTRE_MDC_MOD_RPC
}
EOF

 # Create tuning script
 cat << EOF > $TUNINGS_SCRIPT
#!/bin/bash
exec 1> >(logger -s -t $(basename $0)) 2>&1

```

```
source $FUNCTIONS_SCRIPT

Function to check if Lustre is mounted
is_lustre_mounted() {
 mount | grep -q "type lustre"
}

Function to mount Lustre
mount_lustre() {
 echo "Mounting Lustre filesystem..."
 mkdir -p $MOUNT_POINT
 mount -t lustre ${FSX_DNS}@tcp:/${MOUNT_NAME} $MOUNT_POINT
 return $?
}

Main execution
Try to mount if not already mounted
if ! is_lustre_mounted; then
 echo "Lustre filesystem not mounted, attempting to mount..."
 mount_lustre
fi

Wait for successful mount (up to 5 minutes)
for i in {1..30}; do
 if is_lustre_mounted; then
 echo "Lustre filesystem mounted, applying tunings..."
 apply_lustre_tunings
 exit 0
 fi
 echo "Waiting for Lustre filesystem to be mounted... (attempt $i/30)"
 sleep 10
done

echo "Timeout waiting for Lustre filesystem mount"
exit 1
EOF

Create systemd service

Create systemd directory if it doesn't exist
sudo mkdir -p /etc/systemd/system/

Create service file directly for Ubuntu
cat << EOF > $SERVICE_FILE
```

```
[Unit]
Description=Apply Lustre Performance Tunings
After=network.target remote-fs.target

[Service]
Type=oneshot
ExecStart=/bin/bash -c 'source $FUNCTIONS_SCRIPT && $TUNINGS_SCRIPT'
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
EOF

Make scripts executable and enable service
sudo chmod +x $FUNCTIONS_SCRIPT
sudo chmod +x $TUNINGS_SCRIPT
systemctl enable lustre-tunings.service
systemctl start lustre-tunings.service
}

echo "*****Setting up persistent tuning*****"
setup_persistence

echo "FSx for Lustre configuration completed."
```

### (Optional) Schritt 3. Überprüfen Sie das EFA-Setup

SSH zum Knoten:

```
Get instance ID from EKS console or AWS CLI
ssh -i /path/to/your-key.pem ec2-user@<node-internal-ip>
```

Überprüfen Sie die EFA-Konfiguration:

```
sudo lnctl net show
```

Überprüfen Sie die Setup-Protokolle:

```
sudo cat /var/log/cloud-init-output.log
```

Hier ist ein Beispiel für eine erwartete Ausgabe für `lnctl net show`:



```
net:
 - net type: tcp
 ...
 - net type: efa
 local NI(s):
 - nid: xxx.xxx.xxx.xxx@efa
 status: up
```

## Beispiele für Bereitstellungen

### a. Erstellen Sie claim.yaml

```
#claim.yaml

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: fsx-claim-efa
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: ""
 resources:
 requests:
 storage: 4800Gi
 volumeName: fsx-pv
```

Beantragen Sie den Anspruch:

```
kubectl apply -f claim.yaml
```

### b. Erstellen Sie pv.yaml

Aktualisieren Sie das: <replaceable-placeholders>

```
#pv.yaml

apiVersion: v1
kind: PersistentVolume
metadata:
 name: fsx-pv
spec:
```

```
capacity:
 storage: 4800Gi
volumeMode: Filesystem
accessModes:
 - ReadWriteMany
mountOptions:
 - flock
persistentVolumeReclaimPolicy: Recycle
csi:
 driver: fsx.csi.aws.com
 volumeHandle: fs-<1234567890abcdef0>
 volumeAttributes:
 dnsname: fs-<1234567890abcdef0>.fsx.us-east-1.amazonaws.com
 mountname: <abcdef01>
```

Wenden Sie das persistente Volume an:

```
kubectl apply -f pv.yaml
```

c. Erstellen Sie pod.yaml

```
#pod.yaml

apiVersion: v1
kind: Pod
metadata:
 name: fsx-efa-app
spec:
 containers:
 - name: app
 image: amazonlinux:2
 command: ["/bin/sh"]
 args: ["-c", "while true; do dd if=/dev/urandom bs=100M count=20 > data/test_file;
sleep 10; done"]
 resources:
 requests:
 vpc.amazonaws.com/efa: 1
 limits:
 vpc.amazonaws.com/efa: 1
 volumeMounts:
 - name: persistent-storage
 mountPath: /data
 volumes:
```

```
- name: persistent-storage
 persistentVolumeClaim:
 claimName: fsx-claim-efa
```

Wenden Sie den Pod an:

```
kubectl apply -f pod.yaml
```

## Zusätzliche Bestätigungsbefehle

Stellen Sie sicher, dass der Pod eingebunden und in das Dateisystem geschrieben wird:

```
kubectl exec -ti fsx-efa-app -- df -h | grep data
Expected output:
<192.0.2.0>@tcp:/<abcdef01> 4.5T 1.2G 4.5T 1% /data

kubectl exec -ti fsx-efa-app -- ls /data
Expected output:
test_file
```

Stellen Sie per SSH eine Verbindung zum Knoten her, um zu überprüfen, ob der Datenverkehr über EFA geleitet wird:

```
sudo lnctl net show -v
```

In der erwarteten Ausgabe werden EFA-Schnittstellen mit Verkehrsstatistiken angezeigt.

## Ähnliche Informationen

- [the section called “Stellen Sie den Treiber bereit”](#)
- [the section called “Optimieren \(ohne EFA\)”](#)
- [Amazon FSx für Lustre Performance](#)
- [Elastic Fabric Adapter](#)

## Optimieren Sie die Leistung von Amazon FSx for Lustre auf Knoten (ohne EFA)

Sie können die Leistung von Amazon FSx for Lustre optimieren, indem Sie während der Knoteninitialisierung mithilfe von Benutzerdaten der Startvorlage Optimierungsparameter anwenden.

 Note

- Informationen zur Erstellung und Bereitstellung des CSI-Treibers FSx für Lustre finden Sie unter. [the section called “Stellen Sie den Treiber bereit”](#) Informationen zur Leistungsoptimierung mit EFA-fähigen Knoten finden Sie unter. [the section called “Optimieren \(EFA\)”](#)

## Warum sollten Benutzerdaten der Startvorlage verwendet werden?

- Wendet bei der Initialisierung des Knotens automatisch Optimierungen an.
- Sorgt für eine konsistente Konfiguration auf allen Knoten.
- Macht eine manuelle Knotenkonfiguration überflüssig.

## Überblick über ein Beispielskript

Das in diesem Thema definierte Beispielskript führt die folgenden Operationen aus:

### # 1. Install Lustre client

- Erkennt automatisch Ihre Betriebssystemversion: Amazon Linux 2 (AL2) oder Amazon Linux 2023 (AL2023).
- Installiert das entsprechende Lustre-Client-Paket.

### # 2. Apply network and RPC tunings

- Sätze `ptlrpcd_per_cpt_max=64` für parallel RPC-Verarbeitung.
- Konfiguriert `socklnd credits=2560`, um Netzwerkpuffer zu optimieren.

### # 3. Load Lustre modules

- Entfernt sicher vorhandene Lustre-Module, falls vorhanden.
- Verwaltet das Aushängen vorhandener Dateisysteme.
- Lädt neue Lustre-Module.

## # 4. Lustre Network Initialization

- Initialisiert die Lustre-Netzwerkkonfiguration.
- Richtet die erforderlichen Netzwerkparameter ein.

## # 5. Mount FSx filesystem

- In diesem Abschnitt müssen Sie die Werte für Ihre Umgebung anpassen.

## # 6. Apply tunings

- LRU-Tunings (Lock Resource Unit):
  - `lru_max_age=600000`
  - `lru_size` berechnet auf der Grundlage der CPU-Anzahl
- Client-Cache-Steuerung: `max_cached_mb=64`
- RPC-Steuerelemente:
  - OST `max_rpcs_in_flight=32`
  - MDC `max_rpcs_in_flight=64`
  - MDC `max_mod_rpcs_in_flight=50`

## # 7. Verify tunings

- Überprüft alle angewendeten Einstellungen.
- Meldet Erfolg oder Warnung für jeden Parameter.

## # 8. Setup persistence

- In diesem Abschnitt müssen Sie auch die Werte für Ihre Umgebung anpassen.
- Erkennt automatisch Ihre Betriebssystemversion (AL2 oder AL2 023), um zu bestimmen, welcher Systemd Dienst angewendet werden soll.
- Das System wird gestartet.
- Systemd startet `lustre-tunings` den Dienst (aufgrund von `WantedBy=multi-user.target`).
- Der Dienst läuft `apply_lustre_tunings.sh` welcher:
  - Prüft, ob das Dateisystem eingehängt ist.

- Hängt das Dateisystem ein, falls es nicht eingehängt ist.
- Wartet auf eine erfolgreiche Installation (bis zu fünf Minuten).
- Wendet nach erfolgreicher Installation die Optimierungsparameter an.
- Die Einstellungen bleiben bis zum Neustart aktiv.
- Der Dienst wird nach Abschluss des Skripts beendet.
  - Systemd markiert den Dienst als „aktiv (beendet)“.
- Der Vorgang wiederholt sich beim nächsten Neustart.

## Erstellen einer Startvorlage

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie Vorlagen starten.
3. Wählen Sie Startvorlage erstellen.
4. Suchen Sie unter Erweiterte Details den Abschnitt Benutzerdaten.
5. Fügen Sie das unten stehende Skript ein und aktualisieren Sie alles nach Bedarf.

### Important

Passen Sie diese Werte sowohl im Abschnitt # 5. Mount FSx filesystem als auch in der `setup_persistence()` Funktion von `apply_lustre_tunings.sh` in an Ihre Umgebung an# 8. Setup persistence:

```
FSX_DNS="<your-fsx-filesystem-dns>" # Needs to be adjusted.
MOUNT_NAME="<your-mount-name>" # Needs to be adjusted.
MOUNT_POINT="</your/mount/point>" # Needs to be adjusted.
```

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="MYBOUNDARY"
--==MYBOUNDARY==
Content-Type: text/x-shellscript; charset="us-ascii"
#!/bin/bash
exec 1> >(logger -s -t $(basename $0)) 2>&1
Function definitions
check_success() {
```

```

 if [$? -eq 0]; then
 echo "SUCCESS: $1"
 else
 echo "FAILED: $1"
 return 1
 fi
}

apply_tunings() {
 local NUM_CPUS=$(nproc)
 local LRU_SIZE=$((100 * NUM_CPUS))
 local params=(
 "ldlm.namespaces.*.lru_max_age=600000"
 "ldlm.namespaces.*.lru_size=$LRU_SIZE"
 "llite.*.max_cached_mb=64"
 "osc.*OST*.max_rpcs_in_flight=32"
 "mdc.*.max_rpcs_in_flight=64"
 "mdc.*.max_mod_rpcs_in_flight=50"
)
 for param in "${params[@]}; do
 lctl set_param $param
 check_success "Set ${param%%=*}"
 done
}

verify_param() {
 local param=$1
 local expected=$2
 local actual=$3

 if ["$actual" == "$expected"]; then
 echo "SUCCESS: $param is correctly set to $expected"
 else
 echo "WARNING: $param is set to $actual (expected $expected)"
 fi
}

verify_tunings() {
 local NUM_CPUS=$(nproc)
 local LRU_SIZE=$((100 * NUM_CPUS))
 local params=(
 "ldlm.namespaces.*.lru_max_age:600000"
 "ldlm.namespaces.*.lru_size:$LRU_SIZE"
 "llite.*.max_cached_mb:64"
 "osc.*OST*.max_rpcs_in_flight:32"
 "mdc.*.max_rpcs_in_flight:64"
 "mdc.*.max_mod_rpcs_in_flight:50"
)

```

```

)
echo "Verifying all parameters:"
for param in "${params[@]}; do
 name="${param%*:}"
 expected="${param#*:}"
 actual=$(lctl get_param -n $name | head -1)
 verify_param "${name##*.}" "$expected" "$actual"
done
}

setup_persistence() {
 # Create functions file
 cat << 'EOF' > /usr/local/bin/lustre_functions.sh
#!/bin/bash
apply_lustre_tunings() {
 local NUM_CPUS=$(nproc)
 local LRU_SIZE=$((100 * NUM_CPUS))

 echo "Applying Lustre performance tunings..."
 lctl set_param ldlm.namespaces.*.lru_max_age=600000
 lctl set_param ldlm.namespaces.*.lru_size=$LRU_SIZE
 lctl set_param llite.*.max_cached_mb=64
 lctl set_param osc.*OST*.max_rpcs_in_flight=32
 lctl set_param mdc.*.max_rpcs_in_flight=64
 lctl set_param mdc.*.max_mod_rpcs_in_flight=50
}
EOF
 # Create tuning script
 cat << 'EOF' > /usr/local/bin/apply_lustre_tunings.sh
#!/bin/bash
exec 1> >(logger -s -t $(basename $0)) 2>&1
Source the functions
source /usr/local/bin/lustre_functions.sh
FSx details
FSX_DNS="" # Needs to be adjusted.
MOUNT_NAME="" # Needs to be adjusted.
MOUNT_POINT="" # Needs to be adjusted.
Function to check if Lustre is mounted
is_lustre_mounted() {
 mount | grep -q "type lustre"
}
Function to mount Lustre
mount_lustre() {
 echo "Mounting Lustre filesystem..."
 mkdir -p ${MOUNT_POINT}

```



```

 mount -t lustre ${FSX_DNS}@tcp:${MOUNT_NAME} ${MOUNT_POINT}
 return $?
}
Main execution
Try to mount if not already mounted
if ! is_lustre_mounted; then
 echo "Lustre filesystem not mounted, attempting to mount..."
 mount_lustre
fi
Wait for successful mount (up to 5 minutes)
for i in {1..30}; do
 if is_lustre_mounted; then
 echo "Lustre filesystem mounted, applying tunings..."
 apply_lustre_tunings
 exit 0
 fi
 echo "Waiting for Lustre filesystem to be mounted... (attempt $i/30)"
 sleep 10
done
echo "Timeout waiting for Lustre filesystem mount"
exit 1
EOF

Create systemd service
cat << 'EOF' > /etc/systemd/system/lustre-tunings.service
[Unit]
Description=Apply Lustre Performance Tunings
After=network.target remote-fs.target
StartLimitIntervalSec=0
[Service]
Type=oneshot
ExecStart=/usr/local/bin/apply_lustre_tunings.sh
RemainAfterExit=yes
Restart=on-failure
RestartSec=30
[Install]
WantedBy=multi-user.target
EOF

 chmod +x /usr/local/bin/lustre_functions.sh
 chmod +x /usr/local/bin/apply_lustre_tunings.sh
 systemctl enable lustre-tunings.service
 systemctl start lustre-tunings.service
}
echo "Starting FSx for Lustre configuration..."
1. Install Lustre client

```

```

if grep -q 'VERSION="2"' /etc/os-release; then
 amazon-linux-extras install -y lustre
elif grep -q 'VERSION="2023"' /etc/os-release; then
 dnf install -y lustre-client
fi
check_success "Install Lustre client"
2. Apply network and RPC tunings
export PATH=$PATH:/usr/sbin
echo "Applying network and RPC tunings..."
if ! grep -q "options ptlrpc ptlrpcd_per_cpt_max" /etc/modprobe.d/modprobe.conf; then
 echo "options ptlrpc ptlrpcd_per_cpt_max=64" | tee -a /etc/modprobe.d/
modprobe.conf
 echo "options ksocklnd credits=2560" | tee -a /etc/modprobe.d/modprobe.conf
fi
3. Load Lustre modules
modprobe lustre
check_success "Load Lustre modules" || exit 1
4. Lustre Network Initialization
lctl network up
check_success "Initialize Lustre networking" || exit 1
5. Mount FSx filesystem
FSX_DNS="" # Needs to be adjusted.
MOUNT_NAME="" # Needs to be adjusted.
MOUNT_POINT="" # Needs to be adjusted.
if [! -z "$FSX_DNS"] && [! -z "$MOUNT_NAME"]; then
 mkdir -p $MOUNT_POINT
 mount -t lustre ${FSX_DNS}@tcp:/${MOUNT_NAME} ${MOUNT_POINT}
 check_success "Mount FSx filesystem"
fi
6. Apply tunings
apply_tunings
7. Verify tunings
verify_tunings
8. Setup persistence
setup_persistence
echo "FSx for Lustre configuration completed."
---MYBOUNDARY---

```

6. Wählen Sie beim Erstellen von Amazon EKS-Knotengruppen diese Startvorlage aus. Weitere Informationen finden Sie unter [the section called “Erstellen”](#).

## Ähnliche Informationen

- [the section called “Stellen Sie den Treiber bereit”](#)
- [the section called “Optimieren \(EFA\)”](#)
- [Amazon FSx für Lustre Performance](#)

## Verwenden Sie leistungsstarken App-Speicher mit FSx für NetApp ONTAP

Der NetApp Trident bietet dynamische Speicherorchestrierung mithilfe eines Container-Storage-Interface (CSI) -kompatiblen Treibers. Dadurch können Amazon EKS-Cluster den Lebenszyklus persistenter Volumes (PVs) verwalten, die von Amazon FSx für NetApp ONTAP-Dateisysteme unterstützt werden. Beachten Sie, dass der Amazon FSx for NetApp ONTAP CSI-Treiber nicht mit Amazon EKS-Hybridknoten kompatibel ist. Erste Schritte finden Sie unter [Use Trident with Amazon FSx for NetApp ONTAP](#) in der NetApp Trident-Dokumentation.

Amazon FSx for NetApp ONTAP ist ein Speicherservice, mit dem Sie vollständig verwaltete ONTAP-Dateisysteme in der Cloud starten und ausführen können. NetAppDie Dateisystemtechnologie von ONTAP bietet eine breite Palette von Datenzugriffs- und Datenverwaltungsfunktionen. FSx for ONTAP bietet die Funktionen, die Leistung und die APIs von lokalen NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten Dienstes. AWS Weitere Informationen finden Sie im Benutzerhandbuch [FSx für ONTAP](#).

### Important

Wenn Sie Amazon FSx for NetApp ONTAP zusammen mit dem Amazon EBS CSI-Treiber zur Bereitstellung von EBS-Volumes verwenden, müssen Sie in der Datei angeben, dass keine EBS-Geräte verwendet werden sollen. `multipath.conf` [Informationen zu den unterstützten Methoden finden Sie unter Blacklist für Konfigurationsdateien](#). Ein Beispiel.

```
defaults {
 user_friendly_names yes
 find_multipaths no
}
blacklist {
 device {
 vendor "NVME"
```

```
 product "Amazon Elastic Block Store"
 }
 }
```

## Datenspeicher mit Amazon FSx für OpenZFS verwenden

Amazon FSx for OpenZFS ist ein vollständig verwalteter Dateispeicherservice, der es einfach macht, Daten AWS von lokalen ZFS- oder anderen Linux-basierten Dateiservern zu verschieben. Sie können dies tun, ohne Ihren Anwendungscode oder die Art und Weise, wie Sie Daten verwalten, zu ändern. Es bietet einen äußerst zuverlässigen, skalierbaren, effizienten und featurereichen Dateispeicher, der auf dem Open-Source-Dateisystem OpenZFS basiert. Er kombiniert diese Funktionen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten Services. AWS Weitere Informationen finden Sie im [Amazon FSx for OpenZFS-Benutzerhandbuch](#).

Der FSx für OpenZFS Container Storage Interface (CSI) -Treiber bietet eine CSI-Schnittstelle, die es Amazon EKS-Clustern ermöglicht, den Lebenszyklus von FSx OpenZFS-Volumes zu verwalten. Beachten Sie, dass der Amazon FSx for OpenZFS CSI-Treiber nicht mit Amazon EKS-Hybridknoten kompatibel ist. Informationen zur Bereitstellung des FSx for OpenZFS CSI-Treibers in Ihrem Amazon EKS-Cluster finden Sie unter [aws-fsx-openzfs-csi-driver](#) on GitHub

## Minimierung der Latenz mit Amazon File Cache

Amazon File Cache ist ein vollständig verwalteter Hochgeschwindigkeits-Cache, der zur Verarbeitung von Dateidaten verwendet wird, unabhängig davon, wo die Daten gespeichert sind. AWS Amazon File Cache lädt beim ersten Zugriff automatisch Daten in den Cache und gibt Daten frei, wenn sie nicht verwendet werden. Weitere Informationen finden Sie in [Benutzerhandbuch zu Amazon File Cache](#).

Der Container Storage Interface (CSI)-Treiber für Amazon File Cache bietet eine CSI-Schnittstelle, die es Amazon-EKS-Clustern ermöglicht, den Lebenszyklus von Amazon-Datei-Caches zu verwalten. Beachten Sie, dass der Amazon File Cache CSI-Treiber nicht mit Amazon EKS-Hybridknoten kompatibel ist. Informationen zur Bereitstellung des Amazon File Cache CSI-Treibers in Ihrem Amazon EKS-Cluster finden Sie unter [aws-file-cache-csi-driver](#) on GitHub.

# Greifen Sie mit dem Mountpoint for Amazon S3 CSI-Treiber auf Amazon S3-Objekte zu

Mit dem [Mountpoint for Amazon S3 Container Storage Interface \(CSI\) -Treiber](#) können Ihre Kubernetes-Anwendungen über eine Dateisystemschnittstelle auf Amazon S3 S3-Objekte zugreifen und so einen hohen Gesamtdurchsatz erzielen, ohne dass der Anwendungscode geändert werden muss. Der CSI-Treiber basiert auf [Mountpoint für Amazon S3](#) und präsentiert einen Amazon S3 S3-Bucket als Volume, auf das Container in Amazon EKS und selbstverwalteten Kubernetes-Clustern zugreifen können.

## Überlegungen

- Der Mountpoint for Amazon S3 CSI-Treiber ist derzeit nicht mit Windows-basierten Container-Images kompatibel.
- Der Mountpoint for Amazon S3 CSI-Treiber ist derzeit nicht mit Amazon EKS Hybrid Nodes kompatibel.
- Der Mountpoint for Amazon S3 CSI-Treiber unterstützt AWS Fargate nicht. Container, die in Amazon ausgeführt werden EC2 (entweder mit Amazon EKS oder einer benutzerdefinierten Kubernetes-Installation), werden jedoch unterstützt.
- Der Mountpoint for Amazon S3 CSI-Treiber unterstützt nur statische Bereitstellung. Dynamisches Provisioning oder die Erstellung neuer Buckets wird nicht unterstützt.

### Note

Statische Bereitstellung bezieht sich auf die Verwendung eines vorhandenen Amazon S3 S3-Buckets, der als `bucketName` `volumeAttributes` im `PersistentVolume` Objekt angegeben ist. Weitere Informationen finden Sie unter [Statische Bereitstellung](#) auf GitHub

- Volumes, die mit dem Mountpoint for Amazon S3 CSI-Treiber bereitgestellt wurden, unterstützen nicht alle POSIX-Dateisystemfunktionen. Einzelheiten zum Dateisystemverhalten finden Sie unter Dateisystemverhalten von [Mountpoint für Amazon S3](#). GitHub

Einzelheiten zur Bereitstellung des Treibers finden Sie unter [the section called “Stellen Sie den Treiber bereit”](#) Einzelheiten zum Entfernen des Treibers finden Sie unter [the section called “Entfernen Sie den Treiber”](#).

# Stellen Sie den Mountpoint for Amazon S3 S3-Treiber bereit

Mit dem [Mountpoint for Amazon S3 Container Storage Interface \(CSI\) -Treiber](#) können Ihre Kubernetes-Anwendungen über eine Dateisystemschnittstelle auf Amazon S3 S3-Objekte zugreifen und so einen hohen Gesamtdurchsatz erzielen, ohne dass der Anwendungscode geändert werden muss.

Dieses Verfahren zeigt Ihnen, wie Sie den [Mountpoint for Amazon S3 CSI Amazon EKS-Treiber](#) bereitstellen. [Bevor Sie fortfahren, lesen Sie bitte die Überlegungen.](#)

## Voraussetzungen

- Ein vorhandener AWS Identity and Access Management (IAM) OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Informationen zum Feststellen, ob Sie bereits über einen verfügen oder einen erstellen müssen, finden Sie unter [the section called "IAM OIDC-Anbieter"](#).
- Version 2.12.3 oder höher der AWS CLI, die auf Ihrem Gerät installiert und konfiguriert ist, oder. AWS CloudShell
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called "Richten Sie kubectl und eksctl ein"](#).

## Schritt 1: Erstellen einer IAM-Richtlinie

Der Mountpoint for Amazon S3 CSI-Treiber benötigt Amazon S3 S3-Berechtigungen, um mit Ihrem Dateisystem zu interagieren. In diesem Abschnitt wird erläutert, wie Sie eine IAM-Richtlinie erstellen, die die erforderlichen Berechtigungen gewährt.

Die folgende Beispielrichtlinie folgt den IAM-Berechtigungsempfehlungen für Mountpoint. Alternativ können Sie den Link für AWS verwaltete Richtlinien verwenden:`iam/home?#/policies/arn:aws:iam:::aws:policy/amazons3 FullAccess $jsonEditor [amazonS3, type="console "],` aber diese verwaltete Richtlinie gewährt mehr Berechtigungen `FullAccess`, als für Mountpoint benötigt werden.

Weitere Informationen zu den empfohlenen [Berechtigungen für Mountpoint GitHub finden Sie unter Mountpoint IAM-Berechtigungen](#) für.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Policies aus.
3. Wählen Sie auf der Seite Richtlinien die Option Richtlinie erstellen.
4. Wählen Sie für Richtlinien-Editor die Option JSON aus.
5. Kopieren Sie unter Richtlinien-Editor Folgendes und fügen Sie es ein:

 **Important**

Ersetzen Sie `amzn-s3-demo-bucket1` durch den Namen Ihres eigenen Amazon-S3-Bucket.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "MountpointFullBucketAccess",
 "Effect": "Allow",
 "Action": [
 "s3:ListBucket"
],
 "Resource": [
 "arn:aws:s3:::amzn-s3-demo-bucket1"
]
 },
 {
 "Sid": "MountpointFullObjectAccess",
 "Effect": "Allow",
 "Action": [
 "s3:GetObject",
 "s3:PutObject",
 "s3:AbortMultipartUpload",
 "s3:DeleteObject"
],
 "Resource": [
 "arn:aws:s3:::amzn-s3-demo-bucket1/*"
]
 }
]
}
```

Directory-Buckets, die mit der Amazon S3 Express One Zone-Speicherklasse eingeführt wurden, verwenden einen anderen Authentifizierungsmechanismus als Buckets für allgemeine Zwecke. Anstatt `s3:*` Aktionen zu verwenden, sollten Sie die `s3express:CreateSession` Aktion verwenden. Informationen zu Directory-Buckets finden Sie unter [Directory-Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie mit den geringsten Rechten, die Sie für einen Directory-Bucket verwenden würden.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3express:CreateSession",
 "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-bucket1--usw2-az1--x-s3"
 }
]
}
```

6. Wählen Sie Weiter aus.
7. Geben Sie Ihrer Richtlinie auf der Seite Überprüfen und erstellen einen Namen. In dieser Beispielanleitung wird der Name `AmazonS3CSIDriverPolicy` verwendet.
8. Wählen Sie Richtlinie erstellen aus.

## Schritt 2: Erstellen einer IAM-Rolle

Der Mountpoint for Amazon S3 CSI-Treiber benötigt Amazon S3 S3-Berechtigungen, um mit Ihrem Dateisystem zu interagieren. In diesem Abschnitt wird erläutert, wie Sie eine IAM-Rolle erstellen, mit der Sie diese Berechtigungen delegieren. Um diese Rolle zu erstellen, können Sie eines der folgenden Tools verwenden:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)
- [the section called “AWS CLI”](#)



 Note

Die IAM-Richtlinie AmazonS3CSIDriverPolicy wurde im vorherigen Abschnitt erstellt.

eksctl

Um Ihre Mountpoint for Amazon S3 CSI-Treiber-IAM-Rolle zu erstellen mit **eksctl**

Führen Sie die folgenden Befehle aus, um die IAM-Rolle und das Kubernetes-Dienstkonto zu erstellen. Mit diesen Befehlen wird auch die AmazonS3CSIDriverPolicy IAM-Richtlinie an die Rolle angehängt, das Kubernetes-Dienstkonto (s3-csi-controller-sa) mit dem Amazon-Ressourcennamen (ARN) der IAM-Rolle annotiert und der Vertrauensrichtlinie für die IAM-Rolle der Kubernetes-Dienstkontoname hinzugefügt.

```
CLUSTER_NAME=my-cluster
REGION=region-code
ROLE_NAME=AmazonEKS_S3_CSI_DriverRole
POLICY_ARN=AmazonEKS_S3_CSI_DriverRole_ARN
eksctl create iamserviceaccount \
 --name s3-csi-driver-sa \
 --namespace kube-system \
 --cluster $CLUSTER_NAME \
 --attach-policy-arn $POLICY_ARN \
 --approve \
 --role-name $ROLE_NAME \
 --region $REGION \
 --role-only
```

## AWS Management Console

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
  - a. Wählen Sie im Abschnitt Trusted entity type (Typ der vertrauenswürdigen Entität) die Option Web identity (Web-Identität) aus.

- b. Wählen Sie für Identity provider (Identitätsanbieter) die Option OpenID Connect provider URL (OpenID-Connect-Anbieter-URL) für Ihren Cluster aus (wie unter Overview (Übersicht) in Amazon EKS gezeigt).

[Wenn keine angezeigt werden, überprüfen Sie die Voraussetzungen. URLs](#)

- c. Wählen Sie für Audience (Zielgruppe) sts.amazonaws.com.
  - d. Wählen Sie Weiter aus.
5. Gehen Sie auf der Seite Berechtigungen hinzufügen wie folgt vor:
- a. Geben Sie im Feld Richtlinien filtern den Text AmazonS3-Richtlinie einCSIDriver.



#### Note

Diese Richtlinie wurde im vorherigen Abschnitt erstellt.

- b. Aktivieren Sie das Kontrollkästchen links neben dem Ergebnis für AmazonS3CSIDriverPolicy, das bei der Suche zurückgegeben wurde.
  - c. Wählen Sie Weiter aus.
6. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
- a. Geben Sie als Rollename einen eindeutigen Namen für Ihre Rolle ein, z. B. AmazonEKS\_S3\_CSI\_. DriverRole
  - b. Fügen Sie der Rolle unter Tags hinzufügen (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Markieren von IAM-Ressourcen](#) im IAM-Benutzerhandbuch.
  - c. Wählen Sie Create role (Rolle erstellen) aus.
7. Nachdem die Rolle erstellt wurde, wählen Sie die Rolle in der Konsole aus, um sie zur Bearbeitung zu öffnen.
8. Wählen Sie die Registerkarte Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
9. Suchen Sie die Zeile, die wie folgt aussieht:

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud":
 "sts.amazonaws.com"
```

Fügen Sie am Ende der vorherigen Zeile ein Komma und anschließend die folgende Zeile hinzu. Ersetzen Sie es durch die Region, in der *region-code* sich Ihr Cluster befindet AWS . *EXAMPLED539D4633E53DE1B71EXAMPLE* Ersetzen Sie es durch die OIDC-Anbieter-ID Ihres Clusters.

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub":
"system:serviceaccount:kube-system:s3-csi-driver-sa"
```

10. Stellen Sie sicher, dass der Condition Operator auf eingestellt ist. "StringEquals"

11. Wählen Sie Update Policy (Richtlinie aktualisieren) aus, um den Vorgang abzuschließen.

## AWS CLI

1. Zeigen Sie die OIDC-Anbieter-URL Ihres Clusters an. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Wenn die Ausgabe des Befehls None ist, überprüfen Sie die [Voraussetzungen](#).

```
aws eks describe-cluster --name my-cluster --query "cluster.identity.oidc.issuer" --
output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
https://oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE
```

2. Erstellen Sie die IAM-Rolle und weisen Sie dem Kubernetes-Dienstkonto die AssumeRoleWithWebIdentity-Aktion zu.
  - a. Kopieren Sie den folgenden Inhalt in eine Datei namens `aws-s3-csi-driver-trust-policy.json`. Ersetzen Sie *111122223333* durch Ihre Konto-ID. Ersetzen Sie *EXAMPLED539D4633E53DE1B71EXAMPLE* und *region-code* mit den im vorherigen Schritt zurückgegebenen Werten.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-
code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
```

```

 },
 "Action": "sts:AssumeRoleWithWebIdentity",
 "Condition": {
 "StringEquals": {
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:s3-csi-
driver-sa",
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
 }
 }
 }
]
}

```

- b. Erstellen Sie die -Rolle. Sie können *AmazonEKS\_S3\_CSI\_DriverRole* in einen anderen Namen ändern, aber wenn Sie dies tun, stellen Sie sicher, dass Sie ihn auch in späteren Schritten ändern.

```

aws iam create-role \
 --role-name AmazonEKS_S3_CSI_DriverRole \
 --assume-role-policy-document file://"aws-s3-csi-driver-trust-policy.json"

```

3. Hängen Sie die zuvor erstellte IAM-Richtlinie mit dem folgenden Befehl an die Rolle an.

```

aws iam attach-role-policy \
 --policy-arn arn:aws:iam::aws:policy/AmazonS3CSIDriverPolicy \
 --role-name AmazonEKS_S3_CSI_DriverRole

```

#### Note

Die IAM-Richtlinie AmazonS3CSIDriverPolicy wurde im vorherigen Abschnitt erstellt.

4. Überspringen Sie diesen Schritt, wenn Sie den Treiber als Amazon EKS-Add-on installieren. Erstellen Sie für selbstverwaltete Treiberinstallationen Kubernetes-Dienstkonten, die mit dem ARN der von Ihnen erstellten IAM-Rolle annotiert sind.
- a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `mountpoint-s3-service-account.yaml`. Ersetzen Sie *111122223333* durch Ihre Konto-ID.

```

apiVersion: v1

```

```
kind: ServiceAccount
metadata:
 labels:
 app.kubernetes.io/name: aws-mountpoint-s3-csi-driver
 name: mountpoint-s3-csi-controller-sa
 namespace: kube-system
 annotations:
 eks.amazonaws.com/role-arn: arn:aws:iam::111122223333:role/
 AmazonEKS_S3_CSI_DriverRole
```

- b. Erstellen Sie das Kubernetes-Servicekonto in Ihrem Cluster. Das Kubernetes-Dienstkonto (mountpoint-s3-csi-controller-sa) ist mit dem Namen der IAM-Rolle versehen, die Sie erstellt haben. *AmazonEKS\_S3\_CSI\_DriverRole*

```
kubectl apply -f mountpoint-s3-service-account.yaml
```

 Note

Wenn Sie das Plugin in diesem Verfahren bereitstellen, wird es erstellt und für die Verwendung eines Servicekontos mit dem Namen `s3-csi-driver-sa` konfiguriert.

### Schritt 3: Installieren Sie den Mountpoint for Amazon S3 CSI-Treiber

Sie können den Mountpoint for Amazon S3 CSI-Treiber über das Amazon EKS-Add-on installieren. Sie können die folgenden Tools verwenden, um das Add-on zu Ihrem Cluster hinzuzufügen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)
- [the section called “AWS CLI”](#)

Alternativ können Sie den Mountpoint for Amazon S3 CSI-Treiber als selbstverwaltete Installation installieren. Anweisungen zur Durchführung einer selbstverwalteten Installation finden Sie im GitHub unter [Installation](#).

Ausgehend von können Sie Taints so konfigurieren `env1.8.0`, dass sie für die Pods des CSI-Treibers toleriert werden. Geben Sie dazu entweder einen benutzerdefinierten Satz von Taints an, mit denen Sie tolerieren möchten, `node.tolerations` oder Sie können alle Taints mit tolerieren.

`node.tolerateAllTaints` Weitere Informationen finden Sie unter [Taints and Tolerations](#) in der Kubernetes-Dokumentation.

`eksctl`

Um das Amazon S3 CSI-Add-on hinzuzufügen, verwenden Sie **`eksctl`**

Führen Sie den folgenden Befehl aus. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters, *111122223333* mit Ihrer Konto-ID und *AmazonEKS\_S3\_CSI\_DriverRole* mit dem Namen der [zuvor erstellten IAM-Rolle](#).

```
eksctl create addon --name aws-mountpoint-s3-csi-driver --cluster my-cluster \
 --service-account-role-arn arn:aws:iam::111122223333:role/
 AmazonEKS_S3_CSI_DriverRole --force
```

Wenn Sie die Option *--force* entfernen und eine der Amazon-EKS-Add-on-Einstellungen mit Ihren vorhandenen Einstellungen in Konflikt steht, schlägt die Aktualisierung des Amazon-EKS-Add-ons fehl und Sie erhalten eine Fehlermeldung, die Sie bei der Lösung des Konflikts unterstützt. Bevor Sie diese Option angeben, stellen Sie sicher, dass das Amazon EKS-Add-on keine Einstellungen verwaltet, die Sie verwalten müssen, da diese Einstellungen mit dieser Option überschrieben werden. Weitere Informationen zu anderen Optionen für diese Einstellung finden Sie unter [Add-Ons](#) in der `eksctl`-Dokumentation. Weitere Informationen zur Amazon EKS Kubernetes-Feldverwaltung finden Sie unter [the section called “Felder, die Sie anpassen können”](#)

Sie können `eksctl` mithilfe von Konfigurationsdateien Anpassungen vornehmen. Weitere Informationen finden Sie in der `eksctl` Dokumentation unter [Arbeiten mit Konfigurationswerten](#). Das folgende Beispiel zeigt, wie man alle Taints toleriert.

```
config.yaml
...

addons:
- name: aws-mountpoint-s3-csi-driver
 serviceAccountRoleARN: arn:aws:iam::111122223333:role/AmazonEKS_S3_CSI_DriverRole
 configurationValues: |-
 node:
 tolerateAllTaints: true
```

## AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).

2. Wählen Sie im linken Navigationsbereich Cluster aus.
3. Wählen Sie den Namen des Clusters, für den Sie das Mountpoint for Amazon S3 CSI-Add-on konfigurieren möchten.
4. Wählen Sie die Registerkarte Add-ons.
5. Wählen Sie Weitere Add-Ons erhalten.
6. Führen Sie auf der Seite Add-Ons auswählen die folgenden Schritte aus:
  - a. Aktivieren Sie im Bereich Amazon EKS-Addons das Kontrollkästchen Mountpoint for Amazon S3 CSI Driver.
  - b. Wählen Sie Weiter aus.
7. Gehen Sie auf der Seite Konfigurieren ausgewählter Add-Ons-Einstellungen wie folgt vor:
  - a. Wählen Sie die Version aus, die Sie verwenden möchten.
  - b. Wählen Sie für Select IAM role den Namen einer IAM-Rolle aus, der Sie die Mountpoint for Amazon S3 CSI-Treiber-IAM-Richtlinie angehängt haben.
  - c. (Optional) Aktualisieren Sie die Methode zur Konfliktlösung, nachdem Sie die optionalen Konfigurationseinstellungen erweitert haben. Wenn Sie Override auswählen, können eine oder mehrere Einstellungen für das bestehende Add-on mit den Amazon EKS-Add-On-Einstellungen überschrieben werden. Wenn Sie diese Option nicht aktivieren und ein Konflikt mit Ihren vorhandenen Einstellungen besteht, schlägt der Vorgang fehl. Sie können die sich daraus ergebende Fehlermeldung heranziehen, um den Konflikt zu beheben. Bevor Sie diese Option auswählen, stellen Sie sicher, dass das Amazon EKS-Add-on keine Einstellungen verwaltet, die Sie selbst verwalten müssen.
  - d. (Optional) Konfigurieren Sie Toleranzen im Feld Konfigurationswerte, nachdem Sie die optionalen Konfigurationseinstellungen erweitert haben.
  - e. Wählen Sie Weiter aus.
8. Wählen Sie auf der Seite Überprüfen und hinzufügen die Option Erstellen aus. Nachdem die Installation der Add-Ons abgeschlossen ist, wird Ihr installiertes Add-On angezeigt.

## AWS CLI

So fügen Sie das Mountpoint for Amazon S3 CSI Add-on mit der CLI hinzu AWS

Führen Sie den folgenden Befehl aus. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters, *111122223333* mit Ihrer Konto-ID und *AmazonEKS\_S3\_CSI\_DriverRole* mit dem Namen der zuvor erstellten Rolle.

```
aws eks create-addon --cluster-name my-cluster --addon-name aws-mountpoint-s3-csi-driver \
 --service-account-role-arn arn:aws:iam::111122223333:role/AmazonEKS_S3_CSI_DriverRole
```

Sie können den Befehl mit dem Flag anpassen. `--configuration-values` Das folgende alternative Beispiel zeigt, wie man alle Makel toleriert.

```
aws eks create-addon --cluster-name my-cluster --addon-name aws-mountpoint-s3-csi-driver \
 --service-account-role-arn arn:aws:iam::111122223333:role/AmazonEKS_S3_CSI_DriverRole \
 --configuration-values '{"node":{"tolerateAllTaints":true}}'
```

## Schritt 4: Mountpoint für Amazon S3 konfigurieren

In den meisten Fällen können Sie Mountpoint für Amazon S3 nur mit einem Bucket-Namen konfigurieren. Anweisungen zur Konfiguration von Mountpoint für Amazon S3 finden Sie unter [Mountpoint für Amazon S3 konfigurieren](#) auf GitHub

## Schritt 5: Stellen Sie eine Beispielanwendung bereit

Sie können die statische Bereitstellung des Treibers in einem vorhandenen Amazon S3-Bucket einsetzen. Weitere Informationen finden Sie unter [Statische Bereitstellung](#) auf GitHub.

## Entfernen Sie das Amazon EKS-Add-on Mountpoint für Amazon S3

Sie haben zwei Möglichkeiten, den [Mountpoint for Amazon S3 CSI-Treiber](#) zu entfernen.

- Beibehalten von Add-on-Software auf Ihrem Cluster - Diese Option entfernt die Amazon-EKS-Verwaltung aller Einstellungen. Amazon EKS wird außerdem die Möglichkeit aufgehoben, Sie über Updates zu informieren und das Amazon-EKS-Add-on automatisch zu aktualisieren, nachdem Sie ein Update eingeleitet haben. Es behält jedoch die Add-on-Software auf Ihrem Cluster bei. Diese Option macht das Add-on zu einem selbstverwalteten Add-on statt einem Amazon-EKS-Add-on. Mit dieser Option gibt es keine Ausfallzeiten für das Add-on. Die Befehle in diesem Verfahren verwenden diese Option.
- Entfernen Sie die Add-on-Software vollständig aus Ihrem Cluster – Wir empfehlen, dass Sie das Amazon-EKS-Add-on nur aus Ihrem Cluster entfernen, wenn auf Ihrem Cluster keine Ressourcen



vorhanden sind, die davon abhängig sind. Um diese Option durchzuführen, löschen Sie `--preserve` aus dem Befehl, den Sie für dieses Verfahren verwenden.

Wenn dem Add-on ein IAM-Konto zugeordnet ist, wird das IAM-Konto nicht entfernt.

Sie können die folgenden Tools verwenden, um das Amazon S3 CSI-Add-on zu entfernen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)
- [the section called “AWS CLI”](#)

## eksctl

Um das Amazon S3 CSI-Add-on zu entfernen, verwenden Sie **eksctl**

Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und führen Sie dann den folgenden Befehl aus.

```
eksctl delete addon --cluster my-cluster --name aws-mountpoint-s3-csi-driver --preserve
```

## AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das Amazon-EBS-CSI-Add-on entfernen möchten.
4. Wählen Sie die Registerkarte Add-ons.
5. Wählen Sie Mountpoint for Amazon S3 CSI Driver.
6. Wählen Sie Remove (Entfernen) aus.
7. Gehen Sie im Bestätigungsdialogfeld Remove: aws-mountpoint-s 3-csi-driver wie folgt vor:
  - a. Wenn Amazon EKS die Verwaltung von Einstellungen für das Add-on einstellen soll, wählen Sie Auf dem Cluster beibehalten. Tun Sie dies, wenn Sie die Add-on-Software auf Ihrem Cluster behalten möchten. Auf diese Weise können Sie alle Einstellungen des Add-ons selbst verwalten.
  - b. Geben Sie `aws-mountpoint-s3-csi-driver` ein.

c. Wählen Sie Entfernen aus.

## AWS CLI

So entfernen Sie das Amazon S3 CSI-Add-on mit der AWS CLI

Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und führen Sie dann den folgenden Befehl aus.

```
aws eks delete-addon --cluster-name my-cluster --addon-name aws-mountpoint-s3-csi-driver --preserve
```

## Snapshot-Funktionalität für CSI-Volumes aktivieren

Die Snapshot-Funktionalität ermöglicht point-in-time Kopien Ihrer Daten. Damit diese Funktion in Kubernetes funktioniert, benötigen Sie sowohl einen CSI-Treiber mit Snapshot-Unterstützung (wie den Amazon EBS CSI-Treiber) als auch einen CSI-Snapshot-Controller. Der Snapshot-Controller ist entweder als von Amazon EKS verwaltetes Add-on oder als selbstverwaltete Installation erhältlich.

Die folgenden Punkte sind bei der Verwendung des CSI-Snapshot-Controllers zu beachten.

- Der Snapshot-Controller muss zusammen mit einem CSI-Treiber mit Snapshot-Funktionalität installiert werden. Anweisungen zur Installation des Amazon EBS CSI-Treibers finden Sie unter [the section called “Amazon EBS”](#).
- Kubernetes unterstützt keine Snapshots von Volumes, die über die CSI-Migration bereitgestellt werden, wie z. B. Amazon EBS-Volumes, die einen with Provisioner verwenden. StorageClass `kubernetes.io/aws-efs` Volumes müssen mit einer StorageClass erstellt werden, die auf den CSI-Treiber-Provisioner `ebs.csi.aws.com` verweist.
- Der automatische Modus von Amazon EKS beinhaltet nicht den Snapshot-Controller. Die Speicherfähigkeit des EKS Auto Mode ist mit dem Snapshot-Controller kompatibel.

Wir empfehlen, den CSI-Snapshot über das von Amazon EKS verwaltete Add-on zu installieren. Dieses Add-on enthält die benutzerdefinierten Ressourcendefinitionen (CRDs), die zum Erstellen und Verwalten von Snapshots auf Amazon EKS benötigt werden. Wenn Sie ein Amazon-EKS-Add-on zu Ihrem Cluster hinzufügen möchten, lesen Sie [the section called “Erstellen Sie ein Add-on”](#). Weitere Informationen zu Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

Wenn Sie alternativ eine selbstverwaltete Installation des CSI-Snapshot-Controllers wünschen, finden Sie weitere Informationen unter [Verwendung](#) im external-snapshotter Upstream-Kubernetes unter. GitHub

# Netzwerk für Amazon EKS-Cluster konfigurieren

Ihr Amazon-EKS-Cluster wird in einer VPC erstellt. Pod-Netzwerke werden durch das Amazon VPC Container Network Interface (CNI) -Plugin für Knoten bereitgestellt, die auf AWS der Infrastruktur ausgeführt werden. Wenn Sie Knoten in Ihrer eigenen Infrastruktur ausführen, finden Sie weitere Informationen unter [the section called “CNI konfigurieren”](#). In diesem Kapitel finden Sie die folgenden Themen, um mehr über Networking für Ihren Cluster zu erfahren.

## Themen

- [Fügen Sie über die Managementkonsole ein vorhandenes VPC-Subnetz zu einem Amazon EKS-Cluster hinzu](#)
- [Die Amazon EKS-Netzwerkanforderungen für VPC und Subnetze anzeigen](#)
- [Erstellen Sie eine Amazon VPC für Ihren Amazon EKS-Cluster](#)
- [Amazon EKS-Sicherheitsgruppenanforderungen für Cluster anzeigen](#)
- [Netzwerk-Add-Ons für Amazon EKS-Cluster verwalten](#)

## Fügen Sie über die Managementkonsole ein vorhandenes VPC-Subnetz zu einem Amazon EKS-Cluster hinzu

1. Navigieren Sie in der Managementkonsole zu Ihrem Cluster
2. Wählen Sie auf der Registerkarte Netzwerk die Option VPC-Ressourcen verwalten aus.
3. Wählen Sie in der Dropdownliste Subnetze zusätzliche Subnetze aus der VPC Ihres Clusters aus.

So erstellen Sie ein neues VPC-Subnetz:

- [Überprüfen Sie die EKS-Subnetzanforderungen](#)
- Weitere Informationen finden [Sie unter Erstellen eines Subnetzes](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

# Die Amazon EKS-Netzwerkanforderungen für VPC und Subnetze anzeigen

Wenn Sie einen Cluster erstellen, geben Sie eine [VPC](#) und mindestens zwei Subnetze an, die sich in unterschiedlichen Availability Zones befinden. Dieses Thema bietet einen Überblick über die spezifischen Amazon-EKS-Anforderungen und Überlegen zur VPC und den Subnetzen, die Sie in Ihrem Cluster verwenden. Wenn Sie keine VPC zur Verwendung mit Amazon EKS haben, finden Sie weitere Informationen unter [the section called “Erstellen einer VPC”](#). Wenn Sie einen lokalen oder erweiterten Cluster auf AWS Outposts erstellen, lesen Sie [the section called “Erstellen von VPC und Subnetzen”](#) statt dieses Themas weiter. Der Inhalt dieses Themas gilt für Amazon EKS-Cluster mit Hybridknoten. Zusätzliche Netzwerkanforderungen für Hybridknoten finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#).

## VPC-Anforderungen und -Überlegungen

Wenn Sie einen Cluster erstellen, muss die von Ihnen angegebene VPC die folgenden Anforderungen und Überlegungen erfüllen:

- Die VPC muss über eine ausreichende Anzahl von IP-Adressen für den Cluster, alle Knoten und andere Kubernetes-Ressourcen, die Sie erstellen möchten, verfügen. Wenn die VPC, die Sie verwenden möchten, nicht über eine ausreichende Anzahl von IP-Adressen verfügt, versuchen Sie, die Anzahl der verfügbaren IP-Adressen zu erhöhen.

Sie können dies tun, indem Sie die Clusterkonfiguration aktualisieren, um zu ändern, welche Subnetze und Sicherheitsgruppen der Cluster verwendet. Sie können von der AWS Management Console, der neuesten Version der AWS CLI AWS CloudFormation, und eksctl Version v0.164.0-rc.0 oder höher aus aktualisieren. Möglicherweise müssen Sie dies tun, um Subnetzen mehr verfügbare IP-Adressen zur Verfügung zu stellen, damit eine Clusterversion erfolgreich aktualisiert werden kann.

### Important

Alle Subnetze, die Sie hinzufügen, müssen sich in derselben Gruppe befinden, die ursprünglich bei der AZs Erstellung des Clusters bereitgestellt wurde. Neue Subnetze müssen alle anderen Anforderungen erfüllen, z. B. müssen sie über ausreichend IP-Adressen verfügen.

Angenommen, Sie haben einen Cluster erstellt und vier Subnetze angegeben. In der Reihenfolge, in der Sie sie angegeben haben, befindet sich das erste Subnetz in der us -

west-2a Availability Zone, das zweite und dritte Subnetz in der us-west-2b Availability Zone und das vierte Subnetz in der us-west-2c Availability Zone. Wenn Sie die Subnetze ändern möchten, müssen Sie in jeder der drei Availability Zones mindestens ein Subnetz bereitstellen, und die Subnetze müssen sich in derselben VPC wie die ursprünglichen Subnetze befinden.

Wenn Sie mehr IP-Adressen benötigen, als die CIDR-Blöcke in der VPC haben, können Sie zusätzliche CIDR-Blöcke hinzufügen, indem Sie Ihrer VPC [zusätzliche Classless Inter-Domain Routing \(CIDR\)-Blöcke zuordnen](#). Sie können entweder vor oder nach der Erstellung Ihres Clusters private (RFC 1918) und öffentliche (nicht RFC 1918) CIDR-Blöcke mit Ihrer VPC verbinden.

Sie können den neuen CIDR-Block sofort nach dem Hinzufügen verwenden. Da die Kontrollebene den neuen CIDR-Block jedoch erst erkennt, wenn der Abgleich abgeschlossen ist, kann es bis zu fünf Stunden dauern, bis ein CIDR-Block, den Sie einer VPC zugeordnet haben, erkannt wird. Anschließend können Sie die Befehle und ausführen. `kubectl exec kubectl logs` Wenn Sie Pods haben, die als Webhook-Backend fungieren, müssen Sie außerdem warten, bis der Abgleich der Steuerungsebene abgeschlossen ist.

Sie können bei der Verwendung von IP-Adressen sparen, indem Sie ein Transit-Gateway mit einer Shared-Services-VPC verwenden. Weitere Informationen finden Sie unter [Isoliert VPCs mit Shared Services](#) und [Muster zur Aufbewahrung routingfähiger IP-Adressen von Amazon EKS VPC in einem Hybridnetzwerk](#).

- Wenn Sie möchten, dass Kubernetes Pods und Diensten IPv6 Adressen zuweist, ordnen Sie Ihrer VPC einen IPv6 CIDR-Block zu. Weitere Informationen finden Sie unter [Verknüpfen eines IPv6 CIDR-Blocks mit Ihrer VPC](#) im Amazon VPC-Benutzerhandbuch. Sie können keine IPv6 Adressen mit Pods und Diensten verwenden, die auf Hybridknoten ausgeführt werden, und Sie können keine Hybridknoten mit Clustern verwenden, die mit der IPv6 IP-Adressfamilie konfiguriert sind.
- Die VPC muss DNS-Hostnamen und die DNS-Auflösung unterstützen. Andernfalls können sich Knoten nicht in Ihrem Cluster registrieren. Weitere Informationen finden Sie unter [DNS-Attribute für Ihre VPC](#) im Amazon-VPC-Benutzerhandbuch.
- Die VPC erfordert möglicherweise die Verwendung von VPC-Endpunkten. AWS PrivateLink Weitere Informationen finden Sie unter [the section called "Subnetz-Anforderungen und -Überlegungen"](#).

Wenn Sie einen Cluster mit Kubernetes 1.14 oder früher erstellt haben, hat Amazon EKS das folgende Tag zu Ihrer VPC hinzugefügt:

| Schlüssel                                | Wert  |
|------------------------------------------|-------|
| kubernetes.io/cluster/ <i>my-cluster</i> | owned |

Dieses Tag wurde nur von Amazon EKS verwendet. Sie können das Tag entfernen, ohne Ihre Services zu beeinträchtigen. Sie wird nicht mit Clustern der Version 1.15 oder höher verwendet.

## Subnetz-Anforderungen und -Überlegungen

Wenn Sie einen Cluster erstellen, erstellt Amazon EKS 2–4 [Elastic-Network-Schnittstellen](#) in den von Ihnen angegebenen Subnetzen. Diese Netzwerkschnittstellen ermöglichen die Kommunikation zwischen Ihrem Cluster und Ihrer VPC. Die Netzwerkschnittstellen ermöglichen außerdem Kubernetes-Funktionen wie `kubectl exec` und `kubectl logs`. Jede von Amazon EKS erstellte Netzwerkschnittstelle enthält den Text Amazon EKS *cluster-name* in ihrer Beschreibung.

Amazon EKS kann Netzwerkschnittstellen in jedem Subnetz erstellen, dass Sie bei der Erstellung eines Clusters angeben. Nach der Erstellung Ihres Clusters können Sie ändern, in welchen Subnetzen Amazon EKS seine Netzwerkschnittstellen erstellt. Wenn Sie die Kubernetes-Version eines Clusters aktualisieren, löscht Amazon EKS die ursprünglichen Netzwerkschnittstellen, die es erstellt hat, und erstellt neue Netzwerkschnittstellen. Diese Netzwerkschnittstellen können in denselben Subnetzen wie die ursprünglichen Netzwerkschnittstellen oder in anderen Subnetzen als die ursprünglichen Netzwerkschnittstellen erstellt werden. Um zu steuern, in welchen Subnetzen Netzwerkschnittstellen erstellt werden, können Sie die Anzahl der von Ihnen angegebenen Subnetze beim Erstellen eines Clusters auf zwei beschränken oder die Subnetze nach der Erstellung des Clusters aktualisieren.

### Subnetzanforderungen für Cluster

Die [Subnetze](#), die Sie angeben, wenn Sie einen Cluster erstellen oder aktualisieren, müssen die folgenden Anforderungen erfüllen:

- Die Subnetze müssen jeweils mindestens 6 IP-Adressen zur Verwendung durch Amazon EKS haben. Wir empfehlen jedoch mindestens 16 IP-Adressen.
- Die Subnetze müssen sich in mindestens zwei verschiedenen Availability Zones befinden.

- Die Subnetze können sich nicht in AWS Outposts oder Wavelength befinden. AWS Wenn Sie sich in Ihrer VPC befinden, können Sie jedoch selbstverwaltete Knoten und Kubernetes-Ressourcen für diese Subnetz-Typen bereitstellen. Weitere Informationen zu selbstverwalteten Knoten finden Sie unter. [the section called “Selbstverwaltete Knoten”](#)
- Die Subnetze können öffentlich oder privat sein. Es wird jedoch empfohlen, wenn möglich private Subnetze anzugeben. Ein öffentliches Subnetz ist ein Subnetz mit einer Routing-Tabelle, die eine Route zu einem [Internet-Gateway](#) enthält, wohingegen ein privates Subnetz ein Subnetz mit einer Routing-Tabelle ist, die keine Route zu einem Internet-Gateway enthält.
- Die Subnetze dürfen sich nicht in den folgenden Availability Zones befinden:

| AWS Region   | Name der Region            | Unzulässige Verfügbarkeitszone IDs |
|--------------|----------------------------|------------------------------------|
| us-east-1    | USA Ost (Nord-Virginia)    | use1-az3                           |
| us-west-1    | USA West (Nordkalifornien) | usw1-az2                           |
| ca-central-1 | Kanada (Zentral)           | cac1-az3                           |

## Verwendung der IP-Adressfamilie nach Komponenten

Die folgende Tabelle enthält die IP-Adressfamilie, die von jeder Komponente von Amazon EKS verwendet wird. Sie können ein Network Address Translation (NAT) oder ein anderes Kompatibilitätssystem verwenden, um über Quell-IP-Adressen in Familien mit dem Wert „Nein“ für einen Tabelleneintrag eine Verbindung zu diesen Komponenten herzustellen.

Die Funktionalität kann je nach Einstellung der IP-Familie (ipFamily) des Clusters unterschiedlich sein. Diese Einstellung ändert den Typ der IP-Adressen, die für den CIDR-Block verwendet werden, den Kubernetes Services zuweist. Ein Cluster mit dem Einstellungswert von IPv4 wird als Cluster bezeichnet, und ein IPv4 Cluster mit dem Einstellungswert von IPv6 wird als Cluster bezeichnet. IPv6

| Komponente                        | IPv4 Adressen     | IPv6 adressen     | Dual-Stack-Adressen |
|-----------------------------------|-------------------|-------------------|---------------------|
| Öffentlicher Endpunkt der EKS-API | Ja <sup>1,3</sup> | Ja <sup>1,3</sup> | Ja <sup>1,3</sup>   |



| Komponente                                                      | IPv4 Adressen   | IPv6 adressen   | Dual-Stack-Adressen |
|-----------------------------------------------------------------|-----------------|-----------------|---------------------|
| EKS-API-VPC-Endpunkt                                            | Ja              | Nein            | Nein                |
| Öffentlicher Endpunkt der EKS Auth API (EKS Pod Identity)       | Ja <sup>1</sup> | Ja <sup>1</sup> | Ja <sup>1</sup>     |
| VPC-Endpunkt der EKS-Authentifizierungs-API (EKS-Pod-Identität) | Ja <sup>1</sup> | Ja <sup>1</sup> | Ja <sup>1</sup>     |
| IPv4 Öffentlicher Endpunkt 2 des Kubernetes-Clusters            | Ja              | Nein            | Nein                |
| IPv4 Privater Endpunkt 2 des Kubernetes-Clusters                | Ja              | Nein            | Nein                |
| IPv6 Öffentlicher Endpunkt 2 des Kubernetes-Clusters            | Ja 1,4          | Ja 1,4          | Ja <sup>4</sup>     |
| IPv6 Privater Endpunkt 2 des Kubernetes-Clusters                | Ja 1,4          | Ja 1,4          | Ja <sup>4</sup>     |
| Kubernetes-Cluster-Subnetze                                     | Ja <sup>2</sup> | Nein            | Ja <sup>2</sup>     |
| Primäre IP-Adressen des Knotens                                 | Ja <sup>2</sup> | Nein            | Ja <sup>2</sup>     |
| Cluster-CIDR-Bereich für Service-IP-Adressen                    | Ja <sup>2</sup> | Ja <sup>2</sup> | Nein                |
| Pod-IP-Adressen von der VPC CNI                                 | Ja <sup>2</sup> | Ja <sup>2</sup> | Nein                |

| Komponente              | IPv4 Adressen     | IPv6 adressen     | Dual-Stack-Adressen |
|-------------------------|-------------------|-------------------|---------------------|
| IRSA OIDC-Emittent URLs | Ja <sup>1,3</sup> | Ja <sup>1,3</sup> | Ja <sup>1,3</sup>   |

### Note

<sup>1</sup> Der Endpunkt ist ein Dual-Stack mit beiden IPv4 IPv6 Adressen. Ihre Anwendungen außerhalb AWS, Ihre Knoten für den Cluster und Ihre Pods innerhalb des Clusters können diesen Endpunkt entweder mit IPv4 oder erreichenIPv6.

<sup>2</sup> Wenn Sie einen IPv4 Cluster erstellen, wählen Sie in der IP-Familie (ipFamily) - Einstellung des Clusters zwischen einem Cluster und einem Cluster. Diese Einstellung kann nicht geändert werden. IPv6 Stattdessen müssen Sie eine andere Einstellung wählen, wenn Sie einen weiteren Cluster erstellen und Ihre Workloads migrieren.

<sup>3</sup> Der Dual-Stack-Endpoint wurde im August 2024 eingeführt. Informationen zur Verwendung der Dual-Stack-Endpunkte mit der AWS CLI finden Sie in der Konfiguration von [Dual-Stack- und FIPS-Endpunkten](#) im AWS SDKs Referenzhandbuch zu Tools. Im Folgenden sind die neuen Endpunkte aufgeführt:

Öffentlicher Endpunkt der EKS-API

`eks.region.api.aws`

IRSA OIDC-Emittent URLs

`oidc-eks.region.api.aws`

<sup>4</sup> Der Dual-Stack-Cluster-Endpoint wurde im Oktober 2024 eingeführt. EKS erstellt den folgenden Endpunkt für neue Cluster, die nach diesem Datum erstellt werden und die IPv6 in der Einstellung IP-Familie (IPFamily) des Clusters ausgewählt werden:

Öffentlicher/privater Endpunkt des EKS-Clusters

`eks-cluster.region.api.aws`

## Subnetzanforderungen für Knoten

Sie können Knoten und Kubernetes-Ressourcen in denselben Subnetzen bereitstellen, die Sie beim Erstellen Ihres Clusters angeben. Dies ist jedoch nicht erforderlich. Dies liegt daran, dass Sie Knoten und Kubernetes-Ressourcen auch in Subnetzen bereitstellen können, die Sie bei der Erstellung des Clusters nicht angegeben haben. Wenn Sie Knoten in verschiedenen Subnetzen bereitstellen, erstellt Amazon EKS keine Cluster-Netzwerkschnittstellen in diesen Subnetzen. Jedes Subnetz, für das Sie Knoten und Kubernetes-Ressourcen bereitstellen, muss die folgenden Anforderungen erfüllen:

- Die Subnetze müssen über genügend verfügbare IP-Adressen verfügen, um alle Ihre Knoten und Kubernetes-Ressourcen bereitzustellen.
- Wenn Sie möchten, dass Kubernetes Pods und Diensten IPv6 Adressen zuweist, benötigen Sie einen IPv6 CIDR-Block und einen IPv4 CIDR-Block, die Ihrem Subnetz zugeordnet sind. Weitere Informationen finden Sie unter [Zuordnen eines IPv6 CIDR-Blocks zu Ihrem Subnetz](#) im Amazon VPC-Benutzerhandbuch. Die Routing-Tabellen, die Ihren Subnetzen zugeordnet sind, müssen Routen zu IPv4- und IPv6-Adressen enthalten. Weitere Informationen finden Sie unter [Routen](#) im Amazon-VPC-Benutzerhandbuch. Pods werden nur einer IPv6-Adresse zugewiesen. Die Netzwerkschnittstellen, die Amazon EKS für Ihren Cluster und Ihre Knoten erstellt, werden jedoch einer IPv4- und einer IPv6-Adresse zugewiesen.
- Wenn Sie eingehenden Zugriff aus dem Internet auf Ihre Pods benötigen, stellen Sie sicher, dass mindestens ein öffentliches Subnetz mit ausreichend verfügbaren IP-Adressen für die Bereitstellung von Load Balancern und Ingresses vorhanden ist. Sie können Load Balancer in öffentlichen Subnetzen bereitstellen. Load Balancer können einen Lastenausgleich auf Pods in privaten oder öffentlichen Subnetzen durchführen. Wir empfehlen, Ihre Knoten nach Möglichkeit in privaten Subnetzen bereitzustellen.
- Wenn Sie planen, Knoten in einem öffentlichen Subnetz bereitzustellen, muss das Subnetz automatisch öffentliche IPv4- oder IPv6-Adressen zuweisen. Wenn Sie Knoten in einem privaten Subnetz bereitstellen, das einen zugeordneten IPv6-CIDR-Block hat, muss das private Subnetz zudem IPv6-Adressen automatisch zuweisen. Wenn Sie die von Amazon EKS bereitgestellte AWS CloudFormation Vorlage für die Bereitstellung Ihrer VPC nach dem 26. März 2020 verwendet haben, ist diese Einstellung aktiviert. Wenn Sie die Vorlagen verwendet haben, um Ihre VPC vor diesem Datum bereitzustellen oder Ihre eigene VPC verwenden, müssen Sie diese Einstellung manuell aktivieren. Die Vorlage finden Sie unter [the section called “Erstellen einer VPC”](#). Weitere Informationen finden Sie unter [Ändern des öffentlichen IPv4 Adressierungsattributs für Ihr Subnetz](#) und [Ändern des IPv6 Adressierungsattributs für Ihr Subnetz](#) im [Amazon VPC-Benutzerhandbuch](#).

- Wenn es sich bei dem Subnetz, in dem Sie einen Knoten bereitstellen, um ein privates Subnetz handelt und die Routing-Tabelle keine Route zu einem [NAT-Gerät \(Network Address Translation\)](#) () oder einem [reinen Ausgangsgateway](#) (IPv4IPv6) enthält, fügen Sie Ihrer VPC VPC-Endpunkte hinzu, die Sie verwenden. AWS PrivateLink VPC-Endpunkte werden für alle AWS Dienste benötigt, mit denen Ihre Knoten und Pods kommunizieren müssen. Beispiele hierfür sind Amazon ECR, Elastic Load Balancing CloudWatch, Amazon, AWS Security Token Service und Amazon Simple Storage Service (Amazon S3). Der Endpunkt muss das Subnetz enthalten, in dem sich die Knoten befinden. Nicht alle AWS Dienste unterstützen VPC-Endpunkte. Weitere Informationen finden Sie unter [Was ist? AWS PrivateLink](#) und [AWS Dienste, die sich in integrieren lassen AWS PrivateLink](#). Eine Liste weiterer Amazon-EKS-Anforderungen finden Sie unter [the section called “Private Cluster”](#).
- Wenn Sie Load Balancer in einem Subnetz bereitstellen möchten, muss das Subnetz das folgende Tag haben:
  - Private Subnetze

| Schlüssel                       | Wert |
|---------------------------------|------|
| kubernetes.io/role/internal-elb | 1    |

- Öffentliche Subnetze

| Schlüssel              | Value (Wert) |
|------------------------|--------------|
| kubernetes.io/role/elb | 1            |

Als ein Kubernetes-Cluster dieser Version 1.18 und früher erstellt wurde, fügte Amazon EKS allen angegebenen Subnetzen das folgende Tag hinzu.

| Schlüssel                                | Value (Wert) |
|------------------------------------------|--------------|
| kubernetes.io/cluster/ <i>my-cluster</i> | shared       |

Wenn Sie jetzt einen neuen Kubernetes-Cluster erstellen, fügt Amazon EKS das Tag nicht zu Ihren Subnetzen hinzu. Wenn sich das Tag in Subnetzen befand, die von einem Cluster verwendet wurden,

bei dem es sich um eine frühere Version handelte<sup>1</sup>. 19, wurde das Tag nicht automatisch aus den Subnetzen entfernt, als der Cluster auf eine neuere Version aktualisiert wurde. Für Version 2.1.1 oder früher des Load AWS Balancer Controllers ist dieses Tag erforderlich. Wenn Sie eine neuere Version des Load Balancer Controllers verwenden, können Sie das Tag entfernen, ohne Ihre Services zu unterbrechen. Weitere Informationen zum Controller finden Sie unter [the section called “AWS Load Balancer Controller”](#).

Wenn Sie eine VPC mithilfe einer `eksctl` oder einer der Amazon AWS CloudFormation EKS-VPC-Vorlagen bereitgestellt haben, gilt Folgendes:

- Am oder nach dem 26. März 2020 – Öffentliche IPv4-Adressen werden von öffentlichen Subnetzen automatisch neuen Knoten zugewiesen, die in öffentlichen Subnetzen bereitgestellt werden.
- Vor dem 26. März 2020 — Öffentliche IPv4 Adressen werden von öffentlichen Subnetzen nicht automatisch neuen Knoten zugewiesen, die in öffentlichen Subnetzen bereitgestellt werden.

Diese Änderung wirkt sich folgendermaßen auf neue Knotengruppen aus, die in öffentlichen Subnetzen bereitgestellt werden:

- [Verwaltete Knotengruppen](#) — Wenn die Knotengruppe am oder nach dem 22. April 2020 in einem öffentlichen Subnetz bereitgestellt wird, muss die automatische Zuweisung öffentlicher IP-Adressen für das öffentliche Subnetz aktiviert sein. Weitere Informationen finden Sie unter [Ändern des Attributs für die öffentliche IPv4 Adressierung für Ihr Subnetz](#).
- Selbstverwaltete [Linux](#) -, [Windows](#) - oder [ARM-Knotengruppen](#) — Wenn die Knotengruppe am oder nach dem 26. März 2020 in einem öffentlichen Subnetz bereitgestellt wird, muss die automatische Zuweisung öffentlicher IP-Adressen für das öffentliche Subnetz aktiviert sein. Andernfalls müssen die Knoten mit einer öffentlichen IP-Adresse gestartet werden. Weitere Informationen finden Sie unter [Ändern des Attributs für die öffentliche IPv4 Adressierung für Ihr Subnetz](#) oder [Zuweisen einer öffentlichen IPv4 Adresse beim Instance-Start](#).

## Anforderungen und Überlegungen für gemeinsam genutzte Subnetze

Sie können VPC Sharing verwenden, um Subnetze mit anderen AWS Konten innerhalb derselben AWS Organizations zu teilen. Sie können Amazon-EKS-Cluster in gemeinsam genutzten Subnetzen erstellen. Beachten Sie dabei die folgenden Überlegungen:

- Der Eigentümer des VPC-Subnetzes muss ein Subnetz für ein Teilnehmerkonto freigeben, bevor dieses Konto darin einen Amazon-EKS-Cluster erstellen kann.
- Sie können Ressourcen nicht mit der Standardsicherheitsgruppe für die VPC starten, da sie dem Besitzer gehört. Außerdem können Teilnehmer keine Ressourcen mit Sicherheitsgruppen starten, die anderen Teilnehmern oder dem Eigentümer gehören.
- In einem gemeinsam genutzten Subnetz kontrollieren der Teilnehmer und der Eigentümer die Sicherheitsgruppen innerhalb des jeweiligen Kontos separat. Der Subnetzbesitzer kann von den Teilnehmern erstellte Sicherheitsgruppen zwar anzeigen, jedoch keine Aktionen bei diesen durchführen. Wenn der Subnetzbesitzer diese Sicherheitsgruppen entfernen oder ändern möchte, muss der Teilnehmer, der die Sicherheitsgruppe erstellt hat, die Aktion durchführen.
- Wenn ein Cluster von einem Teilnehmer erstellt wird, gelten die folgenden Überlegungen:
  - Die Cluster-IAM-Rolle und die Knoten-IAM-Rollen müssen in diesem Konto erstellt werden. Weitere Informationen erhalten Sie unter [the section called “Cluster-IAM-Rolle”](#) und [the section called “Knoten-IAM-Rolle”](#).
  - Alle Knoten müssen vom selben Teilnehmer erstellt werden, einschließlich verwalteter Knotengruppen.
- Der Eigentümer einer gemeinsam genutzten VPC kann einen Cluster, den ein Teilnehmer im gemeinsam genutzten Subnetz erstellt, nicht anzeigen, aktualisieren oder löschen. Dies gilt zusätzlich zu den VPC-Ressourcen, auf die jedes Konto unterschiedlich zugreifen kann. Weitere Informationen finden Sie unter [Verantwortlichkeiten und Berechtigungen für Besitzer und Teilnehmer](#) im Amazon-VPC-Benutzerhandbuch.
- Wenn Sie die benutzerdefinierte Netzwerkfunktion des Amazon VPC CNI-Plug-ins für Kubernetes verwenden, müssen Sie die im Besitzerkonto aufgeführten Availability Zone-ID-Zuordnungen verwenden, um jede Zuordnung zu erstellen. ENIConfig Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Netzwerke”](#).

Weitere Informationen zur Freigabe von VPC-Subnetzen finden Sie unter [Freigeben Ihrer VPC für andere Konten](#) im Amazon-VPC-Benutzerhandbuch.

## Erstellen Sie eine Amazon VPC für Ihren Amazon EKS-Cluster

Sie können Amazon Virtual Private Cloud (Amazon VPC) verwenden, um AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ist einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben, sehr ähnlich. Es bietet jedoch die Vorzüge, die mit der Nutzung der skalierbaren Infrastruktur von Amazon Web Services

einhergehen. Bevor Sie sich ein umfassendes Verständnis des Amazon-VPC-Service aneignet, empfehlen wir, dass Sie sich ein umfassendes Verständnis des Amazon-VPC-Service aneignet, bevor Sie sich ein umfassendes Verständnis aneignet. Weitere Informationen finden Sie im [Amazon VPC-Benutzerhandbuch](#).

Ein Amazon-EKS-Cluster, Knoten und Kubernetes-Ressourcen werden auf einer VPC bereitgestellt. Wenn Sie eine vorhandene VPC mit Amazon EKS verwenden möchten, muss diese VPC die unter [the section called “VPC- und Subnetz-Anforderungen”](#) beschriebenen Voraussetzungen erfüllen. In diesem Thema wird beschrieben, wie Sie mithilfe einer von Amazon EKS bereitgestellten AWS CloudFormation Vorlage eine VPC erstellen, die die Amazon EKS-Anforderungen erfüllt. Sobald Sie eine Vorlage bereitgestellt haben, können Sie sich die mit der Vorlage erstellten Ressourcen ansehen, um genau zu wissen, welche Ressourcen mit der Vorlage erstellt wurden und wie diese Ressourcen konfiguriert sind. Wenn Sie Hybridknoten verwenden, muss Ihre VPC Routen in der Routentabelle für Ihr lokales Netzwerk enthalten. Weitere Informationen zu den Netzwerkanforderungen für Hybridknoten finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#)

## Voraussetzungen

Um eine VPC für Amazon EKS zu erstellen, benötigen Sie die erforderlichen IAM-Berechtigungen, um Amazon-VPC-Ressourcen zu erstellen. Bei diesen Ressourcen handelt es sich VPCs um Subnetze, Sicherheitsgruppen, Routingtabellen und Routen sowie Internet- und NAT-Gateways. Weitere Informationen finden [Sie unter Create a VPC with a public subnet example policy](#) im Amazon VPC User Guide und die vollständige Liste der [Aktionen](#) in der [Service](#) Authorization Reference.

Sie können eine VPC mit öffentlichen und privaten Subnetzen, nur öffentlichen Subnetzen oder nur privaten Subnetzen erstellen.

## Öffentliche und private Subnetze

Diese VPC verfügt über zwei öffentliche und zwei private Subnetze. Die einem öffentlichen Subnetz zugeordnete Routing-Tabelle enthält eine Route zu einem Internet-Gateway. Die Routentabelle eines privaten Subnetzes enthält jedoch keine Route zu einem Internet-Gateway. Ein öffentliches und ein privates Subnetz werden in derselben Availability Zone bereitgestellt. Die anderen öffentlichen und privaten Subnetze werden in einer zweiten Availability Zone in derselben AWS Region bereitgestellt. Diese Option wird für die meisten Bereitstellungen empfohlen.

Mit dieser Option können Sie Ihre Knoten in privaten Subnetzen bereitstellen. Diese Option ermöglicht es Kubernetes, Load Balancer für die öffentlichen Subnetze bereitzustellen, die den

Datenverkehr auf Pods verteilen können, die auf Knoten in den privaten Subnetzen ausgeführt werden. Öffentliche IPv4 Adressen werden automatisch Knoten zugewiesen, die in öffentlichen Subnetzen bereitgestellt werden, aber öffentliche IPv4 Adressen werden Knoten, die in privaten Subnetzen bereitgestellt werden, nicht zugewiesen.

Sie können Knoten in öffentlichen und privaten Subnetzen auch IPv6-Adressen zuweisen. Die Knoten in privaten Subnetzen können mit dem Cluster und anderen Diensten kommunizieren. AWS Pods können über ein NAT-Gateway unter Verwendung von IPv4 Adressen oder über ein Internet-Gateway nur für ausgehende Verbindungen mithilfe von Adressen, die in jeder Availability Zone bereitgestellt werden, mit IPv6 dem Internet kommunizieren. Es wird eine Sicherheitsgruppe bereitgestellt, die über Regeln verfügt, die den gesamten eingehenden Datenverkehr von anderen Quellen als dem Cluster oder den Knoten ablehnen, jedoch den gesamten ausgehenden Datenverkehr zulassen. Die Subnetze sind getaggt, damit Kubernetes ihnen Load Balancer bereitstellen kann.

- a. Öffnen Sie die [AWS CloudFormation -Konsole](#).
- b. Wählen Sie in der Navigationsleiste eine AWS Region aus, die Amazon EKS unterstützt.
- c. Klicken Sie auf Create stack (Stack erstellen), With new resources (standard) (Mit neuen Ressourcen (Standard)).
- d. Stellen Sie unter Voraussetzung – Vorbereiten der Vorlage sicher, dass Vorlage ist bereit ausgewählt ist und wählen Sie dann unter Vorlage angeben Amazon-S3-URL aus.
- e. Sie können eine VPC erstellen, die nur IPv4 unterstützt, oder eine VPC, die IPv4 und IPv6 unterstützt. Fügen Sie eine der folgenden Optionen URLs in den Textbereich unter Amazon S3 S3-URL ein und wählen Sie Weiter aus:
  - IPv4

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml
```

- IPv4 und IPv6

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-ipv6-vpc-public-private-subnets.yaml
```



- a. Ändern Sie auf der Seite Specify stack details (Stack-Details angeben) alle Parameter und wählen Sie dann Next (Weiter) aus.
- **Stack-Name:** Wählen Sie einen Stack-Namen für Ihren AWS CloudFormation Stack. Sie können beispielsweise den im vorigen Schritt verwendeten Vorlagennamen nutzen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
  - **VpcBlock:** Wählen Sie einen IPv4 CIDR-Bereich für Ihre VPC. Jedem Knoten, Pod und Load Balancer, den Sie bereitstellen, wird eine IPv4 Adresse aus diesem Block zugewiesen. Die IPv4 Standardwerte bieten ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie sie ändern. Weitere Informationen finden Sie unter [Dimensionierung der VPC und der Subnetze](#) im Amazon VPC Benutzerhandbuch. Sie können der VPC auch zusätzliche CIDR-Blöcke hinzufügen, sobald sie erstellt wurde. Wenn Sie eine IPv6 VPC erstellen, werden Ihnen IPv6 CIDR-Bereiche automatisch aus dem Global Unicast-Adressraum von Amazon zugewiesen.
  - **PublicSubnet01Block:** Geben Sie einen IPv4 CIDR-Block für das öffentliche Subnetz 1 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern. Wenn Sie eine IPv6 VPC erstellen, wird dieser Block in der Vorlage für Sie angegeben.
  - **PublicSubnet02Block:** Geben Sie einen IPv4 CIDR-Block für das öffentliche Subnetz 2 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern. Wenn Sie eine IPv6 VPC erstellen, wird dieser Block in der Vorlage für Sie angegeben.
  - **PrivateSubnet01Block:** Geben Sie einen IPv4 CIDR-Block für das private Subnetz 1 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern. Wenn Sie eine IPv6 VPC erstellen, wird dieser Block in der Vorlage für Sie angegeben.
  - **PrivateSubnet02Block:** Geben Sie einen IPv4 CIDR-Block für das private Subnetz 2 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern. Wenn Sie eine IPv6 VPC erstellen, wird dieser Block in der Vorlage für Sie angegeben.
- b. (Optional) Auf der Seite Configure stack options (Stack-Optionen konfigurieren) können Sie Ihre Stack-Ressourcen markieren und dann Next (Weiter) auswählen.
- c. Wählen Sie auf der Seite Prüfen Stack erstellen aus.

- d. Wenn Ihr Stack erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgänge).
- e. Notieren Sie das VpcId für die VPC, die erstellt wurde. Dies benötigen Sie, wenn Sie Ihren Cluster und Ihre Knoten erstellen.
- f. Notieren Sie SubnetIds für die Subnetze, die erstellt wurden, und ob Sie sie als öffentliche oder private Subnetze erstellt haben. Sie benötigen mindestens zwei davon, wenn Sie Ihren Cluster und Ihre Knoten erstellen.
- g. Wenn Sie eine IPv4-VPC erstellt haben, überspringen Sie diesen Schritt. Wenn Sie eine IPv6-VPC erstellt haben, müssen Sie die Option zum automatischen Zuweisen von IPv6-Adressen für die öffentlichen Subnetze aktivieren, die von der Vorlage erstellt wurden. Diese Einstellung ist für die privaten Subnetze bereits aktiviert. Führen Sie die folgenden Schritte aus, um die Einstellung zu aktivieren:
  - i. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
  - ii. Wählen Sie im linken Navigationsbereich die Option Subnets (Subnetze) aus.
  - iii. Wählen Sie eines Ihrer öffentlichen Subnetze aus (**stack-name**/SubnetPublic01 oder **stack-name**/SubnetPublic02 enthält das Wort öffentlich) und wählen Sie Aktionen, Subnetzeinstellungen bearbeiten.
  - iv. Aktivieren Sie das Kontrollkästchen Automatische IPv6 Adresszuweisung aktivieren und wählen Sie dann Speichern.
  - v. Wiederholen Sie die vorherigen Schritte für Ihr anderes öffentliches Subnetz.

## Nur öffentliche Subnetze

Diese VPC hat drei öffentliche Subnetze, die in verschiedenen Availability Zones in einer AWS Region bereitgestellt werden. Allen Knoten werden automatisch öffentliche IPv4-Adressen zugewiesen und alle Worker-Knoten können Internetdatenverkehr über ein [Internet-Gateway](#) senden und empfangen. Es wird eine [Sicherheitsgruppe](#) bereitgestellt, die den gesamten eingehenden Datenverkehr ablehnt und den gesamten ausgehenden Datenverkehr zulässt. Die Subnetze sind getaggt, damit Kubernetes ihnen Load Balancer bereitstellen kann.

- a. Öffnen Sie die [AWS CloudFormation -Konsole](#).
- b. Wählen Sie in der Navigationsleiste eine AWS Region aus, die Amazon EKS unterstützt.
- c. Klicken Sie auf Create stack (Stack erstellen), With new resources (standard) (Mit neuen Ressourcen (Standard)).

- d. Stellen Sie unter Vorbereiten der Vorlage sicher, dass Vorlage ist bereit ausgewählt ist und wählen Sie dann unter Vorlagenquelle Amazon-S3-URL aus.
- e. Fügen Sie die folgende URL in den Textbereich unter Amazon-S3-URL ein und wählen Sie Weiter aus:

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-vpc-sample.yaml
```

- a. Füllen Sie auf der Seite Specify Details (Details angeben) die Parameter entsprechend aus und klicken Sie dann auf Next (Weiter).
  - Stack-Name: Wählen Sie einen Stack-Namen für Ihren AWS CloudFormation Stack. Sie können ihn beispielsweise *amazon-eks-vpc-sample* nennen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
  - VpcBlock: Wählen Sie einen CIDR-Block für Ihre VPC. Jedem Knoten, Pod und Load Balancer, den Sie bereitstellen, wird eine IPv4 Adresse aus diesem Block zugewiesen. Die IPv4 Standardwerte bieten ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie sie ändern. Weitere Informationen finden Sie unter [Dimensionierung der VPC und der Subnetze](#) im Amazon VPC Benutzerhandbuch. Sie können der VPC auch zusätzliche CIDR-Blöcke hinzufügen, sobald sie erstellt wurde.
  - Subnet01Block: Geben Sie einen CIDR-Block für das Subnetz 1 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern.
  - Subnet02Block: Geben Sie einen CIDR-Block für das Subnetz 2 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern.
  - Subnet03Block: Geben Sie einen CIDR-Block für das Subnetz 3 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern.
- b. (Optional) Markieren Sie auf der Seite Options (Optionen) Ihre Stack-Ressourcen. Wählen Sie Next (Weiter).
- c. Klicken Sie auf der Seite Review auf Create.

- d. Wenn Ihr Stack erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgänge).
- e. Notieren Sie das `VpcId` für die VPC, die erstellt wurde. Dies benötigen Sie, wenn Sie Ihren Cluster und Ihre Knoten erstellen.
- f. Notieren Sie das `SubnetIds` für die Subnetze, die erstellt wurden. Sie benötigen mindestens zwei davon, wenn Sie Ihren Cluster und Ihre Knoten erstellen.
- g. (Optional) Jeder Cluster, den Sie in dieser VPC bereitstellen, kann Ihren Pods und Diensten private IPv4 Adressen zuweisen. Wenn Sie Cluster für diese VPC bereitstellen möchten, um Ihren Pods und Diensten private IPv6 Adressen zuzuweisen, aktualisieren Sie Ihre VPC, Ihr Subnetz, Ihre Routing-Tabellen und Sicherheitsgruppen. Weitere Informationen finden Sie unter [Vorhandenes migrieren VPCs von IPv4 zu IPv6](#) im Amazon VPC-Benutzerhandbuch. Amazon EKS verlangt, dass bei Ihren Subnetzen die Option zum Auto-assign von IPv6-Adressen aktiviert ist. Standardmäßig ist es deaktiviert.

## Nur private Subnetze

Diese VPC hat drei private Subnetze, die in verschiedenen Availability Zones in der AWS Region bereitgestellt werden. Ressourcen, die in den Subnetzen bereitgestellt werden, können nicht auf das Internet zugreifen, und das Internet kann auch nicht auf Ressourcen in den Subnetzen zugreifen. Die Vorlage erstellt [VPC-Endpunkte](#), die AWS PrivateLink für verschiedene AWS Dienste verwendet werden, auf die Knoten normalerweise zugreifen müssen. Wenn Ihre Knoten einen ausgehenden Internetzugang benötigen, können Sie ein öffentliches [NAT-Gateway](#) in der Availability Zone jedes Subnetzes hinzufügen, nachdem die VPC erstellt wurde. Eine [Sicherheitsgruppe](#) wird erstellt, der den gesamten eingehenden Datenverkehr verweigert, mit Ausnahme von Ressourcen, die in den Subnetzen bereitgestellt werden. Eine Sicherheitsgruppe lässt auch den gesamten ausgehenden Datenverkehr zu. Die Subnetze sind getaggt, damit Kubernetes ihnen interne Load Balancer bereitstellen kann. Wenn Sie eine VPC mit dieser Konfiguration erstellen, finden Sie [the section called "Private Cluster"](#) weitere Anforderungen und Überlegungen unter.

- a. Öffnen Sie die [AWS CloudFormation -Konsole](#).
- b. Wählen Sie in der Navigationsleiste eine AWS Region aus, die Amazon EKS unterstützt.
- c. Klicken Sie auf Create stack (Stack erstellen), With new resources (standard) (Mit neuen Ressourcen (Standard)).
- d. Stellen Sie unter Vorbereiten der Vorlage sicher, dass Vorlage ist bereit ausgewählt ist und wählen Sie dann unter Vorlagenquelle Amazon-S3-URL aus.

- e. Fügen Sie die folgende URL in den Textbereich unter Amazon-S3-URL ein und wählen Sie Weiter aus:

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-fully-private-vpc.yaml
```

- a. Füllen Sie auf der Seite Specify Details (Details angeben) die Parameter entsprechend aus und klicken Sie dann auf Next (Weiter).
- **Stack-Name:** Wählen Sie einen Stack-Namen für Ihren AWS CloudFormation Stack. Sie können ihn beispielsweise *amazon-eks-fully-private-vpc* nennen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
  - **VpcBlock:** Wählen Sie einen CIDR-Block für Ihre VPC. Jedem Knoten, Pod und Load Balancer, den Sie bereitstellen, wird eine IPv4 Adresse aus diesem Block zugewiesen. Die IPv4 Standardwerte bieten ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie sie ändern. Weitere Informationen finden Sie unter [Dimensionierung der VPC und der Subnetze](#) im Amazon VPC Benutzerhandbuch. Sie können der VPC auch zusätzliche CIDR-Blöcke hinzufügen, sobald sie erstellt wurde.
  - **PrivateSubnet01Block:** Geben Sie einen CIDR-Block für Subnetz 1 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern.
  - **PrivateSubnet02Block:** Geben Sie einen CIDR-Block für Subnetz 2 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern.
  - **PrivateSubnet03Block:** Geben Sie einen CIDR-Block für Subnetz 3 an. Der Standardwert bietet ausreichend IP-Adressen für die meisten Implementierungen. Wenn dies nicht der Fall ist, können Sie ihn ändern.
- b. (Optional) Markieren Sie auf der Seite Options (Optionen) Ihre Stack-Ressourcen. Wählen Sie Next (Weiter).
- c. Klicken Sie auf der Seite Review auf Create.
- d. Wenn Ihr Stack erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgänge).

- e. Notieren Sie das VpcId für die VPC, die erstellt wurde. Dies benötigen Sie, wenn Sie Ihren Cluster und Ihre Knoten erstellen.
- f. Notieren Sie das SubnetIds für die Subnetze, die erstellt wurden. Sie benötigen mindestens zwei davon, wenn Sie Ihren Cluster und Ihre Knoten erstellen.
- g. (Optional) Jeder Cluster, den Sie in dieser VPC bereitstellen, kann Ihren Pods und Diensten private IPv4 Adressen zuweisen. Wenn Sie Cluster für diese VPC bereitstellen möchten, um Ihren Pods und Diensten private IPv6 Adressen zuzuweisen, aktualisieren Sie Ihre VPC, Ihr Subnetz, Ihre Routing-Tabellen und Sicherheitsgruppen. Weitere Informationen finden Sie unter [Vorhandenes migrieren VPCs von IPv4 zu IPv6](#) im Amazon VPC-Benutzerhandbuch. Amazon EKS setzt voraus, dass in Ihren Subnetzen die Option Auto-assign IPv6 Adressen aktiviert ist (sie ist standardmäßig deaktiviert).

## Amazon EKS-Sicherheitsgruppenanforderungen für Cluster anzeigen

In diesem Thema geht es um die Anforderungen an Sicherheitsgruppen in einem Amazon-EKS-Cluster.

### Standardmäßige Cluster-Sicherheitsgruppe

Wenn Sie einen Cluster erstellen, erstellt Amazon EKS eine Sicherheitsgruppe mit einem Namen `eks-cluster-sg-my-cluster-uniqueID`. Diese Sicherheitsgruppe hat die folgenden Standardregeln:

| Regeltyp  | Protocol (Protokoll) | Ports | Quelle | Ziel                                  |
|-----------|----------------------|-------|--------|---------------------------------------|
| Eingehend | Alle                 | Alle  | Selbst |                                       |
| Ausgehend | Alle                 | Alle  |        | 0.0.0.0/0 (IPv4)<br>oder: ::/0 (IPv6) |
| Ausgehend | Alle                 | Alle  |        | Self (für EFA-Verkehr)                |

Die Standardsicherheitsgruppe umfasst eine ausgehende Regel, die Elastic Fabric Adapter (EFA) - Datenverkehr mit dem Ziel derselben Sicherheitsgruppe zulässt. Dadurch wird EFA-Verkehr innerhalb des Clusters ermöglicht, was für KI/ML- und HPC-Workloads (High Performance Computing) von Vorteil ist. Weitere Informationen finden Sie unter [Elastic Fabric Adapter für KI/ML- und HPC-Workloads auf Amazon EC2 im Amazon Elastic Compute Cloud-Benutzerhandbuch](#).

 **Important**

Wenn Ihr Cluster die ausgehende Regel nicht benötigt, können Sie sie entfernen. Wenn Sie es entfernen, müssen Sie immer noch über die Mindestregeln verfügen, die unter [Einschränkung des Cluster-Datenverkehrs](#) aufgeführt sind. Wenn Sie die eingehende Regel entfernen, wird sie von Amazon EKS bei jeder Aktualisierung des Clusters neu erstellt.

Amazon EKS fügt der Sicherheitsgruppe die folgenden Tags hinzu. Wenn Sie die Tags entfernen, fügt Amazon EKS sie bei jeder Aktualisierung Ihres Clusters wieder zur Sicherheitsgruppe hinzu.

| Schlüssel                                | Wert                                               |
|------------------------------------------|----------------------------------------------------|
| kubernetes.io/cluster/ <i>my-cluster</i> | owned                                              |
| aws:eks:cluster-name                     | <i>my-cluster</i>                                  |
| Name                                     | eks-cluster-sg- <i>my-cluster</i> <i>-uniqueid</i> |

Amazon EKS verknüpft die Sicherheitsgruppe automatisch mit den folgenden Ressourcen, die es ebenfalls erstellt:

- 2 bis 4 Elastic-Network-Schnittstellen (für den Rest dieses Dokuments als Netzwerkschnittstelle bezeichnet), die beim Anlegen des Clusters erstellt werden.
- Netzwerkschnittstellen der Knoten in jeder verwalteten Knotengruppe, die Sie erstellen.

Die Standardregeln ermöglichen es, dass der gesamte Datenverkehr frei zwischen Ihrem Cluster und Ihren Knoten fließt. Außerdem lassen sie den gesamten ausgehenden Datenverkehr zu jedem Ziel zu. Beim Erstellen eines Clusters können Sie (optional) Ihre eigenen Sicherheitsgruppen angeben. Wenn Sie das tun, verknüpft Amazon EKS auch die von Ihnen angegebenen Sicherheitsgruppen mit

den Netzwerkschnittstellen, die es für Ihren Cluster erstellt. Sie werden jedoch keinen Knotengruppen zugeordnet, die Sie erstellen.

Sie können die ID Ihrer Cluster-Sicherheitsgruppe im AWS Management Console Abschnitt Netzwerk des Clusters ermitteln. Sie können dies auch tun, indem Sie den folgenden AWS CLI-Befehl ausführen.

```
aws eks describe-cluster --name my-cluster --query
cluster.resourcesVpcConfig.clusterSecurityGroupId
```

## Einschränken des Clusterverkehrs

Wenn Sie die offenen Ports zwischen dem Cluster und den Knoten einschränken müssen, können Sie die [standardmäßige Ausgangsregel](#) entfernen und die folgenden Mindestregeln hinzufügen, die für den Cluster erforderlich sind. Wenn Sie die [standardmäßige Eingangsregel](#) entfernen, erstellt Amazon EKS sie bei jeder Aktualisierung des Clusters neu.

| Regeltyp        | Protocol (Protokoll) | Port  | Bestimmungsort             |
|-----------------|----------------------|-------|----------------------------|
| Ausgehend       | TCP                  | 443   | Cluster-Sicherheit sgruppe |
| Ausgehend       | TCP                  | 10250 | Cluster-Sicherheit sgruppe |
| Ausgehend (DNS) | TCP und UDP          | 53    | Cluster-Sicherheit sgruppe |

Sie müssen auch Regeln für den folgenden Datenverkehr hinzufügen:

- Jedes Protokoll und alle Ports, von dem Sie erwarten, dass Ihre Knoten für die Kommunikation zwischen Knoten verwenden
- Ausgehender Internetzugang, sodass Knoten zur Cluster-Introspektion und Knotenregistrierung beim Start auf Amazon EKS APIs zugreifen können. Wenn Ihre Knoten keinen Internetzugang haben, finden Sie weitere Überlegungen unter [Private Cluster mit eingeschränktem Internetzugang bereitstellen](#).



- Knotenzugriff zum Abrufen von Container-Images aus Amazon ECR oder anderen Container-Registern APIs , aus denen sie Bilder abrufen müssen, z. B. DockerHub Weitere Informationen finden Sie in der AWS Allgemeinen [AWS Referenz unter IP-Adressbereiche](#).
- Knotenzugriff auf Amazon S3.
- Für IPv4- und IPv6-Adressen sind separate Regeln erforderlich
- Wenn Sie Hybridknoten verwenden, müssen Sie Ihrem Cluster eine zusätzliche Sicherheitsgruppe hinzufügen, um die Kommunikation mit Ihren lokalen Knoten und Pods zu ermöglichen. Weitere Informationen finden Sie unter [the section called “Bereiten Sie das Netzwerk vor”](#).

Wenn Sie erwägen, die Regeln einzuschränken, empfehlen wir Ihnen, alle Ihre Pods gründlich zu testen, bevor Sie Ihre geänderten Regeln auf einen Produktionscluster anwenden.

Wenn Sie ursprünglich einen Cluster mit Kubernetes 1.14 und der Plattformversion eks.3 oder älter bereitgestellt haben, dann bedenken Sie Folgendes:

- Möglicherweise gibt es Sicherheitsgruppen für die Steuerebene und Knoten. Als diese Gruppen erstellt wurden, enthielten sie die in der vorherigen Tabelle aufgeführten eingeschränkten Regeln. Diese Sicherheitsgruppen sind nicht mehr erforderlich und können entfernt werden. Sie müssen jedoch sicherstellen, dass Ihre Cluster-Sicherheitsgruppe die Regeln enthält, die diese Gruppen enthalten.
- Wenn Sie den Cluster direkt über die API bereitgestellt oder ein Tool wie die AWS CLI oder AWS CloudFormation zum Erstellen des Clusters verwendet haben und bei der Clustererstellung keine Sicherheitsgruppe angegeben haben, wurde die Standardsicherheitsgruppe für die VPC auf die Cluster-Netzwerkschnittstellen angewendet, die Amazon EKS erstellt hat.

## Gemeinsam genutzte Sicherheitsgruppen

Amazon EKS unterstützt gemeinsam genutzte Sicherheitsgruppen.

- Sicherheitsgruppen-VPC-Zuordnungen ordnen Sicherheitsgruppen mehreren Gruppen VPCs in demselben Konto und derselben Region zu.
  - Erfahren Sie VPCs im Amazon VPC-Benutzerhandbuch, wie Sie [Sicherheitsgruppen mehreren zuordnen](#).
- Mit gemeinsamen Sicherheitsgruppen können Sie Sicherheitsgruppen mit anderen AWS Konten gemeinsam nutzen. Die Konten müssen sich in derselben AWS Organisation befinden.

- Weitere Informationen zum [Teilen von Sicherheitsgruppen mit Organisationen](#) finden Sie im Amazon VPC-Benutzerhandbuch.
- Sicherheitsgruppen sind immer auf eine einzelne AWS Region beschränkt.

## Überlegungen zu Amazon EKS

- Für EKS gelten dieselben Anforderungen für gemeinsam genutzte oder Multi-VPC-Sicherheitsgruppen wie für Standardsicherheitsgruppen.

## Netzwerk-Add-Ons für Amazon EKS-Cluster verwalten

Für Ihren Amazon-EKS-Cluster sind mehrere Netzwerk-Add-Ons verfügbar.

### Integrierte Add-Ons

#### Note

Wenn Sie einen EKS-Cluster erstellen:

- Verwenden der AWS Konsole: Die integrierten Add-Ons (wie CoreDNS, Kube-Proxy usw.) werden automatisch als Amazon EKS Add-ons installiert. Diese können einfach über die AWS Konsole, CLI oder aktualisierte SDKs werden.
- Verwendung anderer Methoden (CLI SDKs usw.): Dieselben integrierten Add-Ons werden als selbstverwaltete Versionen installiert, die als reguläre Kubernetes-Bereitstellungen ausgeführt werden. Diese erfordern eine manuelle Konfiguration und Updates, da sie nicht über Tools verwaltet werden können. AWS

Wir empfehlen, Amazon EKS-Add-ons anstelle von selbstverwalteten Versionen zu verwenden, um die Add-On-Verwaltung zu vereinfachen und eine zentrale Konfiguration und Updates über AWS Services zu ermöglichen.

### Amazon VPC CNI-Plugin für Kubernetes

Dieses CNI-Add-on erstellt elastische Netzwerkschnittstellen und verbindet sie mit Ihren EC2 Amazon-Knoten. Das Add-on weist jedem Pod und Service außerdem eine private IPv6 Adresse

IPv4 oder Adresse aus Ihrer VPC zu. Dieses Add-on ist standardmäßig auf Ihrem Cluster installiert. Weitere Informationen finden Sie unter [the section called “Amazon VPC CNI”](#). Wenn Sie Hybridknoten verwenden, ist das VPC-CNI weiterhin standardmäßig installiert, es wird jedoch aufgrund einer Anti-Affinitätsregel daran gehindert, auf Ihren Hybridknoten ausgeführt zu werden. Weitere Informationen zu Ihren CNI-Optionen für Hybridknoten finden Sie unter [the section called “CNI konfigurieren”](#).

## CoreDNS

CoreDNS ist ein flexibler, erweiterbarer DNS-Server, der als Kubernetes-Cluster-DNS dienen kann. CoreDNS bietet Namensauflösung für alle Pods im Cluster. Dieses Add-on ist standardmäßig auf Ihrem Cluster installiert. Weitere Informationen finden Sie unter [the section called “CoreDNS”](#).

## kube-proxy

Dieses Add-on verwaltet die Netzwerkregeln auf Ihren EC2 Amazon-Knoten und ermöglicht die Netzwerkkommunikation mit Ihren Pods. Dieses Add-on ist standardmäßig auf Ihrem Cluster installiert. Weitere Informationen finden Sie unter [the section called “kube-proxy”](#).

# Optionale AWS Netzwerk-Add-Ons

## AWS Load Balancer Balancer-Controller

Wenn Sie Kubernetes-Dienstobjekte des Typs `loadbalancer` bereitstellen, erstellt der Controller AWS Network Load Balancer. Wenn Sie Kubernetes-Eingangsobjekte erstellen, erstellt der Controller Application Load Balancer. Wir empfehlen, diesen Controller für die Bereitstellung von Network Load Balancern zu verwenden, anstatt den [alten Cloud Provider-Controller](#) zu verwenden, der in Kubernetes integriert ist. Weitere Informationen finden Sie unter Ressourcen-Tags in der [AWS -Load-Balancer-Controller](#)-Dokumentation.

## AWS Gateway-API-Controller

Mit diesem Controller können Sie Dienste über mehrere Kubernetes-Cluster mithilfe der [Kubernetes-Gateway-API](#) verbinden. Der Controller verbindet Kubernetes-Services, die auf EC2 Amazon-Instances, Containern und serverlosen Funktionen ausgeführt werden, mithilfe des [Amazon VPC](#) Lattice-Dienstes. Weitere Informationen finden Sie in der Dokumentation zu [AWS -Gateway-API-Controller](#).

Weitere Informationen zu Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

## Pods mit dem Amazon VPC CNI zuweisen IPs



**Tip**

Mit Amazon EKS Auto Mode müssen Sie keine Netzwerk-Add-Ons installieren oder aktualisieren. Der automatische Modus umfasst Pod-Netzwerk- und Lastausgleichsfunktionen.

Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).

Das Amazon VPC CNI-Plug-In für Kubernetes wird auf jedem EC2 Amazon-Knoten in Ihrem Amazon EKS-Cluster bereitgestellt. Das Add-on erstellt [elastische Netzwerkschnittstellen](#) und verbindet sie mit Ihren EC2 Amazon-Knoten. Das Add-on weist jedem Pod außerdem eine private IPv6 Adresse IPv4 oder Adresse aus Ihrer VPC zu.

Eine Version des Add-ons wird mit jedem Fargate-Knoten in Ihrem Cluster bereitgestellt, Sie aktualisieren sie jedoch nicht auf Fargate-Knoten. Andere kompatible CNI-Plug-ins sind für die Verwendung auf Amazon EKS-Clustern verfügbar, aber dies ist das einzige CNI-Plugin, das von Amazon EKS für Knoten unterstützt wird, die auf der AWS Infrastruktur ausgeführt werden. Weitere Informationen zu den anderen kompatiblen CNI-Plugins finden Sie unter [the section called “Alternative CNI-Plugins”](#) Die Verwendung des VPC-CNI mit Hybridknoten wird nicht unterstützt. Weitere Informationen zu Ihren CNI-Optionen für Hybridknoten finden Sie unter [the section called “CNI konfigurieren”](#)

In der folgenden Tabelle ist die neueste verfügbare Version des Amazon EKS-Add-On-Typs für jede Kubernetes-Version aufgeführt.

### Amazon VPC CNI-Versionen

| Kubernetes-Version | VPC-CNI-Version vom Typ Amazon EKS |
|--------------------|------------------------------------|
| 1.33               | v1.19.6-eksbuild.1                 |
| 1.32               | v1.19.6-eksbuild.1                 |
| 1,31               | v1.19.6-eksbuild.1                 |
| 1,30               | v1.19.6-eksbuild.1                 |

| Kubernetes-Version | VPC-CNI-Version vom Typ Amazon EKS |
|--------------------|------------------------------------|
| 1,29               | v1.19.6-eksbuild.1                 |
| 1,28               | v1.19.6-eksbuild.1                 |
| 1,27               | v1.19.6-eksbuild.1                 |
| 1,26               | v1.19.6-eksbuild.1                 |

### Important

Wenn Sie dieses Add-on selbst verwalten, stimmen die Versionen in der Tabelle möglicherweise nicht mit den verfügbaren selbstverwalteten Versionen überein. Weitere Hinweise zur Aktualisierung des selbstverwalteten Typs dieses Add-ons finden Sie unter [the section called “Update \(selbst verwaltet\)”](#).

### Important

Um auf VPC CNI v1.12.0 oder höher zu aktualisieren, müssen Sie zuerst auf VPC CNI v1.7.0 aktualisieren. Wir empfehlen Ihnen, jeweils eine Nebenversion zu aktualisieren.

## Überlegungen

Im Folgenden finden Sie Überlegungen zur Verwendung der Funktion.

- Versionen sind angegeben als `major-version.minor-version.patch-version-eksbuild.build-number`.
- Überprüfen Sie die Versionskompatibilität für jede Funktion. Für einige Funktionen der einzelnen Versionen des Amazon VPC CNI-Plug-ins für Kubernetes sind bestimmte Kubernetes-Versionen erforderlich. Wenn Sie verschiedene Amazon EKS-Funktionen verwenden und eine bestimmte Version des Add-ons erforderlich ist, wird dies in der Funktionsdokumentation vermerkt. Falls Sie keinen bestimmten Grund haben, eine frühere Version auszuführen, empfehlen wir, die neueste Version auszuführen.

## Erstellen Sie das Amazon VPC CNI (Amazon EKS-Add-on)

Gehen Sie wie folgt vor, um das Amazon VPC CNI-Plug-In für Kubernetes Amazon EKS zu erstellen.

Bevor Sie beginnen, lesen Sie sich die Überlegungen durch. Weitere Informationen finden Sie unter [the section called “Überlegungen”](#).

### Voraussetzungen

Im Folgenden sind die Voraussetzungen für das Amazon VPC CNI-Plug-In für Kubernetes Amazon EKS aufgeführt.

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#).
- Ein vorhandener AWS Identity and Access Management (IAM) OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Informationen zum Feststellen, ob Sie bereits über einen verfügen oder einen erstellen müssen, finden Sie unter [the section called “IAM OIDC-Anbieter”](#).
- Eine IAM-Rolle, an die die IAM-Richtlinie [Amazoneks\\_CNI\\_Policy](#) (wenn Ihr Cluster die Familie verwendet) oder eine IPv6 Richtlinie (wenn Ihr Cluster die IPv4 Familie verwendet) angehängt ist. IPv6 Weitere Informationen zur VPC-CNI-Rolle finden Sie unter. [the section called “Für IRSA konfigurieren”](#) Informationen zur IPv6 Richtlinie finden Sie unter. [the section called “Erstellen Sie eine IAM-Richtlinie für Cluster, die die IPv6-Familie verwendet”](#)

#### Important

Amazon VPC CNI-Plugin für Kubernetes-Versionen v1.16.0 zur v1.16.1 Implementierung der CNI-Spezifikationsversion. v1.0.0 Weitere Informationen v1.0.0 zur CNI-Spezifikation finden Sie unter [Container Network](#) Interface (CNI) -Spezifikation unter. GitHub

### Verfahren

Nachdem Sie die Voraussetzungen erfüllt haben, führen Sie die folgenden Schritte aus, um das Add-on zu erstellen.

1. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |
cut -d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.16.4-eksbuild.2
```

2. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist. Je nachdem, mit welchem Tool Sie Ihr Cluster erstellt haben, ist der Add-on vom Typ Amazon EKS möglicherweise derzeit nicht auf Ihrem Cluster installiert. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query
addon.addonVersion --output text
```

Wenn eine Versionsnummer zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons auf Ihrem Cluster installiert und müssen die verbleibenden Schritte in diesem Verfahren nicht ausführen. Wenn ein Fehler zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Führen Sie die verbleibenden Schritte dieses Prozesses aus, um es zu installieren.

3. Speichern Sie die Konfiguration Ihres aktuell installierten Add-ons ab.

```
kubectl get daemonset aws-node -n kube-system -o yaml > aws-k8s-cni-old.yaml
```

4. Erstellen Sie das Add-on mit der AWS CLI. Wenn Sie das AWS Management Console oder verwenden möchten, um das Add-on `eksctl` zu erstellen, finden Sie weitere Informationen unter [the section called “Erstellen Sie ein Add-on”](#) und geben Sie `vpc-cni` den Namen des Add-ons an. Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie bei Bedarf die folgenden Änderungen am Befehl vor, und führen Sie dann den geänderten Befehl aus.
  - Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
  - *v1.19.6-eksbuild.1* Ersetzen Sie es durch die neueste Version, die in der Tabelle mit den neuesten Versionen für Ihre Clusterversion aufgeführt ist. Die aktuelle Versionstabelle finden Sie unter [the section called “Amazon VPC CNI-Versionen”](#).
  - *111122223333* Ersetzen Sie es durch Ihre Konto-ID und *AmazonEKSVPCCNIRole* den Namen einer [vorhandenen IAM-Rolle](#), die Sie erstellt haben. Für die Angabe einer Rolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).

```
aws eks create-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version
v1.19.6-eksbuild.1 \
--service-account-role-arn arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole
```

Wenn Sie benutzerdefinierte Einstellungen auf Ihr aktuelles Add-on angewendet haben, die mit den Standardeinstellungen des Amazon EKS-Add-ons in Konflikt stehen, schlägt die Erstellung möglicherweise fehl. Wenn die Erstellung fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Problembeseitigung unterstützt. Alternativ können Sie den vorherigen Befehl mit `--resolve-conflicts OVERWRITE` ergänzen. Dadurch kann das Add-on alle vorhandenen benutzerdefinierten Einstellungen überschreiben. Sobald Sie das Add-on erstellt haben, können Sie es mit Ihren benutzerdefinierten Einstellungen aktualisieren.

5. Vergewissern Sie sich, dass die neueste Version des Add-ons für die Kubernetes-Version Ihres Clusters zu Ihrem Cluster hinzugefügt wurde. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query
addon.addonVersion --output text
```

Es kann einige Sekunden dauern, bis die Erstellung des Add-ons abgeschlossen ist.

Eine Beispielausgabe sieht wie folgt aus.

```
v1.19.6-eksbuild.1
```

6. Wenn Sie vor der Erstellung des Amazon EKS-Add-ons benutzerdefinierte Einstellungen an Ihrem ursprünglichen Add-on vorgenommen haben, verwenden Sie die Konfiguration, die Sie in einem vorherigen Schritt gespeichert haben, um das EKS-Add-on mit Ihren benutzerdefinierten Einstellungen zu aktualisieren. Führen Sie die Schritte unter [the section called “Aktualisieren \(EKS-Add-on\)”](#) aus.
7. (Optional) Installieren Sie `cni-metrics-helper` in Ihrem Cluster. Es erfasst elastic network interface- und IP-Adressinformationen, aggregiert sie auf Clusterebene und veröffentlicht die Metriken auf Amazon CloudWatch. Weitere Informationen finden Sie unter [cni-metrics-helper](#).  
GitHub



## Aktualisieren Sie das Amazon VPC CNI (Amazon EKS-Add-on)

Aktualisieren Sie den Amazon EKS-Typ des Amazon VPC CNI-Plug-ins für Kubernetes. Wenn Sie den Amazon EKS-Typ des Add-ons nicht zu Ihrem Cluster hinzugefügt haben, können Sie es wie folgt installieren [the section called “Erstellen”](#). Oder aktualisieren Sie den anderen Typ der VPC-CNI-Installation wie folgt. [the section called “Update \(selbst verwaltet\)”](#)

1. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist. Ersetzen Sie *my-cluster* mit Ihrem Clusternamen.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query
"addon.addonVersion" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.19.6-eksbuild.1
```

Vergleichen Sie die Version mit der Tabelle der neuesten Versionen unter. [the section called “Amazon VPC CNI-Versionen”](#) Wenn die zurückgegebene Version mit der Version für die Kubernetes-Version Ihres Clusters in der aktuellen Versionstabelle identisch ist, haben Sie die neueste Version bereits auf Ihrem Cluster installiert und müssen den Rest dieses Verfahrens nicht abschließen. Wenn Sie in Ihrer Ausgabe statt einer Versionsnummer eine Fehlermeldung erhalten, ist der Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Sie müssen das Add-on erstellen, bevor Sie es mit diesem Verfahren aktualisieren können. Gehen Sie wie folgt vor, um den Amazon EKS-Typ des VPC CNI-Add-ons zu erstellen. [the section called “Erstellen”](#)

2. Speichern Sie die Konfiguration Ihres aktuell installierten Add-ons ab.

```
kubectl get daemonset aws-node -n kube-system -o yaml > aws-k8s-cni-old.yaml
```

3. Aktualisieren Sie Ihr Add-on mit der AWS CLI. Wenn Sie das AWS Management Console oder verwenden möchten, um das Add-on `eksctl` zu aktualisieren, finden Sie weitere Informationen unter [the section called “Aktualisieren Sie ein Add-on”](#). Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie bei Bedarf die folgenden Änderungen am Befehl vor, und führen Sie dann den geänderten Befehl aus.
  - Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
  - *v1.19.6-eksbuild.1* Ersetzen Sie es durch die neueste Version, die in der Tabelle mit den neuesten Versionen für Ihre Clusterversion aufgeführt ist.

- **111122223333** Ersetzen Sie durch Ihre Konto-ID und **AmazonEKSVPCCNIRole** den Namen einer vorhandenen IAM-Rolle, die Sie erstellt haben. Informationen zum Erstellen einer IAM-Rolle für das VPC-CNI finden Sie unter [the section called “Schritt 1: Erstellen Sie das Amazon VPC CNI-Plug-In für die IAM-Rolle von Kubernetes”](#). Für die Angabe einer Rolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).
- Die `--resolve-conflicts PRESERVE` Option behält die vorhandenen Konfigurationswerte für das Add-on bei. Wenn Sie benutzerdefinierte Werte für Add-On-Einstellungen festgelegt haben und diese Option nicht verwenden, überschreibt Amazon EKS Ihre Werte mit den Standardwerten. Wenn Sie diese Option verwenden, empfehlen wir, dass Sie alle Feld- und Wertänderungen auf einem Nicht-Produktionscluster testen, bevor Sie das Add-on auf Ihrem Produktionscluster aktualisieren. Wenn Sie diesen Wert auf `OVERWRITE` ändern, werden alle Einstellungen auf die Amazon-EKS-Standardwerte geändert. Wenn Sie benutzerdefinierte Werte für Einstellungen festgelegt haben, werden diese möglicherweise mit den Amazon EKS-Standardwerten überschrieben. Wenn Sie diesen Wert auf `ändernnone` ändern, ändert Amazon EKS den Wert aller Einstellungen nicht, aber das Update schlägt möglicherweise fehl. Wenn das Update fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt.
- Wenn Sie eine Konfigurationseinstellung nicht aktualisieren, entfernen Sie sie `--configuration-values '{"env":{"AWS_VPC_K8S_CNI_EXTERNALSNAT":"true"}}'` aus dem Befehl. Wenn Sie eine Konfigurationseinstellung aktualisieren, `"env":{"AWS_VPC_K8S_CNI_EXTERNALSNAT":"true"}` ersetzen Sie sie durch die Einstellung, die Sie festlegen möchten. In diesem Beispiel ist die Umgebungsvariable `AWS_VPC_K8S_CNI_EXTERNALSNAT` auf `true` gesetzt. Der von Ihnen angegebene Wert muss für das Konfigurationsschema gültig sein. Wenn Sie das Konfigurationsschema nicht kennen, führen Sie `aws eks describe-addon-configuration --addon-name vpc-cni --addon-version v1.19.6-eksbuild.1` aus und `v1.19.6-eksbuild.1` ersetzen Sie es durch die Versionsnummer des Add-ons, für das Sie die Konfiguration sehen möchten. Das Schema wird in der Ausgabe zurückgegeben. Wenn Sie über eine bestehende benutzerdefinierte Konfiguration verfügen, diese alle entfernen und die Werte für alle Einstellungen auf die Amazon EKS-Standardwerte zurücksetzen möchten, entfernen Sie sie `"env":{"AWS_VPC_K8S_CNI_EXTERNALSNAT":"true"}` aus dem Befehl, sodass Sie leer `{}` haben. Eine Erläuterung der einzelnen Einstellungen finden Sie unter [CNI-Konfigurationsvariablen](#) unter GitHub

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version
v1.19.6-eksbuild.1 \
 --service-account-role-arn arn:aws: iam::111122223333:role/AmazonEKSVPCCNIRole
\
 --resolve-conflicts PRESERVE --configuration-values '{"env":
{"AWS_VPC_K8S_CNI_EXTERNALSNAT":"true"}}'
```

Es kann einige Sekunden dauern, bis das Update abgeschlossen ist.

4. Vergewissern Sie sich, dass die Add-on-Version aktualisiert wurde. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni
```

Es kann einige Sekunden dauern, bis das Update abgeschlossen ist.

Eine Beispielausgabe sieht wie folgt aus.

```
{
 "addon": {
 "addonName": "vpc-cni",
 "clusterName": "my-cluster",
 "status": "ACTIVE",
 "addonVersion": "v1.19.6-eksbuild.1",
 "health": {
 "issues": []
 },
 "addonArn": "arn:aws: eks:region:111122223333:addon/my-cluster/vpc-
cni/74c33d2f-b4dc-8718-56e7-9fdfa65d14a9",
 "createdAt": "2023-04-12T18:25:19.319000+00:00",
 "modifiedAt": "2023-04-12T18:40:28.683000+00:00",
 "serviceAccountRoleArn": "arn:aws: iam::111122223333:role/
AmazonEKSVPCCNIRole",
 "tags": {},
 "configurationValues": "{\"env\":{\"AWS_VPC_K8S_CNI_EXTERNALSNAT\": \"true
\"}}\"
 }
}
```

## Aktualisieren Sie das Amazon VPC CNI (selbstverwaltetes Add-on)

### Important

Wir empfehlen, den Amazon-EKS-Typ des Add-Ons zu Ihrem Cluster hinzuzufügen, anstatt den selbstverwalteten Typ des Add-Ons zu verwenden. Falls Sie mit den Unterschieden zwischen den Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#). Weitere Informationen zum Hinzufügen eines Amazon-EKS-Add-ons zu Ihrem Cluster finden Sie unter [the section called “Erstellen Sie ein Add-on”](#). Wenn Sie das Amazon EKS-Add-on nicht verwenden können, empfehlen wir Ihnen, ein Problem mit der Begründung, warum Sie das nicht können, an das [GitHub Container-Roadmap-Repository](#) zu senden.

1. Vergewissern Sie sich, dass Sie den Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert haben. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query
addon.addonVersion --output text
```

Wenn eine Fehlermeldung zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Um das Add-on selbst zu verwalten, führen Sie die verbleibenden Schritte in diesem Verfahren aus, um das Add-on zu aktualisieren. Wenn Sie eine Versionsnummer zurückgeben, wird der Amazon-EKS-Typ des Add-Ons auf Ihrem Cluster installiert. Verwenden Sie zum Aktualisieren das Verfahren in [the section called “Aktualisieren Sie ein Add-on”](#) und nicht das Verfahren in diesem Thema. Wenn Sie mit den Unterschieden zwischen den Add-On-Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#).

2. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |
cut -d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.19.6-eksbuild.1
```

Ihre Ausgabe enthält möglicherweise nicht die Build-Nummer.

3. Backup Sie Ihre aktuellen Einstellungen, damit Sie dieselben Einstellungen konfigurieren können, sobald Sie Ihre Version aktualisiert haben.

```
kubectl get daemonset aws-node -n kube-system -o yaml > aws-k8s-cni-old.yaml
```

Einen Überblick über die verfügbaren Versionen und die Änderungen in der Version, auf die Sie aktualisieren möchten, finden Sie unter [Versionen](#) von GitHub. Beachten Sie, dass wir empfehlen, auf dieselbe Version zu aktualisieren `major`, `minor`, `patch` Version, die in der Tabelle mit den neuesten verfügbaren Versionen aufgeführt ist, auch wenn spätere Versionen verfügbar sind GitHub. Die Tabelle mit den neuesten verfügbaren Versionen finden Sie unter [the section called “Amazon VPC CNI-Versionen”](#). Die in der Tabelle aufgeführten Buildversionen sind in den unter GitHub aufgeführten selbstverwalteten Versionen nicht angegeben. Aktualisieren Sie Ihre Version, indem Sie die Aufgaben mit einer der folgenden Optionen ausführen:

- Wenn Sie keine benutzerdefinierten Einstellungen für das Add-on haben, führen Sie den Befehl unter der To `apply this release`: Überschrift GitHub für die [Version](#) aus, auf die Sie aktualisieren möchten.
- Wenn Sie benutzerdefinierte Einstellungen haben, laden Sie die Manifestdatei mit dem folgenden Befehl herunter, anstatt sie anzuwenden. Ändern <https://raw.githubusercontent.com/aws/amazon-vpc-cni-k8s/v1.19.6/config/master/aws-k8s-cni.yaml> Sie die URL für die Version GitHub , auf die Sie aktualisieren möchten.

```
curl -O https://raw.githubusercontent.com/aws/amazon-vpc-cni-k8s/v1.19.6/config/master/aws-k8s-cni.yaml
```

Ändern Sie bei Bedarf die Datei mit den benutzerdefinierten Einstellungen aus dem von Ihnen erstellten Backup und wenden Sie die geänderte Datei dann auf Ihren Cluster an. Wenn Ihre Knoten keinen Zugriff auf die privaten Amazon ECR-Repositorys von Amazon EKS haben, aus denen die Bilder abgerufen werden (siehe die Zeilen, die mit `image:` im Manifest beginnen), müssen Sie die Bilder herunterladen, in Ihr eigenes Repository kopieren und das Manifest so ändern, dass die Bilder aus Ihrem Repository abgerufen werden. Weitere Informationen finden Sie unter [the section called “Kopieren eines Images in ein Repository”](#).

```
kubectl apply -f aws-k8s-cni.yaml
```

4. Vergewissern Sie sich, dass die neue Version jetzt auf Ihrem Cluster installiert ist.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |
cut -d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.19.6
```

5. (Optional) Installieren Sie `cni-metrics-helper` in Ihrem Cluster. Es erfasst elastic network interface- und IP-Adressinformationen, aggregiert sie auf Clusterebene und veröffentlicht die Metriken auf Amazon CloudWatch. Weitere Informationen finden Sie unter [cni-metrics-helper](#).  
GitHub

## Amazon VPC CNI-Plugin für die Verwendung von IRSA konfigurieren

Das [Amazon VPC CNI-Plugin für Kubernetes](#) ist das Netzwerk-Plugin für Pod-Netzwerke in Amazon EKS-Clustern. Das Plugin ist dafür verantwortlich, den Kubernetes-Pods VPC-IP-Adressen zuzuweisen und das erforderliche Netzwerk für Pods auf jedem Knoten zu konfigurieren.

### Note

Das Amazon VPC CNI-Plugin unterstützt auch Amazon EKS Pod Identities. Weitere Informationen finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).

Das Plugin:

- Erfordert AWS Identity and Access Management (IAM) -Berechtigungen. Wenn Ihr Cluster die IPv4 Familie verwendet, sind die Berechtigungen in der [AmazonEKS\\_CNI\\_Policy](#) AWS verwalteten Richtlinie angegeben. Wenn Ihr Cluster die IPv6 Familie verwendet, müssen die Berechtigungen zu einer von Ihnen erstellten IAM-Richtlinie hinzugefügt werden. Anweisungen finden Sie unter [the section called “Erstellen Sie eine IAM-Richtlinie für Cluster, die die IPv6-Familie verwendet”](#). Sie können diese Richtlinie der Amazon-EKS-Knoten-IAM-Rolle oder einer separaten IAM-Rolle anfügen. Anweisungen zum Anhängen der Richtlinie an die IAM-Rolle des Amazon EKS-Knotens finden Sie unter [the section called “Knoten-IAM-Rolle”](#). Wir empfehlen Ihnen, sie einer separaten Rolle zuzuweisen, wie in diesem Thema beschrieben.

- Erstellt ein Kubernetes-Servicekonto, das bei der Bereitstellung benannt wurde als `aws-node`, und ist für dessen Verwendung konfiguriert. Das Servicekonto ist an ein Kubernetes `clusterrole` namens `aws-node` gebunden, dem die erforderlichen Kubernetes-Berechtigungen zugewiesen sind.

#### Note

Die Pods für das Amazon VPC CNI-Plug-In für Kubernetes haben Zugriff auf die Berechtigungen, die der [IAM-Rolle des Amazon EKS-Knotens](#) zugewiesen sind, sofern Sie den Zugriff auf IMDS nicht blockieren. Weitere Informationen finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).

- Erfordert einen vorhandenen Amazon EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#).
- Erfordert einen vorhandenen AWS Identity and Access Management (IAM) OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Informationen zum Feststellen, ob Sie bereits über einen verfügen oder einen erstellen müssen, finden Sie unter [the section called "IAM OIDC-Anbieter"](#).

Schritt 1: Erstellen Sie das Amazon VPC CNI-Plug-In für die IAM-Rolle von Kubernetes

1. Ermitteln Sie die IP-Familie Ihres Clusters.

```
aws eks describe-cluster --name my-cluster | grep ipFamily
```

Eine Beispielausgabe sieht wie folgt aus.

```
"ipFamily": "ipv4"
```

Die Ausgabe kann stattdessen `ipv6` zurückgeben.

2. Erstellen Sie die IAM-Rolle. Sie können `eksctl` oder `kubectl` und die AWS CLI verwenden, um Ihre IAM-Rolle zu erstellen.

`eksctl`

- Erstellen Sie eine IAM-Rolle und fügen Sie der Rolle die IAM-Richtlinie mit dem Befehl zu, der der IP-Familie Ihres Clusters entspricht. Der Befehl erstellt und stellt einen AWS

CloudFormation Stack bereit, der eine IAM-Rolle erstellt, ihr die von Ihnen angegebene Richtlinie anhängt und das vorhandene aws-node Kubernetes-Dienstkonto mit dem ARN der erstellten IAM-Rolle annotiert.

- IPv4

Ersetzen Sie *my-cluster* durch Ihren eigenen Wert.

```
eksctl create iamserviceaccount \
 --name aws-node \
 --namespace kube-system \
 --cluster my-cluster \
 --role-name AmazonEKSVPCCNIRole \
 --attach-policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
 --override-existing-serviceaccounts \
 --approve
```

- IPv6

Ersetzen Sie *my-cluster* durch Ihren eigenen Wert. Ersetzen Sie *111122223333* durch den Namen Ihres Clusters und *AmazonEKS\_CNI\_IPv6\_Policy* durch Ihre IPv6-Richtlinie. Wenn Sie noch keine Richtlinie haben, finden Sie weitere Informationen unter [So erstellen Sie eine IPv6](#). [the section called “Erstellen Sie eine IAM-Richtlinie für Cluster, die die IPv6-Familie verwendet”](#) Um IPv6 mit Ihrem Cluster zu verwenden, muss dieser mehrere Anforderungen erfüllen. Weitere Informationen finden Sie unter [the section called “IPv6”](#).

```
eksctl create iamserviceaccount \
 --name aws-node \
 --namespace kube-system \
 --cluster my-cluster \
 --role-name AmazonEKSVPCCNIRole \
 --attach-policy-arn arn:aws:iam::111122223333:policy/
AmazonEKS_CNI_IPv6_Policy \
 --override-existing-serviceaccounts \
 --approve
```

kubectl und die CLI AWS

- Sehen Sie sich die OIDC-Provider-URL Ihres Clusters an.



```
aws eks describe-cluster --name my-cluster --query
"cluster.identity.oidc.issuer" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
https://oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE
```

Wenn keine Ausgabe erfolgt, müssen Sie [einen IAM-OIDC-Anbieter für Ihr Cluster erstellen](#).

- ii. Kopieren Sie den folgenden Inhalt in eine Datei namens *vpc-cni-trust-policy.json*. Ersetzen Sie *111122223333* durch die ID Ihres Kontos und *EXAMPLED539D4633E53DE1B71EXAMPLE* durch den Wert, der im vorherigen Schritt zurückgegeben wurde. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Federated": "arn:aws:iam::111122223333:oidc-provider/
oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
 },
 "Action": "sts:AssumeRoleWithWebIdentity",
 "Condition": {
 "StringEquals": {
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:aws-
node"
 }
 }
 }
]
}
```

- iii. Erstellen Sie die -Rolle. Sie können *AmazonEKSVPCCNIRole* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
aws iam create-role \
 --role-name AmazonEKSVPCCNIRole \
 --assume-role-policy-document file://\"vpc-cni-trust-policy.json\"
```

iv. Fügen Sie der Rolle die erforderliche IAM-Richtlinie an. Führen Sie den Befehl aus, der der IP-Familie Ihres Clusters entspricht.

- IPv4

```
aws iam attach-role-policy \
 --policy-arn arn:aws: iam::aws:policy/AmazonEKS_CNI_Policy \
 --role-name AmazonEKSVPCCNIRole
```

- IPv6

Ersetzen Sie **111122223333** durch den Namen Ihres Clusters und **AmazonEKS\_CNI\_IPv6\_Policy** durch Ihre IPv6-Richtlinie. Wenn Sie noch keine IPv6 Richtlinie haben, finden Sie weitere Informationen unter [the section called “Erstellen Sie eine IAM-Richtlinie für Cluster, die die IPv6-Familie verwendet”](#) So erstellen Sie eine. Um IPv6 mit Ihrem Cluster zu verwenden, muss dieser mehrere Anforderungen erfüllen. Weitere Informationen finden Sie unter [the section called “IPv6”](#).

```
aws iam attach-role-policy \
 --policy-arn arn:aws: iam::111122223333:policy/AmazonEKS_CNI_IPv6_Policy \
 --role-name AmazonEKSVPCCNIRole
```

v. Führen Sie den folgenden Befehl aus und fügen Sie dem aws-node-Servicekonto den ARN der IAM-Rolle hinzu, die Sie zuvor erstellt haben. Ersetzen Sie **example values** durch Ihre eigenen Werte.

```
kubectl annotate serviceaccount \
 -n kube-system aws-node \
 eks.amazonaws.com/role-arn=arn:aws: iam::111122223333:role/
 AmazonEKSVPCCNIRole
```

3. (Optional) Konfigurieren Sie den AWS Security Token Service-Endpunkttyp, der von Ihrem Kubernetes-Dienstkonto verwendet wird. Weitere Informationen finden Sie unter [the section called “STS-Endpunkte”](#).

## Schritt 2: Stellen Sie das Amazon VPC CNI-Plugin für Kubernetes Pods erneut bereit

1. Löschen Sie alle vorhandenen Pods, die dem Dienstkonto zugeordnet sind, und erstellen Sie sie neu, um die Umgebungsvariablen für die Anmeldeinformationen anzuwenden. Die Anmerkung wird nicht auf Pods angewendet, die derzeit ohne die Anmerkung ausgeführt werden. Mit dem folgenden Befehl werden die vorhandenen `aws-node` DaemonSet Pods gelöscht und mit der Anmerkung zum Dienstkonto bereitgestellt.

```
kubectl delete Pods -n kube-system -l k8s-app=aws-node
```

2. Vergewissern Sie sich, dass alle Pods neu gestartet wurden.

```
kubectl get pods -n kube-system -l k8s-app=aws-node
```

3. Beschreiben Sie einen der Pods und stellen Sie sicher, dass die Umgebungsvariablen `AWS_WEB_IDENTITY_TOKEN_FILE` und die `AWS_ROLE_ARN` Umgebungsvariablen vorhanden sind. `cpjw7` Ersetzen Sie ihn durch den Namen eines Ihrer Pods, der in der Ausgabe des vorherigen Schritts zurückgegeben wurde.

```
kubectl describe pod -n kube-system aws-node-cpjw7 | grep 'AWS_ROLE_ARN:\
AWS_WEB_IDENTITY_TOKEN_FILE: '
```

Eine Beispielausgabe sieht wie folgt aus.

```
AWS_ROLE_ARN: arn:aws: iam::111122223333:role/AmazonEKSVPCCNIRole
 AWS_WEB_IDENTITY_TOKEN_FILE: /var/run/secrets/eks.amazonaws.com/
serviceaccount/token
 AWS_ROLE_ARN: arn:aws: iam::111122223333:role/AmazonEKSVPCCNIRole
 AWS_WEB_IDENTITY_TOKEN_FILE: /var/run/secrets/eks.amazonaws.com/
serviceaccount/token
```

Es werden zwei Sätze doppelter Ergebnisse zurückgegeben, da der Pod zwei Container enthält. Beide Container haben die gleichen Werte.

Wenn Ihr Pod den AWS regionalen Endpunkt verwendet, wird die folgende Zeile auch in der vorherigen Ausgabe zurückgegeben.

```
AWS_STS_REGIONAL_ENDPOINTS=regional
```

### Schritt 3: Entfernen Sie die CNI-Richtlinie aus der Knoten-IAM-Rolle

Wenn Ihrer [Amazon EKS-Knoten-IAM-Rolle](#) derzeit die AmazonEKS\_CNI\_Policy IAM (IPv4) -Richtlinie oder eine [IPv6 Richtlinie](#) angehängt ist und Sie eine separate IAM-Rolle erstellt, ihr stattdessen die Richtlinie angehängt und sie dem aws-node Kubernetes-Servicekonto zugewiesen haben, empfehlen wir Ihnen, die Richtlinie mit dem AWS CLI-Befehl, der der IP-Familie Ihres Clusters entspricht, aus Ihrer Knotenrolle zu entfernen. Ersetzen Sie *AmazonEKSNodeRole* durch den Namen Ihrer Knotenrolle.

- IPv4

```
aws iam detach-role-policy --role-name AmazonEKSNodeRole --policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
```

- IPv6

Ersetzen Sie *111122223333* durch den Namen Ihres Clusters und *AmazonEKS\_CNI\_IPv6\_Policy* durch Ihre IPv6-Richtlinie.

```
aws iam detach-role-policy --role-name AmazonEKSNodeRole --policy-arn arn:aws:iam::111122223333:policy/AmazonEKS_CNI_IPv6_Policy
```

Erstellen Sie eine IAM-Richtlinie für Cluster, die die **IPv6**-Familie verwendet

Wenn Sie einen Cluster erstellt haben, der die IPv6 Familie verwendet, und für den Cluster eine Version 1.10.1 oder eine neuere Version des Amazon VPC CNI-Plug-ins für Kubernetes konfiguriert ist, müssen Sie eine IAM-Richtlinie erstellen, die Sie einer IAM-Rolle zuweisen können. Wenn Sie über einen vorhandenen Cluster verfügen, den Sie bei der Erstellung nicht mit der IPv6 Familie konfiguriert haben, müssen Sie zur Verwendung einen neuen IPv6 Cluster erstellen. Weitere Informationen zur Verwendung von IPv6 mit Ihrem Cluster finden Sie unter [the section called "IPv6"](#).

1. Kopieren Sie den folgenden Text und speichern Sie ihn in einer Datei mit dem Namen `vpc-cni-ipv6-policy.json`.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
```

```

 "Action": [
 "ec2:AssignIpv6Addresses",
 "ec2:DescribeInstances",
 "ec2:DescribeTags",
 "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeInstanceTypes"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:CreateTags"
],
 "Resource": [
 "arn:aws:ec2:*:*:network-interface/*"
]
 }
]
}

```

## 2. Erstellen Sie die IAM-Richtlinie.

```
aws iam create-policy --policy-name AmazonEKS_CNI_IPv6_Policy --policy-document
file://vpc-cni-ipv6-policy.json
```

## Erfahren Sie mehr über VPC CNI-Modi und Konfiguration

Das Amazon VPC CNI-Plugin für Kubernetes bietet Netzwerke für Pods. Verwenden Sie die folgende Tabelle, um mehr über die verfügbaren Netzwerkfunktionen zu erfahren.

| Netzwerkfunktion                                                                              | Weitere Informationen                                    |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Konfigurieren Sie Ihren Cluster so, dass er Clustern, Pods und Diensten IPv6 Adressen zuweist | <a href="#">the section called “IPv6”</a>                |
| Verwenden Sie die Übersetzung der IPv4 Quellnetzwerkadresse für Pods                          | <a href="#">the section called “Ausgehender Verkehr”</a> |

| Netzwerkfunktion                                             | Weitere Informationen                                             |
|--------------------------------------------------------------|-------------------------------------------------------------------|
| Beschränken Sie den Netzwerkverkehr zu und von Ihren Pods    | <a href="#">the section called “Beschränken Sie den Verkehr”</a>  |
| Passen Sie die sekundäre Netzwerkschnittstelle in Knoten an  | <a href="#">the section called “Benutzerdefinierte Netzwerke”</a> |
| Erhöhen Sie die IP-Adressen für Ihren Knoten                 | <a href="#">the section called “Erhöhen Sie die IP-Adressen”</a>  |
| Verwenden Sie Sicherheitsgruppen für den Pod-Netzwerkverkehr | <a href="#">the section called “Sicherheitsgruppen für Pods”</a>  |
| Verwenden Sie mehrere Netzwerkschnittstellen für Pods        | <a href="#">the section called “Mehrere Schnittstellen”</a>       |

Erfahren Sie mehr über IPv6 Adressen für Cluster, Pods und Dienste

Gilt für: Pods mit EC2 Amazon-Instances und Fargate Pods

Standardmäßig weist Kubernetes Ihren Pods und Diensten IPv4 Adressen zu. Anstatt Ihren Pods und Diensten IPv4 Adressen zuzuweisen, können Sie Ihren Cluster so konfigurieren, dass er ihnen Adressen zuweist IPv6. Amazon EKS unterstützt keine Dual-Stack-Pods oder -Services, obwohl Kubernetes dies tut. Daher können Sie Ihren Pods IPv4 und Diensten nicht sowohl als auch IPv6 Adressen zuweisen.

Sie wählen aus, welche IP-Familie Sie für Ihren Cluster verwenden möchten, wenn Sie ihn erstellen. Sie können die Familie nicht ändern, nachdem Sie den Cluster erstellt haben.

Ein Tutorial zur Bereitstellung eines Amazon IPv6 EKS-Clusters finden Sie unter [the section called “Bereitstellen”](#).

Im Folgenden finden Sie Überlegungen zur Verwendung der Funktion:

### **IPv6**Unterstützung von Funktionen

- Keine Windows-Unterstützung: Windows-Pods und -Dienste werden nicht unterstützt.
- Nitro-basierte EC2 Knoten erforderlich: Sie können sie nur IPv6 mit AWS Nitro-basierten Amazon EC2 - oder Fargate-Knoten verwenden.

- EC2 und unterstützte Fargate-Knoten: Sie können sie IPv6 [the section called “Sicherheitsgruppen für Pods”](#) mit EC2 Amazon-Knoten und Fargate-Knoten verwenden.
- Outposts werden nicht unterstützt: Du kannst es nicht IPv6 mit [Amazon EKS auf AWS Outposts](#) verwenden.
- FSx for Lustre wird nicht unterstützt: Das [the section called “Amazon FSx für Lustre”](#) wird nicht unterstützt.
- Benutzerdefiniertes Netzwerk wird nicht unterstützt: Wenn Sie zuvor verwendet haben [the section called “Benutzerdefinierte Netzwerke”](#), um die Erschöpfung von IP-Adressen zu verringern, können Sie stattdessen verwenden IPv6. Sie können benutzerdefinierte Netzwerke nicht mit IPv6 verwenden. Wenn Sie benutzerdefinierte Netzwerke für die Netzwerkisolierung verwenden, müssen Sie möglicherweise weiterhin benutzerdefinierte Netzwerke und die IPv4-Produktfamilie für Ihre Cluster verwenden.

## Zuweisungen von IP-Adressen

- Kubernetes-Dienste: Kubernetes-Diensten werden nur Adressen zugewiesen. IPv6 Ihnen werden keine Adressen zugewiesen. IPv4
- Pods: Pods werden eine IPv6 Adresse und eine lokale IPv4 Hostadresse zugewiesen. Die hostlokale IPv4 Adresse wird mithilfe eines hostlokalen CNI-Plug-ins zugewiesen, das mit VPC CNI verkettet ist, und die Adresse wird nicht an die Kubernetes-Steuerebene gemeldet. Es wird nur verwendet, wenn ein Pod mit externen IPv4 Ressourcen in einer anderen Amazon VPC oder im Internet kommunizieren muss. Die hostlokale IPv4 Adresse wird SNATed (per VPC CNI) an die primäre IPv4 Adresse der primären ENI des Worker-Knotens weitergeleitet.
- Pods und Dienste: Pods und Dienste erhalten nur IPv6 Adressen, keine Adressen. IPv4 Wenn Pods mit externen IPv4 Endpunkten kommunizieren müssen, verwenden sie NAT auf dem Knoten selbst. Diese integrierte NAT-Fähigkeit macht [DNS64 und NAT64](#) überflüssig. Bei Datenverkehr, der einen öffentlichen Internetzugang erfordert, ist der Datenverkehr des Pods eine Quellnetzwerkadresse, die in eine öffentliche IP-Adresse übersetzt wird.
- Routing-Adressen: Wenn ein Pod außerhalb der VPC kommuniziert, wird seine ursprüngliche IPv6 Adresse beibehalten (nicht in die IPv6 Adresse des Knotens übersetzt). Dieser Datenverkehr wird direkt über ein Internet-Gateway oder ein Internet-Gateway nur für ausgehenden Datenverkehr geleitet.
- Knoten: Allen Knoten wird eine UN-Adresse zugewiesen. IPv4 IPv6
- Fargate-Pods: Jeder Fargate-Pod erhält eine IPv6 Adresse vom CIDR, die für das Subnetz angegeben ist, in dem er bereitgestellt wird. Die zugrunde liegende Hardwareeinheit, auf der

Fargate Pods ausgeführt werden, erhält eine eindeutige IPv4 IPv6 Adresse von den CIDRs , die dem Subnetz zugewiesen sind, in dem die Hardwareeinheit bereitgestellt wird.

## Wie benutzt man es mit EKS **IPv6**

- **Neuen Cluster erstellen:** Sie müssen einen neuen Cluster erstellen und angeben, dass Sie die IPv6 Familie für diesen Cluster verwenden möchten. Sie können die IPv6 Familie nicht für einen Cluster aktivieren, den Sie von einer früheren Version aktualisiert haben. Anweisungen zum Erstellen eines neuen Clusters finden Sie unter Überlegungen.
- **Aktuelle VPC-CNI verwenden:** Stellen Sie die Amazon VPC CNI-Version oder höher bereit.  
1.10.1 Diese Version oder höher wird standardmäßig bereitgestellt. Nachdem Sie das Add-on bereitgestellt haben, können Sie Ihr Amazon VPC CNI-Add-on nicht auf eine niedrigere Version herunterstufen, 1.10.1 ohne zuerst alle Knoten in allen Knotengruppen in Ihrem Cluster zu entfernen.
- **VPC CNI konfigurieren für **IPv6**:** Wenn Sie EC2 Amazon-Knoten verwenden, müssen Sie das Amazon VPC CNI-Add-on mit IP-Präfix-Delegierung und konfigurieren. IPv6 Wenn Sie beim Erstellen Ihres Clusters die IPv6-Familie wählen, wird die Version 1.10.1 des Add-ons standardmäßig auf diese Konfiguration festgelegt. Dies ist sowohl bei einem selbstverwalteten als auch bei Amazon EKS Add-on der Fall. Weitere Informationen über die IP-Präfix-Delegation finden Sie unter [the section called "Erhöhen Sie die IP-Adressen"](#).
- **Konfiguration **IPv4** und **IPv6** Adressen:** Wenn Sie einen Cluster erstellen, müssen die von Ihnen angegebene VPC und die Subnetze über einen IPv6 CIDR-Block verfügen, der der von Ihnen angegebenen VPC und den Subnetzen zugewiesen ist. Sie müssen auch über einen IPv4-CIDR-Block verfügen. Dies liegt daran, dass eine VPC, selbst wenn Sie nur IPv6 verwenden möchten, immer noch einen IPv4-CIDR-Block benötigt, um zu funktionieren. Weitere Informationen finden Sie unter [Verknüpfen eines IPv6 CIDR-Blocks mit Ihrer VPC](#) im Amazon VPC-Benutzerhandbuch.
- **Automatische Zuweisung von IPv6 Adressen zu Knoten:** Wenn Sie Ihre Knoten erstellen, müssen Sie Subnetze angeben, die für die automatische IPv6 Zuweisung von Adressen konfiguriert sind. Andernfalls können Sie Ihre Knoten nicht bereitstellen. Diese Konfiguration ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter [Ändern des IPv6 Adressierungsattributs für Ihr Subnetz](#) im Amazon VPC-Benutzerhandbuch.
- **Legen Sie die zu verwendenden Routentabellen festIPv6:** Die Routentabellen, die Ihren Subnetzen zugewiesen sind, müssen Routen für Adressen enthalten. IPv6 Weitere Informationen finden Sie unter [Migrieren zu IPv6](#) im Amazon VPC-Benutzerhandbuch.



- Sicherheitsgruppen einrichten für **IPv6**: Ihre Sicherheitsgruppen müssen IPv6 Adressen zulassen. Weitere Informationen finden Sie unter [Migrieren zu IPv6](#) im Amazon VPC-Benutzerhandbuch.
- Load Balancer einrichten: Verwenden Sie Version 2.3.1 oder höher des Load Balancer Controllers für den AWS Lastenausgleich von HTTP-Anwendungen mithilfe des [the section called “Application Load Balancing”](#) oder des Netzwerkverkehrs mithilfe der [the section called “Netzwerk-Load-Balancer”](#) To IPv6 Pods, wobei sich einer der Load Balancer im IP-Modus, aber nicht im Instanzmodus befindet. Weitere Informationen finden Sie unter [the section called “AWS Load Balancer Balancer-Controller”](#).
- **IPv6IAM-Richtlinie** hinzufügen: Sie müssen Ihrer IPv6 Node-IAM- oder CNI-IAM-Rolle eine IAM-Richtlinie hinzufügen. Zwischen den beiden empfehlen wir, dass Sie sie an eine CNI IAM-Rolle anfügen. Weitere Informationen erhalten Sie unter [the section called “Erstellen Sie eine IAM-Richtlinie für Cluster, die die IPv6-Familie verwendet”](#) und [the section called “Schritt 1: Erstellen Sie das Amazon VPC CNI-Plug-In für die IAM-Rolle von Kubernetes”](#).
- Evaluieren Sie alle Komponenten: Führen Sie vor der Bereitstellung von IPv6 Clustern eine gründliche Bewertung Ihrer Anwendungen, Amazon EKS-Add-ons und AWS Services durch, die Sie integrieren. Dies soll sicherstellen, dass mit IPv6 alles wie erwartet funktioniert.
- Fügen Sie **BootstrapArguments** selbstverwaltete Knotengruppen hinzu: Wenn Sie eine selbstverwaltete Knotengruppe in einem Cluster erstellen, der die IPv6 Familie verwendet, müssen die Benutzerdaten BootstrapArguments für die Datei [bootstrap.sh](#), die beim Start des Knotens ausgeführt wird, Folgendes enthalten. *your-cidr* Ersetzen Sie durch den IPv6 CIDR-Bereich der VPC Ihres Clusters.

```
--ip-family ipv6 --service-ipv6-cidr your-cidr
```

Wenn Sie den IPv6 CIDR Bereich für Ihren Cluster nicht kennen, können Sie ihn mit dem folgenden Befehl anzeigen (erfordert die AWS CLI-Version 2.4.9 oder höher).

```
aws eks describe-cluster --name my-cluster --query
cluster.kubernetesNetworkConfig.serviceIpv6Cidr --output text
```

## Bereitstellung eines Amazon **IPv6** EKS-Clusters und verwalteter Amazon Linux-Knoten

In diesem Tutorial stellen Sie eine IPv6 Amazon VPC, einen Amazon EKS-Cluster mit der IPv6 Familie und eine verwaltete Knotengruppe mit Amazon EC2 Amazon Linux-Knoten bereit. Sie können keine Amazon EC2 Windows-Knoten in einem IPv6 Cluster bereitstellen. Sie können auch Fargate-

Knoten in Ihrem Cluster bereitstellen, obwohl diese Anweisungen der Einfachheit halber nicht in diesem Thema enthalten sind.

## Voraussetzungen

Gehen Sie wie folgt vor, bevor Sie mit dem Tutorial beginnen:

Installieren und konfigurieren Sie die folgenden Tools und Ressourcen, die Sie zum Erstellen und Verwalten eines Amazon EKS-Clusters benötigen.

- Wir empfehlen Ihnen, sich mit allen Einstellungen vertraut zu machen und einen Cluster mit den Einstellungen bereitzustellen, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie [the section called “Erstellen eines -Clusters”](#) unter [the section called “Verwaltete Knotengruppen”](#) und in den [Überlegungen](#) zu diesem Thema. Sie können nur einige Einstellungen aktivieren, wenn Sie Ihren Cluster erstellen.
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Der von Ihnen verwendete IAM-Sicherheitsprinzipal muss über Berechtigungen für die Arbeit mit Amazon EKS-IAM-Rollen, serviceverknüpften Rollen AWS CloudFormation, einer VPC und verwandten Ressourcen verfügen. Weitere Informationen finden Sie unter [Aktionen](#) und [Verwenden von serviceverknüpften Rollen im IAM-Benutzerhandbuch](#).
- Wenn Sie `eksctl` verwenden, installieren Sie Version 0.210.0 oder höher auf Ihrem Computer. Informationen zum Installieren oder Aktualisieren finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI](#)

[in Ihrem Home-Verzeichnis installieren](#). Wenn Sie die verwenden AWS CloudShell, müssen Sie möglicherweise [Version 2.12.3 oder höher oder 1.27.160 oder höher der AWS CLI installieren, da es sich bei der](#) in der installierten AWS Standard-CLI-Version AWS CloudShell möglicherweise um eine frühere Version handelt.

Sie können eksctl oder CLI verwenden, um einen IPv6 Cluster bereitzustellen.

Stellen Sie einen IPv6 Cluster mit eksctl bereit

- a. Erstellen Sie die Datei `ipv6-cluster.yaml`. Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:
  - Ersetzen Sie *my-cluster* durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
  - *region-code* Ersetzen Sie durch eine beliebige AWS Region, die von Amazon EKS unterstützt wird. Eine Liste der AWS Regionen finden Sie unter [Amazon EKS-Endpunkte und Kontingente](#) im AWS Allgemeinen Referenzhandbuch.
  - Der Wert für `version` mit der Version Ihres Clusters. Weitere Informationen finden Sie unter [the section called "Kubernetes-Versionen"](#).
  - Ersetzen Sie *my-nodgroup* durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.
  - Ersetzen Sie *t3.medium* durch jeden beliebigen [Instance-Typ von AWS Nitro System](#).

```
cat >ipv6-cluster.yaml <<EOF

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: my-cluster
 region: region-code
 version: "X.XX"

kubernetesNetworkConfig:
```

```

ipFamily: IPv6

addons:
 - name: vpc-cni
 version: latest
 - name: coredns
 version: latest
 - name: kube-proxy
 version: latest

iam:
 withOIDC: true

managedNodeGroups:
 - name: my-nodegroup
 instanceType: t3.medium
EOF

```

## b. Erstellen Sie Ihren Cluster.

```
eksctl create cluster -f ipv6-cluster.yaml
```

Die Clustererstellung dauert mehrere Minuten. Fahren Sie erst fort, wenn Sie die letzte Ausgabezeile sehen, die der folgenden Ausgabe ähnelt.

```

[...]
[#] EKS cluster "my-cluster" in "region-code" region is ready

```

## c. Vergewissern Sie sich, dass den Standard-Pods IPv6 Adressen zugewiesen sind.

```
kubectl get pods -n kube-system -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                   | READY  | STATUS  | RESTARTS | AGE   | IP                       |                |
|----------------------------------------|--------|---------|----------|-------|--------------------------|----------------|
|                                        | NODE   |         |          |       |                          | NOMINATED NODE |
| READINESS GATES                        |        |         |          |       |                          |                |
| aws-node-rslts                         | 1/1    | Running | 1        | 5m36s |                          |                |
| 2600:1f13:b66:8200:11a5:ade0:c590:6ac8 |        |         |          |       | ip-192-168-34-75.region- |                |
| code.compute.internal                  | <none> |         | <none>   |       |                          |                |

```
aws-node-t74jh 1/1 Running 0 5m32s
 2600:1f13:b66:8203:4516:2080:8ced:1ca9 ip-192-168-253-70.region-
code.compute.internal <none> <none>
coredns-85d5b4454c-cw7w2 1/1 Running 0 56m
 2600:1f13:b66:8203:34e5:: ip-192-168-253-70.region-
code.compute.internal <none> <none>
coredns-85d5b4454c-tx6n8 1/1 Running 0 56m
 2600:1f13:b66:8203:34e5::1 ip-192-168-253-70.region-
code.compute.internal <none> <none>
kube-proxy-btpbk 1/1 Running 0 5m36s
 2600:1f13:b66:8200:11a5:ade0:c590:6ac8 ip-192-168-34-75.region-
code.compute.internal <none> <none>
kube-proxy-jjk2g 1/1 Running 0 5m33s
 2600:1f13:b66:8203:4516:2080:8ced:1ca9 ip-192-168-253-70.region-
code.compute.internal <none> <none>
```

- d. Vergewissern Sie sich, dass Standard-Services IPv6-Adressen zugewiesen wurden.

```
kubectl get services -n kube-system -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME         | TYPE      | CLUSTER-IP        | EXTERNAL-IP | PORT(S)       | AGE  |
|--------------|-----------|-------------------|-------------|---------------|------|
| SELECTOR     |           |                   |             |               |      |
| kube-dns     | ClusterIP | fd30:3087:b6c2::a | <none>      | 53/UDP,53/TCP | 57m  |
| app=kube-dns |           |                   |             |               | k8s- |

- e. (Optional) [Stellen Sie eine Beispielanwendung](#) bereit oder stellen Sie den [Load AWS Balancer Controller](#) und eine Beispielanwendung bereit, um den Lastenausgleich von HTTP-Anwendungen mit [the section called "Application Load Balancing"](#) oder den Netzwerkverkehr mit IPv6 Pods [the section called "Netzwerk-Load-Balancer"](#) durchzuführen.
- f. Nachdem Sie mit dem Cluster und den Knoten fertig sind, die Sie für dieses Tutorial erstellt haben, sollten Sie die Ressourcen bereinigen, die Sie mit dem folgenden Befehl erstellt haben.

```
eksctl delete cluster my-cluster
```

## Bereitstellen eines IPv6 Clusters mit AWS CLI

### Important

- Sie müssen alle Schritte in diesem Verfahren als derselbe Benutzer ausführen. Führen Sie den folgenden Befehl aus, um den aktuellen Benutzer zu überprüfen:

```
aws sts get-caller-identity
```

- Sie müssen alle Schritte in diesem Verfahren in derselben Shell ausführen. In mehreren Schritten in den vorherigen Schritten werden festgelegte Variablen verwendet. Schritte, die Variablen verwenden, funktionieren nicht richtig, wenn die Variablenwerte in einer anderen Shell festgelegt sind. Wenn Sie das [AWS CloudShell](#) folgende Verfahren verwenden, denken Sie daran, dass Ihre Shell-Sitzung beendet wird, wenn Sie etwa 20 bis 30 Minuten lang nicht mit der Tastatur oder dem Zeiger damit interagieren. Laufende Prozesse zählen nicht als Interaktionen.
- Die Anweisungen sind für die Bash-Shell geschrieben und müssen möglicherweise in anderen Shells angepasst werden.

Ersetzen Sie alle *example values* in den Schritten dieses Verfahrens mit eigenen Werten.

- a. Führen Sie die folgenden Befehle aus, um einige in späteren Schritten verwendete Variablen festzulegen. *region-code* Ersetzen Sie es durch die AWS Region, in der Sie Ihre Ressourcen bereitstellen möchten. Der Wert kann eine beliebige AWS Region sein, die von Amazon EKS unterstützt wird. Eine Liste der AWS Regionen finden Sie unter [Amazon EKS-Endpunkte und Kontingente](#) im AWS Allgemeinen Referenzhandbuch. Ersetzen Sie *my-cluster* durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Ersetzen Sie *my-nodegroup* durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Ersetzen Sie *111122223333* durch Ihre Konto-ID.

```
export region_code=region-code
export cluster_name=my-cluster
```

```
export nodegroup_name=my-nodegroup
export account_id=111122223333
```

b. Erstellen Sie eine Amazon VPC mit öffentlichen und privaten Subnetzen, die die Anforderungen von Amazon EKS und IPv6 erfüllt.

- i. Führen Sie den folgenden Befehl aus, um eine Variable für Ihren AWS CloudFormation Stacknamen festzulegen. Sie können *my-eks-ipv6-vpc* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
export vpc_stack_name=my-eks-ipv6-vpc
```

- ii. Erstellen Sie eine IPv6 VPC mithilfe einer AWS CloudFormation Vorlage.

```
aws cloudformation create-stack --region $region_code --stack-name $vpc_stack_name \
 --template-url https://s3.us-west-2.amazonaws.com/amazon-eks/
cloudformation/2020-10-29/amazon-eks-ipv6-vpc-public-private-subnets.yaml
```

Das Erstellen des Stacks nimmt einige Minuten in Anspruch. Führen Sie den folgenden Befehl aus. Fahren Sie erst mit dem nächsten Schritt fort, wenn die Ausgabe des Befehls angezeigt wird `CREATE_COMPLETE`.

```
aws cloudformation describe-stacks --region $region_code --stack-name
$vpc_stack_name --query Stacks[].StackStatus --output text
```

- iii. Rufen Sie IDs der öffentlichen Subnetze ab, die erstellt wurden.

```
aws cloudformation describe-stacks --region $region_code --stack-name
$vpc_stack_name \
 --query='Stacks[].Outputs[?OutputKey==`SubnetsPublic`].OutputValue' --output
text
```

Eine Beispielausgabe sieht wie folgt aus.

```
subnet-0a1a56c486EXAMPLE, subnet-099e6ca77aEXAMPLE
```

- iv. Aktivieren Sie die Option „IPv6-Adressen automatisch zuweisen“ für die erstellten öffentlichen Subnetze.

```
aws ec2 modify-subnet-attribute --region $region_code --subnet-id
subnet-0a1a56c486EXAMPLE --assign-ipv6-address-on-creation
aws ec2 modify-subnet-attribute --region $region_code --subnet-id
subnet-099e6ca77aEXAMPLE --assign-ipv6-address-on-creation
```

- v. Rufen Sie die Namen der Subnetze und Sicherheitsgruppen, die mit der Vorlage erstellt wurden, aus dem bereitgestellten AWS CloudFormation Stack ab und speichern Sie sie in Variablen, um sie in einem späteren Schritt zu verwenden.

```
security_groups=$(aws cloudformation describe-stacks --region $region_code --
stack-name $vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SecurityGroups`].OutputValue' --output
text)

public_subnets=$(aws cloudformation describe-stacks --region $region_code --stack-
name $vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SubnetsPublic`].OutputValue' --output
text)

private_subnets=$(aws cloudformation describe-stacks --region $region_code --
stack-name $vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SubnetsPrivate`].OutputValue' --output
text)

subnets=${public_subnets},${private_subnets}
```

- c. Erstellen Sie eine Cluster-IAM-Rolle und fügen Sie ihr die erforderliche von Amazon EKS IAM verwaltete Richtlinie hinzu. Von Amazon EKS verwaltete Kubernetes-Cluster rufen in Ihrem Namen andere AWS Services auf, um die Ressourcen zu verwalten, die Sie mit dem Service verwenden.
- i. Führen Sie den folgenden Befehl aus, um die Datei `eks-cluster-role-trust-policy.json` zu erstellen.

```
cat >eks-cluster-role-trust-policy.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "eks.amazonaws.com"
 },
 },
],
}
```



```

 "Action": "sts:AssumeRole"
 }
]
}
EOF

```

- ii. Führen Sie den folgenden Befehl aus, um eine Variable für Ihren Rollennamen festzulegen. Sie können *myAmazonEKSClusterRole* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
export cluster_role_name=myAmazonEKSClusterRole
```

- iii. Erstellen Sie die -Rolle.

```
aws iam create-role --role-name $cluster_role_name --assume-role-policy-document
file://"eks-cluster-role-trust-policy.json"
```

- iv. Rufen Sie den ARN der IAM-Rolle ab und speichern Sie ihn für einen späteren Schritt in einer Variablen.

```
CLUSTER_IAM_ROLE=$(aws iam get-role --role-name $cluster_role_name --
query="Role.Arn" --output text)
```

- v. Hängen Sie die erforderliche von Amazon EKS verwaltete IAM-Richtlinie an die Rolle an.

```
aws iam attach-role-policy --policy-arn arn:aws: iam::aws:policy/
AmazonEKSClusterPolicy --role-name $cluster_role_name
```

- d. Erstellen Sie Ihren Cluster.

```
aws eks create-cluster --region $region_code --name $cluster_name --kubernetes-
version 1.XX \
 --role-arn $CLUSTER_IAM_ROLE --resources-vpc-config subnetIds=
$subnets,securityGroupIds=$security_groups \
 --kubernetes-network-config ipFamily=ipv6
```

- i. HINWEIS: Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called “Unzureichende Kapazität”](#).

Die Erstellung des Clusters dauert mehrere Minuten. Führen Sie den folgenden Befehl aus. Fahren Sie erst mit dem nächsten Schritt fort, wenn die Ausgabe des Befehls lautet `ACTIVE`.

```
aws eks describe-cluster --region $region_code --name $cluster_name --query
cluster.status
```

- e. Erstellen oder aktualisieren Sie eine `kubeconfig`-Datei für Ihren Cluster, sodass Sie mit Ihrem Cluster kommunizieren können.

```
aws eks update-kubeconfig --region $region_code --name $cluster_name
```

Standardmäßig wird die `config` Datei in erstellt `~/.kube` oder die Konfiguration des neuen Clusters wird einer vorhandenen `config` Datei in hinzugefügt `~/.kube`.

- f. Erstellen Sie eine Knoten-IAM-Rolle.

- i. Führen Sie den folgenden Befehl aus, um die Datei `vpc-cni-ipv6-policy.json` zu erstellen.

```
cat >vpc-cni-ipv6-policy.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AssignIpv6Addresses",
 "ec2:DescribeInstances",
 "ec2:DescribeTags",
 "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeInstanceTypes"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:CreateTags"
],
 "Resource": [
 "arn:aws: ec2:*:*:network-interface/*"
]
 }
]
}
```

```
 }
]
}
EOF
```

ii. Erstellen Sie die IAM-Richtlinie.

```
aws iam create-policy --policy-name AmazonEKS_CNI_IPv6_Policy --policy-document
file://vpc-cni-ipv6-policy.json
```

iii. Führen Sie den folgenden Befehl aus, um die Datei `node-role-trust-relationship.json` zu erstellen.

```
cat >node-role-trust-relationship.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ec2.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
EOF
```

iv. Führen Sie den folgenden Befehl aus, um eine Variable für Ihren Rollennamen festzulegen. Sie können *AmazonEKSNodeRole* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
export node_role_name=AmazonEKSNodeRole
```

v. Erstellen Sie die IAM-Rolle.

```
aws iam create-role --role-name $node_role_name --assume-role-policy-document
file://"node-role-trust-relationship.json"
```

vi. Fügen Sie die IAM-Richtlinie an die IAM-Rolle an.

```
aws iam attach-role-policy --policy-arn arn:aws: iam::$account_id:policy/
AmazonEKS_CNI_IPv6_Policy \
```

```
--role-name $node_role_name
```

### Important

Der Einfachheit halber wird in diesem Tutorial die Richtlinie an diese IAM-Rolle angehängt. In einem Produktions-Cluster empfehlen wir jedoch, die Richtlinie an eine separate IAM-Rolle anzuhängen. Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).

vii. Hängen Sie die beiden erforderlichen IAM-verwalteten Richtlinien an die IAM-Rolle an.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/
AmazonEKSWorkerNodePolicy \
 --role-name $node_role_name
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/
AmazonEC2ContainerRegistryReadOnly \
 --role-name $node_role_name
```

viii. Rufen Sie den ARN der IAM-Rolle ab und speichern Sie ihn für einen späteren Schritt in einer Variablen.

```
node_iam_role=$(aws iam get-role --role-name $node_role_name --query="Role.Arn" --
output text)
```

g. Erstellen Sie eine verwaltete Knotengruppe.

i. Sehen Sie sich IDs der Subnetze an, die Sie in einem vorherigen Schritt erstellt haben.

```
echo $subnets
```

Eine Beispielausgabe sieht wie folgt aus.

```
subnet-0a1a56c486EXAMPLE, subnet-099e6ca77aEXAMPLE, subnet-0377963d69EXAMPLE, subnet-0c05f819
```

ii. Erstellen Sie die Knotengruppe. Ersetzen Sie *0a1a56c486EXAMPLE*, *099e6ca77aEXAMPLE*, *0377963d69EXAMPLE* und *0c05f819d5EXAMPLE* mit den im vorherigen Schritt zurückgegebenen Werten. Achten Sie darauf, die Kommas zwischen den Subnetzen IDs aus der vorherigen Ausgabe im folgenden Befehl zu entfernen. Sie können *t3.medium* mit jedem beliebigen [AWS -Nitro-System-Instance-Typ](#) ersetzen.

```
aws eks create-nodegroup --region $region_code --cluster-name $cluster_name --
nodegroup-name $nodegroup_name \
 --subnets subnet-0a1a56c486EXAMPLE subnet-099e6ca77aEXAMPLE
 subnet-0377963d69EXAMPLE subnet-0c05f819d5EXAMPLE \
 --instance-types t3.medium --node-role $node_iam_role
```

Das Erstellen der Knotengruppe nimmt einige Minuten in Anspruch. Führen Sie den folgenden Befehl aus. Fahren Sie erst mit dem nächsten Schritt fort, wenn die zurückgegebene Ausgabe **ACTIVE**

```
aws eks describe-nodegroup --region $region_code --cluster-name $cluster_name --
nodegroup-name $nodegroup_name \
 --query nodegroup.status --output text
```

- h. Vergewissern Sie sich, dass den Standard-Pods IPv6 Adressen in der IP Spalte zugewiesen sind.

```
kubectl get pods -n kube-system -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                   | READY  | STATUS  | RESTARTS | AGE   | IP                        |                |
|----------------------------------------|--------|---------|----------|-------|---------------------------|----------------|
|                                        |        |         |          |       |                           | NOMINATED NODE |
| READINESS GATES                        |        |         |          |       |                           |                |
| aws-node-rslts                         | 1/1    | Running | 1        | 5m36s |                           |                |
| 2600:1f13:b66:8200:11a5:ade0:c590:6ac8 |        |         |          |       | ip-192-168-34-75.region-  |                |
| code.compute.internal                  | <none> |         | <none>   |       |                           |                |
| aws-node-t74jh                         | 1/1    | Running | 0        | 5m32s |                           |                |
| 2600:1f13:b66:8203:4516:2080:8ced:1ca9 |        |         |          |       | ip-192-168-253-70.region- |                |
| code.compute.internal                  | <none> |         | <none>   |       |                           |                |
| coredns-85d5b4454c-cw7w2               | 1/1    | Running | 0        | 56m   |                           |                |
| 2600:1f13:b66:8203:34e5::              |        |         |          |       | ip-192-168-253-70.region- |                |
| code.compute.internal                  | <none> |         | <none>   |       |                           |                |
| coredns-85d5b4454c-tx6n8               | 1/1    | Running | 0        | 56m   |                           |                |
| 2600:1f13:b66:8203:34e5::1             |        |         |          |       | ip-192-168-253-70.region- |                |
| code.compute.internal                  | <none> |         | <none>   |       |                           |                |
| kube-proxy-btpbk                       | 1/1    | Running | 0        | 5m36s |                           |                |
| 2600:1f13:b66:8200:11a5:ade0:c590:6ac8 |        |         |          |       | ip-192-168-34-75.region-  |                |
| code.compute.internal                  | <none> |         | <none>   |       |                           |                |

```
kube-proxy-jjk2g 1/1 Running 0 5m33s
2600:1f13:b66:8203:4516:2080:8ced:1ca9 ip-192-168-253-70.region-
code.compute.internal <none> <none>
```

- i. Vergewissern Sie sich, dass den Standard-Services in der IP-Spalte IPv6-Adressen zugewiesen wurden.

```
kubectl get services -n kube-system -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME         | TYPE      | CLUSTER-IP        | EXTERNAL-IP | PORT(S)       | AGE  |
|--------------|-----------|-------------------|-------------|---------------|------|
| SELECTOR     |           |                   |             |               |      |
| kube-dns     | ClusterIP | fd30:3087:b6c2::a | <none>      | 53/UDP,53/TCP | 57m  |
| app=kube-dns |           |                   |             |               | k8s- |

- j. (Optional) [Stellen Sie eine Beispielanwendung](#) bereit oder stellen Sie den [Load AWS Balancer Controller](#) und eine Beispielanwendung bereit, um den Lastenausgleich von HTTP-Anwendungen mit [the section called “Application Load Balancing”](#) oder den Netzwerkverkehr mit IPv6 Pods [the section called “Netzwerk-Load-Balancer”](#) durchzuführen.
- k. Nachdem Sie mit dem Cluster und den Knoten fertig sind, die Sie für dieses Tutorial erstellt haben, sollten Sie die Ressourcen bereinigen, die Sie mit den folgenden Befehlen erstellt haben. Stellen Sie sicher, dass Sie keine der Ressourcen außerhalb dieses Tutorials verwenden, bevor Sie sie löschen.
- i. Wenn Sie diesen Schritt in einer anderen Shell ausführen als die vorherigen Schritte, legen Sie die Werte aller Variablen fest, die in den vorherigen Schritten verwendet wurden, und ersetzen Sie sie durch die *example values* Werte, die Sie beim Ausführen der vorherigen Schritte angegeben haben. Wenn Sie diesen Schritt in derselben Shell ausführen, in der Sie die vorherigen Schritte ausgeführt haben, fahren Sie mit dem nächsten Schritt fort.

```
export region_code=region-code
export vpc_stack_name=my-eks-ipv6-vpc
export cluster_name=my-cluster
export nodegroup_name=my-nodegroup
export account_id=111122223333
export node_role_name=AmazonEKSNodeRole
export cluster_role_name=myAmazonEKSClusterRole
```

- ii. Löschen Sie Ihre Knotengruppe.

```
aws eks delete-nodegroup --region $region_code --cluster-name $cluster_name --
nodegroup-name $nodegroup_name
```

Dies dauert in der Regel einige Minuten. Führen Sie den folgenden Befehl aus. Fahren Sie nicht mit dem nächsten Schritt fort, wenn eine Ausgabe zurückgegeben wird.

```
aws eks list-nodegroups --region $region_code --cluster-name $cluster_name --query
nodegroups --output text
```

### iii. Löschen Sie den Cluster.

```
aws eks delete-cluster --region $region_code --name $cluster_name
```

Das Löschen des Clusters nimmt einige Minuten in Anspruch. Stellen Sie vor dem Fortfahren sicher, dass der Cluster mit dem folgenden Befehl gelöscht wird.

```
aws eks describe-cluster --region $region_code --name $cluster_name
```

Fahren Sie erst mit dem nächsten Schritt fort, wenn Ihre Ausgabe der folgenden Ausgabe ähnelt.

```
An error occurred (ResourceNotFoundException) when calling the DescribeCluster
operation: No cluster found for name: my-cluster.
```

### iv. Löschen Sie die IAM-Ressourcen, die Sie erstellt haben. Ersetzen Sie

*AmazonEKS\_CNI\_IPv6\_Policy* mit dem von Ihnen gewählten Namen, wenn Sie einen anderen Namen als den in den vorherigen Schritten verwendeten gewählt haben.

```
aws iam detach-role-policy --role-name $cluster_role_name --policy-arn arn:aws:
iam::aws:policy/AmazonEKSClusterPolicy
aws iam detach-role-policy --role-name $node_role_name --policy-arn arn:aws:
iam::aws:policy/AmazonEKSWorkerNodePolicy
aws iam detach-role-policy --role-name $node_role_name --policy-arn arn:aws:
iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
aws iam detach-role-policy --role-name $node_role_name --policy-arn arn:aws: iam::
$account_id:policy/AmazonEKS_CNI_IPv6_Policy
aws iam delete-policy --policy-arn arn:aws: iam::$account_id:policy/
AmazonEKS_CNI_IPv6_Policy
aws iam delete-role --role-name $cluster_role_name
```

```
aws iam delete-role --role-name $node_role_name
```

v. Löschen Sie den AWS CloudFormation Stack, der die VPC erstellt hat.

```
aws cloudformation delete-stack --region $region_code --stack-name $vpc_stack_name
```

## Ausgehenden Internetzugang für Pods aktivieren

Gilt für: Linux IPv4 Fargate-Knoten, Linux-Knoten mit Amazon-Instances EC2

Wenn Sie Ihren Cluster mithilfe der IPv6 Familie bereitgestellt haben, gelten die Informationen in diesem Thema nicht für Ihren Cluster, da IPv6 Adressen nicht netzwerkübersetzt werden. Weitere Informationen zur Verwendung von IPv6 mit Ihrem Cluster finden Sie unter [the section called “IPv6”](#).

Standardmäßig wird jedem Pod in Ihrem Cluster eine [private](#) IPv4 Adresse aus einem CIDR-Block (Classless Interdomain Routing) zugewiesen, der der VPC zugeordnet ist, in der der Pod bereitgestellt wird. Pods in derselben VPC kommunizieren miteinander und verwenden diese privaten IP-Adressen als Endpunkte. [Wenn ein Pod mit einer IPv4 Adresse kommuniziert, die sich nicht in einem CIDR-Block befindet, der Ihrer VPC zugeordnet ist, übersetzt das Amazon VPC CNI-Plugin \(sowohl für Linux als auch für Windows\) die IPv4 Adresse des Pods standardmäßig in die primäre private IPv4 Adresse der primären elastic network interface des Knotens, auf dem der Pod läuft, standardmäßig \\*](#).

### Note

Bei Windows-Knoten müssen zusätzliche Details berücksichtigt werden. Standardmäßig ist das [VPC-CNI-Plug-In für Windows](#) mit einer Netzwerkkonfiguration definiert, in der der Datenverkehr zu einem Ziel innerhalb derselben VPC für SNAT ausgeschlossen ist. Das bedeutet, dass für die interne VPC-Kommunikation SNAT deaktiviert ist und die einem Pod zugewiesene IP-Adresse innerhalb der VPC routbar ist. Bei Datenverkehr zu einem Ziel außerhalb der VPC wird die Quell-Pod-IP jedoch an die primäre IP-Adresse der Instanz ENI gesendet. Diese Standardkonfiguration für Windows stellt sicher, dass der Pod genauso auf Netzwerke außerhalb Ihrer VPC zugreifen kann wie die Host-Instance.

Folgen dieses Verhaltens:

- Ihre Pods können nur dann mit Internetressourcen kommunizieren, wenn dem Knoten, auf dem sie ausgeführt werden, eine [öffentliche](#) oder [elastische](#) IP-Adresse zugewiesen wurde und er sich in



einem [öffentlichen Subnetz](#) befindet. Die einem öffentlichen Subnetz zugeordnete [Routing-Tabelle](#) enthält eine Route zu einem Internet-Gateway. Wir empfehlen, Knoten nach Möglichkeit in privaten Subnetzen bereitzustellen.

- Bei früheren Versionen des Plug-ins können Ressourcen 1.8.0, die sich in Netzwerken befinden oder VPCs die über [VPC-Peering](#), eine [Transit-VPC oder AWS Direct Connect mit Ihrer Cluster-VPC](#) verbunden sind, keine Kommunikation mit Ihren Pods hinter sekundären elastischen Netzwerkschnittstellen initiieren. Ihre Pods können jedoch die Kommunikation mit diesen Ressourcen initiieren und Antworten von ihnen erhalten.

Wenn eine der folgenden Aussagen in Ihrer Umgebung zutrifft, ändern Sie die Standardkonfiguration mit dem folgenden Befehl.

- Sie haben Ressourcen in Netzwerken oder VPCs die über [VPC-Peering](#), eine [Transit-VPC oder AWS Direct Connect mit Ihrer Cluster-VPC](#) verbunden sind und die die Kommunikation mit Ihren Pods über eine IPv4 Adresse initiieren müssen und Ihre Plugin-Version ist älter als 1.8.0
- Ihre Pods befinden sich in einem [privaten Subnetz](#) und müssen ausgehend mit dem Internet kommunizieren. Das Subnetz hat eine Route zu einem [NAT-Gateway](#).

```
kubectl set env daemonset -n kube-system aws-node AWS_VPC_K8S_CNI_EXTERNALSNAT=true
```

#### Note

Die Konfigurationsvariablen `AWS_VPC_K8S_CNI_EXTERNALSNAT` und `AWS_VPC_K8S_CNI_EXCLUDE_SNAT_CIDRS` CNI gelten nicht für Windows-Knoten. Die Deaktivierung von SNAT wird für Windows nicht unterstützt. Um eine Liste von IPv4 CIDRs aus SNAT auszuschließen, können Sie dies definieren, indem Sie den `ExcludedSnatCIDRs` Parameter im Windows-Bootstrap-Skript angeben. Weitere Informationen zur Verwendung dieses Parameters finden Sie unter [the section called "Bootstrap-Skript-Konfigurationsparameter"](#).

## Host-Netzwerke

\* Wenn die Spezifikation eines Pods Folgendes enthält `hostNetwork=true` (Standard ist `false`), wird seine IP-Adresse nicht in eine andere Adresse übersetzt. Dies ist standardmäßig für das kube-proxy Amazon VPC CNI-Plugin für Kubernetes-Pods der Fall, die auf Ihrem Cluster ausgeführt

werden. Bei diesen Pods entspricht die IP-Adresse der primären IP-Adresse des Knotens, sodass die IP-Adresse des Pods nicht übersetzt wird. Weitere Informationen zu den `hostNetwork` Einstellungen eines Pods finden Sie unter [PodSpec v1 core](#) in der Kubernetes-API-Referenz.

## Beschränken Sie den Pod-Verkehr mit Kubernetes-Netzwerkrichtlinien

Standardmäßig gibt es in Kubernetes keine Einschränkungen für IP-Adressen, Ports oder Verbindungen zwischen Pods in Ihrem Cluster oder zwischen Ihren Pods und Ressourcen in einem anderen Netzwerk. Sie können die Kubernetes-Netzwerkrichtlinie verwenden, um den Netzwerkverkehr zu und von Ihren Pods einzuschränken. Weitere Informationen finden Sie in der Kubernetes-Dokumentation unter [Netzwerkrichtlinien](#).

Wenn Sie eine Version 1.13 oder eine frühere Version des Amazon VPC CNI-Plug-ins für Kubernetes auf Ihrem Cluster haben, müssen Sie eine Drittanbieterlösung implementieren, um Kubernetes-Netzwerkrichtlinien auf Ihren Cluster anzuwenden. In der Version 1.14 oder höher des Plugins können Netzwerkrichtlinien implementiert werden, sodass Sie keine Drittanbieterlösung verwenden müssen. In diesem Thema erfahren Sie, wie Sie Ihren Cluster so konfigurieren, dass er die Kubernetes-Netzwerkrichtlinie auf Ihrem Cluster verwendet, ohne ein Drittanbieter-Add-on zu verwenden.

Netzwerkrichtlinien im Amazon VPC CNI-Plugin für Kubernetes werden in den folgenden Konfigurationen unterstützt.

- Version 1.14 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes auf Ihrem Cluster.
- Für IPv4- oder IPv6-Adressen konfigurierter Cluster.
- [Sie können Netzwerkrichtlinien mit Sicherheitsgruppen für Pods verwenden](#). Mit Netzwerkrichtlinien können Sie die gesamte Kommunikation innerhalb eines Clusters steuern. Mit Sicherheitsgruppen für Pods können Sie den Zugriff auf AWS Dienste von Anwendungen innerhalb eines Pods aus steuern.
- Sie können Netzwerkrichtlinien mit benutzerdefinierten Netzwerken und Präfixdelegierung verwenden.

## Überlegungen

### Architektur

- Wenn Sie Netzwerkrichtlinien des Amazon VPC CNI-Plug-ins für Kubernetes mit dem Amazon VPC CNI-Plugin für Kubernetes auf Ihren Cluster anwenden, können Sie die Richtlinien nur

auf Amazon Linux-Knoten anwenden. EC2 Sie können die Richtlinien nicht auf Fargate- oder Windows-Knoten anwenden.

- Netzwerkrichtlinien gelten nur für eine IPv4 oder für IPv6 Adressen, aber nicht für beide. In einem IPv4 Cluster weist das VPC-CNI Pods IPv4 Adressen zu und wendet Richtlinien an. IPv4 In einem IPv6 Cluster weist das VPC-CNI Pods IPv6 Adressen zu und wendet Richtlinien an. IPv6 Alle IPv4 Netzwerkrichtlinienregeln, die auf einen IPv6 Cluster angewendet werden, werden ignoriert. Alle IPv6 Netzwerkrichtlinienregeln, die auf einen IPv4 Cluster angewendet werden, werden ignoriert.

## Netzwerkrichtlinien

- Netzwerkrichtlinien werden nur auf Pods angewendet, die Teil einer Bereitstellung sind. Auf eigenständige Pods, für die kein `metadata.ownerReferences` Set vorhanden ist, können keine Netzwerkrichtlinien angewendet werden.
- Du kannst mehrere Netzwerkrichtlinien auf denselben Pod anwenden. Wenn zwei oder mehr Richtlinien konfiguriert sind, die denselben Pod auswählen, werden alle Richtlinien auf den Pod angewendet.
- Die maximale Anzahl eindeutiger Kombinationen von Ports für jedes Protokoll in jedem Protokoll `ingress:` oder jeden `egress:` Selektor in einer Netzwerkrichtlinie beträgt 24.
- Für jeden Ihrer Kubernetes-Dienste muss der Service-Port mit dem Container-Port identisch sein. Wenn Sie benannte Ports verwenden, verwenden Sie denselben Namen auch in der Servicespezifikation.

## Migration

- Wenn Ihr Cluster derzeit eine Drittanbieterlösung zur Verwaltung von Kubernetes-Netzwerkrichtlinien verwendet, können Sie dieselben Richtlinien mit dem Amazon VPC CNI-Plugin für Kubernetes verwenden. Sie müssen jedoch Ihre bestehende Lösung entfernen, damit sie nicht dieselben Richtlinien verwaltet.

## Installation

- Das Netzwerkrichtlinienfeature erstellt und erfordert die Definition einer benutzerdefinierten `PolicyEndpoint`-Ressource (Custom Resource Definition, CRD) namens `policyendpoints.networking.k8s.aws`. `PolicyEndpoint`-Objekte der benutzerdefinierten

Ressource werden von Amazon EKS verwaltet. Sie sollten diese Ressourcen nicht ändern oder löschen.

- Wenn Sie Pods ausführen, die die IAM-Anmeldeinformationen der Instanzrolle verwenden oder eine Verbindung zum EC2 IMDS herstellen, achten Sie darauf, ob Netzwerkrichtlinien vorhanden sind, die den EC2 Zugriff auf das IMDS blockieren würden. Möglicherweise müssen Sie eine Netzwerkrichtlinie hinzufügen, um den Zugriff auf IMDS zu ermöglichen. EC2 Weitere Informationen finden Sie unter [Instance-Metadaten und Benutzerdaten](#) im EC2 Amazon-Benutzerhandbuch.

Pods, die IAM-Rollen für Dienstkonten oder EKS Pod Identity verwenden, greifen nicht auf EC2 IMDS zu.

- Das Amazon VPC CNI-Plugin für Kubernetes wendet keine Netzwerkrichtlinien auf zusätzliche Netzwerkschnittstellen für jeden Pod an, sondern nur auf die primäre Schnittstelle für jeden Pod (`eth0`). Das hat Auswirkungen auf folgende Architekturen:
  - IPv6-Pods, bei denen die Variable `ENABLE_V4_EGRESS` auf `true` festgelegt ist. Diese Variable ermöglicht es der IPv4 Ausgangsfunktion, die IPv6 Pods mit IPv4 Endpunkten wie denen außerhalb des Clusters zu verbinden. Die IPv4 Ausgangsfunktion erstellt eine zusätzliche Netzwerkschnittstelle mit einer lokalen Loopback-Adresse. IPv4
  - Bei Verwendung verketteter Netzwerk-Plugins wie Multus. Da diese Plugins jedem Pod Netzwerkschnittstellen hinzufügen, werden Netzwerkrichtlinien nicht auf die verketteten Netzwerk-Plugins angewendet.

Beschränken Sie den Pod-Netzwerkverkehr mit Kubernetes-Netzwerkrichtlinien

Sie können eine Kubernetes-Netzwerkrichtlinie verwenden, um den Netzwerkverkehr zu und von Ihren Pods einzuschränken. Weitere Informationen finden Sie in der Kubernetes-Dokumentation unter [Netzwerkrichtlinien](#).

Sie müssen Folgendes konfigurieren, um diese Funktion nutzen zu können:

1. Richten Sie die Richtliniendurchsetzung beim Start des Pods ein. Sie tun dies im `aws-node` Container der VPC DaemonSet CNI.
2. Aktivieren Sie den Netzwerkrichtlinienparameter für das Add-on.
3. Konfigurieren Sie Ihren Cluster so, dass er die Kubernetes-Netzwerkrichtlinie verwendet

Bevor Sie beginnen, lesen Sie sich die Überlegungen durch. Weitere Informationen finden Sie unter [the section called “Überlegungen”](#).

## Voraussetzungen

Die folgenden Voraussetzungen müssen für die Funktion erfüllt sein:

### Minimale Cluster-Version

Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#). Auf dem Cluster muss eine der in der folgenden Tabelle aufgeführten Kubernetes-Versionen und Plattform-Versionen ausgeführt werden. Beachten Sie, dass alle Kubernetes- und Plattformversionen, die später als die aufgeführten sind, ebenfalls unterstützt werden. Sie können Ihre aktuelle Kubernetes-Version überprüfen, indem Sie den folgenden Befehl durch den Namen Ihres Clusters ersetzen *my-cluster* und dann den geänderten Befehl ausführen:

```
aws eks describe-cluster
 --name my-cluster --query cluster.version --output
 text
```

| Kubernetes-Version | Plattformversion |
|--------------------|------------------|
| 1.27.4             | eks.5            |
| 1.26.7             | eks.6            |

### VPC-CNI-Mindestversion

Version 1.14 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes auf Ihrem Cluster. Sie können Ihre aktuelle Version mit dem folgenden Befehl überprüfen:

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |
cut -d : -f 3
```

Wenn Ihre Version älter als 1.14 ist, finden Sie unter [the section called “Aktualisieren \(EKS-Add-on\)”](#) Informationen zum Aktualisieren des Plugins auf Version 1.14 oder höher.

## Linux-Kernel-Mindestversion

Ihre Knoten müssen eine Linux-Kernelversion ab Version 5.10 haben. Sie können Ihre Kernelversion mit `uname -r` überprüfen. Wenn Sie die neuesten Versionen von Amazon EKS-optimiertem Amazon Linux, Amazon EKS-optimiertem beschleunigtem Amazon Linux und Bottlerocket AMIs verwenden, verfügen diese bereits über die erforderliche Kernelversion.

Amazon-EKS-optimierte Amazon-Linux-AMI-Versionen ab v20231116 verfügen über Kernel-Version 5.10.

Schritt 1: Richten Sie die Richtliniendurchsetzung beim Start des Pods ein

Das Amazon VPC CNI-Plugin für Kubernetes konfiguriert Netzwerkrichtlinien für Pods parallel zur Pod-Bereitstellung. Bis alle Richtlinien für den neuen Pod konfiguriert sind, beginnen Container im neuen Pod mit einer standardmäßigen Zulassungsrichtlinie. Dies wird als Standardmodus bezeichnet. Eine standardmäßige Zulassungsrichtlinie bedeutet, dass der gesamte eingehende und ausgehende Datenverkehr zu und von den neuen Pods zugelassen ist. Für die Pods werden beispielsweise keine Firewallregeln durchgesetzt (der gesamte Datenverkehr ist zulässig), bis der neue Pod mit den aktiven Richtlinien aktualisiert wurde.

Wenn die `NETWORK_POLICY_ENFORCING_MODE` Variable auf `strict` gesetzt ist, beginnen Pods, die das VPC-CNI verwenden, mit einer Standardverweigerungsrichtlinie. Anschließend werden die Richtlinien konfiguriert. Dies wird als strikter Modus bezeichnet. Im strikten Modus benötigen Sie eine Netzwerkrichtlinie für jeden Endpunkt, auf den Ihre Pods in Ihrem Cluster zugreifen müssen. Beachten Sie, dass diese Anforderung für die CoreDNS-Pods gilt. Die standardmäßige Ablehnungsrichtlinie ist nicht für Pods mit Host-Netzwerk konfiguriert.

Sie können die Standard-Netzwerkrichtlinie ändern, indem Sie die Umgebungsvariable `NETWORK_POLICY_ENFORCING_MODE` `strict` im `aws-node` Container der DaemonSet VPC-CNI auf setzen.

```
env:
 - name: NETWORK_POLICY_ENFORCING_MODE
 value: "strict"
```

Schritt 2: Aktivieren Sie den Netzwerkrichtlinienparameter für das Add-on

Das Netzwerkrichtlinien-Feature verwendet standardmäßig den Port 8162 auf dem Knoten für Metriken. Außerdem verwendete das Feature den Port 8163 für Zustandstests. Wenn Sie eine

andere Anwendung auf die Knoten oder innerhalb von Pods ausführen, die diese Ports verwenden müssen, kann die App nicht ausgeführt werden. In der VPC CNI-Version v1.14.1 oder höher können Sie diese Ports ändern.

Gehen Sie wie folgt vor, um den Netzwerkrichtlinienparameter für das Add-on zu aktivieren.

## AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus. Wählen Sie dann den Namen des Clusters aus, für den Sie das Amazon-VPC-CNI-Add-on konfigurieren möchten.
3. Wählen Sie die Registerkarte Add-ons.
4. Wählen Sie das Kästchen oben rechts in der Add-On-Box aus und wählen Sie dann Edit (Bearbeiten).
5. Auf der Amazon VPC CNI Seite „Konfigurieren“:
  - a. Wählen Sie in der Versionsliste eine v1.14.0-eksbuild.3 oder eine neuere Version aus.
  - b. Erweitern Sie Optionale Konfigurationseinstellungen.
  - c. Geben Sie den JSON-Schlüssel "enableNetworkPolicy": und den Wert "true" in Konfigurationswerte ein. Der resultierende Text muss ein gültiges JSON-Objekt sein. Wenn dieser Schlüssel und dieser Wert die einzigen Daten im Textfeld sind, setzen Sie den Schlüssel und den Wert in geschweifte Klammern { }.

Im folgenden Beispiel ist die Netzwerkrichtlinien-Funktion aktiviert und Messwerte und Integritätstests sind auf die Standard-Portnummern eingestellt:

```
{
 "enableNetworkPolicy": "true",
 "nodeAgent": {
 "healthProbeBindAddr": "8163",
 "metricsBindAddr": "8162"
 }
}
```

## Helm

Wenn Sie das Amazon VPC CNI-Plugin für Kubernetes über installiert haben, können Sie die Konfiguration aktualisierenhelm, um die Ports zu ändern.

1. Führen Sie den folgenden Befehl aus, um die Ports zu ändern. Legen Sie die Portnummer im Wert für Schlüssel `nodeAgent.metricsBindAddr` bzw. Schlüssel `nodeAgent.healthProbeBindAddr` fest.

```
helm upgrade --set nodeAgent.metricsBindAddr=8162 --set
nodeAgent.healthProbeBindAddr=8163 aws-vpc-cni --namespace kube-system eks/aws-vpc-
cni
```

## kubectl

1. Öffnen Sie das DaemonSet `aws-node` in Ihrem Editor.

```
kubectl edit daemonset -n kube-system aws-node
```

2. Ersetzen Sie die Portnummern in den folgenden Befehlsargumenten im `args:` im `aws-network-policy-agent`-Container im `aws-node`-DaemonSet-Manifest von VPC CNI.

```
- args:
 - --metrics-bind-addr=:8162
 - --health-probe-bind-addr=:8163
```

## Schritt 3: Mounten Sie das Berkeley Packet Filter (BPF) -Dateisystem auf Ihren Knoten

Sie müssen das Berkeley Packet Filter (BPF) -Dateisystem auf jedem Ihrer Knoten mounten.

### Note

Wenn es sich bei Ihrem Cluster um eine Version 1.27 oder höher handelt, können Sie diesen Schritt überspringen, da alle Amazon EKS-optimierten Amazon Linux- und Bottlerocket-Versionen AMIs für 1.27 oder später bereits über diese Funktion verfügen. Für alle anderen Clusterversionen können Sie diesen Schritt überspringen, wenn Sie das für Amazon EKS optimierte Amazon-Linux-AMI mindestens auf Version `v20230703` aktualisieren oder das Bottlerocket-AMI mindestens auf Version `v1.0.2` aktualisieren.

1. Mounten Sie das Berkeley Packet Filter (BPF)-Dateisystem auf jedem Ihrer Knoten.



```
sudo mount -t bpf bpffs /sys/fs/bpf
```

2. Fügen Sie dann denselben Befehl zu Ihren Benutzerdaten in Ihrer Startvorlage für Ihre Amazon EC2 Auto Scaling Scaling-Gruppen hinzu.

Schritt 4: Konfigurieren Sie Ihren Cluster für die Verwendung von Kubernetes-Netzwerkrichtlinien

Sie können dies für ein Amazon EKS-Add-on oder ein selbstverwaltetes Add-On festlegen.

#### Amazon-EKS-Add-On

Mithilfe der AWS CLI können Sie den Cluster für die Verwendung von Kubernetes-Netzwerkrichtlinien konfigurieren, indem Sie den folgenden Befehl ausführen. Ersetzen Sie `my-cluster` durch den Namen Ihres Clusters und den IAM-Rollen-ARN durch die Rolle, die Sie verwenden.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version
v1.14.0-eksbuild.3 \
 --service-account-role-arn arn:aws:iam::123456789012:role/AmazonEKSVPCCNIRole \
 --resolve-conflicts PRESERVE --configuration-values '{"enableNetworkPolicy":
"true"}'
```

Gehen Sie wie folgt vor, um dies mit der AWS Management Console zu konfigurieren:

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus. Wählen Sie dann den Namen des Clusters aus, für den Sie das Amazon-VPC-CNI-Add-on konfigurieren möchten.
3. Wählen Sie die Registerkarte Add-ons.
4. Wählen Sie das Kästchen oben rechts in der Add-On-Box aus und wählen Sie dann Edit (Bearbeiten).
5. Auf der Amazon VPC CNI Seite „Konfigurieren“:
  - a. Wählen Sie in der Versionsliste eine `v1.14.0-eksbuild.3` oder eine neuere Version aus.
  - b. Erweitern Sie Optionale Konfigurationseinstellungen.
  - c. Geben Sie den JSON-Schlüssel `"enableNetworkPolicy":` und den Wert `"true"` in Konfigurationswerte ein. Der resultierende Text muss ein gültiges JSON-Objekt sein. Wenn dieser Schlüssel und dieser Wert die einzigen Daten im Textfeld sind, setzen Sie den Schlüssel und den Wert in geschweifte Klammern `{ }`. Das folgende Beispiel zeigt, dass die Netzwerkrichtlinie aktiviert ist:

```
{ "enableNetworkPolicy": "true" }
```

Der folgende Screenshot zeigt ein Beispiel für dieses Szenario.



# Configure Amazon VPC CNI

Amazon VPC CNI

Info

|                                                                                                        |                                |                                                                                                              |
|--------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| Listed by <div></div> | Category <div>networking</div> | Status <div> Active</div> |
|--------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------|

Version

Select the version for this add-on.

v1.17.1-eksbuild.1

Select IAM role

Select an IAM role to use with this add-on. To create a new role, follow the instructions in the [Amazon EKS User Guide](#).

Optional configuration settings

Add-on configuration schema

Refer to the JSON schema below. The configuration values entered in the code editor will be validated against this schema.

```
{
 "$ref": "#/definitions/VpcCni",
 "$schema": "http://json-schema.org/draft-06/schema#",
 "definitions": {
 "Affinity": {
 "type": [
 "object",
 "null"
]
 },
 "EniConfig": {
 "additionalProperties": false,

```

Configuration values

Info

Specify any additional JSON or YAML configurations that should be applied to the add-on.

1

{ "enableNetworkPolicy": "true" }

## Selbstverwaltetes Add-On

### Helm

Wenn Sie das Amazon VPC CNI-Plugin für Kubernetes über installiert haben, können Sie die Konfiguration aktualisieren `helm`, um die Netzwerkrichtlinie zu aktivieren.

1. Führen Sie den folgenden Befehl aus, um die Netzwerkrichtlinie zu aktivieren.

```
helm upgrade --set enableNetworkPolicy=true aws-vpc-cni --namespace kube-system eks/
aws-vpc-cni
```

### kubectl

1. Öffnen Sie das ConfigMap `amazon-vpc-cni` in Ihrem Editor.

```
kubectl edit configmap -n kube-system amazon-vpc-cni -o yaml
```

2. Fügen Sie data in ConfigMap die folgende Zeile hinzu:

```
enable-network-policy-controller: "true"
```

Sobald Sie die Zeile hinzugefügt haben, ConfigMap sollte sie wie im folgenden Beispiel aussehen.

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: amazon-vpc-cni
 namespace: kube-system
data:
 enable-network-policy-controller: "true"
```

3. Öffnen Sie das DaemonSet `aws-node` in Ihrem Editor.

```
kubectl edit daemonset -n kube-system aws-node
```

- a. Ersetzen Sie im Befehlsargument `--enable-network-policy=false` in `args:` im Container `aws-network-policy-agent` im DaemonSet-Manifest `aws-node` von VPC CNI den Wert `false` durch `true`.

```
- args:
 - --enable-network-policy=true
```

## Schritt 5. Nächste Schritte

Nachdem Sie die Konfiguration abgeschlossen haben, vergewissern Sie sich, dass die `aws-node` Pods auf Ihrem Cluster ausgeführt werden.

```
kubectl get pods -n kube-system | grep 'aws-node\|amazon'
```

Eine Beispielausgabe sieht wie folgt aus.

|                |     |         |             |
|----------------|-----|---------|-------------|
| aws-node-gmqp7 | 2/2 | Running | 1 (24h ago) |
| 24h            |     |         |             |
| aws-node-pinsh | 2/2 | Running | 1 (24h ago) |
| 24h            |     |         |             |

In den Versionen 1.14 und höher befinden sich 2 Container in den `aws-node` Pods. In früheren Versionen und wenn die Netzwerkrichtlinie deaktiviert ist, gibt es nur einen einzigen Container in den `aws-node`-Pods.

Sie können jetzt Kubernetes-Netzwerkrichtlinien in Ihrem Cluster bereitstellen.

Um Kubernetes-Netzwerkrichtlinien zu implementieren, erstellen Sie `NetworkPolicy` Kubernetes-Objekte und stellen sie in Ihrem Cluster bereit. `NetworkPolicy`-Objekte sind auf einen Namespace beschränkt. Sie implementieren Richtlinien, um Datenverkehr zwischen Pods auf der Grundlage von Labelselektoren, Namespaces und IP-Adressbereichen zuzulassen oder zu verweigern. Weitere Informationen zum Erstellen von `NetworkPolicy`-Objekten finden Sie in der [Kubernetes-Dokumentation unter Netzwerkrichtlinien](#).

Die Durchsetzung von `NetworkPolicy` Kubernetes-Objekten wird mit dem Extended Berkeley Packet Filter (eBPF) implementiert. Im Vergleich zu iptables-basierten Implementierungen bietet er geringere Latenzzeiten und Leistungsmerkmale, einschließlich einer geringeren CPU-Auslastung und der Vermeidung sequenzieller Suchvorgänge. Darüber hinaus bieten eBPF-Sonden

Zugriff auf kontextreiche Daten, mit deren Hilfe komplexe Probleme auf Kernelebene behoben und die Beobachtbarkeit verbessert werden können. Amazon EKS unterstützt einen EBPF-basierten Exporter, der die Tests nutzt, um Richtlinienergebnisse auf jedem Knoten zu protokollieren und die Daten zur Unterstützung beim Debuggen an externe Protokollsammler zu exportieren. Weitere Informationen finden Sie in der [eBPF-Dokumentation](#).

## Kubernetes-Netzwerkrichtlinien für Amazon EKS Pod-Netzwerkverkehr deaktivieren

Deaktivieren Sie die Kubernetes-Netzwerkrichtlinien, um den Amazon EKS Pod-Netzwerkverkehr nicht mehr einzuschränken

1. Listet alle Kubernetes-Netzwerkrichtlinien auf.

```
kubectl get netpol -A
```

2. Löschen Sie jede Kubernetes-Netzwerkrichtlinie. Sie müssen alle Netzwerkrichtlinien löschen, bevor Sie Netzwerkrichtlinien deaktivieren können.

```
kubectl delete netpol <policy-name>
```

3. Öffnen Sie den aws-Node DaemonSet in Ihrem Editor.

```
kubectl edit daemonset -n kube-system aws-node
```

4. Ersetzen Sie im Befehlsargument `--enable-network-policy=true` in `args:` im Container `aws-network-policy-agent` im DaemonSet-Manifest `aws-node` von VPC CNI den Wert `true` durch `false`.

```
- args:
 - --enable-network-policy=true
```

## Fehlerbehebung bei Kubernetes-Netzwerkrichtlinien für Amazon EKS

Dies ist der Leitfaden zur Fehlerbehebung für die Netzwerkrichtlinien-Funktion der Amazon VPC CNI.

Dieses Handbuch behandelt:

- Installationsinformationen, CRD- und RBAC-Berechtigungen [the section called “Neue policyendpoints CRD und Berechtigungen”](#)

- Protokolle, die bei der Diagnose von Netzwerkrichtlinienproblemen zu untersuchen sind [the section called “Netzwerkrichtlinien-Protokolle”](#)
- Ausführen der eBPF SDK-Toolsammlung zur Fehlerbehebung
- Bekannte Probleme und Lösungen [the section called “Bekannte Probleme und Lösungen”](#)

 Note

Beachten Sie, dass Netzwerkrichtlinien nur auf Pods angewendet werden, die von Kubernetes-Bereitstellungen erstellt wurden. Weitere Einschränkungen der Netzwerkrichtlinien in der VPC-CNI finden Sie unter [the section called “Überlegungen”](#)

Sie können Netzwerkverbindungen, die Netzwerkrichtlinien verwenden, beheben und untersuchen, indem Sie die [Netzwerkrichtlinien-Protokolle](#) lesen und Tools aus dem [eBPF-SDK](#) ausführen.

### Neue **policyendpoints** CRD und Berechtigungen

- CRD: `policyendpoints.networking.k8s.aws`
- Kubernetes-API: aufgerufen `apiservice v1.networking.k8s.io`
- Kubernetes-Ressource: Kind: `NetworkPolicy`
- RBAC: `ClusterRole` aufgerufen `aws-node (VPC CNI)`, `ClusterRole` aufgerufen `eks:network-policy-controller (Netzwerkrichtlinien-Controller in der EKS-Cluster-Steuerebene)`

Für die Netzwerkrichtlinie erstellt die VPC-CNI eine neue CustomResourceDefinition (CRD) namens `policyendpoints.networking.k8s.aws`. Das VPC-CNI muss über Berechtigungen zum Erstellen der CRD und zum Erstellen CustomResources (CR) dieser und der anderen von der VPC CNI () installierten CRD verfügen. `eniconfigs.crd.k8s.amazonaws.com` [Beide CRDs sind in der Datei unter verfügbar. `crds.yaml`](#) GitHub Insbesondere muss das VPC-CNI über die Verbberechtigungen „get“, „list“ und „watch“ für verfügen. `policyendpoints`

Die Kubernetes-Netzwerkrichtlinie ist Teil der `apiservice v1.networking.k8s.io` aufgerufenen und `apiversion: networking.k8s.io/v1` in Ihren Policy-YAML-Dateien. Das VPC-CNI DaemonSet muss über Berechtigungen verfügen, um diesen Teil der Kubernetes-API zu verwenden.

Die VPC-CNI-Berechtigungen befinden sich in einem ClusterRole Aufruf. aws-node Beachten Sie, dass ClusterRole Objekte nicht in Namespaces gruppiert sind. Das Folgende zeigt die aws-node eines Clusters:

```
kubectl get clusterrole aws-node -o yaml
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
 labels:
 app.kubernetes.io/instance: aws-vpc-cni
 app.kubernetes.io/managed-by: Helm
 app.kubernetes.io/name: aws-node
 app.kubernetes.io/version: v1.19.4
 helm.sh/chart: aws-vpc-cni-1.19.4
 k8s-app: aws-node
 name: aws-node
rules:
- apiGroups:
 - crd.k8s.amazonaws.com
 resources:
 - eniconfigs
 verbs:
 - list
 - watch
 - get
- apiGroups:
 - ""
 resources:
 - namespaces
 verbs:
 - list
 - watch
 - get
- apiGroups:
 - ""
 resources:
 - pods
 verbs:
 - list
 - watch
 - get
- apiGroups:
```



```

- ""
resources:
- nodes
verbs:
- list
- watch
- get
- apiGroups:
 - ""
 - events.k8s.io
resources:
- events
verbs:
- create
- patch
- list
- apiGroups:
 - networking.k8s.aws
resources:
- policyendpoints
verbs:
- get
- list
- watch
- apiGroups:
 - networking.k8s.aws
resources:
- policyendpoints/status
verbs:
- get
- apiGroups:
 - vpcresources.k8s.aws
resources:
- cninodes
verbs:
- get
- list
- watch
- patch

```

Außerdem wird in der Steuerungsebene jedes EKS-Clusters ein neuer Controller ausgeführt. Der Controller verwendet die Berechtigungen des ClusterRole `Aufgerufeneneks:network-policy-controller`. Das Folgende zeigt die `eks:network-policy-controller` eines Clusters:

```
kubectl get clusterrole eks:network-policy-controller -o yaml
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
 labels:
 app.kubernetes.io/name: amazon-network-policy-controller-k8s
 name: eks:network-policy-controller
rules:
- apiGroups:
 - ""
 resources:
 - namespaces
 verbs:
 - get
 - list
 - watch
- apiGroups:
 - ""
 resources:
 - pods
 verbs:
 - get
 - list
 - watch
- apiGroups:
 - ""
 resources:
 - services
 verbs:
 - get
 - list
 - watch
- apiGroups:
 - networking.k8s.aws
 resources:
 - policyendpoints
 verbs:
 - create
 - delete
 - get
 - list
 - patch
```

```

- update
- watch
- apiGroups:
 - networking.k8s.aws
 resources:
 - policyendpoints/finalizers
 verbs:
 - update
- apiGroups:
 - networking.k8s.aws
 resources:
 - policyendpoints/status
 verbs:
 - get
 - patch
 - update
- apiGroups:
 - networking.k8s.io
 resources:
 - networkpolicies
 verbs:
 - get
 - list
 - patch
 - update
 - watch

```

## Netzwerkrichtlinien-Protokolle

Jede Entscheidung der VPC-CNI, ob Verbindungen durch eine Netzwerkrichtlinie zugelassen oder verweigert werden, wird in Flow-Protokollen protokolliert. Die Netzwerkrichtlinien-Protokolle auf jedem Knoten enthalten die Flussprotokolle für jeden Pod, der über eine Netzwerkrichtlinie verfügt. Netzwerkrichtlinien-Protokolle werden unter `/var/log/aws-routed-eni/network-policy-agent.log` gespeichert. Das folgende Beispiel stammt aus einer `network-policy-agent.log`-Datei:

```

{"level":"info","timestamp":"2023-05-30T16:05:32.573Z","logger":"ebpf-
client","msg":"Flow Info: ","Src
IP":"192.168.87.155","Src Port":38971,"Dest IP":"64.6.160","Dest
Port":53,"Proto":"UDP","Verdict":"ACCEPT"}

```

Netzwerkrichtlinien-Protokolle sind standardmäßig deaktiviert. Gehen Sie wie folgt vor, um die Netzwerkrichtlinienprotokolle zu aktivieren:

 Note

Netzwerkrichtlinienprotokolle erfordern eine zusätzliche vCPU für den `aws-network-policy-agent` Container im `aws-node` DaemonSet VPC-CNI-Manifest.

## Amazon-EKS-Add-On

### AWS Management Console

- a. Öffnen Sie die [Amazon-EKS-Konsole](#).
- b. Wählen Sie im linken Navigationsbereich die Option Cluster aus. Wählen Sie dann den Namen des Clusters aus, für den Sie das Amazon-VPC-CNI-Add-on konfigurieren möchten.
- c. Wählen Sie die Registerkarte Add-ons.
- d. Wählen Sie das Kästchen oben rechts in der Add-On-Box aus und wählen Sie dann Edit (Bearbeiten).
- e. Auf der Seite „Konfigurieren“: **Amazon VPC CNI**
  - i. Wählen Sie `v1.14.0-eksbuild.3` oder eine neuere Version in der Dropdown-Liste aus.
  - ii. Erweitern Sie Optionale Konfigurationseinstellungen.
  - iii. Geben Sie den JSON-Schlüssel der obersten Ebene `"nodeAgent"`: ein, und der Wert ist ein Objekt mit dem Schlüssel `"enablePolicyEventLogs"`: und dem Wert `"true"` in Konfigurationswerte. Der resultierende Text muss ein gültiges JSON-Objekt sein. Das folgende Beispiel zeigt, dass Netzwerkrichtlinien und Netzwerkrichtlinien-Protokolle aktiviert sind und die Netzwerkrichtlinien-Protokolle an CloudWatch Logs gesendet werden:

```
{
 "enableNetworkPolicy": "true",
 "nodeAgent": {
 "enablePolicyEventLogs": "true"
 }
}
```

Der folgende Screenshot zeigt ein Beispiel für dieses Szenario.

## Amazon VPC CNI [Info](#)



networking

Active

v1.17.1-eksbuild.1

\_\_\_\_\_ ▼



```
{
 "$ref": "#/definitions/VpcCni",
 "$schema": "http://json-schema.org/draft-06/schema#",
 "definitions": {
 "Affinity": {
 "type": [
 "object",
 "null"
]
 },
 },
 "EniConfig": {
 "additionalProperties": false,
 }
}
```

```
1 {
2 "enableNetworkPolicy": "true",
3 "nodeAgent": {
4 "enablePolicyEventLogs": "true"
5 }
6 }
```

## AWS CLI

- a. Führen Sie den folgenden AWS CLI-Befehl aus. Ersetzen Sie `my-cluster` durch den Namen Ihres Clusters und den IAM-Rollen-ARN durch die Rolle, die Sie verwenden.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-
version v1.14.0-eksbuild.3 \
 --service-account-role-arn arn:aws:iam::123456789012:role/AmazonEKSVPCCNIRole
\
 --resolve-conflicts PRESERVE --configuration-values '{"nodeAgent":
{"enablePolicyEventLogs": "true"}}'
```

## Selbstverwaltetes Add-On

### Helm

Wenn Sie das Amazon VPC CNI-Plugin für Kubernetes über installiert haben, können Sie die Konfiguration aktualisieren `helm`, um die Netzwerkrichtlinien-Protokolle zu schreiben.

- a. Führen Sie den folgenden Befehl aus, um die Netzwerkrichtlinie zu aktivieren.

```
helm upgrade --set nodeAgent.enablePolicyEventLogs=true aws-vpc-cni --namespace
kube-system eks/aws-vpc-cni
```

### kubectl

Wenn Sie das Amazon VPC CNI-Plugin für Kubernetes über installiert haben, können Sie die Konfiguration aktualisieren `kubectl`, um die Netzwerkrichtlinien-Protokolle zu schreiben.

- a. Öffnen Sie das DaemonSet `aws-node` in Ihrem Editor.

```
kubectl edit daemonset -n kube-system aws-node
```

- b. Ersetzen Sie das `false` durch `true` im Befehlsargument `--enable-policy-event-logs=false` args: im `aws-network-policy-agent` Container im `aws-node` DaemonSet VPC-CNI-Manifest.

```
- args:
 - --enable-policy-event-logs=true
```

## Netzwerkrichtlinien-Protokolle an Amazon CloudWatch Logs senden

Sie können die Netzwerkrichtlinien-Protokolle mithilfe von Diensten wie Amazon CloudWatch Logs überwachen. Sie können die folgenden Methoden verwenden, um die Netzwerkrichtlinien-Protokolle an Logs zu CloudWatch senden.

Bei EKS-Clustern befinden sich die Richtlinienprotokolle unter `/aws/eks/cluster-name/cluster/` und bei selbstverwalteten K8S-Clustern werden die Protokolle unter `/aws/k8s-cluster/cluster/` gespeichert.

### Netzwerkrichtlinienprotokolle mit dem Amazon VPC CNI-Plugin für Kubernetes senden

Wenn Sie die Netzwerkrichtlinie aktivieren, wird den `aws-node`-Pods ein zweiter Container für einen Konten-Agent hinzugefügt. Dieser Node-Agent kann die Netzwerkrichtlinien-Protokolle an Logs senden. CloudWatch

#### Note

Nur die Netzwerkrichtlinien-Protokolle werden vom Knoten-Agent gesendet. Andere vom VPC CNI erstellte Protokolle sind nicht enthalten.

### Voraussetzungen

- Fügen Sie der IAM-Rolle, die Sie für VPC CNI verwenden, die folgenden Berechtigungen als Abschnitt oder separate Richtlinie hinzu.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": [
 "logs:DescribeLogGroups",
 "logs:CreateLogGroup",
 "logs:CreateLogStream",
 "logs:PutLogEvents"
],
 "Resource": "*"
 }
]
}
```

```
]
}
```

## Amazon-EKS-Add-On

### AWS Management Console

- a. Öffnen Sie die [Amazon-EKS-Konsole](#).
- b. Wählen Sie im linken Navigationsbereich die Option Cluster aus. Wählen Sie dann den Namen des Clusters aus, für den Sie das Amazon-VPC-CNI-Add-on konfigurieren möchten.
- c. Wählen Sie die Registerkarte Add-ons.
- d. Wählen Sie das Kästchen oben rechts in der Add-On-Box aus und wählen Sie dann Edit (Bearbeiten).
- e. Auf der Seite „Konfigurieren **Amazon VPC CNI**“:
  - i. Wählen Sie v1.14.0-eksbuild.3 oder eine neuere Version in der Dropdown-Liste aus.
  - ii. Erweitern Sie Optionale Konfigurationseinstellungen.
  - iii. Geben Sie den JSON-Schlüssel der obersten Ebene "nodeAgent": ein, und der Wert ist ein Objekt mit dem Schlüssel "enableCloudWatchLogs": und dem Wert "true" in Konfigurationen. Der resultierende Text muss ein gültiges JSON-Objekt sein. Das folgende Beispiel zeigt, dass Netzwerkrichtlinien und Netzwerkrichtlinien-Protokolle aktiviert sind und die Protokolle an CloudWatch Logs gesendet werden:

```
{
 "enableNetworkPolicy": "true",
 "nodeAgent": {
 "enablePolicyEventLogs": "true",
 "enableCloudWatchLogs": "true",
 }
}
```

Der folgende Screenshot zeigt ein Beispiel für dieses Szenario.



EKS > Clusters > > Add-on > vpc-cni > Edit add-on

Configure Amazon VPC CNI

Amazon VPC CNI [Info](#)

Listed by



Category

networking

Status

 Active

Version

Select the version for this add-on.

v1.17.1-eksbuild.1

Select IAM role

Select an IAM role to use with this add-on. To create a new role, follow the instructions in the [Amazon EKS User Guide](#).

Optional configuration settings

Add-on configuration schema

Refer to the JSON schema below. The configuration values entered in the code editor will be validated against this schema.

```
{
 "$ref": "#/definitions/VpcCni",
 "$schema": "http://json-schema.org/draft-06/schema#",
 "definitions": {
 "Affinity": {
 "type": [
 "object",
 "null"
]
 },
 "EniConfig": {
 "additionalProperties": false,

```

Configuration values [Info](#)

Specify any additional JSON or YAML configurations that should be applied to the add-on.

1 {

2 "enableNetworkPolicy": "true",

3 "nodeAgent": {

4 "enablePolicyEventLogs": "true",

5 "enableCloudWatchLogs": "true"

6 }

7 }

kubectl

1182

## AWS CLI

- a. Führen Sie den folgenden AWS CLI-Befehl aus. Ersetzen Sie `my-cluster` durch den Namen Ihres Clusters und den IAM-Rollen-ARN durch die Rolle, die Sie verwenden.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version v1.14.0-eksbuild.3 \
 --service-account-role-arn arn:aws:iam::123456789012:role/AmazonEKSVPCCNIRole \
 --resolve-conflicts PRESERVE --configuration-values '{"nodeAgent": {"enablePolicyEventLogs": "true", "enableCloudWatchLogs": "true"}}'
```

## Selbstverwaltetes Add-On

### Helm

Wenn Sie das Amazon VPC CNI-Plugin für Kubernetes über installiert haben, können Sie die Konfiguration aktualisieren `helm`, um Netzwerkrichtlinienprotokolle an Logs zu senden. CloudWatch

- a. Führen Sie den folgenden Befehl aus, um Netzwerkrichtlinien-Protokolle zu aktivieren und sie an Logs zu senden. CloudWatch

```
helm upgrade --set nodeAgent.enablePolicyEventLogs=true --set nodeAgent.enableCloudWatchLogs=true aws-vpc-cni --namespace kube-system eks/aws-vpc-cni
```

### kubectl

- a. Öffnen Sie das DaemonSet `aws-node` in Ihrem Editor.

```
kubectl edit daemonset -n kube-system aws-node
```

- b. Ersetzen Sie das `false` durch `true` in zwei Befehlsargumenten `--enable-policy-event-logs=false` und `--enable-cloudwatch-logs=false` `args:` im `aws-network-policy-agent` Container im `aws-node` DaemonSet VPC-CNI-Manifest.

```
- args:
 - --enable-policy-event-logs=true
 - --enable-cloudwatch-logs=true
```

## Netzwerkrichtlinien-Protokolle mit einem Fluent Bit senden **DaemonSet**

Wenn Sie Fluent Bit in a verwenden, um Protokolle von Ihren Knoten DaemonSet zu senden, können Sie eine Konfiguration hinzufügen, um die Netzwerkrichtlinien-Protokolle aus Netzwerkrichtlinien einzubeziehen. Sie können die folgende Beispielkonfiguration verwenden:

```
[INPUT]
 Name tail
 Tag eksnp.*
 Path /var/log/aws-routed-eni/network-policy-agent*.log
 Parser json
 DB /var/log/aws-routed-eni/flb_npagent.db
 Mem_Buf_Limit 5MB
 Skip_Long_Lines On
 Refresh_Interval 10
```

### Enthaltenes eBPF-SDK

Das Amazon VPC CNI-Plugin für Kubernetes installiert eine eBPF-SDK-Sammlung von Tools auf den Knoten. Sie können die eBPF-SDK-Tools verwenden, um Probleme mit Netzwerkrichtlinien zu identifizieren. Der folgende Befehl listet zum Beispiel die Programme auf, die auf dem Knoten ausgeführt werden.

```
sudo /opt/cni/bin/aws-eks-na-cli ebpf progs
```

Zum Ausführen dieses Befehls können Sie eine beliebige Methode verwenden, um eine Verbindung mit dem Knoten herzustellen.

### Bekannte Probleme und Lösungen

In den folgenden Abschnitten werden bekannte Probleme mit der Amazon VPC CNI-Netzwerkrichtlinien-Funktion und deren Lösungen beschrieben.

Netzwerkrichtlinien-Protokolle wurden generiert, obwohl sie auf `enable-policy-event-logs „false“` gesetzt sind

Problem: EKS VPC CNI generiert Netzwerkrichtlinienprotokolle, auch wenn die `enable-policy-event-logs` Einstellung auf `gesetzt ist. false`

Lösung: `enable-policy-event-logs` Mit dieser Einstellung werden nur die „Entscheidungs“-Protokolle der Richtlinien deaktiviert, nicht jedoch die gesamte Protokollierung des Netzwerkrichtlinien-Agents. Dieses Verhalten ist in der [aws-network-policy-agent README-](#)

[Datei unter](#) dokumentiert. GitHub Um die Protokollierung vollständig zu deaktivieren, müssen Sie möglicherweise andere Protokollierungskonfigurationen anpassen.

### Probleme bei der Bereinigung der Netzwerkrichtlinienübersicht

Problem: Probleme mit dem Netzwerk, das nach dem Löschen von Pods `policyendpoint` immer noch vorhanden ist und nicht bereinigt wird.

Lösung: Dieses Problem wurde durch ein Problem mit der VPC CNI-Add-On-Version 1.19.3-eksbuild.1 verursacht. Aktualisieren Sie auf eine neuere Version des VPC CNI-Add-ons, um dieses Problem zu beheben.

### Netzwerkrichtlinien werden nicht angewendet

Problem: Die Netzwerkrichtlinien-Funktion ist im Amazon VPC CNI-Plugin aktiviert, aber die Netzwerkrichtlinien werden nicht korrekt angewendet.

Wenn Sie eine Netzwerkrichtlinie erstellen `kind: NetworkPolicy` und diese sich nicht auf den Pod auswirkt, überprüfen Sie, ob das `Policyendpoint`-Objekt im selben Namespace wie der Pod erstellt wurde. Wenn die Namespaces keine `policyendpoint` Objekte enthalten, konnte der Netzwerkrichtlinien-Controller (Teil des EKS-Clusters) keine Netzwerkrichtlinienregeln erstellen, die der Netzwerkrichtlinien-Agent (Teil des VPC-CNI) anwenden sollte.

Lösung: Die Lösung besteht darin, die Berechtigungen des VPC-CNI (`ClusterRole:aws-node`) und des Netzwerkrichtlinien-Controllers (`ClusterRole:eks:network-policy-controller`) zu korrigieren und diese Aktionen in jedem Tool zur Durchsetzung von Richtlinien wie Kyverno zuzulassen. Stellen Sie sicher, dass die Kyverno-Richtlinien die Erstellung von Objekten nicht blockieren. `policyendpoint` Informationen zu den erforderlichen Berechtigungen finden Sie im vorherigen Abschnitt unter [the section called "Neue policyendpoints CRD und Berechtigungen"](#)

Pods kehren nach dem Löschen der Richtlinie im strikten Modus nicht zum Standardstatus „Ablehnen“ zurück

Problem: Wenn Netzwerkrichtlinien im strikten Modus aktiviert sind, beginnen Pods mit einer standardmäßigen Ablehnungsrichtlinie. Nachdem die Richtlinien angewendet wurden, ist Datenverkehr zu den angegebenen Endpunkten zulässig. Wenn Richtlinien gelöscht werden, kehrt der Pod jedoch nicht in den Standardstatus „Ablehnen“ zurück, sondern in den Standardstatus „Zulassen“.

Lösung: Dieses Problem wurde in der Version 1.19.3 von VPC CNI behoben, zu der auch die Version 1.2.0 des Network Policy Agent gehörte. Nach dem Fix, bei aktiviertem strikten Modus, kehrt der Pod

nach dem Entfernen der Richtlinien erwartungsgemäß in den standardmäßigen Ablehnungsstatus zurück.

### Sicherheitsgruppen für die Startlatenz von Pods

Problem: Bei Verwendung der Funktion „Sicherheitsgruppen für Pods“ in EKS kommt es zu einer erhöhten Latenz beim Pod-Start.

Lösung: Die Latenz ist auf die Ratenbegrenzung im Resource Controller durch die API-Drosselung auf der `CreateNetworkInterface` API zurückzuführen, die der VPC-Ressourcencontroller verwendet, um Verzweigungen ENIs für die Pods zu erstellen. Prüfen Sie die API-Grenzwerte Ihres Kontos für diesen Vorgang und erwägen Sie, falls erforderlich, eine Erhöhung des Limits zu beantragen.

FailedScheduling aufgrund unzureichender `vpc.amazonaws.com/pod-eni`

Problem: Pods können nicht geplant werden und es wird folgender Fehler angezeigt:

```
FailedScheduling 2m53s (x28 over 137m) default-scheduler 0/5 nodes are available: 5 Insufficient vpc.amazonaws.com/pod-eni. preemption: 0/5 nodes are available: 5 No preemption victims found for incoming pod.
```

Lösung: Wie beim vorherigen Problem erhöht die Zuweisung von Sicherheitsgruppen zu Pods die Latenz bei der Pod-Planung und kann den CNI-Schwellenwert für das Hinzufügen der einzelnen ENI überschreiten, was zu Fehlern beim Starten von Pods führen kann. Dieses Verhalten ist bei der Verwendung von Sicherheitsgruppen für Pods zu erwarten. Berücksichtigen Sie beim Entwerfen Ihrer Workload-Architektur die Auswirkungen auf die Planung.

### IPAM-Konnektivitätsprobleme und Segmentierungsfehler

Problem: Es treten mehrere Fehler auf, darunter IPAM-Konnektivitätsprobleme, Drosselungsanforderungen und Segmentierungsfehler:

- `Checking for IPAM connectivity ...`
- `Throttling request took 1.047064274s`
- `Retrying waiting for IPAM-D`
- `panic: runtime error: invalid memory address or nil pointer dereference`

Lösung: Dieses Problem tritt auf, wenn Sie `systemd-udev` auf AL2 023 installieren, da die Datei neu geschrieben wird, wobei die Richtlinie nicht eingehalten wird. Dies kann passieren, wenn Sie auf ein

anderes Paket aktualisieren `releasever`, das über ein aktualisiertes Paket verfügt, oder wenn Sie das Paket selbst manuell aktualisieren. Vermeiden Sie die Installation oder Aktualisierung `systemd-udev` auf AL2 023-Knoten.

### Fehler beim Finden des Geräts anhand des Namens

Problem: Fehlermeldung:

```
{"level":"error","ts":"2025-02-05T20:27:18.669Z","caller":"ebpf/bpf_client.go:578","msg":"failed to find device by name eni9ea69618bf0: %!w(netlink.LinkNotFoundError={0xc000115310})"}
```

Lösung: Dieses Problem wurde in den neuesten Versionen des Amazon VPC CNI Network Policy Agent (v1.2.0) identifiziert und behoben. Aktualisieren Sie auf die neueste Version von VPC CNI, um dieses Problem zu beheben.

### CVE-Schwachstellen im Multus CNI-Image

Problem: Der erweiterte EKS ImageScan CVE-Bericht identifiziert Sicherheitslücken in der Multus CNI-Image-Version v4.1.4-eksbuild.2\_thick.

Lösung: Aktualisieren Sie auf die neue Version des Multus CNI-Images und des neuen Network Policy Controller-Images, die keine Sicherheitslücken aufweisen. Der Scanner kann aktualisiert werden, um die in der vorherigen Version gefundenen Sicherheitslücken zu beheben.

### Flow Info DENY urteilt in Protokollen

Problem: In den Protokollen der Netzwerkrichtlinien werden DENY-Urteile angezeigt:

```
{"level":"info","ts":"2024-11-25T13:34:24.808Z","logger":"ebpf-client","caller":"events/events.go:193","msg":"Flow Info: ","Src IP":"","Src Port":9096,"Dest IP":"","Dest Port":56830,"Proto":"TCP","Verdict":"DENY"}
```

Lösung: Dieses Problem wurde in der neuen Version des Network Policy Controllers behoben. Aktualisieren Sie auf die neueste Version der EKS-Plattform, um Probleme mit der Protokollierung zu beheben.

### Pod-to-pod Kommunikationsprobleme nach der Migration von Calico

Problem: Nach dem Upgrade eines EKS-Clusters auf Version 1.30 und dem Wechsel von Calico zu Amazon VPC CNI für Netzwerkrichtlinien schlägt die pod-to-pod Kommunikation fehl, wenn

Netzwerkrichtlinien angewendet werden. Die Kommunikation wird wiederhergestellt, wenn Netzwerkrichtlinien gelöscht werden.

Lösung: Für den Netzwerkrichtlinien-Agenten in der VPC-CNI können nicht so viele Ports angegeben werden wie bei Calico. Verwenden Sie stattdessen Portbereiche in den Netzwerkrichtlinien. Die maximale Anzahl eindeutiger Kombinationen von Ports für jedes Protokoll in jedem Protokoll `ingress`: oder für jeden `egress`: Selektor in einer Netzwerkrichtlinie beträgt 24. Verwenden Sie Portbereiche, um die Anzahl der eindeutigen Ports zu reduzieren und diese Einschränkung zu umgehen.

Der Netzwerkrichtlinien-Agent unterstützt keine eigenständigen Pods

Problem: Netzwerkrichtlinien, die auf eigenständige Pods angewendet werden, verhalten sich möglicherweise inkonsistent.

Lösung: Der Network Policy Agent unterstützt derzeit nur Pods, die als Teil einer Bereitstellung/ eines Replikats bereitgestellt werden. Wenn Netzwerkrichtlinien auf eigenständige Pods angewendet werden, kann es zu Inkonsistenzen im Verhalten kommen. Dies ist oben auf dieser Seite, in und in der [the section called “Überlegungen” aws-network-policy-agent GitHub Ausgabe #327](#) am dokumentiert. GitHub Stellen Sie Pods als Teil einer Bereitstellung oder eines Replikats bereit, um ein einheitliches Verhalten der Netzwerkrichtlinien zu gewährleisten.

Stars-Demo der Netzwerkrichtlinien für Amazon EKS

Diese Demo erstellt einen Front-End-, Back-End- und Client-Service in Ihrem Amazon-EKS-Cluster. Außerdem wird in der Demo eine grafische Benutzeroberfläche für die Verwaltung erstellt, in der die verfügbaren Wege für ein- und ausgehenden Datenverkehr zwischen den einzelnen Services dargestellt werden. Wir empfehlen, dass Sie die Demo auf einem Cluster abschließen, auf dem Sie keine Produktionsworkloads ausführen.

Bevor Sie Netzwerkrichtlinien erstellen, können alle Services bidirektional kommunizieren. Nachdem Sie die Netzwerkrichtlinien angewendet haben, können Sie feststellen, dass der Client nur mit dem Front-End-Service kommuniziert und das Back-End nur Datenverkehr vom Front-End akzeptiert.

1. Wenden Sie die Services für Front-End, Back-End, Client und Verwaltungs-Benutzeroberfläche an:

```
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/namespace.yaml
```

```
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/management-ui.yaml
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/backend.yaml
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/frontend.yaml
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/client.yaml
```

## 2. Alle Pods im Cluster anzeigen.

```
kubectl get pods -A
```

Eine Beispielausgabe sieht wie folgt aus.

In Ihrer Ausgabe sollten Pods in den Namespaces aufgeführt sein, die in der folgenden Ausgabe angezeigt werden. Die **NAMES** Anzahl Ihrer Pods und die Anzahl der Pods in der READY Spalte unterscheiden sich von denen in der folgenden Ausgabe. Fahren Sie erst fort, wenn Sie Pods mit ähnlichen Namen sehen, die alle Running in der STATUS Spalte vorkommen.

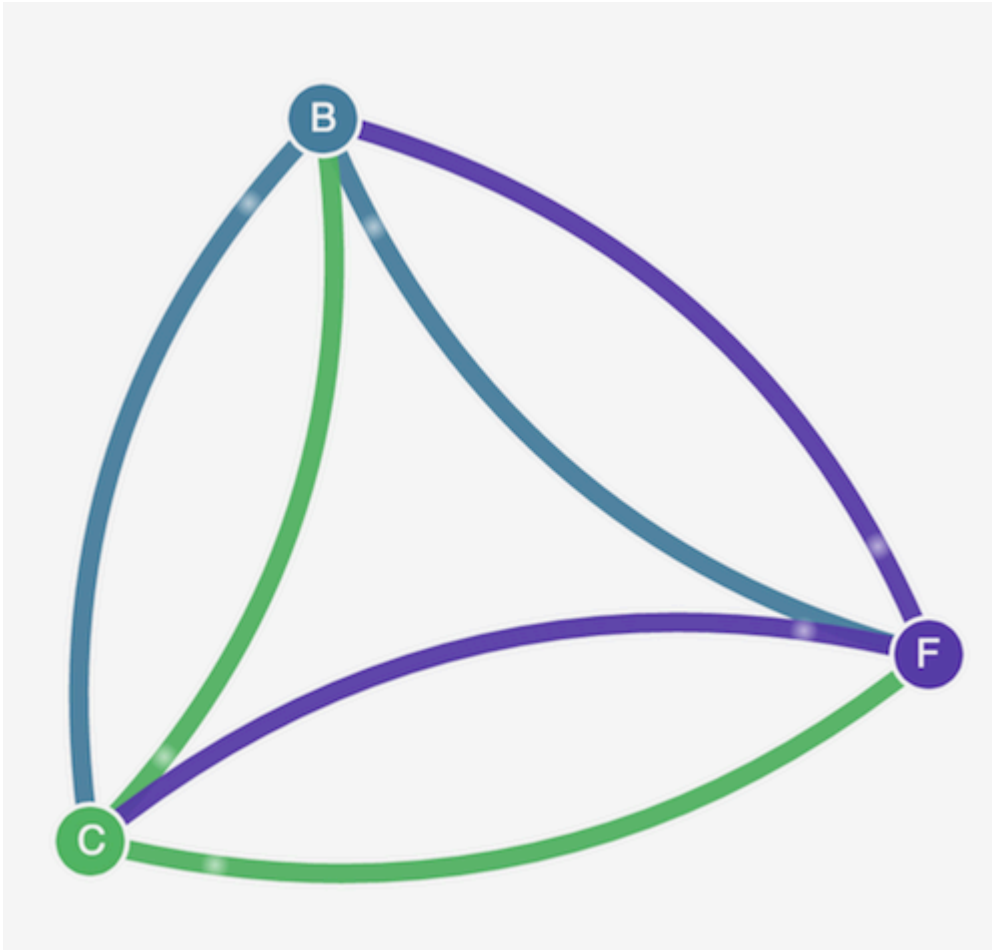
| NAMESPACE     | NAME                | READY | STATUS    |
|---------------|---------------------|-------|-----------|
| RESTARTS      | AGE                 |       |           |
| [...]         |                     |       |           |
| client        | client-xfffc        | 1/1   | Running 0 |
| 5m19s         |                     |       |           |
| [...]         |                     |       |           |
| management-ui | management-ui-qrb2g | 1/1   | Running 0 |
| 5m24s         |                     |       |           |
| stars         | backend-sz87q       | 1/1   | Running 0 |
| 5m23s         |                     |       |           |
| stars         | frontend-cscnf      | 1/1   | Running 0 |
| 5m21s         |                     |       |           |
| [...]         |                     |       |           |

## 3. Zum Herstellen einer Verbindung mit der Verwaltungsbenutzeroberfläche stellen Sie eine Verbindung mit der EXTERNAL-IP des Services her, der auf Ihrem Cluster ausgeführt wird.



```
kubectl get service/management-ui -n management-ui
```

4. Öffnen Sie den Pfad aus dem vorherigen Schritt in einem Browser. Die Verwaltungsb Benutzeroberfläche sollte angezeigt werden. Der C-Knoten ist der Client-Service, der F-Knoten ist der Front-End-Service und der B-Knoten ist der Back-End-Service. Jeder Knoten verfügt über vollständigen Kommunikationszugriff auf alle anderen Knoten, wie durch die fett markierten, farbigen Zeilen angegeben.



5. Wenden Sie die folgende Netzwerkrichtlinie sowohl in den `stars`- als auch in den `client`-Namespaces an, um die Services voneinander zu isolieren:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
 name: default-deny
spec:
 podSelector:
```

```
matchLabels: {}
```

Sie können die folgenden Befehle verwenden, um die Richtlinie auf beide Namespaces anzuwenden:

```
kubectl apply -n stars -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/default-deny.yaml
kubectl apply -n client -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/default-deny.yaml
```

6. Aktualisieren Sie Ihren Browser. Sie sehen, dass die Verwaltungsbenzutzeroberfläche keinen der Knoten mehr erreichen kann, sodass sie nicht in der Benutzeroberfläche angezeigt werden.
7. Wenden Sie die folgenden verschiedenen Netzwerkrichtlinien an, um der Verwaltungsbenzutzeroberfläche den Zugriff auf die Services zu erlauben: Wenden Sie diese Richtlinie an, um die Benutzeroberfläche zuzulassen:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
 namespace: stars
 name: allow-ui
spec:
 podSelector:
 matchLabels: {}
 ingress:
 - from:
 - namespaceSelector:
 matchLabels:
 role: management-ui
```

Wenden Sie diese Richtlinie an, um den Client zuzulassen:

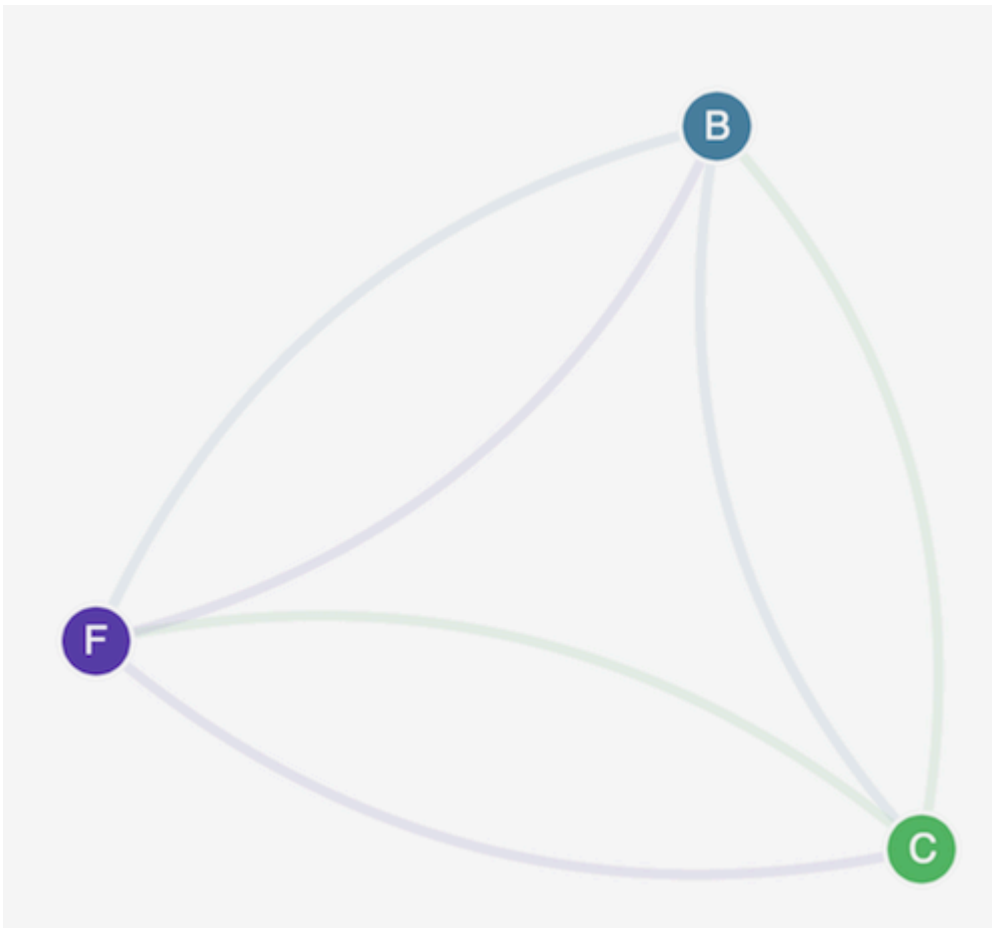
```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
 namespace: client
 name: allow-ui
spec:
 podSelector:
```

```
matchLabels: {}
ingress:
 - from:
 - namespaceSelector:
 matchLabels:
 role: management-ui
```

Sie können die folgenden Befehle verwenden, um beide Richtlinien anzuwenden:

```
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/allow-ui.yaml
kubectl apply -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/allow-ui-client.yaml
```

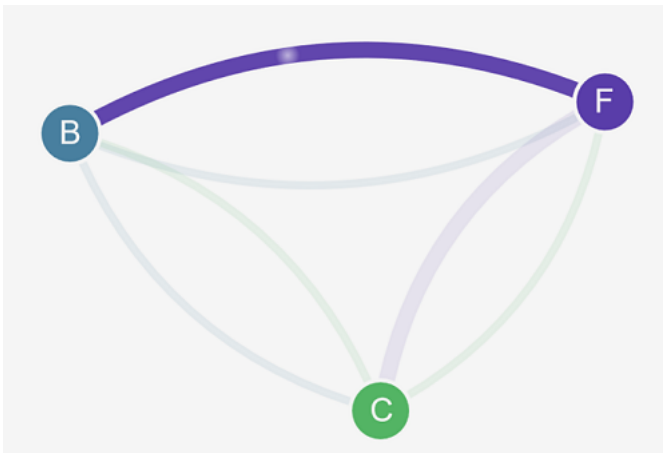
8. Aktualisieren Sie Ihren Browser. Wie Sie feststellen, können die Knoten nun wieder über die Verwaltungs-Benutzeroberfläche erreicht werden, sie können jedoch nicht miteinander kommunizieren.



9. Wenden Sie die folgende Netzwerkrichtlinie an, um Verkehr vom Front-End-Service zum Back-End-Service zuzulassen:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
 namespace: stars
 name: backend-policy
spec:
 podSelector:
 matchLabels:
 role: backend
 ingress:
 - from:
 - podSelector:
 matchLabels:
 role: frontend
 ports:
 - protocol: TCP
 port: 6379
```

10. Aktualisieren Sie Ihren Browser. Wie Sie feststellen, kann das Front-End mit dem Back-End kommunizieren.

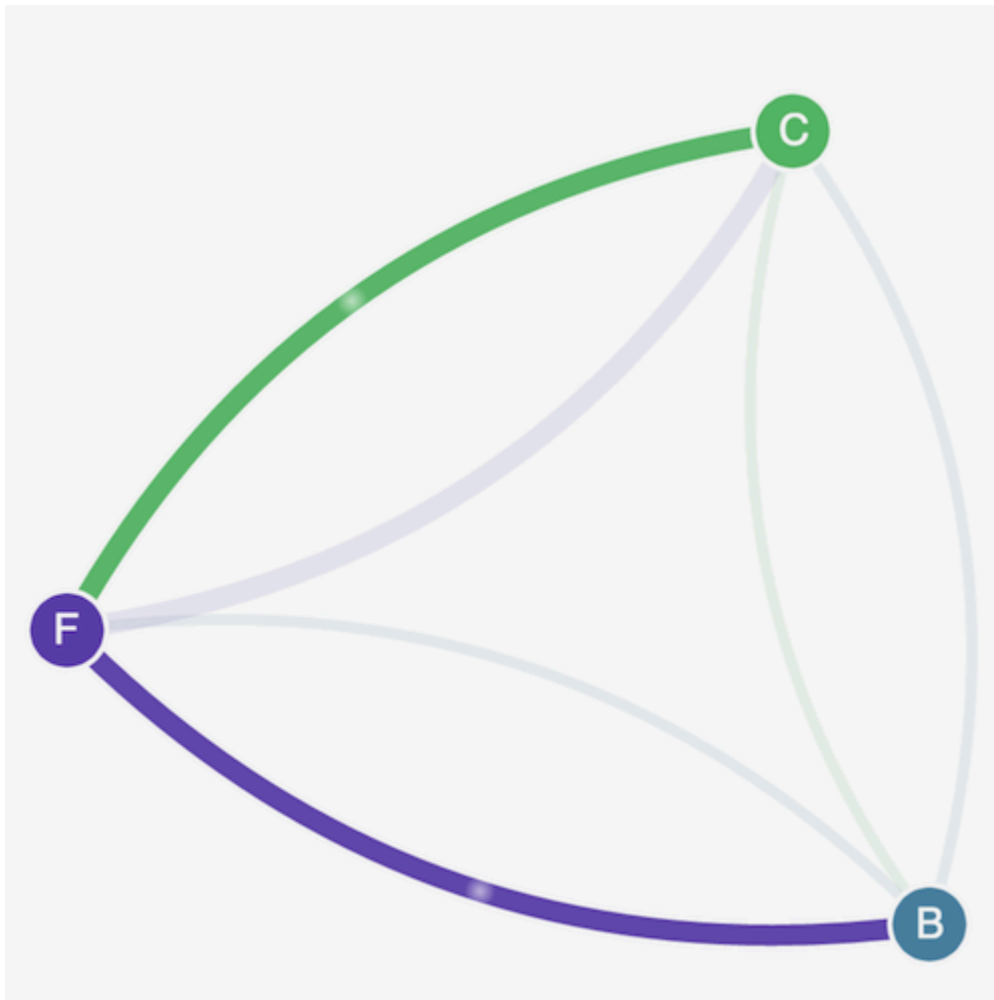


11. Wenden Sie die folgende Netzwerkrichtlinie an, um Datenverkehr vom Client zum Front-End-Service zuzulassen:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
 namespace: stars
```

```
name: frontend-policy
spec:
 podSelector:
 matchLabels:
 role: frontend
 ingress:
 - from:
 - namespaceSelector:
 matchLabels:
 role: client
 ports:
 - protocol: TCP
 port: 80
```

12 Aktualisieren Sie Ihren Browser. Wie Sie feststellen, kann der Client mit dem Front-End-Service kommunizieren. Der Front-End-Service kann nach wie vor mit dem Back-End-Service kommunizieren.



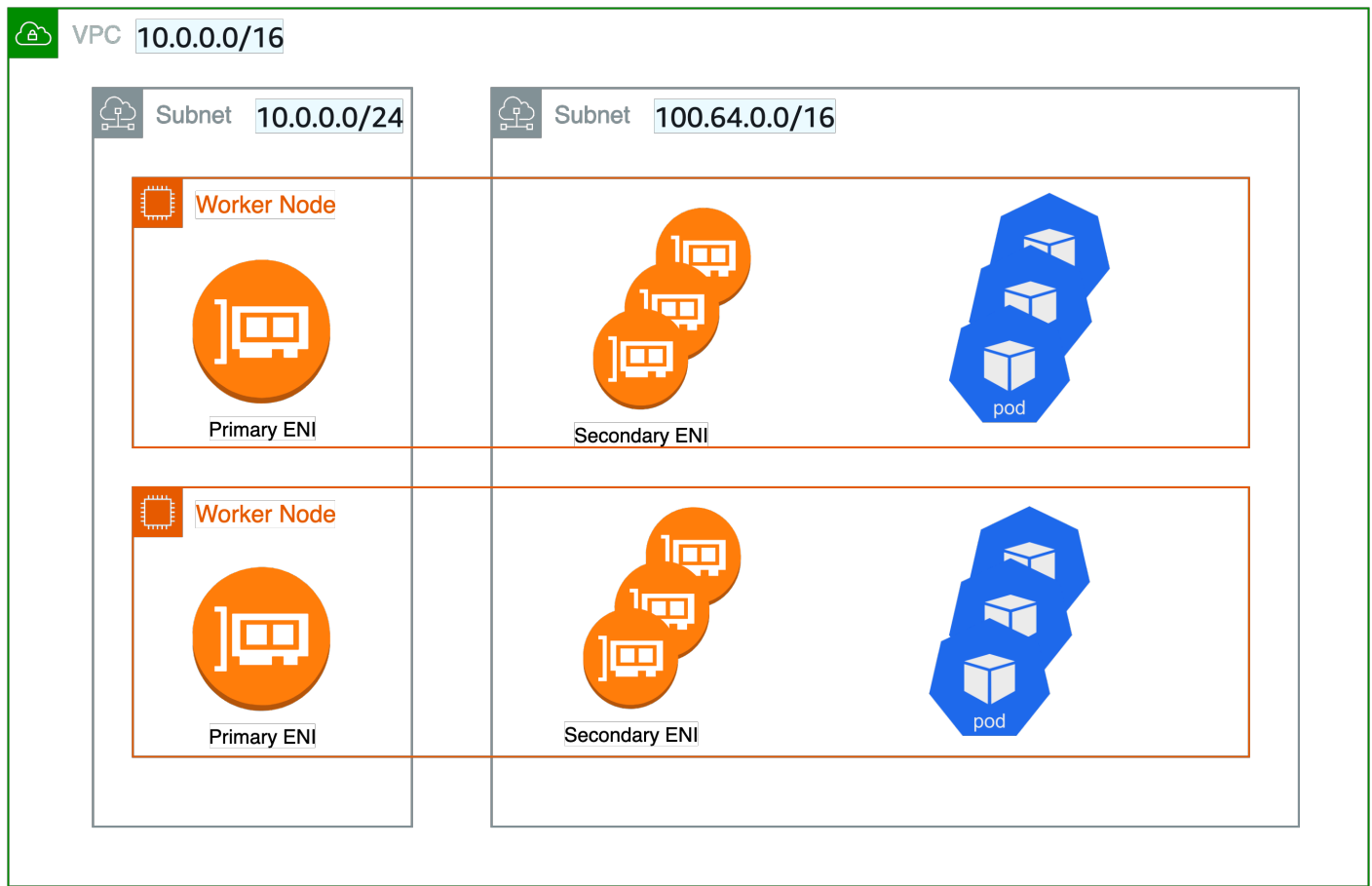
13(Optional) Wenn Sie die Demo abgeschlossen haben, können Sie die zugehörigen Ressourcen löschen.

```
kubectl delete -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/client.yaml
kubectl delete -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/frontend.yaml
kubectl delete -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/backend.yaml
kubectl delete -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/management-ui.yaml
kubectl delete -f https://raw.githubusercontent.com/aws-samples/eks-workshop/2f9d29ed3f82ed6b083649e975a0e574fb8a4058/content/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/namespace.yaml
```

Auch nach dem Löschen der Ressourcen können noch Netzwerkrichtlinien-Endpunkte auf den Knoten vorhanden sein, die die Vernetzung in Ihrem Cluster auf unerwartete Weise stören können. Die einzige sichere Möglichkeit, diese Regeln zu entfernen, besteht darin, die Knoten neu zu starten oder alle Knoten zu beenden und sie zu recyceln. Um alle Knoten zu beenden, legen Sie entweder die Anzahl der gewünschten Auto Scaling-Gruppen auf 0 und anschließend wieder auf die gewünschte Zahl fest oder beenden einfach die Knoten.

Stellen Sie Pods in alternativen Subnetzen mit benutzerdefiniertem Netzwerk bereit

Gilt für: Linux IPv4 Fargate-Knoten, Linux-Knoten mit Amazon-Instances EC2



Wenn das Amazon VPC CNI-Plugin für Kubernetes sekundäre [elastische Netzwerkschnittstellen \(Netzwerkschnittstellen\)](#) für Ihren EC2 Amazon-Knoten erstellt, erstellt es diese standardmäßig im selben Subnetz wie die primäre Netzwerkschnittstelle des Knotens. Es verknüpft auch dieselben Sicherheitsgruppen mit der sekundären Netzwerkschnittstelle, die mit der primären Netzwerkschnittstelle verknüpft sind. Aus einem oder mehreren der folgenden Gründe möchten Sie möglicherweise, dass das Plugin sekundäre Netzwerkschnittstellen in einem anderen Subnetz erstellt oder Sie möchten den sekundären Netzwerkschnittstellen oder beiden verschiedene Sicherheitsgruppen zuordnen:

- In dem Subnetz, in dem IPv4 sich die primäre Netzwerkschnittstelle befindet, ist eine begrenzte Anzahl von Adressen verfügbar. Dies kann die Anzahl der Pods einschränken, die Sie im Subnetz erstellen können. Durch die Verwendung eines anderen Subnetzes für sekundäre Netzwerkschnittstellen können Sie die Anzahl der verfügbaren IPv4 Adressen für Pods erhöhen.
- Aus Sicherheitsgründen müssen Ihre Pods möglicherweise ein anderes Subnetz oder andere Sicherheitsgruppen als die primäre Netzwerkschnittstelle des Knotens verwenden.

- Die Knoten sind in öffentlichen Subnetzen konfiguriert, und Sie möchten die Pods in privaten Subnetzen platzieren. Die einem öffentlichen Subnetz zugeordnete Routing-Tabelle enthält eine Route zu einem Internet-Gateway. Die einem privaten Subnetz zugeordnete Routentabelle enthält keine Route zu einem Internet-Gateway.

 Tip

Sie können Ihrem Amazon EKS-Cluster auch direkt ein neues oder vorhandenes Subnetz hinzufügen, ohne ein benutzerdefiniertes Netzwerk zu verwenden. Weitere Informationen finden Sie unter [the section called “Fügen Sie über die Managementkonsole ein vorhandenes VPC-Subnetz zu einem Amazon EKS-Cluster hinzu”](#).

## Überlegungen

Im Folgenden finden Sie Überlegungen zur Verwendung der Funktion.

- Wenn das benutzerdefinierte Netzwerk aktiviert ist, werden Pods keine IP-Adressen zugewiesen, die der primären Netzwerkschnittstelle zugewiesen sind. Pods werden nur IP-Adressen von sekundären Netzwerkschnittstellen zugewiesen.
- Wenn Ihr Cluster die IPv6 Familie verwendet, können Sie kein benutzerdefiniertes Netzwerk verwenden.
- Wenn Sie vorhaben, benutzerdefinierte Netzwerke zu verwenden, um die IPv4-Adresserschöpfung zu verhindern, können Sie stattdessen einen Cluster über die IPv6-Familie erstellen. Weitere Informationen finden Sie unter [the section called “IPv6”](#).
- Obwohl Pods, die in Subnetzen bereitgestellt werden, die für sekundäre Netzwerkschnittstellen spezifiziert sind, andere Subnetze und Sicherheitsgruppen verwenden können als die primäre Netzwerkschnittstelle des Knotens, müssen sich die Subnetze und Sicherheitsgruppen in derselben VPC wie der Knoten befinden.
- Bei Fargate werden Subnetze über das Fargate-Profil gesteuert. Weitere Informationen finden Sie unter [the section called “Definieren Sie Profile”](#).

Passen Sie die sekundäre Netzwerkschnittstelle in Amazon EKS-Knoten an

Gehen Sie wie folgt vor, bevor Sie mit dem Tutorial beginnen:

- Lesen Sie sich die Überlegungen durch



- Vertrautheit damit, wie das Amazon VPC CNI-Plugin für Kubernetes sekundäre Netzwerkschnittstellen erstellt und Pods IP-Adressen zuweist. Weitere Informationen finden Sie unter [ENI-Zuweisung](#) auf GitHub.
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yumapt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Wir empfehlen, dass Sie die Schritte in diesem Thema in einer Bash-Shell ausführen. Wenn Sie keine Bash-Shell verwenden, müssen einige Skriptbefehle wie Zeilenfortsetzungszeichen und die Art und Weise, wie Variablen gesetzt und verwendet werden, an Ihrer Shell angepasst werden. Darüber hinaus können die Zitier- und Escape-Regeln für Ihre Shell unterschiedlich sein. Weitere Informationen finden Sie unter [Verwenden von Anführungszeichen mit Zeichenfolgen in der AWS CLI](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

Für dieses Tutorial empfehlen wir, die Beispielwerte zu verwenden, es sei denn, es wird darauf hingewiesen, dass sie ersetzt werden sollen. Sie können alle Beispielwert ersetzen, wenn Sie die Schritte für einen Produktions-Cluster ausführen. Wir empfehlen, alle Schritte auf demselben Terminal auszuführen. Dies liegt daran, dass Variablen während der gesamten Schritte festgelegt und verwendet werden und nicht in verschiedenen Terminals existieren.

Die Befehle in diesem Thema werden anhand der Konventionen formatiert, die unter [Verwenden der AWS CLI-Beispiele](#) aufgeführt sind. Wenn Sie Befehle über die Befehlszeile für Ressourcen ausführen, die sich in einer anderen AWS Region als der AWS Standardregion befinden, die in dem von Ihnen verwendeten AWS [CLI-Profil](#) definiert ist, müssen Sie die Befehle ergänzen `--region us-west-2` und durch Ihre AWS Region `us-west-2` ersetzen.

Wenn Sie benutzerdefinierte Netzwerke in Ihrem Produktions-Cluster bereitstellen möchten, fahren Sie mit [the section called “Schritt 2: Konfigurieren Ihrer VPC”](#) fort.

## Schritt 1: Erstellen einer Test-VPC und eines Clusters

Mit den folgenden Verfahren können Sie eine Test-VPC und einen Cluster erstellen und benutzerdefinierte Netzwerke für diesen Cluster konfigurieren. Es wird nicht empfohlen, den Testcluster für Produktionsworkloads zu verwenden, da mehrere Funktionen, die nichts miteinander zu tun haben, die Sie möglicherweise in Ihrem Produktionscluster verwenden, in diesem Thema nicht behandelt werden. Weitere Informationen finden Sie unter [the section called “Erstellen eines - Clusters”](#).

1. Führen Sie den folgenden Befehl aus, um die Variable zu definieren. `account_id`

```
account_id=$(aws sts get-caller-identity --query Account --output text)
```

2. Erstellen Sie eine VPC.

- a. Wenn Sie die Bereitstellung auf einem Testsystem durchführen, erstellen Sie eine VPC mithilfe einer Amazon AWS CloudFormation EKS-Vorlage.

```
aws cloudformation create-stack --stack-name my-eks-custom-networking-vpc \
 --template-url https://s3.us-west-2.amazonaws.com/amazon-eks/
cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml \
 --parameters ParameterKey=VpcBlock,ParameterValue=192.168.0.0/24 \
 ParameterKey=PrivateSubnet01Block,ParameterValue=192.168.0.64/27 \
 ParameterKey=PrivateSubnet02Block,ParameterValue=192.168.0.96/27 \
 ParameterKey=PublicSubnet01Block,ParameterValue=192.168.0.0/27 \
 ParameterKey=PublicSubnet02Block,ParameterValue=192.168.0.32/27
```

- b. Die Erstellung des AWS CloudFormation Stacks dauert einige Minuten. Führen Sie den folgenden Befehl aus, um den Bereitstellungsstatus des Stacks zu überprüfen.

```
aws cloudformation describe-stacks --stack-name my-eks-custom-networking-vpc --
query Stacks\[\].StackStatus --output text
```

Fahren Sie erst mit dem nächsten Schritt fort, wenn die Ausgabe des Befehls angezeigt wird `CREATE_COMPLETE`.

- c. Definieren Sie Variablen mit den Werten des privaten Subnetzes, das durch die Vorlage IDs erstellt wurde.

```
subnet_id_1=$(aws cloudformation describe-stack-resources --stack-name my-eks-
custom-networking-vpc \
 --query "StackResources[?
LogicalResourceId=='PrivateSubnet01'].PhysicalResourceId" --output text)
subnet_id_2=$(aws cloudformation describe-stack-resources --stack-name my-eks-
custom-networking-vpc \
 --query "StackResources[?
LogicalResourceId=='PrivateSubnet02'].PhysicalResourceId" --output text)
```

- d. Definieren Sie Variablen mit den Availability Zones der im vorherigen Schritt abgerufenen Subnetze.

```
az_1=$(aws ec2 describe-subnets --subnet-ids $subnet_id_1 --query
'Subnets[*].AvailabilityZone' --output text)
az_2=$(aws ec2 describe-subnets --subnet-ids $subnet_id_2 --query
'Subnets[*].AvailabilityZone' --output text)
```

### 3. Erstellen Sie eine Cluster-IAM-Rolle.

- a. Führen Sie den folgenden Befehl aus, um eine JSON-Datei für eine IAM-Vertrauensrichtlinie zu erstellen.

```
cat >eks-cluster-role-trust-policy.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "eks.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
EOF
```

- b. Erstellen Sie die Amazon-EKS-Cluster-IAM-Rolle. Falls erforderlich, stellen Sie `eks-cluster-role-trust-policy.json` den Pfad auf Ihrem Computer voran, in den Sie im vorherigen Schritt die Datei geschrieben haben. Der Befehl verknüpft die im vorherigen Schritt erstellte Vertrauensrichtlinie mit der Rolle. Um eine IAM-Rolle zu erstellen, muss dem [IAM-Prinzipal](#), der die Rolle erstellt, die `iam:CreateRole`-Aktion (Berechtigung) zugewiesen werden.

```
aws iam create-role --role-name myCustomNetworkingAmazonEKSClusterRole --assume-
role-policy-document file://"eks-cluster-role-trust-policy.json"
```

- c. Fügen Sie der Rolle die von Amazon EKS verwaltete Richtlinie mit dem Namen [Amazon EKSCluster Policy](#) hinzu. Um eine IAM-Richtlinie an einen [IAM-Prinzipal](#) anzuhängen, muss dem Prinzipal, der die Richtlinie anhängt, eine der folgenden IAM-Aktionen (Berechtigungen) zugewiesen werden: `iam:AttachUserPolicy` oder `iam:AttachRolePolicy`.

```
aws iam attach-role-policy --policy-arn arn:aws: iam::aws:policy/
AmazonEKSClusterPolicy --role-name myCustomNetworkingAmazonEKSClusterRole
```

4. Erstellen Sie einen Amazon-EKS-Cluster und konfigurieren Sie Ihr Gerät für die Kommunikation mit diesem.

- a. Erstellen Sie einen Cluster.

```
aws eks create-cluster --name my-custom-networking-cluster \
 --role-arn arn:aws: iam::$account_id:role/
myCustomNetworkingAmazonEKSClusterRole \
 --resources-vpc-config subnetIds=$subnet_id_1","$subnet_id_2
```

 Note

Möglicherweise erhalten Sie die Fehlermeldung, dass eine der Availability Zones in Ihrer Anfrage nicht über genügend Kapazität verfügt, um einen Amazon EKS-Cluster zu erstellen. Wenn dies der Fall ist, enthält die Fehlerausgabe die Availability Zones, die einen neuen Cluster unterstützen können. Versuchen Sie, Ihren Cluster mit mindestens zwei Subnetzen erneut zu erstellen, die sich in den unterstützten Availability Zones für Ihr Konto befinden. Weitere Informationen finden Sie unter [the section called "Unzureichende Kapazität"](#).

- b. Die Erstellung des Clusters dauert mehrere Minuten. Führen Sie den folgenden Befehl aus, um den Bereitstellungsstatus des Clusters zu überprüfen.

```
aws eks describe-cluster --name my-custom-networking-cluster --query
cluster.status
```

Fahren Sie erst mit dem nächsten Schritt fort, wenn die Ausgabe des Befehls angezeigt wird "ACTIVE".

- c. Konfigurieren Sie `kubectl` für die Kommunikation mit Ihrem Cluster.

```
aws eks update-kubeconfig --name my-custom-networking-cluster
```

## Schritt 2: Konfigurieren Ihrer VPC

Für dieses Tutorial wird die VPC in [the section called “Schritt 1: Erstellen einer Test-VPC und eines Clusters”](#) erstellt. Passen Sie für einen Produktions-Cluster die Schritte entsprechend Ihrer VPC an, indem Sie alle Beispielwerte durch eigene Werte ersetzen.

1. Vergewissern Sie sich, dass Ihr aktuell installiertes Amazon VPC CNI-Plugin für Kubernetes die neueste Version ist. Informationen zur Ermittlung der neuesten Version für den Amazon-EKS-Add-On-Typ und zur Aktualisierung Ihrer Version auf diese Version finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#). Informationen dazu, wie Sie die neueste Version für den selbstverwalteten Add-On-Typ ermitteln und Ihre Version darauf aktualisieren können, finden Sie unter [the section called “Amazon VPC CNI”](#).
2. Rufen Sie die ID Ihrer Cluster-VPC ab und speichern Sie diese zur Verwendung in späteren Schritten in einer Variable.

```
vpc_id=$(aws eks describe-cluster --name my-custom-networking-cluster --query
"cluster.resourcesVpcConfig.vpcId" --output text)
```

3. Ordnen Sie der VPC Ihres Clusters einen zusätzlichen CIDR-Block (Classless Inter-Domain Routing) zu. Der CIDR-Block darf sich nicht mit vorhandenen zugehörigen CIDR-Blöcken überschneiden.
  - a. Zeigen Sie die aktuellen CIDR-Blöcke an, die Ihrer VPC zugeordnet sind.

```
aws ec2 describe-vpcs --vpc-ids $vpc_id \
 --query 'Vpcs[*].CidrBlockAssociationSet[*].{CIDRBlock: CidrBlock, State:
 CidrBlockState.State}' --out table
```

Eine Beispielausgabe sieht wie folgt aus.

```

| DescribeVpcs |
```

```
+-----+-----+
| CIDRBlock | State |
+-----+-----+
| 192.168.0.0/24 | associated |
+-----+-----+
```

- b. Ordnen Sie Ihrer VPC zusätzliche CIDR-Blöcke zu. Ersetzen Sie den CIDR-Blockwert im folgenden Befehl. Weitere Informationen finden Sie unter [Zusätzliche IPv4 CIDR-Blöcke mit Ihrer VPC verknüpfen](#) im Amazon VPC-Benutzerhandbuch.

```
aws ec2 associate-vpc-cidr-block --vpc-id $vpc_id --cidr-block 192.168.1.0/24
```

- c. Bestätigen Sie, dass der neue Block zugeordnet ist.

```
aws ec2 describe-vpcs --vpc-ids $vpc_id --query
'Vpcs[*].CidrBlockAssociationSet[*].{CIDRBlock: CidrBlock, State:
CidrBlockState.State}' --out table
```

Eine Beispielausgabe sieht wie folgt aus.

```

| DescribeVpcs |
+-----+-----+
| CIDRBlock | State |
+-----+-----+
| 192.168.0.0/24 | associated |
| 192.168.1.0/24 | associated |
+-----+-----+
```

Fahren Sie erst mit dem nächsten Schritt fort, wenn Ihr neuer CIDR-Block fertig ist. State associated

4. Erstellen Sie so viele Subnetze, wie Sie in jeder Availability Zone verwenden möchten, in denen sich Ihre vorhandenen Subnetze befinden. Geben Sie einen CIDR-Block an, der sich innerhalb des CIDR-Blocks befindet, den Sie in einem vorherigen Schritt mit Ihrer VPC verknüpft haben.
  - a. Erstellen Sie neue Subnetze. Ersetzen Sie die CIDR-Blockwerte im folgenden Befehl. Die Subnetze müssen in einem anderen VPC-CIDR-Block erstellt werden als Ihre vorhandenen Subnetze, jedoch in denselben Availability Zones wie Ihre vorhandenen Subnetze. In diesem Beispiel wird ein Subnetz im neuen CIDR-Block jeder Availability Zone erstellt, in der die aktuellen privaten Subnetze vorhanden sind. Die IDs erstellten Subnetze werden in Variablen

gespeichert, um sie in späteren Schritten zu verwenden. Die Name-Werte entsprechen den Werten, die den Subnetzen zugewiesen wurden, die in einem vorherigen Schritt mit der Amazon-EKS-VPC-Vorlage erstellt wurden. Namen sind nicht erforderlich. Sie können verschiedene Namen verwenden.

```
new_subnet_id_1=$(aws ec2 create-subnet --vpc-id $vpc_id --availability-zone $az_1
--cidr-block 192.168.1.0/27 \
 --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=my-eks-custom-
networking-vpc-PrivateSubnet01},{Key=kubernetes.io/role/internal-elb,Value=1}]' \
 --query Subnet.SubnetId --output text)
new_subnet_id_2=$(aws ec2 create-subnet --vpc-id $vpc_id --availability-zone $az_2
--cidr-block 192.168.1.32/27 \
 --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=my-eks-custom-
networking-vpc-PrivateSubnet02},{Key=kubernetes.io/role/internal-elb,Value=1}]' \
 --query Subnet.SubnetId --output text)
```

### Important

Standardmäßig sind Ihre neuen Subnetze implizit mit der [Haupt-Routing-Tabelle](#) Ihrer VPC verknüpft. Diese Routing-Tabelle ermöglicht die Kommunikation zwischen allen Ressourcen, die in der VPC bereitgestellt werden. Es erlaubt jedoch keine Kommunikation mit Ressourcen, deren IP-Adressen sich außerhalb der CIDR-Blöcke befinden, die Ihrer VPC zugeordnet sind. Sie können Ihre eigene Routing-Tabelle Ihren Subnetzen zuordnen, um dieses Verhalten zu ändern. Weitere Informationen finden Sie unter [Subnetz-Routing-Tabellen](#) im Amazon-VPC-Benutzerhandbuch.

b. Zeigen Sie die aktuellen Subnetze in Ihrer VPC an.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=$vpc_id" \
 --query 'Subnets[*].{SubnetId: SubnetId,AvailabilityZone:
AvailabilityZone,CidrBlock: CidrBlock}' \
 --output table
```

Eine Beispielausgabe sieht wie folgt aus.

```

| DescribeSubnets |
+-----+-----+-----+-----+
| AvailabilityZone | CidrBlock | SubnetId |
```

|            |                 |                 |         |
|------------|-----------------|-----------------|---------|
| +-----+    | +-----+         | +-----+         | +-----+ |
| us-west-2d | 192.168.0.0/27  | subnet-example1 |         |
| us-west-2a | 192.168.0.32/27 | subnet-example2 |         |
| us-west-2a | 192.168.0.64/27 | subnet-example3 |         |
| us-west-2d | 192.168.0.96/27 | subnet-example4 |         |
| us-west-2a | 192.168.1.0/27  | subnet-example5 |         |
| us-west-2d | 192.168.1.32/27 | subnet-example6 |         |
| +-----+    | +-----+         | +-----+         | +-----+ |

Sie können sehen, dass die Subnetze im CIDR-Block 192.168.1.0, den Sie erstellt haben, in denselben Availability Zones liegen wie die Subnetze im CIDR-Block 192.168.0.0.

### Schritt 3: Konfigurieren von Kubernetes-Ressourcen

1. Setzen Sie die `AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG` Umgebungsvariable auf `true` in `aws-node` DaemonSet

```
kubectl set env daemonset aws-node -n kube-system
AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG=true
```

2. Rufen Sie die ID der [Cluster-Sicherheitsgruppe](#) ab und speichern Sie diese in einer Variablen zur Verwendung im nächsten Schritt. Amazon EKS erstellt diese Sicherheitsgruppe automatisch, wenn Sie Ihren Cluster erstellen.

```
cluster_security_group_id=$(aws eks describe-cluster --name my-custom-networking-cluster --query cluster.resourcesVpcConfig.clusterSecurityGroupId --output text)
```

3. Erstellen Sie eine `ENIConfig` benutzerdefinierte Ressource für jedes Subnetz, in dem Sie Pods bereitstellen möchten.
  - a. Erstellen Sie für jede Konfiguration der Netzwerkschnittstelle eine eindeutige Datei.

Die folgenden Befehle erstellen separate `ENIConfig`-Dateien für die beiden Subnetze, die in einem vorherigen Schritt erstellt wurden. Der Wert für `name` muss eindeutig sein. Der Name entspricht der Availability Zone, in der sich das Subnetz befindet. Die Cluster-Sicherheitsgruppe ist dem `ENIConfig` zugeordnet.

```
cat >$az_1.yaml <<EOF
apiVersion: crd.k8s.amazonaws.com/v1alpha1
kind: ENIConfig
metadata:
```



```
name: $az_1
spec:
 securityGroups:
 - $cluster_security_group_id
 subnet: $new_subnet_id_1
EOF
```

```
cat >$az_2.yaml <<EOF
apiVersion: crd.k8s.amazonaws.com/v1alpha1
kind: ENIConfig
metadata:
 name: $az_2
spec:
 securityGroups:
 - $cluster_security_group_id
 subnet: $new_subnet_id_2
EOF
```

Für einen Produktions-Cluster können Sie die folgenden Änderungen an den vorherigen Befehlen vornehmen:

- Ersetzen Sie `$cluster_security_group_id` durch die ID einer vorhandenen [Sicherheitsgruppe](#), die Sie für jede Gruppe verwenden möchten. ENIConfig
- Wir empfehlen, dass Sie, wann immer möglich, denselben Namen wie ENIConfigs die Availability Zone angeben, für die Sie die Option verwenden werden. ENIConfig Unter Umständen müssen Sie für Ihre ENIConfigs andere Namen verwenden als für die Availability Zones. Wenn Sie beispielsweise mehr als zwei Subnetze in derselben Availability Zone haben und beide mit benutzerdefinierten Netzwerken verwenden möchten, benötigen Sie mehrere ENIConfigs für dieselbe Availability Zone. Da für jede ENIConfig Variante ein eindeutiger Name erforderlich ist, können Sie nicht mehr als eine von Ihnen benennen, ENIConfigs indem Sie den Availability Zone-Namen verwenden.

Wenn Ihre ENIConfig Namen nicht alle mit Availability Zonen-Namen identisch sind, ersetzen Sie `$az_1` und `$az_2` in den vorherigen Befehlen durch Ihre eigenen Namen und [kommentieren Sie Ihre Knoten später in diesem Tutorial mit](#) den entsprechenden. ENIConfig

 Note

Wenn Sie keine gültige Sicherheitsgruppe für die Verwendung mit einem Produktionscluster angeben und Folgendes verwenden:

- Version 1.8.0 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes, dann werden die Sicherheitsgruppen verwendet, die der primären elastic network interface des Knotens zugeordnet sind.
- eine Version des Amazon VPC CNI-Plug-ins für Kubernetes, die älter ist als 1.8.0, dann wird die Standardsicherheitsgruppe für die VPC sekundären Netzwerkschnittstellen zugewiesen.

 Important

- `AWS_VPC_K8S_CNI_EXTERNALSNAT=false` ist eine Standardeinstellung in der Konfiguration für das Amazon-VPC-CNI-Plugin für Kubernetes. Wenn Sie die Standardeinstellung verwenden, verwendet Traffic, der für IP-Adressen bestimmt ist, die sich nicht in einem der mit Ihrer VPC verknüpften CIDR-Blöcke befinden, die Sicherheitsgruppen und Subnetze der primären Netzwerkschnittstelle Ihres Knotens. Die in Ihrem definierten Subnetze und Sicherheitsgruppen ENIConfigs, die zur Erstellung sekundärer Netzwerkschnittstellen verwendet werden, werden für diesen Datenverkehr nicht verwendet. Weitere Informationen zu dieser Einstellung finden Sie unter [the section called “Ausgehender Verkehr”](#).
- Wenn Sie auch Sicherheitsgruppen für Pods verwenden, `SecurityGroupPolicy` wird die in `a` angegebene Sicherheitsgruppe anstelle der Sicherheitsgruppe verwendet, die in der ENIConfigs angegeben ist. Weitere Informationen finden Sie unter [the section called “Sicherheitsgruppen für Pods”](#).

- b. Wenden Sie alle benutzerdefinierten Ressourcendateien, die Sie zuvor erstellt haben, mit den folgenden Befehlen auf Ihren Cluster an:

```
kubectl apply -f $az_1.yaml
kubectl apply -f $az_2.yaml
```

4. Bestätigen Sie, dass Ihre ENIConfigs erstellt wurden.

```
kubectl get ENIConfigs
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME       | AGE  |
|------------|------|
| us-west-2a | 117s |
| us-west-2d | 105s |

5. Wenn Sie benutzerdefinierte Netzwerke auf einem Produktionscluster aktivieren und Ihrem Namen einen anderen ENIConfig Namen als die Availability Zone geben, für die Sie sie verwenden, fahren Sie mit dem [nächsten Schritt fort](#), um EC2 Amazon-Knoten bereitzustellen.

Ermöglichen Sie Kubernetes, die Option ENIConfig für eine Availability Zone automatisch auf alle neuen EC2 Amazon-Knoten anzuwenden, die in Ihrem Cluster erstellt wurden.

- a. Gehen Sie für den Test-Cluster in diesem Tutorial zum [nächsten Schritt](#).

Prüfen Sie bei einem Produktionscluster, ob eine Anmerkung mit dem Schlüssel `k8s.amazonaws.com/eniConfig` für die [ENI\\_CONFIG\\_ANNOTATION\\_DEF](#) Umgebungsvariable in der Containerspezifikation für vorhanden ist. `aws-node` DaemonSet

```
kubectl describe daemonset aws-node -n kube-system | grep
ENI_CONFIG_ANNOTATION_DEF
```

Wenn eine Ausgabe zurückgegeben wird, ist die Anmerkung vorhanden. Wenn keine Ausgabe zurückgegeben wird, ist die Variable nicht gesetzt. Für einen Produktions-Cluster können Sie entweder diese Einstellung oder die Einstellung im folgenden Schritt verwenden. Wenn Sie diese Einstellung verwenden, überschreibt sie die Einstellung im folgenden Schritt. In diesem Tutorial wird die Einstellung im nächsten Schritt verwendet.

- b. Aktualisieren Sie Ihre `aws-node` DaemonSet , sodass die Option ENIConfig für eine Availability Zone automatisch auf alle neuen EC2 Amazon-Knoten angewendet wird, die in Ihrem Cluster erstellt wurden.

```
kubectl set env daemonset aws-node -n kube-system
ENI_CONFIG_LABEL_DEF=topology.kubernetes.io/zone
```

## Schritt 4: EC2 Amazon-Knoten bereitstellen

1. Erstellen Sie eine Knoten-IAM-Rolle.

- a. Führen Sie den folgenden Befehl aus, um eine JSON-Datei für eine IAM-Vertrauensrichtlinie zu erstellen.

```
cat >node-role-trust-relationship.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ec2.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
EOF
```

- b. Erstellen Sie eine IAM-Rolle und speichern Sie den zurückgegebenen Amazon-Ressourcennamen (ARN) in einer Variablen, um sie in einem späteren Schritt zu verwenden.

```
node_role_arn=$(aws iam create-role --role-name myCustomNetworkingNodeRole --
assume-role-policy-document file://"node-role-trust-relationship.json" \
--query Role.Arn --output text)
```

- c. Hängen Sie die drei erforderlichen verwalteten IAM-Richtlinien an die IAM-Rolle an.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy \
--role-name myCustomNetworkingNodeRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly \
--role-name myCustomNetworkingNodeRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
--role-name myCustomNetworkingNodeRole
```

### Important

Der Einfachheit halber ist in diesem Tutorial die [AmazonEKS\\_CNI\\_Policy-Richtlinie an die Node-IAM-Rolle](#) angehängt. In einem Produktionscluster empfehlen wir jedoch,

die Richtlinie einer separaten IAM-Rolle zuzuordnen, die nur mit dem Amazon VPC CNI-Plugin für Kubernetes verwendet wird. Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).

2. Erstellen Sie einen der folgenden Typen von Knotengruppen. Informationen zum Bestimmen des Instance-Typs, den Sie bereitstellen möchten, finden Sie unter [the section called “EC2 Amazon-Instance-Typen”](#). Füllen Sie für dieses Tutorial die Option Verwaltet, Ohne Startvorlage oder mit Startvorlage ohne angegebene AMI-ID aus. Wenn Sie die Knotengruppe für Produktionsworkloads verwenden möchten, empfehlen wir Ihnen, sich mit allen Optionen für verwaltete [Knotengruppen und selbstverwaltete Knotengruppen vertraut zu machen, bevor Sie die Knotengruppe](#) bereitstellen.

- Verwaltet – Stellen Sie Ihre Knotengruppe mit einer der folgenden Optionen bereit:
  - Ohne Startvorlage oder mit Startvorlage ohne angegebene AMI-ID – Führen Sie den folgenden Befehl aus. Verwenden Sie für dieses Tutorial die Beispielwerte: Ersetzen Sie bei einer Produktionsknotengruppe alle Beispielwerte durch Ihre eigenen. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten.

```
aws eks create-nodegroup --cluster-name my-custom-networking-cluster --nodegroup-name my-nodegroup \
 --subnets $subnet_id_1 $subnet_id_2 --instance-types t3.medium --node-role $node_role_arn
```

- Mit einer Startvorlage mit einer angegebenen AMI-ID
  - A. Ermitteln Sie die von Amazon EKS empfohlene Anzahl an maximalen Pods für Ihre Knoten. Folgen Sie den Anweisungen in den von [Amazon EKS empfohlenen maximalen Pods für jeden EC2 Amazon-Instance-Typ](#) und fügen Sie `--cni-custom-networking-enabled` Schritt 3 in diesem Thema hinzu. Notieren Sie die Ausgabe zur Verwendung im nächsten Schritt.
  - B. Geben Sie in Ihrer Startvorlage eine Amazon-EKS-optimierte AMI-ID oder ein benutzerdefiniertes AMI an, das auf dem Amazon-EKS-optimierten AMI basiert. [Stellen Sie dann die Knotengruppe mithilfe einer Startvorlage bereit](#) und geben Sie die folgenden Benutzerdaten in der Startvorlage an. Diese Benutzerdaten übergeben Argumente an die `bootstrap.sh`-Datei. Weitere Informationen zur Bootstrap-Datei finden Sie unter [bootstrap.sh](#) auf GitHub. Sie können 20 entweder durch den Wert aus dem vorherigen Schritt (empfohlen) oder Ihren eigenen Wert ersetzen.

```
/etc/eks/bootstrap.sh my-custom-networking-cluster --use-max-pods false --
kubelet-extra-args '--max-pods=20'
```

Wenn Sie ein benutzerdefiniertes AMI erstellt haben, das nicht auf dem für Amazon EKS optimierten AMI basiert, müssen Sie die Konfiguration selbst anpassen.

- Selbstverwaltet
  - i. Ermitteln Sie die von Amazon EKS empfohlene Anzahl an maximalen Pods für Ihre Knoten. Befolgen Sie die Anweisungen in [the section called “Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen”](#) und fügen Sie `--cni-custom-networking-enabled` zu Schritt 3 in diesem Thema hinzu. Notieren Sie die Ausgabe zur Verwendung im nächsten Schritt.
  - ii. Stellen Sie die Knotengruppe mithilfe der Anweisungen in [the section called “Amazon Linux”](#) bereit. Geben Sie den folgenden Text für den `BootstrapArgumentsParameter` an. Sie können 20 entweder durch den Wert aus dem vorherigen Schritt (empfohlen) oder Ihren eigenen Wert ersetzen.

```
--use-max-pods false --kubelet-extra-args '--max-pods=20'
```

#### Note

Wenn Sie möchten, dass Knoten in einem Produktionscluster eine deutlich höhere Anzahl von Pods unterstützen, führen Sie das Skript [the section called “Amazon EKS hat die maximale Anzahl an Pods für jeden EC2 Amazon-Instance-Typ empfohlen”](#) erneut aus. Fügen Sie außerdem die Option `--cni-prefix-delegation-enabled` zu dem Befehl hinzu. Beispielsweise wird 110 für einen `m5.large`-Instance-Typ zurückgegeben. Anweisungen, wie Sie diese Funktion aktivieren, finden Sie unter [the section called “Erhöhen Sie die IP-Adressen”](#). Sie können diese Funktion mit benutzerdefinierten Netzwerken verwenden.

3. Die Erstellung der Knotengruppe dauert mehrere Minuten. Sie können den Status der Erstellung einer verwalteten Knotengruppe mit dem folgenden Befehl überprüfen.

```
aws eks describe-nodegroup --cluster-name my-custom-networking-cluster --nodegroup-
name my-nodegroup --query nodegroup.status --output text
```

Fahren Sie erst mit dem nächsten Schritt fort, wenn die zurückgegebene ACTIVE Ausgabe

4. Für das Tutorial können Sie diesen Schritt überspringen.

Wenn Sie bei einem Produktionscluster nicht ENIConfigs den gleichen Namen wie die Availability Zone angegeben haben, für die Sie ihn verwenden, müssen Sie Ihre Knoten mit dem ENIConfig Namen versehen, der für den Knoten verwendet werden soll. Dieser Schritt ist nicht erforderlich, wenn Sie in jeder Availability Zone nur ein Subnetz haben und Sie Ihre ENIConfigs mit den gleichen Namen wie Ihre Availability Zones benannt haben. [Dies liegt daran, dass das Amazon VPC CNI-Plugin für Kubernetes automatisch den richtigen Knoten für Sie zuordnet, wenn Sie es in ENIConfig einem vorherigen Schritt dafür aktiviert haben.](#)

a. Rufen Sie die Liste der Knoten in Ihrem Cluster ab.

```
kubectl get nodes
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                                       | STATUS | ROLES  | AGE   | VERSION  |
|------------------------------------------------------------|--------|--------|-------|----------|
| ip-192-168-0-126.us-west-2.compute.internal<br>eks-810597c | Ready  | <none> | 8m49s | v1.22.9- |
| ip-192-168-0-92.us-west-2.compute.internal<br>eks-810597c  | Ready  | <none> | 8m34s | v1.22.9- |

b. Bestimmen Sie, in welcher Availability Zone sich jeder Knoten befindet. Führen Sie den folgenden Befehl für jeden Knoten aus, der im vorherigen Schritt zurückgegeben wurde, und ersetzen Sie dabei die IP-Adressen, die auf der vorherigen Ausgabe basieren.

```
aws ec2 describe-instances --filters Name=network-interface.private-dns-name,Values=ip-192-168-0-126.us-west-2.compute.internal \
--query 'Reservations[].Instances[].{AvailabilityZone: Placement.AvailabilityZone, SubnetId: SubnetId}'
```

Eine Beispielausgabe sieht wie folgt aus.

```
[
 {
 "AvailabilityZone": "us-west-2d",
 "SubnetId": "subnet-Example5"
 }
]
```

]

- c. Kommentieren Sie jeden Knoten mit der ENIConfig, die Sie für die Subnetz-ID und die Availability Zone erstellt haben. Sie können einen Knoten nur mit einer ENIConfig kommentieren, aber es können mehrere Knoten mit derselben ENIConfig kommentiert werden. Ersetzen Sie die Beispielwerte durch Ihre eigenen Werte.

```
kubectl annotate node ip-192-168-0-126.us-west-2.compute.internal
k8s.amazonaws.com/eniConfig=EniConfigName1
kubectl annotate node ip-192-168-0-92.us-west-2.compute.internal
k8s.amazonaws.com/eniConfig=EniConfigName2
```

5. Wenn Sie vor der Umstellung auf die benutzerdefinierte Netzwerkfunktion Knoten in einem Produktionscluster mit laufenden Pods hatten, führen Sie die folgenden Aufgaben aus:
- Stellen Sie sicher, dass es verfügbare Knoten gibt, das benutzerdefinierte Netzwerkfeature verwenden.
  - Sperren und entleeren Sie die Knoten, um die Pods ordnungsgemäß herunterzufahren. Weitere Informationen finden Sie unter [Sicheres Entleeren eines Knotens](#) in der Kubernetes-Dokumentation.
  - Beenden Sie die Knoten. Wenn sich die Knoten in einer vorhandenen verwalteten Knotengruppe befinden, können Sie die Knotengruppe löschen. Führen Sie den folgenden Befehl aus.

```
aws eks delete-nodegroup --cluster-name my-custom-networking-cluster --nodegroup-name my-nodegroup
```

Nur neue Knoten, die mit der Bezeichnung `k8s.amazonaws.com/eniConfig` registriert sind, verwenden das neue benutzerdefinierte Netzwerkfeature.

6. Vergewissern Sie sich, dass den Pods eine IP-Adresse aus einem CIDR-Block zugewiesen wird, der einem der Subnetze zugeordnet ist, die Sie in einem vorherigen Schritt erstellt haben.

```
kubectl get pods -A -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

| NAMESPACE | NAME | READY | STATUS | RESTARTS  | AGE  | IP        |
|-----------|------|-------|--------|-----------|------|-----------|
|           | NODE |       |        | NOMINATED | NODE | READINESS |
| GATES     |      |       |        |           |      |           |



```

kube-system aws-node-2rkn4 1/1 Running 0 7m19s
192.168.0.92 ip-192-168-0-92.us-west-2.compute.internal <none>
<none>
kube-system aws-node-k96wp 1/1 Running 0 7m15s
192.168.0.126 ip-192-168-0-126.us-west-2.compute.internal <none>
<none>
kube-system coredns-657694c6f4-smcgr 1/1 Running 0 56m
192.168.1.23 ip-192-168-0-92.us-west-2.compute.internal <none>
<none>
kube-system coredns-657694c6f4-stwv9 1/1 Running 0 56m
192.168.1.28 ip-192-168-0-92.us-west-2.compute.internal <none>
<none>
kube-system kube-proxy-jgshq 1/1 Running 0 7m19s
192.168.0.92 ip-192-168-0-92.us-west-2.compute.internal <none>
<none>
kube-system kube-proxy-wx9vk 1/1 Running 0 7m15s
192.168.0.126 ip-192-168-0-126.us-west-2.compute.internal <none>
<none>

```

Sie können sehen, dass den Coredns Pods IP-Adressen aus dem 192.168.1.0 CIDR-Block zugewiesen wurden, den Sie zu Ihrer VPC hinzugefügt haben. Ohne benutzerdefiniertes Netzwerk wären diesen Adressen aus dem CIDR-Block 192.168.0.0 zugewiesen worden, da dies der einzige ursprünglich mit der VPC verbundene CIDR-Block war.

Wenn ein Pod spec enthält `hostNetwork=true`, wird ihm die primäre IP-Adresse des Nodes zugewiesen. Ihm wird keine Adresse aus den Subnetzen zugewiesen, die Sie hinzugefügt haben. Standardmäßig ist dieser Wert auf `false` festgelegt. Dieser Wert ist `true` für das kube-proxy Amazon VPC CNI-Plugin für Kubernetes (aws-node) -Pods, die auf Ihrem Cluster ausgeführt werden, auf gesetzt. Aus diesem Grund wurden den Pods kube-proxy und den aws-node Pods des Plugins in der vorherigen Ausgabe keine 192.168.1.x-Adressen zugewiesen. Weitere Informationen zur `hostNetwork` Einstellung eines Pods finden Sie unter [PodSpec v1 core](#) in der Kubernetes-API-Referenz.

## Schritt 5: Löschen von Tutorial-Ressourcen

Nachdem Sie das Tutorial abgeschlossen haben, empfehlen wir, dass Sie die erstellten Ressourcen löschen. Sie können dann die Schritte anpassen, um benutzerdefinierte Netzwerke für einen Produktions-Cluster zu aktivieren.

1. Wenn die von Ihnen erstellte Knotengruppe nur zum Testen gedacht ist, löschen Sie sie.

```
aws eks delete-nodegroup --cluster-name my-custom-networking-cluster --nodegroup-name my-nodegroup
```

2. Selbst wenn die AWS CLI-Ausgabe besagt, dass der Cluster gelöscht wurde, ist der Löschvorgang möglicherweise noch nicht abgeschlossen. Der Löschvorgang dauert einige Minuten. Bestätigen Sie, dass der Vorgang abgeschlossen ist, indem Sie den folgenden Befehl ausführen.

```
aws eks describe-nodegroup --cluster-name my-custom-networking-cluster --nodegroup-name my-nodegroup --query nodegroup.status --output text
```

Fahren Sie erst fort, wenn die zurückgegebene Ausgabe der folgenden Ausgabe ähnelt.

```
An error occurred (ResourceNotFoundException) when calling the DescribeNodegroup operation: No node group found for name: my-nodegroup.
```

3. Wenn die von Ihnen erstellte Knotengruppe nur zum Testen gedacht ist, löschen Sie den Knoten IAM-Rolle.
- a. Trennen Sie die Richtlinien von der Rolle.

```
aws iam detach-role-policy --role-name myCustomNetworkingNodeRole --policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
aws iam detach-role-policy --role-name myCustomNetworkingNodeRole --policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
aws iam detach-role-policy --role-name myCustomNetworkingNodeRole --policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
```

- b. Löschen Sie die Rolle.

```
aws iam delete-role --role-name myCustomNetworkingNodeRole
```

4. Löschen Sie den Cluster.

```
aws eks delete-cluster --name my-custom-networking-cluster
```

Bestätigen Sie, dass der Cluster gelöscht ist, indem Sie den folgenden Befehl ausführen.

```
aws eks describe-cluster --name my-custom-networking-cluster --query cluster.status --output text
```

Wird eine Ausgabe ähnlich der folgenden zurückgegeben, wurde der Cluster erfolgreich gelöscht.

```
An error occurred (ResourceNotFoundException) when calling the DescribeCluster operation: No cluster found for name: my-custom-networking-cluster.
```

## 5. Löschen Sie die Cluster-IAM-Rolle.

### a. Trennen Sie die Richtlinien von der Rolle.

```
aws iam detach-role-policy --role-name myCustomNetworkingAmazonEKSClusterRole --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
```

### b. Löschen Sie die Rolle.

```
aws iam delete-role --role-name myCustomNetworkingAmazonEKSClusterRole
```

## 6. Löschen Sie die Subnetze, die Sie in einem vorherigen Schritt erstellt haben.

```
aws ec2 delete-subnet --subnet-id $new_subnet_id_1
aws ec2 delete-subnet --subnet-id $new_subnet_id_2
```

## 7. Löschen Sie die VPC, die Sie erstellt haben.

```
aws cloudformation delete-stack --stack-name my-eks-custom-networking-vpc
```

## Weisen Sie Amazon EKS-Knoten mehr IP-Adressen mit Präfixen zu

Gilt für: Linux- und Windows-Knoten mit EC2 Amazon-Instances

Gilt für: Öffentliche und private Subnetze

Jede EC2 Amazon-Instance unterstützt eine maximale Anzahl von Elastic Network-Schnittstellen und eine maximale Anzahl von IP-Adressen, die jeder Netzwerkschnittstelle zugewiesen werden können. Jeder Knoten benötigt eine IP-Adresse für jede Netzwerkschnittstelle. Alle anderen verfügbaren IP-Adressen können Pods zugewiesen werden. Jeder Pod benötigt seine eigene IP-Adresse. Daher verfügen Sie möglicherweise über Knoten, die über verfügbare Rechen- und Speicherressourcen verfügen, aber keine zusätzlichen Ressourcen aufnehmen können, Pods da dem Knoten die IP-Adressen ausgehen, denen er zuweisen kann Pods.

Sie können die Anzahl der IP-Adressen, denen Knoten zuweisen können, erhöhen, Pods indem Sie IP-Präfixe zuweisen, anstatt Ihren Knoten einzelne sekundäre IP-Adressen zuzuweisen. Jedes Präfix enthält mehrere IP-Adressen. Wenn Sie Ihren Cluster nicht für die Zuweisung von IP-Präfixen konfigurieren, muss Ihr Cluster mehr API-Aufrufe (Amazon EC2 Application Programming Interface) tätigen, um Netzwerkschnittstellen und IP-Adressen zu konfigurieren, die für die Pod-Konnektivität erforderlich sind. Wenn Cluster immer größer werden, kann die Häufigkeit dieser API-Aufrufe zu längeren Startzeiten für Pods und Instances führen. Dies führt zu Verzögerungen bei der Skalierung, um den Anforderungen großer und anspruchsvoller Workloads gerecht zu werden, und erhöht den Kosten- und Verwaltungsaufwand, da Sie zusätzliche Cluster bereitstellen und Skalierungsanforderungen erfüllen VPCs müssen. Weitere Informationen finden Sie unter Schwellenwerte für [Kubernetes-Skalierbarkeit](#) auf GitHub

Kompatibilität mit den Funktionen des Amazon VPC CNI-Plug-ins für Kubernetes-Funktionen

Sie können IP-Präfixe mit den folgenden Funktionen verwenden:

- IPv4 Übersetzung der Quellnetzwerkadresse — Weitere Informationen finden Sie unter [the section called “Ausgehender Verkehr”](#).
- IPv6 Adressen für Cluster, Pods und Dienste — Weitere Informationen finden Sie unter [the section called “IPv6”](#).
- Den Datenverkehr mithilfe von Kubernetes-Netzwerkrichtlinien einschränken — Weitere Informationen finden Sie unter [the section called “Kubernetes-Richtlinien”](#)

Die folgende Liste enthält Informationen zu den geltenden Amazon VPC CNI-Plug-in-Einstellungen. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter [amazon-vpc-cni-k8s](#) on GitHub

- WARM\_IP\_TARGET
- MINIMUM\_IP\_TARGET
- WARM\_PREFIX\_TARGET

Überlegungen

Beachten Sie bei der Verwendung dieser Funktion Folgendes:

- Jeder EC2 Amazon-Instance-Typ unterstützt eine maximale Anzahl von Pods. Wenn Ihre verwaltete Knotengruppe aus mehreren Instance-Typen besteht, wird die kleinste maximale Anzahl an Pods für eine Instance im Cluster auf alle Knoten im Cluster angewendet.
- Standardmäßig ist die maximale Anzahl von Pods, die Sie auf einem Knoten ausführen können, 110, aber Sie können diese Anzahl ändern. Wenn Sie die Anzahl ändern und eine verwaltete Knotengruppe haben, führt die nächste AMI- oder Startvorlagenaktualisierung Ihrer Knotengruppe dazu, dass neue Knoten mit dem geänderten Wert erstellt werden.
- Beim Übergang von der Zuweisung von IP-Adressen zur Zuweisung von IP-Präfixen empfehlen wir, dass Sie neue Knotengruppen erstellen, um die Anzahl der verfügbaren IP-Adressen zu erhöhen, anstatt die vorhandenen Knoten fortlaufend zu ersetzen. Das Ausführen von Pods auf einem Knoten, dem sowohl IP-Adressen als auch Präfixe zugewiesen sind, kann zu Inkonsistenzen bei der angekündigten IP-Adresskapazität führen, was sich auf die future Workloads auf dem Knoten auswirkt. Die empfohlene Methode zur Durchführung des Übergangs finden Sie unter [Ersetzen aller Knoten während der Migration vom sekundären IP-Modus in den Präfix-Delegierungsmodus oder umgekehrt](#) im Amazon-EKS-Leitfaden mit bewährten Methoden.
- [Der Geltungsbereich der Sicherheitsgruppe befindet sich auf Knotenebene. Weitere Informationen finden Sie unter Sicherheitsgruppe.](#)
- IP-Präfixe, die einer Netzwerkschnittstelle zugewiesen sind, unterstützen eine hohe Pod-Dichte pro Knoten und haben die beste Startzeit.
- IP-Präfixe und IP-Adressen sind mit standardmäßigen Amazon EC2 Elastic Network-Schnittstellen verknüpft. Pods, die bestimmte Sicherheitsgruppen erfordern, wird die primäre IP-Adresse einer Zweigstellen-Netzwerkschnittstelle zugewiesen. Sie können Pods, die IP-Adressen oder IP-Adressen aus IP-Präfixen beziehen, mit Pods kombinieren, die Zweignetzwerkschnittstellen auf demselben Knoten erhalten.
- Nur für Cluster mit Linux-Knoten.
  - Nachdem Sie das Add-on so konfiguriert haben, dass es Netzwerkschnittstellen Präfixe zuweist, können Sie Ihr Amazon VPC CNI-Plug-In für Kubernetes nicht auf eine niedrigere Version als 1.9.0 (oder 1.10.1) herunterstufen, ohne alle Knoten in allen Knotengruppen in Ihrem Cluster zu entfernen.
  - Wenn Sie auch Sicherheitsgruppen für Pods mit `POD_SECURITY_GROUP_ENFORCING_MODE = standard` und `AWS_VPC_K8S_CNI_EXTERNALSNAT = false` verwenden, werden bei der Kommunikation Ihrer Pods mit Endpunkten außerhalb Ihrer VPC die Sicherheitsgruppen des Knotens verwendet und nicht die Sicherheitsgruppen, die Sie Ihren Pods zugewiesen haben.

Wenn Sie auch [Sicherheitsgruppen für Pods](#) mit `POD_SECURITY_GROUP_ENFORCING_MODE = strict`, werden die Pod's Sicherheitsgruppen verwendet, wenn Sie mit Endpunkten außerhalb Ihrer VPC Pods kommunizieren.

Erhöhen Sie die verfügbaren IP-Adressen für Ihren Amazon EKS-Knoten

Sie können die Anzahl der IP-Adressen erhöhen, die Knoten Pods zuweisen können, indem Sie IP-Präfixe zuweisen, anstatt Ihren Knoten einzelne sekundäre IP-Adressen zuzuweisen.

### Voraussetzungen

- Sie benötigen einen vorhandenen Cluster. Informationen zum Bereitstellen finden Sie unter [the section called “Erstellen eines -Clusters”](#).
- Die Subnetze, in denen sich Ihre Amazon-EKS-Knoten befinden, müssen über ausreichend zusammenhängende /28 (für IPv4-Cluster) oder /80 (für IPv6-Cluster) CIDR-Blöcke (Classless Inter-Domain Routing) verfügen. Sie können nur Linux-Knoten in einem IPv6-Cluster haben. Die Verwendung von IP-Präfixen kann fehlschlagen, wenn IP-Adressen im Subnetz-CIDR verstreut sind. Wir empfehlen Folgendes:
  - Verwendung einer Subnetz-CIDR-Reservierung, sodass IP-Adressen, die sich innerhalb des reservierten Bereichs befinden, nach ihrer Freigabe nicht neu zugewiesen werden. Dadurch wird sichergestellt, dass Präfixe für die Zuweisung ohne Segmentierung verfügbar sind.
  - Verwenden Sie neue Subnetze, die speziell für die Ausführung der Workloads verwendet werden, denen IP-Präfixe zugewiesen sind. Sowohl Windows- als auch Linux-Workloads können bei der Zuweisung von IP-Präfixen im selben Subnetz ausgeführt werden.
- Um Ihren Knoten IP-Präfixe zuzuweisen, müssen Ihre Knoten Nitro-basiert sein. AWS Instances, die nicht auf Nitro basieren, weisen weiterhin einzelne sekundäre IP-Adressen zu, haben aber eine deutlich geringere Anzahl von IP-Adressen, die Pods zugewiesen werden können als Nitro-basierte Instances.
- Nur für Cluster mit Linux-Knoten — Wenn Ihr Cluster für die IPv4 Familie konfiguriert ist, müssen Sie Version 1.9.0 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes installiert haben. Sie können Ihre aktuelle Version mit dem folgenden Befehl überprüfen.

```
kubectl describe daemonset aws-node --namespace kube-system | grep Image | cut -d "/"
-f 2
```

Wenn Ihr Cluster für die IPv6-Familie konfiguriert ist, müssen Sie die Version 1.10.1 des Add-ons installiert haben. Wenn Ihre Plugin-Version älter ist als die erforderlichen Versionen, müssen Sie sie aktualisieren. Weitere Informationen finden Sie in den Aktualisierungsabschnitten von [Assign IPs to Pods with the Amazon VPC CNI](#).

- Nur für Cluster mit Windows-Knoten
- Ihr Cluster und seine Plattformversion müssen mindestens den Versionen in der folgenden Tabelle entsprechen. Lesen Sie [the section called “Kubernetes-Version aktualisieren”](#), um Ihre Cluster-Version zu aktualisieren. Wenn Ihr Cluster nicht die Plattform-Mindestversion hat, können Sie Ihren Knoten keine IP-Präfixe zuweisen, bis Amazon EKS Ihre Plattformversion aktualisiert hat.

| Kubernetes-Version | Plattformversion |
|--------------------|------------------|
| 1.27               | eks.3            |
| 1.26               | eks.4            |

Sie können Ihre aktuelle Kubernetes- und Plattformversion überprüfen, indem Sie den folgenden Befehl durch den Namen Ihres Clusters ersetzen *my-cluster* und dann den geänderten Befehl ausführen: `aws eks describe-cluster --name my-cluster --query 'cluster.{\"Kubernetes Version\": version, \"Platform Version\": platformVersion}'`

- Sie müssen die Windows-Unterstützung für Ihren Cluster aktiviert haben. Weitere Informationen finden Sie unter [the section called “Aktivieren Sie die Windows-Unterstützung”](#).

Weisen Sie den Knoten IP-Adresspräfixe zu

Konfigurieren Sie Ihren Cluster, um Knoten IP-Adresspräfixe zuzuweisen. Schließen Sie das Verfahren ab, das dem Betriebssystem Ihres Knotens entspricht.

## Linux

1. Aktivieren Sie den Parameter, um Netzwerkschnittstellen für das Amazon VPC CNI Präfixe zuzuweisen. `DaemonSet` Wenn Sie einen Cluster bereitstellen, wird Version 1.10.1 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes zusammen mit diesem bereitgestellt. Wenn Sie den Cluster mit der IPv6-Familie erstellt haben, wurde für diese Einstellung standardmäßig `true`

festgelegt. Wenn Sie den Cluster mit der IPv4-Familie erstellt haben, wurde für diese Einstellung standardmäßig `false` festgelegt.

```
kubectl set env daemonset aws-node -n kube-system ENABLE_PREFIX_DELEGATION=true
```

### Important

Selbst wenn Ihr Subnetz über verfügbare IP-Adressen verfügt, wird im Amazon VPC CNI-Plugin für Kubernetes-Protokolle der folgende Fehler angezeigt, wenn das Subnetz keine zusammenhängenden /28 Blöcke zur Verfügung hat.

```
InsufficientCidrBlocks: The specified subnet does not have enough free cidr blocks to satisfy the request
```

Dies kann aufgrund der Fragmentierung vorhandener sekundärer IP-Adressen auftreten, die über ein Subnetz verteilt sind. Um diesen Fehler zu beheben, erstellen Sie entweder ein neues Subnetz und starten Sie Pods dort, oder verwenden Sie eine CIDR-Reservierung für das EC2 Amazon-Subnetz, um Speicherplatz innerhalb eines Subnetzes für die Verwendung mit Präfixzuweisung zu reservieren. Weitere Informationen erhalten Sie unter [Subnetz-CIDR-Reservierungen](#) im Amazon-VPC-Benutzerhandbuch.

2. Wenn Sie planen, eine verwaltete Knotengruppe ohne Startvorlage oder mit einer Startvorlage bereitzustellen, in der Sie keine AMI-ID angegeben haben, und Sie eine Version des Amazon VPC CNI-Plug-ins für Kubernetes verwenden, die den in den Voraussetzungen aufgeführten Versionen entspricht oder höher ist, dann fahren Sie mit dem nächsten Schritt fort. Managed Node Groups berechnet automatisch die maximale Anzahl von Pods für Sie.

Wenn Sie eine selbstverwaltete Knotengruppe oder eine verwaltete Knotengruppe mit einer Startvorlage bereitstellen, in der Sie eine AMI-ID angegeben haben, müssen Sie die von Amazon EKS empfohlene Anzahl von maximalen Pods für Ihre Knoten ermitteln. Folgen Sie den Anweisungen in den von [Amazon EKS empfohlenen maximalen Pods für jeden EC2 Amazon-Instance-Typ](#) und fügen Sie Schritt 3 `--cni-prefix-delegation-enabled` hinzu. Notieren Sie sich die Ausgabe zur Verwendung in einem späteren Schritt.

### Important

Verwaltete Knotengruppen erzwingen eine maximale Anzahl für den Wert von `maxPods`. Für Instances mit weniger als 30 V ist CPUs die maximale Anzahl 110 und für alle



anderen Instances ist die maximale Anzahl 250. Diese maximale Anzahl wird angewendet, unabhängig davon, ob die Präfixdelegierung aktiviert ist oder nicht.

3. Wenn Sie einen Cluster verwenden IPv6, für den konfiguriert ist, fahren Sie mit dem nächsten Schritt fort.

Geben Sie die Parameter in einer der folgenden Optionen an. Informationen dazu, welche Option für Sie die richtige ist und welchen Wert Sie dafür angeben müssen, finden Sie unter [WARM\\_PREFIX\\_TARGET](#), [WARM\\_IP\\_TARGET](#) und [MINIMUM\\_IP\\_TARGET](#). [GitHub](#)

Sie können die *example values* durch einen Wert größer als Null ersetzen.

- WARM\_PREFIX\_TARGET

```
kubectl set env ds aws-node -n kube-system WARM_PREFIX_TARGET=1
```

- WARM\_IP\_TARGET oder MINIMUM\_IP\_TARGET – Wenn einer der Werte festgelegt ist, überschreibt er alle Werte, die für WARM\_PREFIX\_TARGET festgelegt wurden.

```
kubectl set env ds aws-node -n kube-system WARM_IP_TARGET=5
```

```
kubectl set env ds aws-node -n kube-system MINIMUM_IP_TARGET=2
```

4. Erstellen Sie einen der folgenden Typen von Knotengruppen mit mindestens einem Amazon EC2 Nitro Amazon Linux 2-Instance-Typ. Eine Liste der Nitro-Instance-Typen finden Sie unter [Instances built on the Nitro System](#) im EC2 Amazon-Benutzerhandbuch. Diese Funktion wird unter Windows nicht unterstützt. Für die Optionen, die **110** enthalten, ersetzen Sie es entweder durch den Wert aus Schritt 3 (empfohlen) oder Ihren eigenen Wert.

- Selbstverwaltet — Stellen Sie die Knotengruppe gemäß den Anweisungen unter [Selbstverwaltete Amazon Linux-Knoten erstellen](#) bereit. Geben Sie den folgenden Text für den Parameter an BootstrapArguments.

```
--use-max-pods false --kubelet-extra-args '--max-pods=110'
```

Wenn Sie die Knotengruppe `eksctl` zum Erstellen verwenden, können Sie den folgenden Befehl verwenden.

```
eksctl create nodegroup --cluster my-cluster --managed=false --max-pods-per-node 110
```

- Verwaltet – Stellen Sie Ihre Knotengruppe mit einer der folgenden Optionen bereit:
  - Ohne Startvorlage oder mit einer Startvorlage ohne angegebene AMI-ID — Schließen Sie das Verfahren unter [Erstellen einer verwalteten Knotengruppe für Ihren Cluster](#) ab. Verwaltete Knotengruppen berechnen automatisch den von Amazon EKS empfohlenen max-pods-Wert für Sie.
  - Mit einer Startvorlage mit einer angegebenen AMI-ID – Geben Sie in Ihrer Startvorlage eine Amazon EKS-optimierte AMI-ID oder ein benutzerdefiniertes AMI an, das auf dem Amazon EKS-optimierten AMI basiert, [stellen Sie dann die Knotengruppe mithilfe einer Startvorlage bereit](#) und geben Sie die folgenden Benutzerdaten an in der Startvorlage. Diese Benutzerdaten übergeben Argumente an die `bootstrap.sh`-Datei. Weitere Informationen zur Bootstrap-Datei finden Sie unter [bootstrap.sh](#) auf GitHub.

```
/etc/eks/bootstrap.sh my-cluster \
--use-max-pods false \
--kubenet-extra-args '--max-pods=110'
```

Wenn Sie die Knotengruppe erstellen `eksctl` möchten, können Sie den folgenden Befehl verwenden.

```
eksctl create nodegroup --cluster my-cluster --max-pods-per-node 110
```

Wenn Sie ein benutzerdefiniertes AMI erstellt haben, das nicht auf dem für Amazon EKS optimierten AMI basiert, müssen Sie die Konfiguration selbst anpassen.

#### Note

Wenn Sie Pods auch IP-Adressen aus einem anderen Subnetz als dem der Instance zuweisen möchten, müssen Sie die Funktion in diesem Schritt aktivieren. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Netzwerke”](#).

## Windows

1. Aktivieren Sie die Zuweisung von IP-Präfixen.

- a. Öffnen Sie die `amazon-vpc-cni` ConfigMap zum Bearbeiten.

```
kubectl edit configmap -n kube-system amazon-vpc-cni -o yaml
```

- b. Fügen Sie dem Abschnitt `data` die folgende Zeile hinzu.

```
enable-windows-prefix-delegation: "true"
```

- c. Speichern Sie die Datei und schließen Sie den Editor.
- d. Vergewissern Sie sich, dass die Anmerkung der ConfigMap hinzugefügt wurde.

```
kubectl get configmap -n kube-system amazon-vpc-cni -o "jsonpath={.data.enable-windows-prefix-delegation}"
```

Wenn die zurückgegebene Ausgabe dies nicht ist `true`, liegt möglicherweise ein Fehler vor. Versuchen Sie erneut, den Schritt abzuschließen.

#### Important

Selbst wenn Ihr Subnetz über verfügbare IP-Adressen verfügt, wird im Amazon VPC CNI-Plugin für Kubernetes-Protokolle der folgende Fehler angezeigt, wenn das Subnetz keine zusammenhängenden /28 Blöcke zur Verfügung hat.

```
InsufficientCidrBlocks: The specified subnet does not have enough free cidr blocks to satisfy the request
```

Dies kann aufgrund der Fragmentierung vorhandener sekundärer IP-Adressen auftreten, die über ein Subnetz verteilt sind. Um diesen Fehler zu beheben, erstellen Sie entweder ein neues Subnetz und starten Sie Pods dort, oder verwenden Sie eine CIDR-Reservierung für das EC2 Amazon-Subnetz, um Speicherplatz innerhalb eines Subnetzes für die Verwendung mit Präfixzuweisung zu reservieren. Weitere Informationen erhalten Sie unter [Subnetz-CIDR-Reservierungen](#) im Amazon-VPC-Benutzerhandbuch.

2. (Optional) Geben Sie eine zusätzliche Konfiguration an, um das Verhalten Ihres Clusters vor der Skalierung und der dynamischen Skalierung zu steuern. Weitere Informationen finden Sie unter [Konfigurationsoptionen mit aktiviertem Präfix-Delegierungsmodus](#) unter Windows. GitHub

- a. Öffnen Sie die `amazon-vpc-cni` ConfigMap zum Bearbeiten.

```
kubectl edit configmap -n kube-system amazon-vpc-cni -o yaml
```

- b. Ersetzen Sie die *example values* durch einen Wert größer als Null und fügen Sie die benötigten Einträge zum Abschnitt data der ConfigMap hinzu. Wenn Sie für warm-ip-target oder minimum-ip-target einen Wert festlegen, überschreibt der Wert jeden Wert, der für warm-prefix-target festgelegt wurde.

```
warm-prefix-target: "1"
warm-ip-target: "5"
minimum-ip-target: "2"
```

- c. Speichern Sie die Datei und schließen Sie den Editor.
3. Erstellen Sie Windows-Knotengruppen mit mindestens einem Amazon EC2 Nitro-Instance-Typ. Eine Liste der Nitro-Instance-Typen finden Sie unter [Instances built on the Nitro System](#) im EC2 Amazon-Benutzerhandbuch. Standardmäßig ist die maximale Anzahl von Pods, die Sie auf einem Knoten bereitstellen können, 110. Wenn Sie diese Zahl erhöhen oder verringern möchten, geben Sie in den Benutzerdaten für die Bootstrap-Konfiguration Folgendes an. Ersetzen Sie *max-pods-quantity* durch Ihren Wert für die maximale Anzahl von Pods.

```
-KubeletExtraArgs '--max-pods=max-pods-quantity'
```

Wenn Sie verwaltete Knotengruppen bereitstellen, muss diese Konfiguration der Startvorlage hinzugefügt werden. Weitere Informationen finden Sie unter [the section called "Startvorlagen"](#). Weitere Informationen zu den Konfigurationsparametern für das Windows-Bootstrap-Skript finden Sie unter [the section called "Bootstrap-Skript-Konfigurationsparameter"](#).

Ermitteln Sie die maximale Anzahl an Pods und die verfügbaren IP-Adressen

1. Nachdem Ihre Knoten bereitgestellt wurden, zeigen Sie die Knoten in Ihrem Cluster an.

```
kubectl get nodes
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                                         | STATUS | ROLES  | AGE | VERSION  |
|--------------------------------------------------------------|--------|--------|-----|----------|
| ip-192-168-22-103.region-code.compute.internal<br>eks-6b7464 | Ready  | <none> | 19m | v1.XX.X- |

```
ip-192-168-97-94.region-code.compute.internal Ready <none> 19m v1.XX.X-eks-6b7464
```

2. Beschreiben Sie einen der Knoten, um den Wert von `max-pods` für den Knoten und die Anzahl der verfügbaren IP-Adressen zu bestimmen. Ersetzen Sie **192.168.30.193** durch die IPv4-Adresse im Namen eines Ihrer Knoten, der in der Ausgabe des vorherigen Schritts zurückgegeben wurde.

```
kubectl describe node ip-192-168-30-193.region-code.compute.internal | grep 'pods\|PrivateIPv4Address'
```

Eine Beispielausgabe sieht wie folgt aus.

```
pods: 110
vpc.amazonaws.com/PrivateIPv4Address: 144
```

In der vorherigen Ausgabe 110 ist dies die maximale Anzahl von Pods, die Kubernetes auf dem Knoten bereitstellen wird, obwohl **144** IP-Adressen verfügbar sind.

## Weisen Sie einzelnen Pods Sicherheitsgruppen zu

Gilt für: Linux-Knoten mit EC2 Amazon-Instances

Gilt für: Private Subnetze

Sicherheitsgruppen für Pods integrieren EC2 Amazon-Sicherheitsgruppen in Kubernetes Pods. Sie können EC2 Amazon-Sicherheitsgruppen verwenden, um Regeln zu definieren, die eingehenden und ausgehenden Netzwerkverkehr zu und von Pods zulassen, die Sie auf Knoten bereitstellen, die auf vielen EC2 Amazon-Instance-Typen und Fargate laufen. Eine ausführliche Erläuterung dieser Funktion finden Sie im Blogbeitrag [Einführung in Sicherheitsgruppen für Pods](#).

Kompatibilität mit den Funktionen des Amazon VPC CNI-Plug-ins für Kubernetes-Funktionen

Sie können Sicherheitsgruppen für Pods mit den folgenden Funktionen verwenden:

- IPv4 Übersetzung der Quellnetzwerkadresse — Weitere Informationen finden Sie unter [the section called “Ausgehender Verkehr”](#).
- IPv6 Adressen für Cluster, Pods und Dienste — Weitere Informationen finden Sie unter [the section called “IPv6”](#).

- Den Datenverkehr mithilfe von Kubernetes-Netzwerkrichtlinien einschränken — Weitere Informationen finden Sie unter [the section called “Kubernetes-Richtlinien”](#)

## Überlegungen

Beachten Sie vor der Bereitstellung von Sicherheitsgruppen für Pods die folgenden Einschränkungen und Bedingungen:

- Sicherheitsgruppen für Pods können nicht mit Windows-Knoten verwendet werden.
- Sicherheitsgruppen für Pods können mit Clustern verwendet werden, die für die IPv6 Familie konfiguriert sind und EC2 Amazon-Knoten enthalten. Verwenden Sie dazu Version 1.16.0 oder höher des Amazon VPC CNI-Plug-ins. Sie können Sicherheitsgruppen für Pods mit Clustern verwenden und IPv6 Familien konfigurieren, die nur Fargate-Knoten enthalten, indem Sie Version 1.7.7 oder höher des Amazon VPC CNI-Plug-ins verwenden. Weitere Informationen finden Sie unter [the section called “IPv6”](#).
- Sicherheitsgruppen für Pods werden von den meisten [Nitro-basierten](#) EC2 Amazon-Instance-Familien unterstützt, allerdings nicht von allen Generationen einer Familie. Beispielsweise werden die m5 r6g Instance-Familie und die Instance-Generationen c5 r5 m6gc6g,,, und unterstützt. Es werden keine Instance-Typen in der t-Familie unterstützt. Eine vollständige Liste der unterstützten Instance-Typen finden Sie in der Datei [limits.go](#) unter. GitHub Ihre Knoten müssen von einem der aufgelisteten Instance-Typen sein, die in der Datei mit `IsTrunkingCompatible: true` gekennzeichnet sind.
- Wenn Sie benutzerdefinierte Netzwerk- und Sicherheitsgruppen für Pods zusammen verwenden, wird die in den Sicherheitsgruppen für Pods angegebene Sicherheitsgruppe anstelle der in der angegebenen Sicherheitsgruppe verwendet. `ENIConfig`
- Wenn Sie eine Version 1.10.2 oder eine frühere Version des Amazon VPC CNI-Plug-ins verwenden und die `terminationGracePeriodSeconds` Einstellung in Ihre Pod-Spezifikation aufnehmen, darf der Wert für die Einstellung nicht Null sein.
- Wenn Sie eine Version 1.10 oder eine frühere Version des Amazon VPC CNI-Plug-ins oder eine Version 1.11 mit `POD_SECURITY_GROUP_ENFORCING_MODE = verwendenstrict`, was die Standardeinstellung ist, werden Kubernetes-Services des Typs `NodePort` und die `LoadBalancer` Verwendung von Instance-Zielen mit der `externalTrafficPolicy` Einstellung auf `Local` nicht mit Pods unterstützt, denen Sie Sicherheitsgruppen zuweisen. Weitere Informationen zur Verwendung eines Load Balancers mit Instance-Zielen finden Sie unter [the section called “Netzwerk-Load-Balancer”](#).

- Wenn Sie eine Version 1.10 oder eine frühere Version des Amazon VPC CNI-Plug-ins oder eine Version 1.11 mit `POD_SECURITY_GROUP_ENFORCING_MODE = verwendenstrict`, was die Standardeinstellung ist, ist die Quell-NAT für ausgehenden Datenverkehr von Pods mit zugewiesenen Sicherheitsgruppen deaktiviert, sodass die Regeln für ausgehende Sicherheitsgruppen angewendet werden. Um auf das Internet zuzugreifen, müssen Pods mit zugewiesenen Sicherheitsgruppen auf Knoten gestartet werden, die in einem privaten Subnetz bereitgestellt werden, das mit einem NAT-Gateway oder einer NAT-Instance konfiguriert ist. Pods mit zugewiesenen Sicherheitsgruppen, welche in öffentlichen Subnetzen bereitgestellt werden, können nicht auf das Internet zugreifen.

Wenn Sie die Version 1.11 oder eine neuere Version des Plugins mit `POD_SECURITY_GROUP_ENFORCING_MODE = verwendenstandard`, wird der Pod-Verkehr, der für außerhalb der VPC bestimmt ist, in die IP-Adresse der primären Netzwerkschnittstelle der Instance übersetzt. Für diesen Datenverkehr werden die Regeln in den Sicherheitsgruppen für die primäre Netzwerkschnittstelle verwendet und nicht die Regeln in den Sicherheitsgruppen des Pods.

- Um die Calico-Netzwerkrichtlinie mit Pods zu verwenden, denen Sicherheitsgruppen zugeordnet sind, müssen Sie Version 1.11.0 oder höher des Amazon VPC CNI-Plug-ins verwenden und `= setzen. POD_SECURITY_GROUP_ENFORCING_MODE standard` Andernfalls unterliegt der Verkehrsfluss zu und von Pods mit zugehörigen Sicherheitsgruppen nicht der Durchsetzung der Calico-Netzwerkrichtlinien und ist nur auf die Durchsetzung von EC2 Amazon-Sicherheitsgruppen beschränkt. Informationen zum Aktualisieren Ihrer Version von Amazon VPC CNI finden Sie unter [the section called “Amazon VPC CNI”](#).
- Pods, die auf EC2 Amazon-Knoten ausgeführt werden und Sicherheitsgruppen in Clustern verwenden, die diese verwenden, [NodeLocal DNSCache](#) werden nur mit Version 1.11.0 oder höher des Amazon VPC CNI-Plug-ins und mit `POD_SECURITY_GROUP_ENFORCING_MODE = unterstützt. standard` Informationen zum Aktualisieren Ihrer Version des Amazon-VPC-CNI-Plug-ins finden Sie unter [the section called “Amazon VPC CNI”](#).
- Sicherheitsgruppen für Pods können zu einer höheren Pod-Startlatenz für Pods mit hoher Kundenabwanderung führen. Dies ist auf eine Ratenbegrenzung im Ressourcencontroller zurückzuführen.
- [Der Geltungsbereich der EC2 Sicherheitsgruppe liegt auf Pod-Ebene. Weitere Informationen finden Sie unter Sicherheitsgruppe.](#)

Wenn Sie `POD_SECURITY_GROUP_ENFORCING_MODE=standard` und festlegen `AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, verwendet der Datenverkehr, der für

Endpunkte außerhalb der VPC bestimmt ist, die Sicherheitsgruppen des Knotens, nicht die Sicherheitsgruppen des Pods.

Konfigurieren Sie das Amazon VPC CNI-Plugin für Kubernetes für Sicherheitsgruppen für Amazon EKS Pods

Wenn Sie Pods mit EC2 Amazon-Instances verwenden, müssen Sie das Amazon VPC CNI-Plugin für Kubernetes für Sicherheitsgruppen konfigurieren

Wenn Sie nur Fargate Pods verwenden und keine EC2 Amazon-Knoten in Ihrem Cluster haben, finden Sie weitere Informationen unter [the section called "SecurityGroupPolicy"](#).

1. Überprüfen Sie Ihre aktuelle Version des Amazon VPC CNI-Plug-ins für Kubernetes mit dem folgenden Befehl:

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |
cut -d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.7.6
```

Wenn Ihr Amazon VPC CNI-Plug-In für Kubernetes eine ältere Version als ist `1.7.7`, aktualisieren Sie das Plugin auf Version oder höher. `1.7.7` Weitere Informationen finden Sie unter [the section called "Amazon VPC CNI"](#).

2. Fügen Sie den Link: `iam/home#/policies/arn:aws:iam::aws:policy/AmazonEKSVPCResourceController` [Amazon EKSVPCResource Controller, type="console "] verwaltete IAM-Richtlinie zur [Cluster-Rolle hinzu, die Ihrem Amazon EKS-Cluster zugeordnet](#) ist. Die Richtlinie ermöglicht es der Rolle, Netzwerkschnittstellen, ihre privaten IP-Adressen sowie deren An- und Abkopplung an und von Netzwerk-Instances zu verwalten.
  - a. Rufen Sie den Namen Ihrer Cluster-IAM-Rolle ab und speichern Sie ihn in einer Variablen. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
cluster_role=$(aws eks describe-cluster --name my-cluster --query cluster.roleArn
--output text | cut -d / -f 2)
```

- b. Fügen Sie der Rolle die -Richtlinie an.



```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/
AmazonEKSVPCResourceController --role-name $cluster_role
```

3. Aktivieren Sie das Amazon VPC CNI-Add-on zur Verwaltung von Netzwerkschnittstellen für Pods, indem Sie die `ENABLE_POD_ENI` Variable `true` in der auf setzen. `aws-node` DaemonSet  
Sobald diese Einstellung auf gesetzt ist `true`, erstellt das Add-on für jeden Knoten im Cluster eine `cninode` benutzerdefinierte Ressource. Der VPC-Ressourcen-Controller erstellt und verknüpft eine spezielle Netzwerkschnittstelle, die als Trunk-Netzwerkschnittstelle mit der Beschreibung `aws-k8s-trunk-eni` bezeichnet wird.

```
kubectl set env daemonset aws-node -n kube-system ENABLE_POD_ENI=true
```

#### Note

Die Trunk-Netzwerkschnittstelle ist in der maximalen Anzahl von Netzwerkschnittstellen enthalten, die vom Instance-Typ unterstützt werden. Eine Liste der maximalen Anzahl von Netzwerkschnittstellen, die von jedem Instance-Typ unterstützt werden, finden Sie unter [IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ](#) im EC2 Amazon-Benutzerhandbuch. Wenn an Ihren Knoten bereits die maximale Anzahl an Standardnetzwerkschnittstellen angeschlossen ist, reserviert der VPC-Ressourcencontroller einen Speicherplatz. Sie müssen Ihre laufenden Pods soweit herunterskalieren, dass der Controller eine Standard-Netzwerkschnittstelle trennen und löschen, die Trunk-Netzwerkschnittstelle erstellen und sie mit der Instance verbinden kann.

4. Mit dem folgenden Befehl können Sie ermitteln, welche Ihrer Knoten über eine benutzerdefinierte Ressource vom Typ `CNINode` verfügen. Wenn `No resources found` zurückgegeben wird, warten Sie einige Sekunden und versuchen Sie es dann erneut. Der vorherige Schritt erfordert einen Neustart des Amazon VPC CNI-Plug-ins für Kubernetes Pods, was mehrere Sekunden dauert.

```
kubectl get cninode -A
NAME FEATURES
ip-192-168-64-141.us-west-2.compute.internal [{"name":"SecurityGroupsForPods"}]
ip-192-168-7-203.us-west-2.compute.internal [{"name":"SecurityGroupsForPods"}]
```

Wenn Sie VPC-CNI-Versionen verwenden, die älter als 1.15 sind, wurden anstelle der benutzerdefinierten `CNINode`-Ressource Knotenbezeichnungen verwendet. Mit dem folgenden

Befehl können Sie sehen, auf welchen Ihrer Knoten die Knotenbezeichnung `aws-k8s-trunk-eni` gesetzt `true` ist. Wenn `No resources found` zurückgegeben wird, warten Sie einige Sekunden und versuchen Sie es dann erneut. Der vorherige Schritt erfordert einen Neustart des Amazon VPC CNI-Plug-ins für Kubernetes Pods, was mehrere Sekunden dauert.

```
kubectl get nodes -o wide -l vpc.amazonaws.com/has-trunk-attached=true
-
```

Sobald die Trunk-Netzwerkschnittstelle erstellt ist, werden den Pods sekundäre IP-Adressen aus dem Trunk oder den Standard-Netzwerkschnittstellen zugewiesen. Die Trunk-Schnittstelle wird automatisch gelöscht, wenn der Knoten gelöscht wird.

Wenn Sie in einem späteren Schritt eine Sicherheitsgruppe für einen Pod bereitstellen, erstellt der VPC-Ressourcencontroller eine spezielle Netzwerkschnittstelle, die so genannte Branch-Netzwerkschnittstelle, mit einer Beschreibung der Sicherheitsgruppen `aws-k8s-branch-eni` und ordnet sie ihr zu. Neben den an den Knoten angeschlossenen Standard- und Amtsnetzwerkstellen werden Nebenstellennetzwerkstellen erstellt.

Wenn Sie Verfügbarkeits- oder Bereitschaftstests verwenden, müssen Sie außerdem TCP-Early-Demux deaktivieren, damit sie über TCP eine Verbindung zu Pods auf Zweignetzwerkstellen herstellen können. Führen Sie den folgenden Befehl aus, um TCP-Early-Demux zu deaktivieren:

```
kubectl patch daemonset aws-node -n kube-system \
 -p '{"spec": {"template": {"spec": {"initContainers": [{"env": [{"name": "DISABLE_TCP_EARLY_DEMUX", "value": "true"}], "name": "aws-vpc-cni-init"}]}}}'
```

#### Note

Wenn Sie das Amazon VPC CNI-Plug-In für Kubernetes `1.11.0` oder eine neuere Version verwenden und standard, wie im nächsten Schritt beschrieben, `POD_SECURITY_GROUP_ENFORCING_MODE = seten`, müssen Sie den vorherigen Befehl nicht ausführen.

5. Wenn Ihr Cluster die Calico-Netzwerkrichtlinie für Ihre Pods verwendet `NodeLocal DNSCache`, die über eigene Sicherheitsgruppen verfügen, oder wenn Sie über Kubernetes-Dienste des Typs `NodePort` und Instanzziele `LoadBalancer` verwenden möchten, `Local` für Pods, denen Sie Sicherheitsgruppen zuweisen möchten, verwenden möchten, müssen Sie Version

1.11.0 oder höher des Amazon VPC CNI-Plug-ins für Kubernetes verwenden und die folgende `externalTrafficPolicy` Einstellung aktivieren:

```
kubectl set env daemonset aws-node -n kube-system
 POD_SECURITY_GROUP_ENFORCING_MODE=standard
```

WICHTIG: Pod-Sicherheitsgruppenregeln werden nicht auf den Datenverkehr zwischen Pods oder zwischen Pods und Diensten wie **kubelet** oder **angewendetnodeLocalDNS**, die sich auf demselben Knoten befinden. Pods, die unterschiedliche Sicherheitsgruppen auf demselben Knoten verwenden, können nicht kommunizieren, da sie in unterschiedlichen Subnetzen konfiguriert sind und das Routing zwischen diesen Subnetzen deaktiviert ist. Ausgehender Datenverkehr von Pods zu Adressen außerhalb der VPC ist eine Netzwerkadresse, die in die IP-Adresse der primären Netzwerkschnittstelle der Instance übersetzt wird (sofern Sie dies nicht auch festgelegt `AWS_VPC_K8S_CNI_EXTERNALSNAT=true` haben). Für diesen Datenverkehr werden die Regeln in den Sicherheitsgruppen für die primäre Netzwerkschnittstelle verwendet und nicht die Regeln in den Sicherheitsgruppen des Pods. \*\* Damit diese Einstellung für bestehende Pods gilt, müssen Sie die Pods oder die Knoten, auf denen die Pods ausgeführt werden, neu starten.

6. Informationen zur Verwendung einer Sicherheitsgruppenrichtlinie für Ihren Pod finden Sie unter [the section called “SecurityGroupPolicy”](#).

Verwenden Sie eine Sicherheitsgruppenrichtlinie für einen Amazon EKS-Pod

Um Sicherheitsgruppen für Pods verwenden zu können, müssen Sie über eine bestehende Sicherheitsgruppe verfügen. Die folgenden Schritte zeigen Ihnen, wie Sie die Sicherheitsgruppenrichtlinie für einen Pod verwenden. Sofern nicht anders angegeben, führen Sie alle Schritte von demselben Terminal aus, da in den folgenden Schritten Variablen verwendet werden, die nicht terminalübergreifend gültig sind.

Wenn Sie einen Pod mit EC2 Amazon-Instances haben, müssen Sie das Plugin konfigurieren, bevor Sie dieses Verfahren verwenden. Weitere Informationen finden Sie unter [the section called “Konfiguration”](#).

1. Erstellen Sie einen Kubernetes-Namespace, in dem -Ressourcen bereitgestellt werden sollen. Sie können es *my-namespace* durch den Namen eines Namespaces ersetzen, den Sie verwenden möchten.

```
kubectl create namespace my-namespace
```

## 2. Stellen Sie ein Amazon EKS SecurityGroupPolicy in Ihrem Cluster bereit.

- a. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Sie können es durch *podSelector* ersetzen, *serviceAccountSelector* wenn Sie Pods lieber anhand der Dienstkontobezeichnungen auswählen möchten. Sie müssen den einen oder anderen Selektor angeben. Ein leeres Feld *podSelector* (Beispiel:`podSelector: {}`) wählt alle Pods im Namespace aus. Sie können *my-role* zum Namen Ihrer Rolle wechseln. Ein leeres *serviceAccountSelector* wählt alle Servicekonten im Namespace aus. Sie können ihn *my-security-group-policy* durch einen Namen für sich *SecurityGroupPolicy* und *my-namespace* durch den Namespace ersetzen, *SecurityGroupPolicy* in dem Sie die Datei erstellen möchten.

Sie müssen es *my\_pod\_security\_group\_id* durch die ID einer vorhandenen Sicherheitsgruppe ersetzen. Wenn Sie noch keine Sicherheitsgruppe haben, müssen Sie eine erstellen. Weitere Informationen finden Sie unter [EC2 Amazon-Sicherheitsgruppen für Linux-Instances](#) im [EC2 Amazon-Benutzerhandbuch](#). Sie können eine Sicherheitsgruppe von 1 bis 5 angeben IDs. Wenn Sie mehr als eine ID angeben, gilt die Kombination aller Regeln in allen Sicherheitsgruppen für die ausgewählten Pods.

```
cat >my-security-group-policy.yaml <<EOF
apiVersion: vpcresources.k8s.aws/v1beta1
kind: SecurityGroupPolicy
metadata:
 name: my-security-group-policy
 namespace: my-namespace
spec:
 podSelector:
 matchLabels:
 role: my-role
 securityGroups:
 groupIds:
 - my_pod_security_group_id
EOF
```

### Important

Die Sicherheitsgruppe oder Gruppen, die Sie für Ihre Pods angeben, müssen die folgenden Kriterien erfüllen:

- Sie müssen vorhanden sein. Wenn sie nicht existieren, bleibt Ihr Pod bei der Bereitstellung eines Pods, der dem Selektor entspricht, im Erstellungsprozess hängen. Wenn du den Pod beschreibst, wird dir eine

Fehlermeldung ähnlich der folgenden angezeigt: An error occurred (InvalidSecurityGroupID.NotFound) when calling the CreateNetworkInterface operation: The securityGroup ID '*sg-05b1d815d1EXAMPLE*' does not exist.

- Sie müssen eingehende Kommunikation von der Sicherheitsgruppe, die auf Ihre Knoten (für kubernetes) angewendet wurde, über alle Ports zulassen, für die Sie Sonden konfiguriert haben.
- Sie müssen ausgehende Kommunikation über TCP und UDP Ports 53 zu einer Sicherheitsgruppe zulassen, die den Pods (oder Knoten, auf denen die Pods ausgeführt werden) zugewiesen ist, auf denen CoreDNS ausgeführt wird. Die Sicherheitsgruppe für Ihre CoreDNS-Pods muss eingehenden TCP und UDP Port 53-Verkehr von der von Ihnen angegebenen Sicherheitsgruppe zulassen.
- Sie müssen über die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr verfügen, um mit anderen Pods kommunizieren zu können, mit denen sie kommunizieren müssen.
- Sie müssen über Regeln verfügen, die es den Pods ermöglichen, mit der Kubernetes-Steuerebene zu kommunizieren, wenn Sie die Sicherheitsgruppe mit Fargate verwenden. Am einfachsten erreichen Sie dies, indem Sie die Cluster-Sicherheitsgruppe als eine der Sicherheitsgruppen angeben.

Sicherheitsgruppenrichtlinien gelten nur für neu geplante Pods. Sie wirken sich nicht auf den Betrieb von Pods aus.

b. Die Richtlinie bereitstellen.

```
kubectl apply -f my-security-group-policy.yaml
```

3. Stellen Sie eine Beispielanwendung mit einem Label bereit, die dem *my-role*-Wert für *podSelector* entspricht, den Sie in einem vorherigen Schritt angegeben haben.

- a. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie den *example values* durch Ihren eigenen und führen Sie dann den geänderten Befehl aus. Wenn Sie ersetzen *my-role*, stellen Sie sicher, dass es mit dem Wert übereinstimmt, den Sie in einem vorherigen Schritt für den Selektor angegeben haben.

```
cat >sample-application.yaml <<EOF
apiVersion: apps/v1
kind: Deployment
metadata:
```

```
name: my-deployment
namespace: my-namespace
labels:
 app: my-app
spec:
 replicas: 4
 selector:
 matchLabels:
 app: my-app
 template:
 metadata:
 labels:
 app: my-app
 role: my-role
 spec:
 terminationGracePeriodSeconds: 120
 containers:
 - name: nginx
 image: public.ecr.aws/nginx/nginx:1.23
 ports:
 - containerPort: 80

apiVersion: v1
kind: Service
metadata:
 name: my-app
 namespace: my-namespace
 labels:
 app: my-app
spec:
 selector:
 app: my-app
 ports:
 - protocol: TCP
 port: 80
 targetPort: 80
EOF
```

- b. Stellen Sie die Anwendung mit dem folgenden Befehl bereit. Wenn Sie die Anwendung bereitstellen, entspricht das Amazon VPC CNI-Plugin für Kubernetes dem `role` Label und die Sicherheitsgruppen, die Sie im vorherigen Schritt angegeben haben, werden auf den Pod angewendet.

```
kubectl apply -f sample-application.yaml
```

4. Sehen Sie sich die Pods an, die mit der Beispielanwendung bereitgestellt wurden. Für den Rest dieses Themas wird dieses Terminal als TerminalA bezeichnet.

```
kubectl get pods -n my-namespace -o wide
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                          | READY | STATUS  | RESTARTS  | AGE   | IP              |
|-----------------------------------------------|-------|---------|-----------|-------|-----------------|
| NODE                                          |       |         | NOMINATED | NODE  | READINESS GATES |
| my-deployment-5df6f7687b-4fbjm                | 1/1   | Running | 0         | 7m51s | 192.168.53.48   |
| ip-192-168-33-28.region-code.compute.internal |       |         | <none>    |       | <none>          |
| my-deployment-5df6f7687b-j9fl4                | 1/1   | Running | 0         | 7m51s | 192.168.70.145  |
| ip-192-168-92-33.region-code.compute.internal |       |         | <none>    |       | <none>          |
| my-deployment-5df6f7687b-rjxcz                | 1/1   | Running | 0         | 7m51s | 192.168.73.207  |
| ip-192-168-92-33.region-code.compute.internal |       |         | <none>    |       | <none>          |
| my-deployment-5df6f7687b-zmb42                | 1/1   | Running | 0         | 7m51s | 192.168.63.27   |
| ip-192-168-33-28.region-code.compute.internal |       |         | <none>    |       | <none>          |

### Note

Probieren Sie diese Tipps aus, falls irgendwelche Pods hängen bleiben.

- Wenn irgendwelche Pods im `Waiting` Status feststecken, führen Sie `kubectl describe pod my-deployment-xxxxxxxxxx-xxxxx -n my-namespace`. Wenn Sie `Insufficient permissions: Unable to create Elastic Network Interface` sehen, bestätigen Sie, dass Sie die IAM-Richtlinie in einem vorherigen Schritt zur IAM-Cluster-Rolle hinzugefügt haben.
- Wenn Pods im `Pending` Status hängen bleiben, vergewissern Sie sich, dass Ihr Node-Instance-Typ in [limits.go](https://docs.aws.amazon.com/eks/latest/userguide/limits.html) aufgeführt ist und dass das Produkt aus der maximalen Anzahl der vom Instance-Typ unterstützten Zweignetzwerkschnittstellen multipliziert mit der Anzahl der Knoten in Ihrer Knotengruppe noch nicht erreicht wurde. Eine `m5.large`-Instance unterstützt beispielsweise neun Zweigstellen-Netzwerkschnittstellen. Wenn Ihre Knotengruppe fünf Knoten hat, können maximal 45 Zweigstellen-Netzwerkschnittstellen für die Knotengruppe erstellt werden. Der 46. Pod,

den Sie bereitstellen möchten, bleibt so lange im Pending Status, bis ein anderer Pod gelöscht wird, dem Sicherheitsgruppen zugeordnet sind.

Wenn Sie `kubectl describe pod my-deployment-xxxxxxxxxx-xxxxx -n my-namespace` ausführen und eine Meldung ähnlich der folgenden Meldung angezeigt wird, kann sie problemlos ignoriert werden. Diese Meldung wird möglicherweise angezeigt, wenn das Amazon VPC CNI-Plug-In für Kubernetes versucht, ein Host-Netzwerk einzurichten, und dies bei der Erstellung der Netzwerkschnittstelle fehlschlägt. Das Plug-In protokolliert dieses Ereignis, bis die Netzwerkschnittstelle erstellt wird.

```
Failed to create Pod sandbox: rpc error: code = Unknown desc = failed to set up
sandbox container "e24268322e55c8185721f52df6493684f6c2c3bf4fd59c9c121fd4cdc894579f"
network for Pod "my-deployment-5df6f7687b-4fbjm": networkPlugin
cni failed to set up Pod "my-deployment-5df6f7687b-4fbjm-c89wx_my-namespace" network:
add cmd: failed to assign an IP address to container
```

Sie können die maximale Anzahl von Pods, die auf dem Instance-Typ ausgeführt werden können, nicht überschreiten. Eine Liste der maximalen Anzahl von Pods, die Sie auf jedem Instance-Typ ausführen können, finden Sie unter [eni-max-pods.txt](#) on GitHub. Wenn Sie einen Pod löschen, dem Sicherheitsgruppen zugeordnet sind, oder den Knoten löschen, auf dem der Pod ausgeführt wird, löscht der VPC-Ressourcencontroller die Zweignetzwerkschnittstelle. Wenn Sie einen Cluster mit Pods löschen, die Pods für Sicherheitsgruppen verwenden, löscht der Controller die Netzwerkschnittstellen der Zweigstellen nicht, sodass Sie sie selbst löschen müssen. Informationen zum Löschen von Netzwerkschnittstellen finden Sie unter [Löschen einer Netzwerkschnittstelle](#) im EC2 Amazon-Benutzerhandbuch.

- Öffnen Sie in einem separaten Terminal die Shell in einen der Pods. Für den Rest dieses Themas wird dieses Terminal als TerminalB bezeichnet. `5df6f7687b-4fbjm` Ersetzen Sie es durch die ID eines der Pods, die in Ihrer Ausgabe aus dem vorherigen Schritt zurückgegeben wurden.

```
kubectl exec -it -n my-namespace my-deployment-5df6f7687b-4fbjm -- /bin/bash
```

- Überprüfen Sie in der Shell von TerminalB, dass die Beispielanwendung funktioniert.

```
curl my-app
```

Eine Beispielausgabe sieht wie folgt aus.



```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
[...]
```

Sie haben die Ausgabe erhalten, weil alle Pods, auf denen die Anwendung ausgeführt wird, der Sicherheitsgruppe zugeordnet sind, die Sie erstellt haben. Diese Gruppe enthält eine Regel, die den gesamten Verkehr zwischen allen Pods zulässt, denen die Sicherheitsgruppe zugeordnet ist. DNS-Datenverkehr wird von dieser Sicherheitsgruppe an die Cluster-Sicherheitsgruppe übertragen, die mit Ihren Knoten verknüpft ist. Auf den Knoten werden die CoreDNS-Pods ausgeführt, nach denen Ihre Pods eine Namenssuche durchgeführt haben.

7. Entfernen Sie von TerminalA aus die Sicherheitsgruppenregeln, die die DNS-Kommunikation mit der Cluster-Sicherheitsgruppe ermöglichen, aus Ihrer Sicherheitsgruppe. Wenn Sie die DNS-Regeln nicht in einem vorherigen Schritt zur Cluster-Sicherheitsgruppe hinzugefügt haben, `$my_cluster_security_group_id` ersetzen Sie sie durch die ID der Sicherheitsgruppe, in der Sie die Regeln erstellt haben.

```
aws ec2 revoke-security-group-ingress --group-id $my_cluster_security_group_id --
security-group-rule-ids $my_tcp_rule_id
aws ec2 revoke-security-group-ingress --group-id $my_cluster_security_group_id --
security-group-rule-ids $my_udp_rule_id
```

8. Versuchen Sie über TerminalB noch einmal, auf die Anwendung zuzugreifen.

```
curl my-app
```

Eine Beispielausgabe sieht wie folgt aus.

```
curl: (6) Could not resolve host: my-app
```

Der Versuch schlägt fehl, weil der Pod nicht mehr auf die CoreDNS-Pods zugreifen kann, denen die Cluster-Sicherheitsgruppe zugeordnet ist. Die Cluster-Sicherheitsgruppe verfügt nicht mehr über die Sicherheitsgruppenregeln, die die DNS-Kommunikation von der Sicherheitsgruppe aus zulassen, die Ihrem Pod zugeordnet ist.

Wenn Sie versuchen, mithilfe der IP-Adressen, die in einem vorherigen Schritt für einen der Pods zurückgegeben wurden, auf die Anwendung zuzugreifen, erhalten Sie trotzdem eine Antwort, da alle Ports zwischen Pods zulässig sind, denen die Sicherheitsgruppe zugeordnet ist, und eine Namenssuche nicht erforderlich ist.

9. Sobald Sie mit dem Experimentieren fertig sind, können Sie die Beispielsicherheitsgruppenrichtlinie, die Anwendung und die Sicherheitsgruppe, die Sie erstellt haben, entfernen. Führen Sie die folgenden Befehle über TerminalA aus.

```
kubectl delete namespace my-namespace
aws ec2 revoke-security-group-ingress --group-id $my_pod_security_group_id --
security-group-rule-ids $my_inbound_self_rule_id
wait
sleep 45s
aws ec2 delete-security-group --group-id $my_pod_security_group_id
```

## Schließen Sie mit Multus mehrere Netzwerkschnittstellen an Pods an

Multus CNI ist ein Container-Netzwerkschnittstellen-Plugin (CNI) für Amazon EKS, das das Anhängen mehrerer Netzwerkschnittstellen an einen Pod ermöglicht. Weitere Informationen finden Sie in der [Multus-CNI](#)-Dokumentation auf GitHub.

In Amazon EKS hat jeder Pod eine Netzwerkschnittstelle, die vom Amazon VPC CNI-Plugin zugewiesen wurde. Mit Multus können Sie einen mehrfach vernetzten Pod mit mehreren Schnittstellen erstellen. Dies wird dadurch erreicht, dass Multus als „Meta-Plugin“ fungiert; ein CNI-Plugin, das mehrere andere CNI-Plugins aufrufen kann. AWS Die Unterstützung für Multus wird mit dem Amazon VPC CNI-Plugin als Standard-Delegate-Plugin konfiguriert.

- Amazon EKS wird keine CNI-Plugins für Single Root I/O Virtualization (SR-IOV) und Data Plane Development Kit (DPDK) entwickeln und veröffentlichen. Sie können jedoch eine Paketbeschleunigung erreichen, indem Sie über Multus verwaltete Host-Geräte und Plug-ins eine direkte Verbindung zu Amazon EC2 Elastic Network Adapters (ENA) herstellen. `ipvlan`
- Amazon EKS unterstützt Multus, das einen generischen Prozess bereitstellt, der eine einfache Verkettung zusätzlicher CNI-Plugins ermöglicht. Multus und der Prozess der Verkettung werden unterstützt, bieten jedoch AWS keine Unterstützung für alle kompatiblen CNI-Plugins, die verkettet werden können, oder für Probleme, die bei diesen CNI-Plugins auftreten können, die nichts mit der Verkettungskonfiguration zu tun haben.

- Amazon EKS bietet Support und Lebenszyklusmanagement für das Multus-Plugin, ist jedoch nicht verantwortlich für IP-Adressen oder zusätzliche Verwaltung im Zusammenhang mit den zusätzlichen Netzwerkschnittstellen. Die IP-Adresse und Verwaltung der Standard-Netzwerkschnittstelle, die das Amazon-VPC-CNI-Plugin verwendet, bleibt unverändert.
- Nur das Amazon-VPC-CNI-Plugin wird offiziell als Standard-Delegierungs-Plugin unterstützt. Sie müssen das veröffentlichte Multus-Installationsmanifest ändern, um das Standard-Delegierten-Plugin auf ein alternatives CNI umzukonfigurieren, wenn Sie das Amazon VPC-CNI-Plugin nicht für das primäre Netzwerk verwenden möchten.
- Multus wird nur unterstützt, wenn das Amazon-VPC-CNI als primäres CNI verwendet wird. Wir unterstützen das Amazon-VPC-CNI nicht, wenn es für Schnittstellen höherer Ordnung verwendet wird, sekundär oder anderweitig.
- Um zu verhindern, dass das Amazon VPC CNI-Plugin versucht, zusätzliche Netzwerkschnittstellen zu verwalten, die Pods zugewiesen sind, fügen Sie der Netzwerkschnittstelle das folgende Tag hinzu:

key

: node.k8s.amazonaws.com/no\_manage

Wert

: true

- Multus ist mit Netzwerkrichtlinien kompatibel, die Richtlinie muss jedoch um Ports und IP-Adressen erweitert werden, die Teil zusätzlicher Netzwerkschnittstellen sein können, die an Pods angeschlossen sind.

Eine Einführung in die Implementierung finden Sie im [Multus-Einrichtungsanleitung](#) auf GitHub.

## Alternative CNI-Plugins für Amazon EKS-Cluster

Das [Amazon VPC CNI-Plugin für Kubernetes](#) ist das einzige CNI-Plugin, das von Amazon EKS mit Amazon-Knoten unterstützt wird. EC2 Amazon EKS unterstützt die Kernfunktionen von Cilium und Calico für Amazon EKS-Hybridknoten. Amazon EKS führt Upstream-Kubernetes aus, sodass Sie alternative kompatible CNI-Plugins auf EC2 Amazon-Knoten in Ihrem Cluster installieren können. Wenn Sie Fargate-Knoten in Ihrem Cluster haben, befindet sich das Amazon VPC CNI-Plugin für Kubernetes bereits auf Ihren Fargate-Knoten. Es ist das einzige CNI-Plugin, das Sie mit Fargate-Knoten verwenden können. Ein Versuch, ein alternatives CNI-Plugin auf Fargate-Knoten zu installieren, schlägt fehl.

Wenn Sie beabsichtigen, ein alternatives CNI-Plugin auf EC2 Amazon-Nodes zu verwenden, empfehlen wir Ihnen, kommerziellen Support für das Plugin in Anspruch zu nehmen oder über das interne Fachwissen zu verfügen, um Fehler zu beheben und Korrekturen für das CNI-Plug-in-Projekt vorzunehmen.

Amazon EKS pflegt Beziehungen zu einem Netzwerk von Partnern, die Support für alternative kompatible CNI-Plugins bieten. Einzelheiten zu den Versionen, Qualifizierungen und durchgeführten Tests finden Sie in der folgenden Partnerdokumentation.

| Partner   | Produkt                                                  | Dokumentation                            |
|-----------|----------------------------------------------------------|------------------------------------------|
| Tigera    | <a href="#">Calico</a>                                   | <a href="#">Installationsanleitungen</a> |
| Isovalent | <a href="#">Cilium</a>                                   | <a href="#">Installationsanleitungen</a> |
| Juniper   | <a href="#">Cloud-natives Contrail Networking () CN2</a> | <a href="#">Installationsanleitungen</a> |
| VMware    | <a href="#">Antrea</a>                                   | <a href="#">Installationsanleitungen</a> |

Amazon EKS bemüht sich, Ihnen eine große Auswahl an Optionen zu bieten, um alle Anwendungsfälle abzudecken.

## Alternative kompatible Plug-ins für Netzwerkrichtlinien

[Calico](#) ist eine weit verbreitete Lösung für Container-Netzwerke und Sicherheit. Die Verwendung von Calico auf EKS ermöglicht eine vollständig konforme Durchsetzung der Netzwerkrichtlinien für Ihre EKS-Cluster. Darüber hinaus können Sie sich für das Netzwerk von Calico entscheiden, das IP-Adressen von Ihrer zugrunde liegenden VPC speichert. [Calico Cloud](#) erweitert die Funktionen von Calico Open Source und bietet erweiterte Sicherheits- und Beobachtbarkeitsfunktionen.

Der Datenverkehr zu und von Pods mit zugehörigen Sicherheitsgruppen unterliegt nicht der Durchsetzung von Calico-Netzwerkrichtlinien und ist nur auf die Durchsetzung von Amazon VPC-Sicherheitsgruppen beschränkt.

Wenn Sie die Durchsetzung von Netzwerkrichtlinien in Calico verwenden, empfehlen wir Ihnen, die Umgebungsvariable auf zu setzen, um ein bekanntes Problem mit Kubernetes `ANNOTATE_POD_IP` `true` zu vermeiden. Um diese Funktion nutzen zu können, müssen Sie dem die `patch` Berechtigung

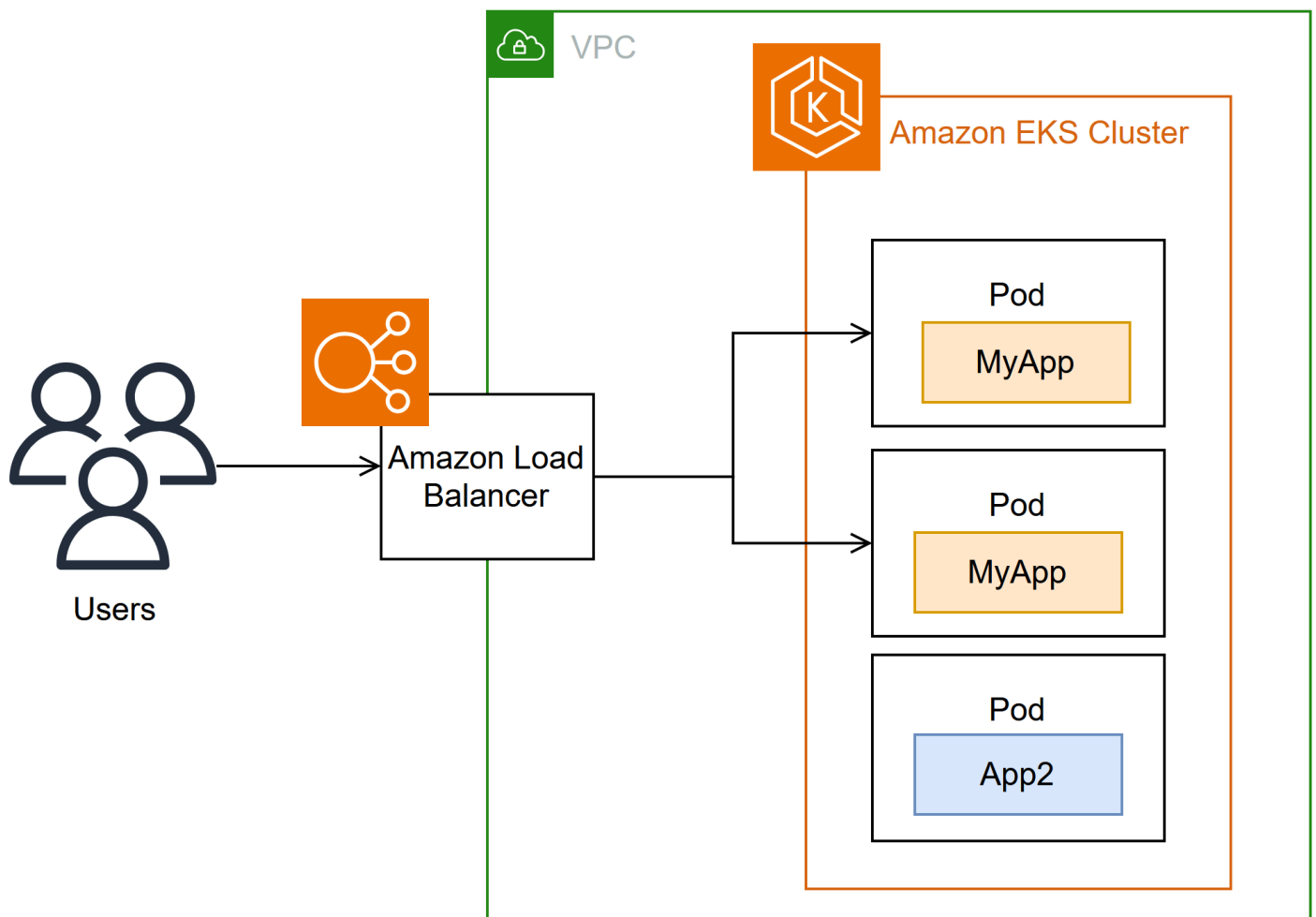
für Pods hinzufügen. `aws-node` ClusterRole Beachten Sie, dass das Hinzufügen von Patch-Berechtigungen den Sicherheitsbereich für das Plugin `aws-node` DaemonSet erhöht. Weitere Informationen finden Sie unter [ANNOTATE\\_POD\\_IP](#) im VPC CNI-Repo unter. GitHub

## Überlegungen zum Amazon EKS Auto Mode

Amazon EKS Auto Mode unterstützt keine alternativen CNI-Plug-ins oder Netzwerkrichtlinien-Plug-ins. Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).

## Internetverkehr mit AWS Load Balancer Controller weiterleiten

Der Load AWS Balancer Controller verwaltet AWS Elastic Load Balancers für einen Kubernetes-Cluster. Sie können den Controller verwenden, um Ihre Cluster-Apps dem Internet zugänglich zu machen. Der Controller stellt AWS Load Balancer bereit, die auf Clusterdienst- oder Ingress-Ressourcen verweisen. Mit anderen Worten, der Controller erstellt eine einzelne IP-Adresse oder einen einzelnen DNS-Namen, der auf mehrere Pods in Ihrem Cluster verweist.



Der Controller sucht nach Kubernetes-Ingress- oder Service-Ressourcen. Als Reaktion darauf erstellt es die entsprechenden AWS Elastic Load Balancing Balancing-Ressourcen. Sie können das spezifische Verhalten der Load Balancer konfigurieren, indem Sie Anmerkungen auf die Kubernetes-Ressourcen anwenden. Sie können beispielsweise mithilfe von Anmerkungen AWS Sicherheitsgruppen an Load Balancer anhängen.

Der Controller stellt die folgenden Ressourcen bereit:

## Kubernetes **Ingress**

Der LBC erstellt einen [AWS Application Load Balancer \(ALB\)](#), wenn Sie ein Kubernetes Ingress [Überprüfen Sie die Anmerkungen, die Sie auf eine Ingress-Ressource anwenden können.](#)

## Kubernetes-Dienst des Typs **LoadBalancer**

Der LBC erstellt einen [AWS Network Load Balancer \(NLB\)](#), wenn Sie einen Kubernetes-Dienst vom Typ erstellen. LoadBalancer [Überprüfen Sie die Anmerkungen, die Sie auf eine Servicereource anwenden können.](#)

In der Vergangenheit wurde der Kubernetes Network Load Balancer für Instanzziele verwendet, aber der LBC wurde für IP-Ziele verwendet. Mit der Load AWS Balancer Controller-Version 2.3.0 oder höher können Sie NLBs mit beiden Zieltypen erstellen. Weitere Informationen zu NLB-Zieltypen finden Sie unter [Zieltyp](#) im Benutzerhandbuch für Network Load Balancer.

Der Controller ist ein [Open-Source-Projekt](#), auf dem verwaltet wird. GitHub

Wir empfehlen Ihnen, sich vor der Bereitstellung des Controllers mit den Voraussetzungen und Überlegungen zur [Weiterleitung von Anwendungs- und HTTP-Verkehr mit Application Load Balancers](#) und vertraut zu machen. [the section called “Netzwerk-Load-Balancer”](#) In diesen Themen stellen Sie eine Beispiel-App bereit, die einen AWS Load Balancer enthält.

## Installieren Sie den Controller

Sie können eines der folgenden Verfahren verwenden, um den Load AWS Balancer Controller zu installieren:

- Wenn Sie Amazon EKS noch nicht kennen, empfehlen wir Ihnen, Helm für die Installation zu verwenden, da dies die Installation des Load AWS Balancer Controllers vereinfacht. Weitere Informationen finden Sie unter [the section called “Mit Helm installieren”](#).

- Verwenden Sie für erweiterte Konfigurationen, wie z. B. Cluster mit eingeschränktem Netzwerkzugriff auf öffentliche Container-Registries, Kubernetes-Manifeste. Weitere Informationen finden Sie unter [the section called “Mit Manifesten installieren”](#).

## Migrieren Sie von veralteten Controller-Versionen

- Wenn Sie veraltete Versionen des Load AWS Balancer Controllers installiert haben, finden Sie weitere Informationen unter [the section called “Migrieren Sie von einer veralteten Version”](#)
- Veraltete Versionen können nicht aktualisiert werden. Sie müssen entfernt und eine aktuelle Version des Load AWS Balancer Controllers installiert werden.
- Zu den veralteten Versionen gehören:
  - AWS ALB Ingress Controller für Kubernetes („Ingress Controller“), ein Vorgänger des Load Balancer Controllers. AWS
  - Beliebige `0.1.x` Version des AWS Load Balancer Controllers

## Legacy-Cloud-Anbieter

Kubernetes beinhaltet einen Legacy-Cloud-Anbieter für AWS. Der ältere Cloud-Anbieter ist in der Lage, AWS Load Balancer bereitzustellen, ähnlich wie der AWS Load Balancer Controller. Der Legacy-Cloud-Anbieter erstellt Classic Load Balancers. Wenn Sie den Load AWS Balancer Controller nicht installieren, verwendet Kubernetes standardmäßig den alten Cloud-Anbieter. Sie sollten den Load AWS Balancer Controller installieren und vermeiden, den alten Cloud-Anbieter zu verwenden.

### Important

In den Versionen 2.5 und neuer wird der Load AWS Balancer Controller mit dem zum Standardcontroller für Kubernetes-Dienstressourcen *type: LoadBalancer* und erstellt für jeden Dienst einen AWS Network Load Balancer (NLB). Dies geschieht durch einen mutierenden Webhook für Services, der das Feld `spec.loadBalancerClass` auf `service.k8s.aws/nlb` für neue Services von `type: LoadBalancer` setzt. Sie können dieses Feature deaktivieren und wieder den [alten Cloud Provider](#) als Standard-Controller verwenden, indem Sie den Wert für den Helm-Chart `enableServiceMutatorWebhook` auf `false` setzen. Der Cluster stellt keine neuen Classic Load Balancer für Ihre Dienste bereit, es sei denn, Sie deaktivieren diese Funktion. Bestehende Classic Load Balancer werden weiterhin funktionieren.

## Installieren Sie den AWS Load Balancer Controller mit Helm



### Tip

Mit Amazon EKS Auto Mode müssen Sie keine Netzwerk-Add-Ons installieren oder aktualisieren. Der automatische Modus umfasst Pod-Netzwerk- und Lastausgleichsfunktionen.

Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).

In diesem Thema wird beschrieben, wie Sie den Load AWS Balancer Controller mit Helm, einem Paketmanager für Kubernetes, und installieren. `eksctl` Der Controller wird mit Standardoptionen installiert. Weitere Informationen zum Controller, einschließlich Einzelheiten zur Konfiguration mit Anmerkungen, finden Sie in der [Load AWS Balancer Controller-Dokumentation](#) unter GitHub

Ersetzen Sie in den folgenden Schritten das *example values* durch Ihre eigenen Werte.

### Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie einen Amazon-EKS-Cluster. Informationen zum Erstellen finden Sie unter [Erste Schritte](#).
- Installieren Sie [Helm](#) auf Ihrem lokalen Computer.
- [Stellen Sie sicher, dass Ihr Amazon VPC CNI-Plug-In für Kubernetes und Ihre kube-proxy CoreDNS-Add-Ons die unter Service-Konto-Tokens aufgeführten Mindestversionen haben.](#)
- Erfahren Sie mehr über die Konzepte von AWS Elastic Load Balancing. Weitere Informationen finden Sie im [Elastic Load Balancing-Benutzerhandbuch](#).
- Erfahren Sie mehr über die [Service](#) - und [Ingress-Ressourcen](#) von Kubernetes.

### Überlegungen

Bevor Sie mit den Konfigurationsschritten auf dieser Seite fortfahren, sollten Sie Folgendes beachten:

- Die IAM-Richtlinie und die Rolle (`AmazonEKSLoadBalancerControllerRole`) können für mehrere EKS-Cluster im selben AWS Konto wiederverwendet werden.
- Wenn Sie den Controller auf demselben Cluster installieren, in dem die Rolle (`AmazonEKSLoadBalancerControllerRole`) ursprünglich erstellt wurde, fahren Sie mit [Schritt](#)



[2: Load Balancer Controller installieren](#) fort, nachdem Sie überprüft haben, ob die Rolle vorhanden ist.

- Wenn Sie IAM Roles for Service Accounts (IRSA) verwenden, muss IRSA für jeden Cluster eingerichtet werden, und der OpenID Connect (OIDC) -Anbieter-ARN in der Vertrauensrichtlinie der Rolle ist für jeden EKS-Cluster spezifisch. Wenn Sie den Controller auf einem neuen Cluster mit einem vorhandenen Cluster installieren `AmazonEKSLoadBalancerControllerRole`, aktualisieren Sie außerdem die Vertrauensrichtlinie der Rolle, sodass sie den OIDC-Anbieter des neuen Clusters einbezieht, und erstellen Sie ein neues Dienstkonto mit der entsprechenden Rollenanmerkung. Informationen darüber, ob Sie bereits einen OIDC-Anbieter haben oder wie Sie einen erstellen können, finden Sie unter [the section called “IAM OIDC-Anbieter”](#)

Schritt 1: Erstellen Sie eine IAM-Rolle mit **eksctl**

Die folgenden Schritte beziehen sich auf die Release-Version des Load AWS Balancer Controller v2.13.0. Weitere Informationen zu allen Versionen finden Sie auf der [Load AWS Balancer Controller-Release-Seite](#) unter GitHub.

1. Laden Sie eine IAM-Richtlinie für den Load AWS Balancer Controller herunter, mit der er in AWS APIs Ihrem Namen Anrufe tätigen kann.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.13.0/docs/install/iam_policy.json
```

- Wenn es sich bei Ihrer Partition um eine nicht standardmäßige AWS Partition handelt, wie z. B. eine Regierung oder eine Region China, [lesen Sie die Richtlinien auf GitHub](#) und laden Sie die entsprechende Richtlinie für Ihre Region herunter.
2. Erstellen Sie eine IAM-Richtlinie mit der im vorherigen Schritt heruntergeladenen Richtlinie.

```
aws iam create-policy \
 --policy-name AWSLoadBalancerControllerIAMPolicy \
 --policy-document file://iam_policy.json
```

#### Note

Wenn Sie sich die Richtlinie in ansehen AWS Management Console, zeigt die Konsole Warnungen für den ELB-Dienst an, aber nicht für den ELB v2-Dienst. Dies liegt daran,

dass einige der Maßnahmen in der Richtlinie für ELB v2, aber nicht für ELB gelten. Sie können diese Warnungen für ELB ignorieren.

### 3. Ersetzen Sie die Werte für Clustername, Regionalcode und Konto-ID.

```
eksctl create iamserviceaccount \
 --cluster=<cluster-name> \
 --namespace=kube-system \
 --name=aws-load-balancer-controller \
 --attach-policy-arn=arn:aws:iam::<AWS_ACCOUNT_ID>:policy/
AWSLoadBalancerControllerIAMPolicy \
 --override-existing-serviceaccounts \
 --region <aws-region-code> \
 --approve
```

## Schritt 2: AWS Load Balancer Controller installieren

### 1. Fügen Sie das eks-charts Helm-Chart-Repository hinzu. AWS unterhält [dieses Repository](#) auf GitHub.

```
helm repo add eks https://aws.github.io/eks-charts
```

### 2. Aktualisieren Sie Ihr lokales Repository, um sicherzustellen, dass Sie über die neuesten Charts verfügen.

```
helm repo update eks
```

### 3. Installieren Sie den AWS Load Balancer Controller.

Wenn Sie den Controller auf EC2 Amazon-Knoten bereitstellen, die [eingeschränkten Zugriff auf den Amazon EC2 Instance Metadata Service \(IMDS\)](#) haben, oder wenn Sie ihn auf Fargate- oder Amazon EKS-Hybridknoten bereitstellen, fügen Sie dem folgenden helm Befehl die folgenden Flags hinzu:

- `--set region=region-code`
- `--set vpcId=vpc-xxxxxxxx`

Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Im folgenden Befehl ist `aws-load-balancer-controller` das Kubernetes-Servicekonto, das Sie in einem vorherigen Schritt erstellt haben.

Weitere Informationen zur Konfiguration des Helmdiagramms finden Sie unter [values.yaml](#) on GitHub

```
helm install aws-load-balancer-controller eks/aws-load-balancer-controller \
 -n kube-system \
 --set clusterName=my-cluster \
 --set serviceAccount.create=false \
 --set serviceAccount.name=aws-load-balancer-controller \
 --version 1.13.0
```

### Important

Das bereitgestellte Diagramm erhält nicht automatisch Sicherheitsupdates. Sie müssen manuell auf ein neueres Diagramm aktualisieren, wenn es verfügbar wird. Wechseln Sie beim Upgrade *install* zum *upgrade* vorherigen Befehl.

Der `helm install` Befehl installiert automatisch die benutzerdefinierten Ressourcendefinitionen (CRDs) für den Controller. Der `helm upgrade` Befehl tut dies nicht. Wenn Sie verwenden `helm upgrade`, müssen Sie das manuell installieren CRDs. Führen Sie den folgenden Befehl aus, um das zu installieren CRDs:

```
wget https://raw.githubusercontent.com/aws/eks-charts/master/stable/aws-load-balancer-controller/crds/crds.yaml
kubectl apply -f crds.yaml
```

Schritt 3: Stellen Sie sicher, dass der Controller installiert ist

1. Stellen Sie sicher, dass der Controller installiert ist.

```
kubectl get deployment -n kube-system aws-load-balancer-controller
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                         | READY | UP-TO-DATE | AVAILABLE | AGE |
|------------------------------|-------|------------|-----------|-----|
| aws-load-balancer-controller | 2/2   | 2          | 2         | 84s |

Sie erhalten die vorherige Ausgabe, wenn Sie mit Helm bereitgestellt haben. Wenn Sie mit dem Kubernetes-Manifest bereitgestellt haben, haben Sie nur ein Replikat.

2. Bevor Sie den Controller zur Bereitstellung von AWS Ressourcen verwenden können, muss Ihr Cluster bestimmte Anforderungen erfüllen. Weitere Informationen erhalten Sie unter [the section called “Application Load Balancing”](#) und [the section called “Netzwerk-Load-Balancer”](#).

## Installieren Sie den AWS Load Balancer Controller mit Manifesten

### Tip

Mit Amazon EKS Auto Mode müssen Sie keine Netzwerk-Add-Ons installieren oder aktualisieren. Der automatische Modus umfasst Pod-Netzwerk- und Lastausgleichsfunktionen.

Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).

In diesem Thema wird beschrieben, wie Sie den Controller installieren, indem Sie Kubernetes-Manifeste herunterladen und anwenden. Sie können die vollständige [Dokumentation](#) für den Controller auf GitHub anzeigen.

Ersetzen Sie in den folgenden Schritten das *example values* durch Ihre eigenen Werte.

### Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie einen Amazon-EKS-Cluster. Informationen zum Erstellen finden Sie unter [Erste Schritte](#).
- Installieren Sie [Helm](#) auf Ihrem lokalen Computer.
- [Stellen Sie sicher, dass Ihr Amazon VPC CNI-Plug-In für Kubernetes und Ihre kube-proxy CoreDNS-Add-Ons die unter Service-Konto-Tokens aufgeführten Mindestversionen haben.](#)
- Erfahren Sie mehr über die Konzepte von AWS Elastic Load Balancing. Weitere Informationen finden Sie im [Elastic Load Balancing-Benutzerhandbuch](#).
- Erfahren Sie mehr über die [Service](#) - und [Ingress-Ressourcen](#) von Kubernetes.

## Überlegungen

Bevor Sie mit den Konfigurationsschritten auf dieser Seite fortfahren, sollten Sie Folgendes beachten:

- Die IAM-Richtlinie und die Rolle (AmazonEKSLoadBalancerControllerRole) können für mehrere EKS-Cluster im selben AWS Konto wiederverwendet werden.
- Wenn Sie den Controller auf demselben Cluster installieren, in dem die Rolle (AmazonEKSLoadBalancerControllerRole) ursprünglich erstellt wurde, fahren Sie mit [Schritt 2: Cert-Manager installieren](#) fort, nachdem Sie überprüft haben, ob die Rolle vorhanden ist.
- Wenn Sie IAM Roles for Service Accounts (IRSA) verwenden, muss IRSA für jeden Cluster eingerichtet werden, und der OpenID Connect (OIDC) -Anbieter-ARN in der Vertrauensrichtlinie der Rolle ist für jeden EKS-Cluster spezifisch. Wenn Sie den Controller auf einem neuen Cluster mit einem vorhandenen Cluster installieren AmazonEKSLoadBalancerControllerRole, aktualisieren Sie außerdem die Vertrauensrichtlinie der Rolle, sodass sie den OIDC-Anbieter des neuen Clusters einbezieht, und erstellen Sie ein neues Dienstkonto mit der entsprechenden Rollenangabe. Informationen darüber, ob Sie bereits einen OIDC-Anbieter haben oder wie Sie einen erstellen können, finden Sie unter [the section called "IAM OIDC-Anbieter"](#)

### Schritt 1: IAM konfigurieren

Die folgenden Schritte beziehen sich auf die Release-Version des Load AWS Balancer Controller v2.11.0. Weitere Informationen zu allen Versionen finden Sie auf der [Load AWS Balancer Controller-Release-Seite](#) unter GitHub.

1. Laden Sie eine IAM-Richtlinie für den Load AWS Balancer Controller herunter, mit der er in AWS APIs Ihrem Namen Anrufe tätigen kann.

#### Example

##### AWS

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/install/iam_policy.json
```

##### AWS GovCloud (US)

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/install/iam_policy_us-gov.json
```

```
mv iam_policy_us-gov.json iam_policy.json
```

2. Erstellen Sie eine IAM-Richtlinie mit der im vorherigen Schritt heruntergeladenen Richtlinie.

```
aws iam create-policy \
 --policy-name AWSLoadBalancerControllerIAMPolicy \
 --policy-document file://iam_policy.json
```

### Note

Wenn Sie sich die Richtlinie in ansehen AWS Management Console, zeigt die Konsole Warnungen für den ELB-Dienst an, aber nicht für den ELB v2-Dienst. Dies liegt daran, dass einige der Maßnahmen in der Richtlinie für ELB v2, aber nicht für ELB gelten. Sie können diese Warnungen für ELB ignorieren.

## Example

### eksctl

- Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters, *111122223333* durch Ihre Konto-ID und führen Sie dann den Befehl aus.

```
eksctl create iamserviceaccount \
 --cluster=my-cluster \
 --namespace=kube-system \
 --name=aws-load-balancer-controller \
 --role-name AmazonEKSLoadBalancerControllerRole \
 --attach-policy-arn=arn:aws:iam::111122223333:policy/
AWSLoadBalancerControllerIAMPolicy \
 --approve
```

## AWS CLI and kubectl

- Rufen Sie die OIDC-Provider-ID Ihres Clusters ab und speichern Sie sie in einer Variablen.

```
oidc_id=$(aws eks describe-cluster --name my-cluster --query
 "cluster.identity.oidc.issuer" --output text | cut -d '/' -f 5)
```

- b. Stellen Sie fest, ob ein IAM-OIDC-Anbieter mit der ID Ihres Clusters bereits in Ihrem Konto vorhanden ist. Sie müssen OIDC sowohl für den Cluster als auch für IAM konfiguriert haben.

```
aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4
```

Wenn die Ausgabe zurückgegeben wird, haben Sie bereits einen IAM-OIDC-Anbieter für Ihren Cluster. Wenn keine Ausgabe erfolgt, müssen Sie einen IAM-OIDC-Anbieter für Ihr Cluster erstellen. Weitere Informationen finden Sie unter [the section called "IAM OIDC-Anbieter"](#).

- c. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie **111122223333** durch Ihre Konto-ID. Ersetzen Sie es **region-code** durch die AWS Region, in der sich Ihr Cluster befindet. Ersetzen Sie **EXAMPLED539D4633E53DE1B71EXAMPLE** mit den im vorherigen Schritt zurückgegebenen Ausgaben.

```
cat >load-balancer-role-trust-policy.json <<EOF
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Federated": "arn:aws:iam::111122223333:oidc-provider/
oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
 },
 "Action": "sts:AssumeRoleWithWebIdentity",
 "Condition": {
 "StringEquals": {
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
 "oidc.eks.region-code.amazonaws.com/id/
EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:aws-
load-balancer-controller"
 }
 }
 }
]
}
EOF
```

- d. Erstellen Sie die IAM-Rolle.

```
aws iam create-role \
```

```
--role-name AmazonEKSLoadBalancerControllerRole \
--assume-role-policy-document file://"load-balancer-role-trust-policy.json"
```

- e. Hängen Sie die erforderliche von Amazon EKS verwaltete IAM-Richtlinie an die IAM-Rolle an. Ersetzen Sie **111122223333** durch Ihre Konto-ID.

```
aws iam attach-role-policy \
 --policy-arn arn:aws:iam::111122223333:policy/
 AWSLoadBalancerControllerIAMPolicy \
 --role-name AmazonEKSLoadBalancerControllerRole
```

- f. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie **111122223333** durch Ihre Konto-ID. Nachdem Sie den Text ersetzt haben, führen Sie den geänderten Befehl aus, um die Datei `aws-load-balancer-controller-service-account.yaml` zu erstellen.

```
cat >aws-load-balancer-controller-service-account.yaml <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
 labels:
 app.kubernetes.io/component: controller
 app.kubernetes.io/name: aws-load-balancer-controller
 name: aws-load-balancer-controller
 namespace: kube-system
 annotations:
 eks.amazonaws.com/role-arn: arn:aws:iam::111122223333:role/
 AmazonEKSLoadBalancerControllerRole
EOF
```

- g. Erstellen Sie das Kubernetes-Servicekonto in Ihrem Cluster. Das angegebene Kubernetes-Dienstkonto `aws-load-balancer-controller` ist mit der IAM-Rolle versehen, die Sie mit dem Namen erstellt haben. **AmazonEKSLoadBalancerControllerRole**

```
kubectl apply -f aws-load-balancer-controller-service-account.yaml
```

## Schritt 2: Installieren **cert-manager**

Installieren Sie `cert-manager` mit einer der beiden folgenden Methoden, um die Zertifikatskonfiguration in die Webhooks einzufügen. Weitere Informationen finden Sie unter [Erste Schritte](#) in der `cert-manager`-Dokumentation.



Wir empfehlen, für die Installation die `quay.io` Container-Registry zu verwenden. `cert-manager`  
Wenn Ihre Knoten keinen Zugriff auf die `quay.io` Container-Registry haben, installieren Sie die  
Installation `cert-manager` mithilfe von Amazon ECR (siehe unten).

## Example

### Quay.io

- a. Wenn die Knoten Zugriff auf die `quay.io`-Container-Registry haben, installieren Sie `cert-manager`, um die Zertifikatskonfiguration in die Webhooks einzufügen.

```
kubectl apply \
 --validate=false \
 -f https://github.com/jetstack/cert-manager/releases/download/v1.13.5/cert-
manager.yaml
```

### Amazon ECR

- a. Installieren Sie `cert-manager` mit einer der beiden folgenden Methoden, um die Zertifikatskonfiguration in die Webhooks einzufügen. Weitere Informationen finden Sie unter [Erste Schritte](#) in der `cert-manager`-Dokumentation.
- b. Laden Sie das Manifest herunter.

```
curl -Lo cert-manager.yaml https://github.com/jetstack/cert-manager/releases/
download/v1.13.5/cert-manager.yaml
```

- c. Rufen Sie die folgenden Images ab und verschieben Sie sie in ein Repository, auf das die Knoten Zugriff haben. Weitere Informationen zum Abrufen, Markieren und Verschieben der Images in ein eigenes Repository finden Sie unter [the section called “Kopieren eines Images in ein Repository”](#).

```
quay.io/jetstack/cert-manager-cainjector:v1.13.5
quay.io/jetstack/cert-manager-controller:v1.13.5
quay.io/jetstack/cert-manager-webhook:v1.13.5
```

- d. Ersetzen Sie `quay.io` im Manifest für die drei Images durch den Namen Ihrer eigenen Registrierung. Der folgende Befehl geht davon aus, dass der Name Ihres privaten Repositories mit dem Namen des Quell-Repositories identisch ist. Ersetzen Sie **`111122223333.dkr.ecr.region-code.amazonaws.com`** durch Ihr privates Register.

```
sed -i.bak -e 's|quay.io|111122223333.dkr.ecr.region-code.amazonaws.com|' ./cert-
manager.yaml
```

#### e. Das Manifest anwenden.

```
kubectl apply \
 --validate=false \
 -f ./cert-manager.yaml
```

### Schritt 3: AWS Load Balancer Controller installieren

1. Laden Sie die Controller-Spezifikation herunter. Weitere Informationen zum Controller finden Sie in der [Dokumentation](#) auf GitHub.

```
curl -Lo v2_11_0_full.yaml https://github.com/kubernetes-sigs/aws-load-balancer-
controller/releases/download/v2.11.0/v2_11_0_full.yaml
```

2. Nehmen Sie die folgenden Änderungen an der Datei vor.
  - a. Wenn Sie die Datei `v2_11_0_full.yaml` heruntergeladen haben, führen Sie den folgenden Befehl aus, um den Abschnitt `ServiceAccount` im Manifest zu entfernen. Wenn Sie diesen Abschnitt nicht entfernen, wird die erforderliche Anmerkung, die Sie in einem vorherigen Schritt zum Dienstkonto gemacht haben, überschrieben. Außerdem wird durch das Entfernen dieses Abschnitts das in einem vorherigen Schritt erstellte Servicekonto beibehalten, wenn Sie den Controller löschen.

```
sed -i.bak -e '690,698d' ./v2_11_0_full.yaml
```

Wenn Sie eine andere Dateiversion heruntergeladen haben, öffnen Sie die Datei in einem Editor und entfernen Sie die folgenden Zeilen.

```
apiVersion: v1
kind: ServiceAccount
metadata:
 labels:
 app.kubernetes.io/component: controller
 app.kubernetes.io/name: aws-load-balancer-controller
name: aws-load-balancer-controller
namespace: kube-system
```

```

```

- b. Ersetzen Sie `your-cluster-name` im Deployment spec-Abschnitt der Datei durch den Namen Ihres Clusters, indem Sie *my-cluster* durch den Namen Ihres Cluster ersetzen.

```
sed -i.bak -e 's|your-cluster-name|my-cluster|' ./v2_11_0_full.yaml
```

- c. Wenn Ihre Knoten keinen Zugriff auf die Amazon ECR-Image-Repositorys von Amazon EKS haben, müssen Sie das folgende Bild abrufen und in ein Repository übertragen, auf das Ihre Knoten Zugriff haben. Weitere Informationen zum Abrufen, Markieren und Verschieben von Images in ein eigenes Repository finden Sie unter [the section called “Kopieren eines Images in ein Repository”](#).

```
public.ecr.aws/eks/aws-load-balancer-controller:v2.11.0
```

Fügen Sie den Namen Ihrer Registrierung zum Manifest hinzu. Der folgende Befehl geht davon aus, dass der Name Ihres privaten Repositorys mit dem Namen des Quell-Repositorys übereinstimmt, und fügt der Datei den Namen Ihrer privaten Registrierung hinzu. Ersetzen Sie *111122223333.dkr.ecr.region-code.amazonaws.com* durch Ihr Register. In dieser Zeile wird davon ausgegangen, dass Sie Ihr privates Repository genauso benannt haben wie das Quell-Repository. Andernfalls ändern Sie den Text `eks/aws-load-balancer-controller` nach den Namen Ihrer privaten Registrierung in den Namen Ihres Repositorys.

```
sed -i.bak -e 's|public.ecr.aws/eks/aws-load-balancer-controller|
111122223333.dkr.ecr.region-code.amazonaws.com/eks/aws-load-balancer-
controller|' ./v2_11_0_full.yaml
```

- d. (Nur für Fargate oder Restricted IMDS erforderlich)

Wenn Sie den Controller auf EC2 Amazon-Knoten bereitstellen, die [eingeschränkten Zugriff auf den Amazon EC2 Instance Metadata Service \(IMDS\)](#) haben, oder wenn Sie ihn auf Fargate- oder Amazon EKS-Hybridknoten bereitstellen, fügen Sie das following parameters unter hinzu. - args:

```
[...]
spec:
 containers:
 - args:
 - --cluster-name=your-cluster-name
 - --ingress-class=alb
```

```
- --aws-vpc-id=vpc-xxxxxxx
- --aws-region=region-code
```

```
[...]
```

3. Wenden Sie die Datei an.

```
kubectl apply -f v2_11_0_full.yaml
```

4. Laden Sie das IngressClass- und IngressClassParams-Manifest in Ihren Cluster herunter.

```
curl -Lo v2_11_0_ingclass.yaml https://github.com/kubernetes-sigs/aws-load-balancer-controller/releases/download/v2.11.0/v2_11_0_ingclass.yaml
```

5. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f v2_11_0_ingclass.yaml
```

Schritt 4: Stellen Sie sicher, dass der Controller installiert ist

1. Stellen Sie sicher, dass der Controller installiert ist.

```
kubectl get deployment -n kube-system aws-load-balancer-controller
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                         | READY | UP-TO-DATE | AVAILABLE | AGE |
|------------------------------|-------|------------|-----------|-----|
| aws-load-balancer-controller | 2/2   | 2          | 2         | 84s |

Sie erhalten die vorherige Ausgabe, wenn Sie mit Helm bereitgestellt haben. Wenn Sie mit dem Kubernetes-Manifest bereitgestellt haben, haben Sie nur ein Replikat.

2. Bevor Sie den Controller zur Bereitstellung von AWS Ressourcen verwenden können, muss Ihr Cluster bestimmte Anforderungen erfüllen. Weitere Informationen erhalten Sie unter [the section called “Application Load Balancing”](#) und [the section called “Netzwerk-Load-Balancer”](#).

## Apps vom veralteten ALB Ingress Controller migrieren

In diesem Thema wird beschrieben, wie Sie von veralteten Controller-Versionen migrieren. Insbesondere wird beschrieben, wie veraltete Versionen des AWS Load Balancer Controllers entfernt werden.

- Veraltete Versionen können nicht aktualisiert werden. Sie müssen sie zuerst entfernen und dann eine aktuelle Version installieren.
- Zu den veralteten Versionen gehören:
  - AWS ALB Ingress Controller für Kubernetes („Ingress Controller“), ein Vorgänger des Load Balancer Controllers. AWS
  - Beliebige `0.1.x` Version des AWS Load Balancer Controllers

Entfernen Sie die veraltete Controller-Version

### Note

Möglicherweise haben Sie die veraltete Version mit Helm oder manuell mit Kubernetes-Manifesten installiert. Führen Sie den Vorgang mit dem Tool aus, mit dem Sie ihn ursprünglich installiert haben.

1. Wenn Sie das `incubator/aws-alb-ingress-controller-Helm-Chart` installiert haben, deinstallieren Sie es.

```
helm delete aws-alb-ingress-controller -n kube-system
```

2. Wenn Sie Version `0.1.x` des `eks-charts/aws-load-balancer-controller-Charts` installiert haben, deinstallieren Sie es. Das Upgrade von der Version `0.1.x` zur Version `1.0.0` funktioniert aufgrund der Inkompatibilität mit der Webhook-API-Version nicht.

```
helm delete aws-load-balancer-controller -n kube-system
```

3. Überprüfen Sie, ob der Controller derzeit installiert ist.

```
kubectl get deployment -n kube-system alb-ingress-controller
```

Dies ist die Ausgabe, wenn der Controller nicht installiert ist.

```
Error from server (NotFound): deployments.apps "alb-ingress-controller" not found
```

Dies ist die Ausgabe, falls der Controller installiert ist.

| NAME                   | READY | UP-TO-DATE | AVAILABLE | AGE  |
|------------------------|-------|------------|-----------|------|
| alb-ingress-controller | 1/1   | 1          | 1         | 122d |

4. Geben Sie die folgenden Befehle ein, um den Controller zu entfernen.

```
kubectl delete -f https://raw.githubusercontent.com/kubernetes-sigs/aws-alb-ingress-controller/v1.1.8/docs/examples/alb-ingress-controller.yaml
kubectl delete -f https://raw.githubusercontent.com/kubernetes-sigs/aws-alb-ingress-controller/v1.1.8/docs/examples/rbac-role.yaml
```

Zum AWS Load Balancer Controller migrieren

Um vom ALB Ingress Controller für Kubernetes zum Load AWS Balancer Controller zu migrieren, müssen Sie:

1. Entfernen Sie den ALB Ingress Controller (siehe oben).
2. [Installieren Sie den AWS Load Balancer Controller.](#)
3. Fügen Sie der vom Load AWS Balancer Controller verwendeten IAM-Rolle eine zusätzliche Richtlinie hinzu. Diese Richtlinie ermöglicht es dem LBC, Ressourcen zu verwalten, die vom ALB Ingress Controller für Kubernetes erstellt wurden.
4. Laden Sie die IAM-Richtlinie herunter. Diese Richtlinie ermöglicht es dem Load AWS Balancer Controller, Ressourcen zu verwalten, die vom ALB Ingress Controller für Kubernetes erstellt wurden. Sie können auch [die Richtlinie anzeigen](#).

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/install/iam_policy_v1_to_v2_additional.json
```

5. Wenn sich Ihr Cluster in den Regionen AWS GovCloud (USA-Ost) oder AWS GovCloud (US-West) befindet, ersetzen Sie ihn durch. AWS `arn:aws:` `arn:aws-us-gov:`

```
sed -i.bak -e 's|arn:aws:|arn:aws-us-gov:|' iam_policy_v1_to_v2_additional.json
```

6. Erstellen Sie die IAM-Richtlinie und notieren Sie den zurückgegebenen ARN.

```
aws iam create-policy \
 --policy-name AWSLoadBalancerControllerAdditionalIAMPolicy \
 --policy-document file://iam_policy_v1_to_v2_additional.json
```

7. Hängen Sie die IAM-Richtlinie an die IAM-Rolle an, die vom AWS Load Balancer Controller verwendet wird. *your-role-name* Ersetzen Sie durch den Namen der Rolle, z. B.

AmazonEKSLoadBalancerControllerRole

Wenn Sie die Rolle `miteksctl`, erstellt haben, öffnen Sie die [AWS CloudFormation Konsole](#) und wählen Sie den eksctl- *my-cluster* - `addon-iamserviceaccount-kube-system - aws-load-balancer-controller` Stack aus, um den Rollennamen zu finden, der erstellt wurde. Wählen Sie die Registerkarte für Resources (Ressourcen). Der Rollename befindet sich in der Spalte Physische ID.

```
aws iam attach-role-policy \
 --role-name your-role-name \
 --policy-arn arn:aws:iam::111122223333:policy/
AWSLoadBalancerControllerAdditionalIAMPolicy
```

## CoreDNS für DNS in Amazon EKS-Clustern verwalten



### Tip

Mit Amazon EKS Auto Mode müssen Sie keine Netzwerk-Add-Ons installieren oder aktualisieren. Der automatische Modus umfasst Pod-Netzwerk- und Lastausgleichsfunktionen.

Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).

CoreDNS ist ein flexibler, erweiterbarer DNS-Server, der als Kubernetes-Cluster-DNS dienen kann. Wenn Sie einen Amazon-EKS-Cluster mit mindestens einem Knoten starten, werden standardmäßig zwei Replikate des CoreDNS-Image bereitgestellt, unabhängig von der Anzahl der in Ihrem Cluster bereitgestellten Knoten. Die CoreDNS-Pods bieten eine Namensauflösung für alle Pods im Cluster. Die CoreDNS-Pods können auf Fargate-Knoten bereitgestellt werden, wenn Ihr Cluster ein [Fargate-Profil](#) mit einem Namespace enthält, der dem Namespace für die CoreDNS entspricht. deployment Weitere Informationen zu CoreDNS finden Sie unter [Verwenden von CoreDNS für die Serviceerkennung](#) in der Kubernetes-Dokumentation.

## CoreDNS-Versionen

In der folgenden Tabelle ist die neueste Version des Amazon EKS-Add-On-Typs für jede Kubernetes-Version aufgeführt.

| Kubernetes-Version | CoreDNS-Version     |
|--------------------|---------------------|
| 1.33               | v1.12.1-eksbuild.2  |
| 1.32               | v1.11.4-eksbuild.14 |
| 1.31               | v1.11.4-eksbuild.14 |
| 1.30               | v1.11.4-eksbuild.14 |
| 1.29               | v1.11.4-eksbuild.14 |
| 1.28               | v1.10.1-eksbuild.18 |
| 1.27               | v1.10.1-eksbuild.18 |
| 1.26               | v1.9.3-eksbuild.22  |

### Important

Wenn Sie dieses Add-on selbst verwalten, stimmen die Versionen in der Tabelle möglicherweise nicht mit den verfügbaren selbstverwalteten Versionen überein. Weitere Hinweise zur Aktualisierung des selbstverwalteten Typs dieses Add-ons finden Sie unter [the section called “Update \(selbst verwaltet\)”](#).

## Wichtige Überlegungen zum CoreDNS-Upgrade

- CoreDNS-Updates verwenden ein PodDisruptionBudget, um die Verfügbarkeit des DNS-Dienstes während des Aktualisierungsvorgangs aufrechtzuerhalten.
- Um die Stabilität und Verfügbarkeit des CoreDNS-Einsatzes zu verbessern, v1.10.1-eksbuild.3 werden Versionen v1.9.3-eksbuild.6 und höher mit einem bereitgestellt. PodDisruptionBudget Wenn Sie eine bestehende Version bereitgestellt



habenPodDisruptionBudget, schlägt Ihr Upgrade auf diese Versionen möglicherweise fehl. Schlägt das Upgrade fehl, sollte das Problem durch Ausführen einer der folgenden Aufgaben gelöst werden:

- Wenn Sie das Upgrade des Amazon-EKS-Add-ons durchführen, entscheiden Sie sich dafür, die vorhandenen Einstellungen als Konfliktlösungsoption zu überschreiben. Wenn Sie andere benutzerdefinierte Einstellungen für das Deployment vorgenommen haben, stellen Sie sicher, dass Sie Ihre Einstellungen vor dem Upgrade sichern, damit Sie Ihre anderen benutzerdefinierten Einstellungen nach dem Upgrade erneut anwenden können.
- Entfernen Sie Ihr vorhandenes PodDisruptionBudget und versuchen Sie das Upgrade erneut.
- In EKS-Add-On-Versionen v1.9.3-eksbuild.3 und höher v1.10.1-eksbuild.6 und höher legt das CoreDNS-Deployment fest, readinessProbe dass der Endpunkt verwendet wird/ready. Dieser Endpunkt ist in der Corefile Konfigurationsdatei für CoreDNS aktiviert.

Wenn Sie ein benutzerdefiniertes Plugin verwendenCorefile, müssen Sie das ready Plugin zur Konfiguration hinzufügen, sodass der /ready Endpunkt in CoreDNS aktiv ist, damit der Test ihn verwenden kann.

- In EKS-Add-On-Versionen v1.9.3-eksbuild.7 und höher sowie v1.10.1-eksbuild.4 und höher können Sie das PodDisruptionBudget ändern. Sie können das Add-on bearbeiten und diese Einstellungen in den optionalen Konfigurationseinstellungen mithilfe der Felder im folgenden Beispiel ändern. Dieses Beispiel zeigt das Standard-PodDisruptionBudget.

```
{
 "podDisruptionBudget": {
 "enabled": true,
 "maxUnavailable": 1
 }
}
```

Sie können maxUnavailable oder festlegenminAvailable, aber Sie können nicht beide in einem einzigen festlegen. PodDisruptionBudget Weitere Informationen zu PodDisruptionBudgets finden Sie unter [Angabe von a PodDisruptionBudget](#) in der Kubernetes-Dokumentation.

Beachten Sie, dass, wenn Sie enabled auf einstellenfalse, der PodDisruptionBudget nicht entfernt wird. Nachdem Sie dieses Feld auf false gesetzt haben, müssen Sie das PodDisruptionBudget-Objekt löschen. Ebenso wird das Add-on PodDisruptionBudget

nicht entfernt, wenn Sie das Add-on nach dem Upgrade auf eine Version mit einem so bearbeiten, dass es eine ältere Version des Add-ons verwendet (das Add-On herabstufen). PodDisruptionBudget Führen Sie den folgenden Befehl aus, um das PodDisruptionBudget zu löschen:

```
kubectl delete poddisruptionbudget coredns -n kube-system
```

- Ändern Sie in EKS-Add-On-Versionen v1.10.1-eksbuild.5 und höher die Standardtoleranz von `node-role.kubernetes.io/master:NoSchedule` auf `node-role.kubernetes.io/control-plane:NoSchedule` um sie an KEP 2067 anzupassen. Weitere Informationen zu KEP 2067 finden Sie unter [KEP-2067: Rename the kubeadm „master“ -Label and taint in den Kubernetes Enhancement Proposals](#) () on. KEPs GitHub

In EKS-Add-On-Versionen v1.8.7-eksbuild.8 und höher v1.9.3-eksbuild.9 und höher sind beide Toleranzen so eingestellt, dass sie mit jeder Kubernetes-Version kompatibel sind.

- In EKS-Add-On-Versionen v1.9.3-eksbuild.11 v1.10.1-eksbuild.7 und höher legt das CoreDNS-Deployment einen Standardwert für `topologySpreadConstraints` fest. Der Standardwert stellt sicher, dass die CoreDNS-Pods über die Availability Zones verteilt sind, wenn Knoten in mehreren Availability Zones verfügbar sind. Sie können einen benutzerdefinierten Wert festlegen, der anstelle des Standardwerts verwendet wird. Der Standardwert lautet wie folgt:

```
topologySpreadConstraints:
 - maxSkew: 1
 topologyKey: topology.kubernetes.io/zone
 whenUnsatisfiable: ScheduleAnyway
 labelSelector:
 matchLabels:
 k8s-app: kube-dns
```

## Überlegungen CoreDNS CoreDNS-Upgrade v1.11

- In EKS-Add-On-Versionen v1.11.1-eksbuild.4 und höher basiert das Container-Image auf einem [minimalen Basis-Image](#), das von Amazon EKS Distro verwaltet wird. Es enthält nur minimale Pakete und keine Shells. Weitere Informationen finden Sie unter [Amazon-EKS-Distro](#). Die Verwendung und Fehlerbehebung des CoreDNS-Images bleibt unverändert.

## Erstellen Sie das CoreDNS Amazon EKS Add-on

Erstellen Sie das CoreDNS Amazon EKS Add-on. Sie müssen über einen Cluster verfügen, bevor Sie das Add-on erstellen können. Weitere Informationen finden Sie unter [the section called “Erstellen eines -Clusters”](#).

1. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist.

```
kubectl describe deployment coredns --namespace kube-system | grep coredns: | cut -d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.10.1-eksbuild.13
```

2. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist. Je nachdem, mit welchem Tool Sie Ihr Cluster erstellt haben, ist der Add-on vom Typ Amazon EKS möglicherweise derzeit nicht auf Ihrem Cluster installiert. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query addon.addonVersion --output text
```

Wenn eine Versionsnummer zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons auf Ihrem Cluster installiert und müssen die verbleibenden Schritte in diesem Verfahren nicht ausführen. Wenn ein Fehler zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Führen Sie die verbleibenden Schritte dieses Prozesses aus, um es zu installieren.

3. Speichern Sie die Konfiguration Ihres aktuell installierten Add-ons ab.

```
kubectl get deployment coredns -n kube-system -o yaml > aws-k8s-coredns-old.yaml
```

4. Erstellen Sie das Add-on mit der AWS CLI. Wenn Sie das AWS Management Console oder verwenden möchten, um das Add-on `eksctl` zu erstellen, finden Sie weitere Informationen unter [the section called “Erstellen Sie ein Add-on”](#) und geben Sie `coredns` den Namen des Add-ons an. Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie bei Bedarf die folgenden Änderungen am Befehl vor, und führen Sie dann den geänderten Befehl aus.

- Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

- Ersetzen Sie `v1.11.3-eksbuild.1` durch die neueste Version, die in der [neuesten Versionstabelle](#) für Ihre Cluster-Version aufgeführt ist.

```
aws eks create-addon --cluster-name my-cluster --addon-name coredns --addon-version v1.11.3-eksbuild.1
```

Wenn Sie benutzerdefinierte Einstellungen auf Ihr aktuelles Add-on angewendet haben, die mit den Standardeinstellungen des Amazon EKS-Add-ons in Konflikt stehen, schlägt die Erstellung möglicherweise fehl. Wenn die Erstellung fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Problembeseitigung unterstützt. Alternativ können Sie den vorherigen Befehl mit `--resolve-conflicts OVERWRITE` ergänzen. Dadurch kann das Add-on alle vorhandenen benutzerdefinierten Einstellungen überschreiben. Sobald Sie das Add-on erstellt haben, können Sie es mit Ihren benutzerdefinierten Einstellungen aktualisieren.

5. Vergewissern Sie sich, dass die neueste Version des Add-ons für die Kubernetes-Version Ihres Clusters zu Ihrem Cluster hinzugefügt wurde. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query addon.addonVersion --output text
```

Es kann einige Sekunden dauern, bis die Erstellung des Add-ons abgeschlossen ist.

Eine Beispielausgabe sieht wie folgt aus.

```
v1.11.3-eksbuild.1
```

6. Wenn Sie benutzerdefinierte Einstellungen für Ihr ursprüngliches Add-on vorgenommen haben, bevor Sie das Add-on vom Typ Amazon EKS erstellt haben, verwenden Sie die Konfiguration, die Sie in einem vorherigen Schritt gespeichert haben, um das Add-on vom Typ Amazon EKS mit Ihren benutzerdefinierten Einstellungen zu aktualisieren. Anweisungen zum Aktualisieren des Add-ons finden Sie unter [the section called “Aktualisieren \(EKS-Add-on\)”](#)

## Aktualisieren Sie das CoreDNS Amazon EKS Add-on

Erstellen Sie das Add-on vom Typ Amazon EKS. Wenn Sie das Amazon EKS-Add-on nicht zu Ihrem Cluster hinzugefügt haben, [fügen Sie es entweder hinzu](#) oder sehen Sie nach [the section called “Update \(selbst verwaltet\)”](#).

Bevor Sie beginnen, lesen Sie sich die Überlegungen zum Upgrade durch. Weitere Informationen finden Sie unter [the section called “Wichtige Überlegungen zum CoreDNS-Upgrade”](#).

1. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist. Ersetzen Sie *my-cluster* mit Ihrem Clusternamen.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query
"addon.addonVersion" --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.10.1-eksbuild.13
```

Wenn die zurückgegebene Version mit der Version für die Kubernetes-Version Ihres Clusters in der [aktuellen Versionstabelle](#) identisch ist, haben Sie die neueste Version bereits auf Ihrem Cluster installiert und müssen den Rest dieses Verfahrens nicht abschließen. Wenn Sie in Ihrer Ausgabe statt einer Versionsnummer eine Fehlermeldung erhalten, ist der Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Sie müssen [das Add-on erstellen](#), bevor Sie es mit diesem Verfahren aktualisieren können.

2. Speichern Sie die Konfiguration Ihres aktuell installierten Add-ons ab.

```
kubectl get deployment coredns -n kube-system -o yaml > aws-k8s-coredns-old.yaml
```

3. Aktualisieren Sie Ihr Add-on mit der AWS CLI. Wenn Sie das AWS Management Console oder verwenden möchten, um das Add-on `eksctl` zu aktualisieren, finden Sie weitere Informationen unter [the section called “Aktualisieren Sie ein Add-on”](#). Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie bei Bedarf die folgenden Änderungen am Befehl vor, und führen Sie dann den geänderten Befehl aus.

- Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
- Ersetzen Sie *v1.11.3-eksbuild.1* durch die neueste Version, die in der [neuesten Versionstabelle](#) für Ihre Cluster-Version aufgeführt ist.
- Die `--resolve-conflicts`*PRESERVE* Option behält die vorhandenen Konfigurationswerte für das Add-on bei. Wenn Sie benutzerdefinierte Werte für Add-On-Einstellungen festgelegt haben und diese Option nicht verwenden, überschreibt Amazon EKS Ihre Werte mit den Standardwerten. Wenn Sie diese Option verwenden, empfehlen wir, dass Sie alle Feld- und Wertänderungen auf einem Nicht-Produktionscluster testen, bevor Sie das Add-on auf Ihrem Produktionscluster aktualisieren. Wenn Sie diesen Wert auf `OVERWRITE` ändern, werden alle

Einstellungen auf die Amazon-EKS-Standardwerte geändert. Wenn Sie benutzerdefinierte Werte für Einstellungen festgelegt haben, werden diese möglicherweise mit den Amazon EKS-Standardwerten überschrieben. Wenn Sie diesen Wert auf `ändernnone` ändern, ändert Amazon EKS den Wert aller Einstellungen nicht, aber das Update schlägt möglicherweise fehl. Wenn das Update fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt.

- Wenn Sie eine Konfigurationseinstellung nicht aktualisieren, entfernen Sie sie `--configuration-values '{"replicaCount":3}'` aus dem Befehl. Wenn Sie eine Konfigurationseinstellung aktualisieren, `"replicaCount":3` ersetzen Sie sie durch die Einstellung, die Sie festlegen möchten. In diesem Beispiel ist die Anzahl der Replikate von CoreDNS auf festgelegt. 3 Der von Ihnen angegebene Wert muss für das Konfigurationsschema gültig sein. Wenn Sie das Konfigurationsschema nicht kennen, führen Sie `aws eks describe-addon-configuration --addon-name coredns --addon-version v1.11.3-eksbuild.1`, führen Sie es aus und `v1.11.3-eksbuild.1` ersetzen Sie es durch die Versionsnummer des Add-ons, für das Sie die Konfiguration sehen möchten. Das Schema wird in der Ausgabe zurückgegeben. Wenn Sie über eine bestehende benutzerdefinierte Konfiguration verfügen, diese alle entfernen und die Werte für alle Einstellungen auf die Amazon EKS-Standardwerte zurücksetzen möchten, entfernen Sie `"replicaCount":3` aus dem Befehl, sodass Sie leer `{}` haben. Weitere Informationen zu den CoreDNS-Einstellungen finden Sie unter [Customizing DNS Service](#) in der Kubernetes-Dokumentation.

```
aws eks update-addon --cluster-name my-cluster --addon-name coredns --addon-version
v1.11.3-eksbuild.1 \
 --resolve-conflicts PRESERVE --configuration-values '{"replicaCount":3}'
```

Es kann einige Sekunden dauern, bis das Update abgeschlossen ist.

4. Vergewissern Sie sich, dass die Add-on-Version aktualisiert wurde. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns
```

Es kann einige Sekunden dauern, bis das Update abgeschlossen ist.

Eine Beispielausgabe sieht wie folgt aus.

```
{
 "addon": {
```

```
{
 "addonName": "coredns",
 "clusterName": "my-cluster",
 "status": "ACTIVE",
 "addonVersion": "v1.11.3-eksbuild.1",
 "health": {
 "issues": []
 },
 "addonArn": "arn:aws:eks:region:111122223333:addon/my-cluster/coredns/d2c34f06-1111-2222-1eb0-24f64ce37fa4",
 "createdAt": "2023-03-01T16:41:32.442000+00:00",
 "modifiedAt": "2023-03-01T18:16:54.332000+00:00",
 "tags": {},
 "configurationValues": "{\"replicaCount\":3}"
}
```

## Aktualisieren Sie das selbstverwaltete CoreDNS Amazon EKS Add-on

### Important

Wir empfehlen, den Amazon-EKS-Typ des Add-Ons zu Ihrem Cluster hinzuzufügen, anstatt den selbstverwalteten Typ des Add-Ons zu verwenden. Falls Sie mit den Unterschieden zwischen den Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#). Weitere Informationen zum Hinzufügen eines Amazon-EKS-Add-ons zu Ihrem Cluster finden Sie unter [the section called “Erstellen Sie ein Add-on”](#). Wenn Sie das Amazon EKS-Add-on nicht verwenden können, empfehlen wir Ihnen, ein Problem mit der Begründung, warum Sie das nicht können, an das [GitHub Container-Roadmap-Repository](#) zu senden.

Bevor Sie beginnen, lesen Sie sich die Überlegungen zum Upgrade durch. Weitere Informationen finden Sie unter [the section called “Wichtige Überlegungen zum CoreDNS-Upgrade”](#).

1. Vergewissern Sie sich, dass Sie das selbstverwaltete Add-On auf Ihrem Cluster installiert haben. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query
addon.addonVersion --output text
```

Wenn Sie eine Fehlermeldung erhalten, wird das Add-On als selbstverwaltetes Add-On auf Ihrem Cluster installiert. Führen Sie die verbleibenden Schritte in diesem Verfahren aus. Wenn Sie eine Versionsnummer zurückgeben, wird der Amazon-EKS-Typ des Add-Ons auf Ihrem Cluster installiert. Um den Amazon EKS-Typ des Add-ons zu aktualisieren, verwenden Sie das Verfahren unter [Aktualisieren des CoreDNS Amazon EKS-Add-ons](#), anstatt dieses Verfahren zu verwenden. Wenn Sie mit den Unterschieden zwischen den Add-On-Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#)

2. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist.

```
kubectl describe deployment coredns -n kube-system | grep Image | cut -d ":" -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.8.7-eksbuild.2
```

3. Wenn Ihre aktuelle CoreDNS-Version v1.5.0 oder höher ist, aber älter als die in der Tabelle mit den [CoreDNS-Versionen](#) aufgeführte Version ist, überspringen Sie diesen Schritt. Wenn Ihre aktuelle Version älter als ist1.5.0, müssen Sie das ConfigMap für CoreDNS so ändern, dass es das Forward-Add-on anstelle des Proxy-Add-Ons verwendet.

- a. Öffnen Sie das ConfigMap mit dem folgenden Befehl.

```
kubectl edit configmap coredns -n kube-system
```

- b. Ersetzen Sie proxy in der folgenden Zeile durch forward. Speichern Sie die Datei und schließen Sie den Editor.

```
proxy . /etc/resolv.conf
```

4. Wenn Sie Ihren Cluster ursprünglich auf Kubernetes 1.17 oder früher bereitgestellt haben, müssen Sie möglicherweise eine nicht mehr eingestellte Zeile aus Ihrem CoreDNS-Manifest entfernen.

#### Important

Sie müssen diesen Schritt abschließen1.7.0, bevor Sie auf die CoreDNS-Version aktualisieren. Es wird jedoch empfohlen, diesen Schritt auch dann abzuschließen, wenn Sie auf eine frühere Version aktualisieren.



- a. Überprüfen Sie, ob Ihr CoreDNS-Manifest die Zeile enthält.

```
kubectl get configmap coredns -n kube-system -o jsonpath='{$.data.Corefile}' |
grep upstream
```

Wenn keine Ausgabe zurückgegeben wird, enthält Ihr Manifest die Zeile nicht und Sie können mit dem nächsten Schritt zur Aktualisierung von CoreDNS fortfahren. Wenn eine Ausgabe zurückgegeben wird, müssen Sie die Zeile entfernen.

- b. Bearbeiten Sie das ConfigMap mit dem folgenden Befehl und entfernen Sie die Zeile in der Datei, die das Wort `upstream` enthält. Ändern Sie sonst nichts in der Datei. Nachdem die Linie entfernt wurde, speichern Sie die Änderungen.

```
kubectl edit configmap coredns -n kube-system -o yaml
```

5. Rufen Sie Ihre aktuelle CoreDNS-Image-Version ab:

```
kubectl describe deployment coredns -n kube-system | grep Image
```

Eine Beispielausgabe sieht wie folgt aus.

```
602401143452.dkr.ecr.region-code.amazonaws.com/eks/coredns:v1.8.7-eksbuild.2
```

6. Wenn Sie auf CoreDNS 1.8.3 oder höher aktualisieren, müssen Sie die `endpointslices` Berechtigung zu Kubernetes hinzufügen. `system:coredns clusterrole`

```
kubectl edit clusterrole system:coredns -n kube-system
```

Fügen Sie die folgenden Zeilen unter den vorhandenen Berechtigungszeilen im `rules`-Abschnitt der Datei hinzu.

```
[...]
- apiGroups:
 - discovery.k8s.io
 resources:
 - endpointslices
 verbs:
 - list
```

```
- watch
[...]
```

7. Aktualisieren Sie das CoreDNS-Add-On, indem Sie die Werte aus der Ausgabe ersetzen **602401143452**, die in einem vorherigen Schritt zurückgegeben wurden. **region-code v1.11.3-eksbuild.1** Ersetzen Sie durch die CoreDNS-Version, die in der [Tabelle mit den neuesten Versionen](#) für Ihre Kubernetes-Version aufgeführt ist.

```
kubectl set image deployment.apps/coredns -n kube-system
coredns=602401143452.dkr.ecr.region-code.amazonaws.com/eks/coredns:v1.11.3-
eksbuild.1
```

Eine Beispielausgabe sieht wie folgt aus.

```
deployment.apps/coredns image updated
```

8. Überprüfen Sie die Container-Image-Version erneut, um sicherzustellen, dass sie auf die Version aktualisiert wurde, die Sie im vorherigen Schritt angegeben haben.

```
kubectl describe deployment coredns -n kube-system | grep Image | cut -d ":" -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.11.3-eksbuild.1
```

## Skalieren Sie CoreDNS-Pods für hohen DNS-Verkehr

Wenn Sie einen Amazon EKS-Cluster mit mindestens einem Knoten starten, wird standardmäßig eine Bereitstellung von zwei Replikaten CoreDNS CoreDNS-Images bereitgestellt, unabhängig von der Anzahl der in Ihrem Cluster bereitgestellten Knoten. Die CoreDNS-Pods bieten eine Namensauflösung für alle Pods im Cluster. Anwendungen verwenden die Namensauflösung, um eine Verbindung zu Pods und Diensten im Cluster sowie zu Diensten außerhalb des Clusters herzustellen. Wenn die Anzahl der Anfragen zur Namensauflösung (Abfragen) von Pods zunimmt, können die CoreDNS-Pods überfordert und langsamer werden und Anfragen ablehnen, die die Pods nicht verarbeiten können.

Um die erhöhte Belastung der CoreDNS-Pods zu bewältigen, sollten Sie ein Autoscaling-System für CoreDNS in Betracht ziehen. Amazon EKS kann die automatische Skalierung der CoreDNS-

Bereitstellung in der EKS-Add-on-Version von CoreDNS verwalten. Dieser CoreDNS-Autoscaler überwacht kontinuierlich den Clusterstatus, einschließlich der Anzahl der Knoten und CPU-Kerne. Basierend auf diesen Informationen passt der Controller die Anzahl der Replikate der CoreDNS-Bereitstellung in einem EKS-Cluster dynamisch an. Diese Funktion funktioniert für CoreDNS v1.9 und höher. Weitere Informationen darüber, welche Versionen mit CoreDNS Autoscaling kompatibel sind, finden Sie im folgenden Abschnitt.

Wir empfehlen, diese Funktion in Verbindung mit anderen [bewährten Methoden für EKS-Cluster-Autoscaling](#) zu verwenden, um die allgemeine Anwendungsverfügbarkeit und die Skalierbarkeit des Clusters zu verbessern.

## Voraussetzungen

Damit Amazon EKS Ihre CoreDNS-Bereitstellung skalieren kann, gibt es drei Voraussetzungen:

- Sie müssen die EKS Add-on-Version von CoreDNS verwenden.
- Auf Ihrem Cluster müssen mindestens die Cluster-Mindestversionen und Plattformversionen ausgeführt werden.
- Auf Ihrem Cluster muss mindestens die Mindestversion des EKS-Add-ons von CoreDNS ausgeführt werden.

## Minimale Cluster-Version

Die automatische Skalierung von CoreDNS erfolgt durch eine neue Komponente in der Cluster-Steuerebene, die von Amazon EKS verwaltet wird. Aus diesem Grund müssen Sie Ihren Cluster auf eine EKS-Version aktualisieren, die die minimale Plattformversion unterstützt, die die neue Komponente enthält.

Ein neuer Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#). Auf dem Cluster muss eine der in der folgenden Tabelle aufgeführten Kubernetes-Versionen und Plattformversionen oder eine spätere Version ausgeführt werden. Beachten Sie, dass alle Kubernetes- und Plattformversionen, die später als die aufgeführten sind, ebenfalls unterstützt werden. Sie können Ihre aktuelle Kubernetes-Version überprüfen, indem Sie den folgenden Befehl durch den Namen Ihres Clusters ersetzen *my-cluster* und dann den geänderten Befehl ausführen:

```
aws eks describe-cluster --name my-cluster --query cluster.version --output text
```

| Kubernetes-Version | Plattformversion |
|--------------------|------------------|
| 1.29.3             | eks.7            |
| 1.28.8             | eks.13           |
| 1.27.12            | eks.17           |
| 1.26.15            | eks.18           |

 Note

Jede Plattformversion späterer Kubernetes-Versionen wird ebenfalls unterstützt, z. B. die Kubernetes-Version ab und ab 1.30 eks.1

## Mindestversion des EKS-Add-ons

| Kubernetes-Version | 1.29                   | 1,28                    | 1,27                    | 1,26                   |
|--------------------|------------------------|-------------------------|-------------------------|------------------------|
|                    | v1.11.1-e<br>ksbuild.9 | v1.10.1-e<br>ksbuild.11 | v1.10.1-e<br>ksbuild.11 | v1.9.3-ek<br>sbuild.15 |

## Konfiguration von CoreDNS Autoscaling in AWS Management Console

1. Stellen Sie sicher, dass Ihr Cluster die Cluster-Mindestversion erreicht oder höher ist.

Amazon EKS aktualisiert Cluster zwischen Plattformversionen derselben Kubernetes-Version automatisch, und Sie können diesen Vorgang nicht selbst starten. Stattdessen können Sie Ihren Cluster auf die nächste Kubernetes-Version aktualisieren, und der Cluster wird auf diese K8s-Version und die neueste Plattformversion aktualisiert.

Neue Kubernetes-Versionen führen oft bedeutende Änderungen ein. Daher empfehlen wir Ihnen, das Verhalten Ihrer Anwendungen zu testen, indem Sie einen separaten Cluster der neuen Kubernetes-Version verwenden, bevor Sie Ihre Produktionscluster aktualisieren.

Um einen Cluster auf eine neue Kubernetes-Version zu aktualisieren, folgen Sie den Anweisungen unter [Bestehenden Cluster auf neue Kubernetes-Version aktualisieren](#).

2. Stellen Sie sicher, dass Sie über das EKS-Add-on für CoreDNS und nicht über das selbstverwaltete CoreDNS-Deployment verfügen.

Je nachdem, mit welchem Tool Sie Ihr Cluster erstellt haben, ist der Add-on vom Typ Amazon EKS möglicherweise derzeit nicht auf Ihrem Cluster installiert. Um zu sehen, welcher Typ des Add-ons auf Ihrem Cluster installiert ist, können Sie den folgenden Befehl ausführen. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query
addon.addonVersion --output text
```

Wenn eine Versionsnummer zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons auf Ihrem Cluster installiert und können mit dem nächsten Schritt fortfahren. Wenn ein Fehler zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Führen Sie die verbleibenden Schritte des Verfahrens aus. [Erstellen Sie das CoreDNS Amazon EKS-Add-on, um die selbstverwaltete Version durch das Amazon EKS-Add-on](#) zu ersetzen.

3. Stellen Sie sicher, dass Ihr EKS-Add-on für CoreDNS eine Version hat, die der Mindestversion von EKS Add-on entspricht oder diese höher ist.

Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist. Sie können den folgenden Befehl einchecken AWS Management Console oder ausführen:

```
kubectl describe deployment coredns --namespace kube-system | grep coredns: | cut -
d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.10.1-eksbuild.13
```

Vergleichen Sie diese Version mit der Mindestversion des EKS Add-ons aus dem vorherigen Abschnitt. Falls erforderlich, aktualisieren Sie das EKS-Add-on auf eine höhere Version, indem Sie das Verfahren [Aktualisieren des CoreDNS Amazon EKS-Add-ons](#) befolgen.

4. Fügen Sie die Autoscaling-Konfiguration zu den optionalen Konfigurationseinstellungen des EKS-Add-ons hinzu.
  - a. Öffnen Sie die [Amazon-EKS-Konsole](#).
  - b. Wählen Sie im linken Navigationsbereich Clusters (Cluster) aus. Wählen Sie anschließend den Namen des Clusters aus, für den Sie das Add-On konfigurieren möchten.
  - c. Wählen Sie die Registerkarte Add-ons.
  - d. Wählen Sie das Feld oben rechts im CoreDNS-Add-On-Feld aus und wählen Sie dann Bearbeiten.
  - e. Gehen Sie auf der Seite CoreDNS konfigurieren wie folgt vor:
    - i. Wählen Sie die Version aus, die Sie verwenden möchten. Wir empfehlen, dieselbe Version wie im vorherigen Schritt beizubehalten und die Version und Konfiguration in separaten Aktionen zu aktualisieren.
    - ii. Erweitern Sie Optionale Konfigurationseinstellungen.
    - iii. Geben Sie den JSON-Schlüssel "autoscaling": und den JSON-Wert eines verschachtelten JSON-Objekts mit einem Schlüssel "enabled": und einem Wert true in das Feld Konfigurationswerte ein. Der resultierende Text muss ein gültiges JSON-Objekt sein. Wenn dieser Schlüssel und dieser Wert die einzigen Daten im Textfeld sind, setzen Sie den Schlüssel und den Wert in geschweifte Klammern { }. Das folgende Beispiel zeigt, dass Autoscaling aktiviert ist:

```
{
 "autoScaling": {
 "enabled": true
 }
}
```

- iv. (Optional) Sie können Mindest- und Höchstwerte angeben, auf die Autoscaling die Anzahl der CoreDNS-Pods skalieren kann.

Das folgende Beispiel zeigt, dass Autoscaling aktiviert ist und alle optionalen Schlüssel Werte haben. Wir empfehlen, dass die Mindestanzahl von CoreDNS-Pods immer größer als 2 ist, um die Stabilität des DNS-Dienstes im Cluster zu gewährleisten.

```
{
 "autoScaling": {
 "enabled": true,
 "minReplicas": 2,

```

```
 "maxReplicas": 10
 }
}
```

- f. Um die neue Konfiguration anzuwenden, indem die CoreDNS-Pods ersetzt werden, wählen Sie Änderungen speichern.

Amazon EKS wendet Änderungen an den EKS-Add-Ons mithilfe eines Rollouts der Kubernetes-Bereitstellung für CoreDNS an. Sie können den Status des Rollouts im Update-Verlauf des Add-ons in und mit verfolgen. AWS Management Console `kubectl rollout status deployment/coredns --namespace kube-system`

`kubectl rollout`that die folgenden Befehle:

```
kubectl rollout

history -- View rollout history
pause -- Mark the provided resource as paused
restart -- Restart a resource
resume -- Resume a paused resource
status -- Show the status of the rollout
undo -- Undo a previous rollout
```

Wenn der Rollout zu lange dauert, macht Amazon EKS den Rollout rückgängig und eine Meldung mit dem Typ Addon-Update und dem Status Fehlgeschlagen wird zum Update-Verlauf des Add-ons hinzugefügt. Um Probleme zu untersuchen, beginnen Sie mit dem Verlauf des Rollouts und führen Sie ihn `kubectl logs` auf einem CoreDNS-Pod aus, um die Protokolle von CoreDNS einzusehen.

5. Wenn der neue Eintrag in der Update-Historie den Status Erfolgreich hat, ist der Rollout abgeschlossen und das Add-on verwendet die neue Konfiguration in allen CoreDNS-Pods. Wenn Sie die Anzahl der Knoten und CPU-Kerne der Knoten im Cluster ändern, skaliert Amazon EKS die Anzahl der Repliken der CoreDNS-Bereitstellung.

## Konfiguration von CoreDNS-Autoscaling in der Befehlszeilenschnittstelle AWS

1. Stellen Sie sicher, dass Ihr Cluster der Cluster-Mindestversion entspricht oder diese übersteigt.

Amazon EKS aktualisiert Cluster zwischen Plattformversionen derselben Kubernetes-Version automatisch, und Sie können diesen Vorgang nicht selbst starten. Stattdessen können Sie Ihren

Cluster auf die nächste Kubernetes-Version aktualisieren, und der Cluster wird auf diese K8s-Version und die neueste Plattformversion aktualisiert.

Neue Kubernetes-Versionen führen oft bedeutende Änderungen ein. Daher empfehlen wir Ihnen, das Verhalten Ihrer Anwendungen zu testen, indem Sie einen separaten Cluster der neuen Kubernetes-Version verwenden, bevor Sie Ihre Produktionscluster aktualisieren.

Um einen Cluster auf eine neue Kubernetes-Version zu aktualisieren, folgen Sie den Anweisungen unter [Bestehenden Cluster auf neue Kubernetes-Version aktualisieren](#).

2. Stellen Sie sicher, dass Sie über das EKS-Add-on für CoreDNS und nicht über das selbstverwaltete CoreDNS-Deployment verfügen.

Je nachdem, mit welchem Tool Sie Ihr Cluster erstellt haben, ist der Add-on vom Typ Amazon EKS möglicherweise derzeit nicht auf Ihrem Cluster installiert. Um zu sehen, welcher Typ des Add-ons auf Ihrem Cluster installiert ist, können Sie den folgenden Befehl ausführen. Ersetzen Sie `my-cluster` mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query
addon.addonVersion --output text
```

Wenn Sie eine Versionsnummer zurückgeben, wird der Amazon-EKS-Typ des Add-ons auf Ihrem Cluster installiert. Wenn ein Fehler zurückgegeben wird, haben Sie den Amazon EKS-Typ des Add-ons nicht auf Ihrem Cluster installiert. Führen Sie die verbleibenden Schritte des Verfahrens aus. [Erstellen Sie das CoreDNS Amazon EKS-Add-on, um die selbstverwaltete Version durch das Amazon EKS-Add-on](#) zu ersetzen.

3. Stellen Sie sicher, dass Ihr EKS-Add-on für CoreDNS eine Version hat, die der Mindestversion von EKS Add-on entspricht oder diese höher ist.

Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist. Sie können den folgenden Befehl einchecken AWS Management Console oder ausführen:

```
kubectl describe deployment coredns --namespace kube-system | grep coredns: | cut -
d : -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.10.1-eksbuild.13
```



Vergleichen Sie diese Version mit der Mindestversion des EKS Add-ons aus dem vorherigen Abschnitt. Falls erforderlich, aktualisieren Sie das EKS-Add-on auf eine höhere Version, indem Sie das Verfahren [Aktualisieren des CoreDNS Amazon EKS-Add-ons](#) befolgen.

4. Fügen Sie die Autoscaling-Konfiguration zu den optionalen Konfigurationseinstellungen des EKS-Add-ons hinzu.

Führen Sie den folgenden AWS CLI-Befehl aus. Ersetzen Sie `my-cluster` durch den Namen Ihres Clusters und den IAM-Rollen-ARN durch die Rolle, die Sie verwenden.

```
aws eks update-addon --cluster-name my-cluster --addon-name coredns \
 --resolve-conflicts PRESERVE --configuration-values '{"autoScaling":
{"enabled":true}}'
```

Amazon EKS wendet Änderungen an den EKS-Add-Ons mithilfe eines Rollouts der Kubernetes-Bereitstellung für CoreDNS an. Sie können den Status des Rollouts im Update-Verlauf des Add-ons in und mit verfolgen. AWS Management Console `kubectl rollout status deployment/coredns --namespace kube-system`

`kubectl rollout`that die folgenden Befehle:

```
kubectl rollout

history -- View rollout history
pause -- Mark the provided resource as paused
restart -- Restart a resource
resume -- Resume a paused resource
status -- Show the status of the rollout
undo -- Undo a previous rollout
```

Wenn der Rollout zu lange dauert, macht Amazon EKS den Rollout rückgängig und eine Meldung mit dem Typ Addon-Update und dem Status Fehlgeschlagen wird zum Update-Verlauf des Add-ons hinzugefügt. Um Probleme zu untersuchen, beginnen Sie mit dem Verlauf des Rollouts und führen Sie ihn `kubectl logs` auf einem CoreDNS-Pod aus, um die Protokolle von CoreDNS einzusehen.

5. (Optional) Sie können Mindest- und Höchstwerte angeben, auf die Autoscaling die Anzahl der CoreDNS-Pods skalieren kann.

Das folgende Beispiel zeigt, dass Autoscaling aktiviert ist und alle optionalen Schlüssel Werte haben. Wir empfehlen, dass die Mindestanzahl von CoreDNS-Pods immer größer als 2 ist, um die Stabilität des DNS-Dienstes im Cluster zu gewährleisten.

```
aws eks update-addon --cluster-name my-cluster --addon-name coredns \
 --resolve-conflicts PRESERVE --configuration-values '{"autoScaling":
{"enabled":true,"minReplicas":2,"maxReplicas":10}}'
```

6. Überprüfen Sie den Status des Updates für das Add-on, indem Sie den folgenden Befehl ausführen:

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns
```

Wenn Sie diese Zeile sehen: "status": "ACTIVE", dann ist der Rollout abgeschlossen und das Add-on verwendet die neue Konfiguration in allen CoreDNS-Pods. Wenn Sie die Anzahl der Knoten und CPU-Kerne der Knoten im Cluster ändern, skaliert Amazon EKS die Anzahl der Replikate der CoreDNS-Bereitstellung.

## Überwachen Sie die Kubernetes-DNS-Auflösung mit CoreDNS-Metriken

CoreDNS als EKS-Add-On macht die Metriken von CoreDNS am Port 9153 im Prometheus-Format im Service verfügbar. kube-dns Sie können Prometheus, den CloudWatch Amazon-Agenten oder ein anderes kompatibles System verwenden, um diese Metriken zu erfassen (zu sammeln).

Ein Beispiel für eine Scrape-Konfiguration, die sowohl mit Prometheus als auch mit dem CloudWatch Agenten kompatibel ist, finden Sie unter [CloudWatch Agentenkonfiguration für Prometheus](#) im Amazon-Benutzerhandbuch. CloudWatch

## kube-proxy In Amazon EKS-Clustern verwalten

### Tip

Mit Amazon EKS Auto Mode müssen Sie keine Netzwerk-Add-Ons installieren oder aktualisieren. Der automatische Modus umfasst Pod-Netzwerk- und Lastausgleichsfunktionen.

Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).

Wir empfehlen, den Amazon-EKS-Typ des Add-Ons zu Ihrem Cluster hinzuzufügen, anstatt den selbstverwalteten Typ des Add-Ons zu verwenden. Falls Sie mit den Unterschieden zwischen den Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#). Weitere Informationen zum Hinzufügen eines Amazon-EKS-Add-ons zu Ihrem Cluster finden Sie unter [the section called “Erstellen Sie ein Add-on”](#). Wenn Sie das Amazon EKS-Add-on nicht verwenden können, empfehlen wir Ihnen, ein Problem mit der Begründung, warum Sie das nicht können, an das [GitHub Container-Roadmap-Repository](#) zu senden.

Das kube-proxy Add-on wird auf jedem EC2 Amazon-Knoten in Ihrem Amazon EKS-Cluster bereitgestellt. Es verwaltet die Netzwerkregeln auf Ihren Knoten und ermöglicht die Netzwerkkommunikation mit Ihren Pods. Das Add-on wird nicht auf Fargate-Knoten in Ihrem Cluster bereitgestellt. Weitere Informationen finden Sie unter [kube-proxy](#) in der Kubernetes-Dokumentation.

## Als Amazon EKS Add-on installieren

### kube-proxy-Versionen

In der folgenden Tabelle ist die neueste Version des Amazon EKS-Add-On-Typs für jede Kubernetes-Version aufgeführt.

| Kubernetes-Version | kube-proxy -Version  |
|--------------------|----------------------|
| 1.33               | v1.33.0-eksbuild.2   |
| 1.32               | v1.32.5-eksbuild.2   |
| 1,31               | v1.31.9-eksbuild.2   |
| 1,30               | v1.30.13-eksbuild.2  |
| 1,29               | v1.29.15-eksbuild.7  |
| 1,28               | v1.28.15-eksbuild.22 |
| 1,27               | v1.27.16-eksbuild.32 |
| 1,26               | v1.26.15-eksbuild.35 |

**Note**

Eine frühere Version der Dokumentation war falsch. kube-proxy-Versionen v1.28.5, v1.27.9, und v1.26.12 sind nicht verfügbar.

Wenn Sie dieses Add-on selbst verwalten, stimmen die Versionen in der Tabelle möglicherweise nicht mit den verfügbaren selbstverwalteten Versionen überein.

## kube-proxy-Container-Image

Das kube-proxy Container-Image basiert auf einem [minimalen Basis-Image](#), das von Amazon EKS Distro verwaltet wird. Es enthält nur wenige Pakete und hat keine Shells. Weitere Informationen finden Sie unter [Amazon-EKS-Distro](#).

In der folgenden Tabelle sind die neuesten verfügbaren selbstverwalteten kube-proxy Container-Image-Versionen für jede Amazon EKS-Cluster-Version aufgeführt.

| Version | kube-proxy                   |
|---------|------------------------------|
| 1.33    | v1.33.0-minimal-eksbuild.2   |
| 1.32    | v1.32.5-minimal-eksbuild.2   |
| 1.31    | v1.31.9-minimal-eksbuild.2   |
| 1.30    | v1.30.13-minimal-eksbuild.2  |
| 1.29    | v1.29.15-minimal-eksbuild.7  |
| 1.28    | v1.28.15-minimal-eksbuild.22 |
| 1.27    | v1.27.16-minimal-eksbuild.32 |
| 1.26    | v1.26.15-minimal-eksbuild.35 |

Wenn Sie ein [Add-on vom Typ Amazon EKS aktualisieren](#), geben Sie eine gültige Amazon-EKS-Add-on-Version an, bei der es sich möglicherweise nicht um eine in dieser Tabelle aufgeführte Version handelt. Dies liegt daran, dass die [Amazon EKS-Add-On-Versionen](#) nicht immer mit den Container-Image-Versionen übereinstimmen, die bei der Aktualisierung des selbstverwalteten Typs dieses Add-

ons angegeben wurden. Wenn Sie den selbstverwalteten Typ dieses Add-ons aktualisieren, geben Sie eine gültige Container-Image-Version an, die in dieser Tabelle aufgeführt ist.

## Aktualisieren Sie das selbstverwaltete Kubernetes-Add-on **kube-proxy**

### Important

Wir empfehlen, den Amazon-EKS-Typ des Add-Ons zu Ihrem Cluster hinzuzufügen, anstatt den selbstverwalteten Typ des Add-Ons zu verwenden. Falls Sie mit den Unterschieden zwischen den Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#). Weitere Informationen zum Hinzufügen eines Amazon-EKS-Add-ons zu Ihrem Cluster finden Sie unter [the section called “Erstellen Sie ein Add-on”](#). Wenn Sie das Amazon EKS-Add-on nicht verwenden können, empfehlen wir Ihnen, ein Problem mit der Begründung, warum Sie das nicht können, an das [GitHub Container-Roadmap-Repository](#) zu senden.

### Voraussetzungen

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#).

### Überlegungen

- Kube-proxy hat auf einem Amazon EKS-Cluster dieselbe [Kompatibilitäts- und Schrägstellungsrichtlinie wie Kubernetes](#). Erfahren Sie, wie Sie die [Kompatibilität der Amazon EKS-Add-On-Version mit einem Cluster überprüfen](#) können.
1. Vergewissern Sie sich, dass Sie das selbstverwaltete Add-On auf Ihrem Cluster installiert haben. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-addon --cluster-name my-cluster --addon-name kube-proxy --query
addon.addonVersion --output text
```

Wenn Sie eine Fehlermeldung erhalten, wird das Add-On als selbstverwaltetes Add-On auf Ihrem Cluster installiert. Die verbleibenden Schritte in diesem Thema beziehen sich auf die Aktualisierung des selbstverwalteten Typs des Add-Ons. Wenn Sie eine Versionsnummer zurückgeben, wird der Amazon-EKS-Typ des Add-Ons auf Ihrem Cluster installiert. Um es zu aktualisieren, verwenden Sie das Verfahren unter [Aktualisieren eines Amazon EKS-Add-](#)

[ons](#), anstatt das Verfahren in diesem Thema zu verwenden. Wenn Sie mit den Unterschieden zwischen den Add-On-Typen nicht vertraut sind, finden Sie weitere Informationen unter [the section called “Amazon-EKS-Add-ons”](#).

2. Sehen Sie, welche Version des Container-Images derzeit auf Ihrem Cluster installiert ist.

```
kubectl describe daemonset kube-proxy -n kube-system | grep Image
```

Eine Beispielausgabe sieht wie folgt aus.

```
Image: 602401143452.dkr.ecr.region-code.amazonaws.com/eks/kube-proxy:v1.29.1-eksbuild.2
```

In der Beispielausgabe *v1.29.1-eksbuild.2* ist die Version auf dem Cluster installiert.

3. Aktualisieren Sie das kube-proxy Add-on, indem Sie *602401143452* und *region-code* durch die Werte aus Ihrer Ausgabe im vorherigen Schritt ersetzen. *v1.30.6-eksbuild.3* Ersetzen Sie sie durch die kube-proxy Version, die in der Tabelle [Letzte verfügbare selbstverwaltete Kube-Proxy-Container-Image-Version für jede Amazon EKS-Cluster-Version](#) aufgeführt ist.

#### Important

Die Manifeste für jeden Image-Typ sind unterschiedlich und zwischen den Standard - und Minimal-Image-Typen nicht kompatibel. Sie müssen denselben Bildtyp wie das vorherige Bild verwenden, damit der Einstiegspunkt und die Argumente übereinstimmen.

```
kubectl set image daemonset.apps/kube-proxy -n kube-system kube-proxy=602401143452.dkr.ecr.region-code.amazonaws.com/eks/kube-proxy:v1.30.6-eksbuild.3
```

Eine Beispielausgabe sieht wie folgt aus.

```
daemonset.apps/kube-proxy image updated
```

4. Vergewissern Sie sich, dass die neue Version jetzt auf Ihrem Cluster installiert ist.

```
kubectl describe daemonset kube-proxy -n kube-system | grep Image | cut -d ":" -f 3
```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.30.0-eksbuild.3
```

5. Wenn Sie Arm and-Knoten im selben Cluster verwenden x86 und Ihr Cluster vor dem 17. August 2020 bereitgestellt wurde. Bearbeiten Sie dann Ihr kube-proxy-Manifest, um einen Knotenselektor für mehrere Hardwarearchitekturen mit dem folgenden Befehl einzuschließen. Dies ist ein einmaliger Vorgang. Nachdem Sie den Selektor zu Ihrem Manifest hinzugefügt haben, müssen Sie ihn nicht jedes Mal hinzufügen, wenn Sie das Add-on aktualisieren. Wenn Ihr Cluster am oder nach dem 17. August 2020 bereitgestellt wurde, ist kube-proxy bereits Multi-Architektur-fähig.

```
kubectl edit -n kube-system daemonset/kube-proxy
```

Fügen Sie der Datei im Editor den folgenden Knotenselektor hinzu und speichern Sie die Datei. Ein Beispiel dafür, wo dieser Text in den Editor eingefügt werden soll, finden Sie in der [CNI-Manifest](#)-Datei auf GitHub. Auf diese Weise kann Kubernetes das richtige Hardware-Image basierend auf der Hardwarearchitektur des Knotens abrufen.

```
- key: "kubernetes.io/arch"
 operator: In
 values:
 - amd64
 - arm64
```

6. Wenn Ihr Cluster ursprünglich mit der Kubernetes-Version 1.14 oder einer späteren Version erstellt wurde, können Sie diesen Schritt überspringen, da er kube-proxy bereits enthalten ist. Affinity Rule Wenn Sie ursprünglich einen Amazon EKS-Cluster mit einer Kubernetes-Version 1.13 oder einer früheren Version erstellt haben und beabsichtigen, Fargate-Knoten in Ihrem Cluster zu verwenden, bearbeiten Sie Ihr kube-proxy Manifest so, dass es eine NodeAffinity Regel enthält, die verhindert, dass kube-proxy Pods auf Fargate-Knoten geplant werden. Dies ist eine einmalige Bearbeitung. Sobald Sie das Affinity Rule zu Ihrem Manifest hinzugefügt haben, müssen Sie es nicht jedes Mal hinzufügen, wenn Sie das Add-on aktualisieren. Bearbeiten Sie Ihre kube-proxy DaemonSet.

```
kubectl edit -n kube-system daemonset/kube-proxy
```

Fügen Sie dem DaemonSet spec Abschnitt der Datei im Editor Folgendes Affinity Rule hinzu und speichern Sie die Datei dann. Ein Beispiel dafür, wo dieser Text in den Editor eingefügt werden soll, finden Sie in der [CNI-Manifest](#)-Datei auf GitHub.

```
- key: eks.amazonaws.com/compute-type
 operator: NotIn
 values:
 - fargate
```



# Erfahren Sie, wie Sie Workloads und Add-Ons für Amazon EKS bereitstellen

Ihre Workloads werden in Containern bereitgestellt, die in Pods in Kubernetes bereitgestellt werden. Ein Pod umfasst einen oder mehrere Container. In der Regel werden ein oder mehrere Pods, die denselben Dienst bereitstellen, in einem Kubernetes-Dienst bereitgestellt. Sobald Sie mehrere Pods bereitgestellt haben, die denselben Dienst bereitstellen, können Sie:

- [Anzeigen von Informationen über die Workloads](#), die auf jedem Ihrer Cluster laufen mithilfe von AWS Management Console ausgeführt wird.
- Skalieren Sie Pods mit dem Kubernetes [Vertical Pod Autoscaler vertikal](#) nach oben oder unten.
- [Mit dem Kubernetes Horizontal Pod Autoscaler können Sie die Anzahl der Pods, die zur Deckung des Bedarfs benötigt werden, horizontal nach oben oder unten skalieren.](#)
- Erstellen Sie einen externen (für Pods, auf die über das Internet zugegriffen werden kann) oder einen internen (für private Pods) [Netzwerk-Loadbalancer, um den Netzwerkverkehr](#) zwischen Pods zu verteilen. Der Load Balancer leitet den Datenverkehr an Layer 4 des OSI-Modells weiter.
- Erstellen Sie einen [Application Load Balancer](#), um den Anwendungsdatenverkehr zwischen Pods zu verteilen. Der Application Load Balancer leitet den Datenverkehr auf Layer 7 des OSI-Modells weiter.
- Wenn Sie mit Kubernetes noch nicht vertraut sind, hilft Ihnen dieses Thema bei der [Bereitstellung einer Beispielanwendung](#).
- Sie können [IP-Adressen einschränken, die einem Service zugewiesen werden können](#) mit externalIPs.

## Stellen Sie eine Beispielanwendung unter Linux bereit

In diesem Thema stellen Sie eine Beispielanwendung für Ihren Cluster auf Linux-Knoten bereit.

### Voraussetzungen

- Ein vorhandener Kubernetes-Cluster mit mindestens einem Knoten. Wenn Sie noch keinen Amazon EKS-Cluster haben, können Sie einen mithilfe einer der Anleitungen unter [bereitstellen Erste Schritte](#).

- `kubectl` auf Ihrem Computer installiert. Weitere Informationen finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- `kubectl` für die Kommunikation mit Ihrem Cluster konfiguriert. Weitere Informationen finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).
- Wenn Sie vorhaben, Ihre Beispiel-Workload in Fargate bereitzustellen, müssen Sie über ein vorhandenes [Fargate-Profil](#) verfügen, das denselben in diesem Tutorial erstellten Namespace enthält, nämlich `eks-sample-app`, es sei denn, Sie ändern den Namen. Wenn Sie einen Cluster mit einem der Leitfäden erstellt haben [Erste Schritte](#), müssen Sie ein neues Profil erstellen oder den Namespace zu Ihrem vorhandenen Profil hinzufügen, da das in den Leitfäden für die ersten Schritte erstellte Profil den in diesem Tutorial verwendeten Namespace nicht spezifiziert. Ihre VPC muss auch über mindestens ein privates Subnetz verfügen.

Obwohl viele Variablen in den folgenden Schritten veränderbar sind, empfehlen wir, Variablenwerte nur zu ändern, wo angegeben. Sobald Sie ein besseres Verständnis von Kubernetes-Pods, Bereitstellungen und Diensten haben, können Sie mit der Änderung anderer Werte experimentieren.

## Namespaces erstellen

Ein Namespace ermöglicht es Ihnen, Ressourcen in Kubernetes zu gruppieren. Weitere Informationen finden Sie unter [Namespaces](#) in der Kubernetes-Dokumentation. Wenn Sie planen, Ihre Beispielanwendung zur [Vereinfachung der Rechenverwaltung mit AWS Fargate](#) bereitzustellen, stellen Sie sicher, dass der Wert für namespace „[Definieren Sie, welche Pods AWS Fargate verwenden, wenn sie gestartet werden](#)“ lautet. `eks-sample-app`

```
kubectl create namespace eks-sample-app
```

## Erstellen Sie eine Kubernetes-Bereitstellung

Erstellen Sie eine Kubernetes-Bereitstellung. Bei dieser Beispielbereitstellung wird ein Container-Image aus einem öffentlichen Repository abgerufen und drei Replikate (einzelne Pods) davon in Ihrem Cluster bereitgestellt. Weitere Informationen finden Sie unter [Bereitstellungen](#) in der Kubernetes-Dokumentation.

1. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `eks-sample-deployment.yaml`. Die Container in der Beispielanwendung verwenden keinen Netzwerkspeicher, aber Sie haben möglicherweise Anwendungen, die dies benötigen. Weitere Informationen finden Sie unter [App-Datenspeicher](#).

- Das `amd64` oder `arm64` values unter dem Schlüssel `kubernetes.io/arch` bedeutet, dass die Anwendung in einer der beiden Hardwarearchitekturen bereitgestellt werden kann (wenn Sie beide in Ihrem Cluster haben). Dies ist möglich, weil dieses Image ein Multi-Architektur-Image ist, aber das sind nicht alle. Sie können die Hardwarearchitektur ermitteln, auf der das Image unterstützt wird, indem Sie sich die [Image-Details](#) im Repository ansehen, aus dem Sie es abrufen. Wenn Sie Images bereitstellen, die einen Hardwarearchitekturtyp nicht unterstützen oder für die das Image nicht bereitgestellt werden soll, entfernen Sie diesen Typ aus dem Manifest. Weitere Informationen finden Sie unter [Bekannte Labels, Anmerkungen und Taints](#) in der Kubernetes-Dokumentation.
- Der Eintrag `kubernetes.io/os: linux` bedeutet, dass, wenn Sie beispielsweise Windows- und Linux-Knoten in Ihrem Cluster hätten, das Image nur auf Linux-Knoten bereitgestellt würde. Weitere Informationen finden Sie unter [Bekannte Labels, Anmerkungen und Taints](#) in der Kubernetes-Dokumentation.

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: eks-sample-linux-deployment
 namespace: eks-sample-app
 labels:
 app: eks-sample-linux-app
spec:
 replicas: 3
 selector:
 matchLabels:
 app: eks-sample-linux-app
 template:
 metadata:
 labels:
 app: eks-sample-linux-app
 spec:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: kubernetes.io/arch
 operator: In
 values:
 - amd64
 - arm64
```

```
containers:
- name: nginx
 image: public.ecr.aws/nginx/nginx:1.23
 ports:
 - name: http
 containerPort: 80
 imagePullPolicy: IfNotPresent
nodeSelector:
 kubernetes.io/os: linux
```

2. Wenden Sie das Bereitstellungs-Manifest auf Ihren Cluster an.

```
kubectl apply -f eks-sample-deployment.yaml
```

## Einen Service erstellen

Mit einem Service können Sie über eine einzige IP-Adresse oder einen einzigen Namen auf alle Replikate zugreifen. Weitere Informationen dazu finden Sie unter [Service](#) in der Kubernetes-Dokumentation. Es ist zwar nicht in der Beispielanwendung implementiert, aber wenn Sie über Anwendungen verfügen, die mit anderen AWS Diensten interagieren müssen, empfehlen wir Ihnen, Kubernetes-Dienstkonten für Ihre Pods zu erstellen und diese mit AWS IAM-Konten zu verknüpfen. Durch die Angabe von Dienstkonten verfügen Ihre Pods nur über die Mindestberechtigungen, die Sie für die Interaktion mit anderen Diensten angeben. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#).

1. Speichern Sie die folgenden Inhalte in einer Datei namens `eks-sample-service.yaml`. Kubernetes weist dem Service eine eigene IP-Adresse zu, auf die nur innerhalb des Clusters zugegriffen werden kann. Um von außerhalb des Clusters auf den Service zuzugreifen, stellen Sie den [AWS Load Balancer Controller](#) bereit, um den [Anwendungs](#)- oder [Netzwerk](#)-Datenverkehr an den Service auszugleichen.

```
apiVersion: v1
kind: Service
metadata:
 name: eks-sample-linux-service
 namespace: eks-sample-app
 labels:
 app: eks-sample-linux-app
spec:
 selector:
```

```

app: eks-sample-linux-app
ports:
 - protocol: TCP
 port: 80
 targetPort: 80

```

2. Wenden Sie das Service-Manifest auf Ihren Cluster an.

```
kubectl apply -f eks-sample-service.yaml
```

## Überprüfen Sie die erstellten Ressourcen

1. Zeigen Sie alle im eks-sample-app-Namespace vorhandenen Ressourcen an.

```
kubectl get all -n eks-sample-app
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                              | READY | STATUS  | RESTARTS | AGE |
|---------------------------------------------------|-------|---------|----------|-----|
| pod/eks-sample-linux-deployment-65b7669776-m6qxz  | 1/1   | Running | 0        | 27m |
| pod/eks-sample-linux-deployment-65b7669776-mmxxvd | 1/1   | Running | 0        | 27m |
| pod/eks-sample-linux-deployment-65b7669776-qzn22  | 1/1   | Running | 0        | 27m |

| NAME                             | TYPE      | CLUSTER-IP  | EXTERNAL-IP | PORT(S) |
|----------------------------------|-----------|-------------|-------------|---------|
| service/eks-sample-linux-service | ClusterIP | 10.100.74.8 | <none>      | 80/TCP  |

| NAME                                        | READY | UP-TO-DATE | AVAILABLE | AGE |
|---------------------------------------------|-------|------------|-----------|-----|
| deployment.apps/eks-sample-linux-deployment | 3/3   | 3          | 3         | 27m |

| NAME                                                   | DESIRED | CURRENT | READY |
|--------------------------------------------------------|---------|---------|-------|
| replicaset.apps/eks-sample-linux-deployment-776d8f8fd8 | 3       | 3       | 3     |

In der Ausgabe sehen Sie den Service und die Bereitstellung, die in den Beispielmanifesten, der vorherigen Schritte, angegeben wurden. Sie sehen auch drei Pods. Dies liegt daran, dass 3 replicas im Beispielmanifest angegeben wurden. Weitere Informationen zu Pods finden Sie unter [Pods](#) in der Kubernetes-Dokumentation. Kubernetes erstellt die replicaset Ressource

automatisch, auch wenn sie nicht in den Beispielmanifesten angegeben ist. Weitere Informationen zu ReplicaSets finden Sie [ReplicaSet](#) in der Kubernetes-Dokumentation.

#### Note

Kubernetes behält die Anzahl der Replikat bei, die im Manifest angegeben sind. Wenn es sich um eine Produktionsbereitstellung handelt und Sie möchten, dass Kubernetes die Anzahl der Replikat horizontal oder die Rechenressourcen für die Pods vertikal skaliert, verwenden Sie dazu die Optionen [Pod-Bereitstellungen skalieren mit horizontalem Pod-Autoscaler](#) und [Pod-Ressourcen anpassen mit vertikalem Pod-Autoscaler](#).

2. Zeigen Sie die Details des bereitgestellten Services an.

```
kubectl -n eks-sample-app describe service eks-sample-linux-service
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name: eks-sample-linux-service
Namespace: eks-sample-app
Labels: app=eks-sample-linux-app
Annotations: <none>
Selector: app=eks-sample-linux-app
Type: ClusterIP
IP Families: <none>
IP: 10.100.74.8
IPs: 10.100.74.8
Port: <unset> 80/TCP
TargetPort: 80/TCP
Endpoints: 192.168.24.212:80,192.168.50.185:80,192.168.63.93:80
Session Affinity: None
Events: <none>
```

In der vorherigen Ausgabe IP: ist der Wert für eine eindeutige IP-Adresse, die von jedem Knoten oder Pod innerhalb des Clusters aus erreicht werden kann, aber nicht von außerhalb des Clusters erreicht werden kann. Die Werte für Endpoints sind IP-Adressen, die den Pods, die Teil des Dienstes sind, innerhalb Ihrer VPC zugewiesen wurden.

3. Zeigen Sie die Details eines der in der Ausgabe aufgeführten Pods an, wenn Sie in einem vorherigen Schritt den [Namespace angezeigt haben](#). `776d8f8fd8-78w66` Ersetzen Sie es durch den Wert, der für einen Ihrer Pods zurückgegeben wurde.

```
kubectl -n eks-sample-app describe pod eks-sample-linux-deployment-65b7669776-m6qxz
```

## Verkürzte Beispielausgabe

```
Name: eks-sample-linux-deployment-65b7669776-m6qxz
Namespace: eks-sample-app
Priority: 0
Node: ip-192-168-45-132.us-west-2.compute.internal/192.168.45.132
[...]
IP: 192.168.63.93
IPs:
 IP: 192.168.63.93
Controlled By: ReplicaSet/eks-sample-linux-deployment-65b7669776
[...]
Conditions:
 Type Status
 Initialized True
 Ready True
 ContainersReady True
 PodScheduled True
[...]
Events:
 Type Reason Age From
 Message

 Normal Scheduled 3m20s default-scheduler
 Successfully assigned eks-sample-app/eks-sample-linux-deployment-65b7669776-m6qxz to
 ip-192-168-45-132.us-west-2.compute.internal
 [...]
```

In der vorherigen Ausgabe **IP:** ist der Wert für eine eindeutige IP, die dem Pod aus dem CIDR-Block zugewiesen wurde, der dem Subnetz zugewiesen ist, in dem sich der Knoten befindet. Wenn Sie es vorziehen, Pods IP-Adressen aus verschiedenen CIDR-Blöcken zuzuweisen, können Sie das Standardverhalten ändern. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Netzwerke”](#). Sie können auch sehen, dass der Kubernetes-Scheduler den Pod auf dem Node mit der IP-Adresse **192.168.45.132** geplant hat.

 Tip

Anstatt die Befehlszeile zu verwenden, können Sie viele Details zu Pods, Diensten, Bereitstellungen und anderen Kubernetes-Ressourcen in der [einsehen](#). AWS Management Console Weitere Informationen finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

## Führen Sie eine Shell auf einem Pod aus

1. Führen Sie eine Shell auf dem Pod aus, die Sie im vorherigen Schritt beschrieben haben, und `65b7669776-m6qxz` ersetzen Sie sie durch die ID eines Ihrer Pods.

```
kubectl exec -it eks-sample-linux-deployment-65b7669776-m6qxz -n eks-sample-app -- /bin/bash
```

2. Sehen Sie sich in der Pod-Shell die Ausgabe des Webserver an, der in einem vorherigen Schritt zusammen mit Ihrer Bereitstellung installiert wurde. Sie müssen nur den Servicenamen angeben. Es wird von CoreDNS, das standardmäßig mit einem Amazon EKS-Cluster bereitgestellt wird, in die IP-Adresse des Dienstes aufgelöst.

```
curl eks-sample-linux-service
```

Eine Beispielausgabe sieht wie folgt aus.

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
[...]
```

3. Zeigen Sie in der Pod-Shell den DNS-Server für den Pod an.

```
cat /etc/resolv.conf
```

Eine Beispielausgabe sieht wie folgt aus.

```
nameserver 10.100.0.10
```



```
search eks-sample-app.svc.cluster.local svc.cluster.local cluster.local us-
west-2.compute.internal
options ndots:5
```

In der vorherigen Ausgabe wird `10.100.0.10` automatisch als nameserver für alle Pods zugewiesen, die im Cluster bereitgestellt werden.

4. Trennen Sie die Verbindung mit dem Pod, indem Sie `exit` eingeben.
5. Sobald Sie mit der Beispielanwendung fertig sind, können Sie den Beispiel-Namespace, den Service und die Bereitstellung mit dem folgenden Befehl entfernen.

```
kubectl delete namespace eks-sample-app
```

## Nächste Schritte

Nachdem Sie die Beispielanwendung bereitgestellt haben, möchten Sie vielleicht einige der folgenden Übungen ausprobieren:

- [Leiten Sie Anwendungs- und HTTP-Verkehr mit Application Load Balancers weiter](#)
- [Leiten Sie TCP- und UDP-Verkehr mit Network Load Balancers weiter](#)

## Stellen Sie eine Beispielanwendung unter Windows bereit

In diesem Thema stellen Sie eine Beispielanwendung auf Ihrem Cluster auf Windows-Knoten bereit.

### Voraussetzungen

- Ein vorhandener Kubernetes-Cluster mit mindestens einem Knoten. Wenn Sie noch keinen Amazon EKS-Cluster haben, können Sie einen mithilfe einer der Anleitungen unter [bereitstellenErste Schritte](#). Sie müssen die [Windows-Unterstützung](#) für Ihren Cluster und mindestens einen Amazon EC2 Windows-Knoten aktiviert haben.
- `kubectl` auf Ihrem Computer installiert. Weitere Informationen finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- `kubectl` für die Kommunikation mit Ihrem Cluster konfiguriert. Weitere Informationen finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).
- Wenn Sie vorhaben, Ihre Beispiel-Workload in Fargate bereitzustellen, müssen Sie über ein vorhandenes [Fargate-Profil](#) verfügen, das denselben in diesem Tutorial erstellten Namespace

enthält, nämlich `eks-sample-app`, es sei denn, Sie ändern den Namen. Wenn Sie einen Cluster mit einer der Anleitungen erstellt haben [Erste Schritte](#), müssen Sie ein neues Profil erstellen oder den Namespace zu Ihrem vorhandenen Profil hinzufügen, da das in den Handbüchern für die ersten Schritte erstellte Profil den in diesem Tutorial verwendeten Namespace nicht spezifiziert. Ihre VPC muss auch über mindestens ein privates Subnetz verfügen.

Obwohl viele Variablen in den folgenden Schritten veränderbar sind, empfehlen wir, Variablenwerte nur zu ändern, wo angegeben. Sobald Sie ein besseres Verständnis von Kubernetes-Pods, Bereitstellungen und Diensten haben, können Sie mit der Änderung anderer Werte experimentieren.

## Namespaces erstellen

Ein Namespace ermöglicht es Ihnen, Ressourcen in Kubernetes zu gruppieren. Weitere Informationen finden Sie unter [Namespaces](#) in der Kubernetes-Dokumentation. Wenn Sie planen, Ihre Beispielanwendung zur [Vereinfachung der Rechenverwaltung mit AWS Fargate](#) bereitzustellen, stellen Sie sicher, dass der Wert für namespace „[Definieren Sie, welche Pods AWS Fargate beim Start verwenden](#)“ lautet. `eks-sample-app`

```
kubectl create namespace eks-sample-app
```

## Erstellen Sie eine Kubernetes-Bereitstellung

Bei dieser Beispielbereitstellung wird ein Container-Image aus einem öffentlichen Repository abgerufen und drei Replikat (einzelne Pods) davon in Ihrem Cluster bereitgestellt. Weitere Informationen finden Sie unter [Bereitstellungen](#) in der Kubernetes-Dokumentation.

1. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `eks-sample-deployment.yaml`. Die Container in der Beispielanwendung verwenden keinen Netzwerkspeicher, aber Sie haben möglicherweise Anwendungen, die dies benötigen. Weitere Informationen finden Sie unter [App-Datenspeicher](#).
  - Der Eintrag `kubernetes.io/os: windows` bedeutet, dass, wenn Sie beispielsweise Windows- und Linux-Knoten in Ihrem Cluster hätten, das Image nur auf Linux-Knoten bereitgestellt würde. Weitere Informationen finden Sie unter [Bekannte Labels, Anmerkungen und Taints](#) in der Kubernetes-Dokumentation.

```
apiVersion: apps/v1
kind: Deployment
```

```

metadata:
 name: eks-sample-windows-deployment
 namespace: eks-sample-app
 labels:
 app: eks-sample-windows-app
spec:
 replicas: 3
 selector:
 matchLabels:
 app: eks-sample-windows-app
 template:
 metadata:
 labels:
 app: eks-sample-windows-app
 spec:
 affinity:
 nodeAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 nodeSelectorTerms:
 - matchExpressions:
 - key: kubernetes.io/arch
 operator: In
 values:
 - amd64
 containers:
 - name: windows-server-iis
 image: mcr.microsoft.com/windows/servercore:ltsc2019
 ports:
 - name: http
 containerPort: 80
 imagePullPolicy: IfNotPresent
 command:
 - powershell.exe
 - -command
 - "Add-WindowsFeature Web-Server; Invoke-WebRequest -UseBasicParsing
 -Uri 'https://dotnetbinaries.blob.core.windows.net/servicemonitor/2.0.1.6/
 ServiceMonitor.exe' -OutFile 'C:\\ServiceMonitor.exe'; echo '<html><body>

<marquee><H1>Hello EKS!!!<H1><marquee></body><html>' > C:\\inetpub\\wwwroot\\
 \\default.html; C:\\ServiceMonitor.exe 'w3svc'; "
 nodeSelector:
 kubernetes.io/os: windows

```

## 2. Wenden Sie das Bereitstellungs-Manifest auf Ihren Cluster an.

```
kubectl apply -f eks-sample-deployment.yaml
```

## Einen Service erstellen

Mit einem Service können Sie über eine einzige IP-Adresse oder einen einzigen Namen auf alle Replikate zugreifen. Weitere Informationen dazu finden Sie unter [Service](#) in der Kubernetes-Dokumentation. Obwohl in der Beispielanwendung nicht implementiert, empfehlen wir Ihnen, Kubernetes-Dienstknoten für Ihre Pods zu erstellen und diese mit AWS IAM-Konten zu verknüpfen, falls Sie über Anwendungen verfügen, die mit anderen AWS Diensten interagieren müssen. Durch die Angabe von Dienstknoten verfügen Ihre Pods nur über die Mindestberechtigungen, die Sie für die Interaktion mit anderen Diensten angeben. Weitere Informationen finden Sie unter [the section called "Referenzen bei IRSA"](#).

1. Speichern Sie die folgenden Inhalte in einer Datei namens `eks-sample-service.yaml`. Kubernetes weist dem Service eine eigene IP-Adresse zu, auf die nur innerhalb des Clusters zugegriffen werden kann. Um von außerhalb des Clusters auf den Service zuzugreifen, stellen Sie den [AWS Load Balancer Controller](#) bereit, um den [Anwendungs](#)- oder [Netzwerk](#)-Datenverkehr an den Service auszugleichen.

```
apiVersion: v1
kind: Service
metadata:
 name: eks-sample-windows-service
 namespace: eks-sample-app
 labels:
 app: eks-sample-windows-app
spec:
 selector:
 app: eks-sample-windows-app
 ports:
 - protocol: TCP
 port: 80
 targetPort: 80
```

2. Wenden Sie das Service-Manifest auf Ihren Cluster an.

```
kubectl apply -f eks-sample-service.yaml
```

## Überprüfen Sie die erstellten Ressourcen

1. Zeigen Sie alle im `eks-sample-app`-Namespace vorhandenen Ressourcen an.

```
kubectl get all -n eks-sample-app
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                               | READY | STATUS  | RESTARTS | AGE |
|----------------------------------------------------|-------|---------|----------|-----|
| pod/eks-sample-windows-deployment-65b7669776-m6qxz | 1/1   | Running | 0        | 27m |
| pod/eks-sample-windows-deployment-65b7669776-mmxd  | 1/1   | Running | 0        | 27m |
| pod/eks-sample-windows-deployment-65b7669776-qzn22 | 1/1   | Running | 0        | 27m |

| NAME                               | TYPE      | CLUSTER-IP  | EXTERNAL-IP | PORT(S) |
|------------------------------------|-----------|-------------|-------------|---------|
| service/eks-sample-windows-service | ClusterIP | 10.100.74.8 | <none>      | 80/     |
| TCP                                |           |             |             | 32m     |

| NAME                                          | READY | UP-TO-DATE | AVAILABLE | AGE |
|-----------------------------------------------|-------|------------|-----------|-----|
| deployment.apps/eks-sample-windows-deployment | 3/3   | 3          | 3         | 27m |

| NAME                                                     | DESIRED | CURRENT | READY |
|----------------------------------------------------------|---------|---------|-------|
| replicaset.apps/eks-sample-windows-deployment-776d8f8fd8 | 3       | 3       | 3     |
| AGE                                                      |         |         | 27m   |

In der Ausgabe sehen Sie den Service und die Bereitstellung, die in den Beispielmanifesten, der vorherigen Schritte, angegeben wurden. Sie sehen auch drei Pods. Dies liegt daran, dass 3 replicas im Beispielmanifest angegeben wurden. Weitere Informationen zu Pods finden Sie unter [Pods](#) in der Kubernetes-Dokumentation. Kubernetes erstellt die replicaset Ressource automatisch, auch wenn sie nicht in den Beispielmanifesten angegeben ist. Weitere Informationen zu ReplicaSets finden Sie [ReplicaSet](#) in der Kubernetes-Dokumentation.

### Note

Kubernetes behält die Anzahl der Replikate bei, die im Manifest angegeben sind. Wenn es sich um eine Produktionsbereitstellung handelt und Sie möchten, dass Kubernetes die Anzahl der Replikate horizontal oder die Rechenressourcen für die Pods vertikal skaliert,

verwenden Sie dazu die Optionen [Pod-Bereitstellungen skalieren mit horizontalem Pod-Autoscaler](#) und [Pod-Ressourcen anpassen mit vertikalem Pod-Autoscaler](#).

## 2. Zeigen Sie die Details des bereitgestellten Services an.

```
kubectl -n eks-sample-app describe service eks-sample-windows-service
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name: eks-sample-windows-service
Namespace: eks-sample-app
Labels: app=eks-sample-windows-app
Annotations: <none>
Selector: app=eks-sample-windows-app
Type: ClusterIP
IP Families: <none>
IP: 10.100.74.8
IPs: 10.100.74.8
Port: <unset> 80/TCP
TargetPort: 80/TCP
Endpoints: 192.168.24.212:80,192.168.50.185:80,192.168.63.93:80
Session Affinity: None
Events: <none>
```

In der vorherigen Ausgabe IP: ist der Wert für eine eindeutige IP-Adresse, die von jedem Knoten oder Pod innerhalb des Clusters aus erreicht werden kann, aber nicht von außerhalb des Clusters erreicht werden kann. Die Werte für Endpoints sind IP-Adressen, die den Pods, die Teil des Dienstes sind, innerhalb Ihrer VPC zugewiesen wurden.

## 3. Zeigen Sie die Details eines der in der Ausgabe aufgeführten Pods an, wenn Sie in einem vorherigen Schritt den [Namespace angezeigt haben](#). `776d8f8fd8-78w66` Ersetzen Sie es durch den Wert, der für einen Ihrer Pods zurückgegeben wurde.

```
kubectl -n eks-sample-app describe pod eks-sample-windows-deployment-65b7669776-m6qxz
```

Verkürzte Beispielausgabe

```
Name: eks-sample-windows-deployment-65b7669776-m6qxz
Namespace: eks-sample-app
Priority: 0
```

```

Node: ip-192-168-45-132.us-west-2.compute.internal/192.168.45.132
[...]
IP: 192.168.63.93
IPs:
 IP: 192.168.63.93
Controlled By: ReplicaSet/eks-sample-windows-deployment-65b7669776
[...]
Conditions:
 Type Status
 Initialized True
 Ready True
 ContainersReady True
 PodScheduled True
[...]
Events:
 Type Reason Age From
 Message
 ---- -

 Normal Scheduled 3m20s default-scheduler
 Successfully assigned eks-sample-app/eks-sample-windows-deployment-65b7669776-m6qxz
 to ip-192-168-45-132.us-west-2.compute.internal
 [...]

```

In der vorherigen Ausgabe **IP:** ist der Wert für eine eindeutige IP, die dem Pod aus dem CIDR-Block zugewiesen wurde, der dem Subnetz zugewiesen ist, in dem sich der Knoten befindet. Wenn Sie es vorziehen, Pods IP-Adressen aus verschiedenen CIDR-Blöcken zuzuweisen, können Sie das Standardverhalten ändern. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Netzwerke”](#). Sie können auch sehen, dass der Kubernetes-Scheduler den Pod auf dem Node mit der IP-Adresse **192.168.45.132** geplant hat.

#### Tip

Anstatt die Befehlszeile zu verwenden, können Sie viele Details zu Pods, Diensten, Bereitstellungen und anderen Kubernetes-Ressourcen in der [AWS Management Console](#) sehen. Weitere Informationen finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

## Führen Sie eine Shell auf einem Pod aus

1. Führen Sie eine Shell auf dem Pod aus, die Sie im vorherigen Schritt beschrieben haben, und `65b7669776-m6qxz` ersetzen Sie sie durch die ID eines Ihrer Pods.

```
kubectl exec -it eks-sample-windows-deployment-65b7669776-m6qxz -n eks-sample-app -- powershell.exe
```

2. Sehen Sie sich in der Pod-Shell die Ausgabe des Webserver an, der in einem vorherigen Schritt zusammen mit Ihrer Bereitstellung installiert wurde. Sie müssen nur den Servicenamen angeben. Es wird von CoreDNS, das standardmäßig mit einem Amazon EKS-Cluster bereitgestellt wird, in die IP-Adresse des Dienstes aufgelöst.

```
Invoke-WebRequest -uri eks-sample-windows-service/default.html -UseBasicParsing
```

Eine Beispielausgabe sieht wie folgt aus.

```
StatusCode : 200
StatusDescription : OK
Content : < h t m l > < b o d y > < b r / > < b r / > < m a r q u e e > < H
 1 > H e l l o
 E K S ! ! ! < H 1 > < m a r q u e e > < / b o d y > < h t m l >
```

3. Zeigen Sie in der Pod-Shell den DNS-Server für den Pod an.

```
Get-NetIPConfiguration
```

Gekürzte Ausgabe

```
InterfaceAlias : vEthernet
[...]
IPv4Address : 192.168.63.14
[...]
DNSServer : 10.100.0.10
```

In der vorherigen Ausgabe wird `10.100.0.10` automatisch als DNS-Server für alle Pods zugewiesen, die im Cluster bereitgestellt werden.

4. Trennen Sie die Verbindung mit dem Pod, indem Sie `exit` eingeben.



5. Sobald Sie mit der Beispielanwendung fertig sind, können Sie den Beispiel-Namespace, den Service und die Bereitstellung mit dem folgenden Befehl entfernen.

```
kubectl delete namespace eks-sample-app
```

## Nächste Schritte

Nachdem Sie die Beispielanwendung bereitgestellt haben, möchten Sie vielleicht einige der folgenden Übungen ausprobieren:

- [Leiten Sie Anwendungs- und HTTP-Verkehr mit Application Load Balancers weiter](#)
- [Leiten Sie TCP- und UDP-Verkehr mit Network Load Balancers weiter](#)

## Passen Sie die Pod-Ressourcen mit Vertical Pod Autoscaler an

Der Kubernetes [Vertical Pod Autoscaler](#) passt die CPU- und Speicherreservierungen für Ihre Pods automatisch an, um Ihre Anwendungen „richtig dimensionieren“ zu können. Diese Anpassung kann die Nutzung der Cluster-Ressourcen verbessern und CPU und Speicher für andere Pods freigeben. In diesem Thema können Sie den Vertical Pod Autoscaler für Ihren Cluster bereitstellen und überprüfen, ob er funktioniert.

- Sie haben einen Amazon EKS-Cluster. Wenn nicht, sehen Sie nach [Erste Schritte](#).
- Sie haben den Kubernetes-Metrik-Server installiert. Weitere Informationen finden Sie unter [the section called “Kennzahlen-Server”](#).
- Sie verwenden einen `kubectl`-Client, der [für die Kommunikation mit Ihrem Amazon EKS-Cluster konfiguriert](#) ist.
- OpenSSL 1.1.1 oder höher ist auf Ihrem Gerät installiert.

## Bereitstellen des Vertical Pod Autoscalers

In diesem Abschnitt stellen Sie den Vertical Pod Autoscaler für Ihren Cluster bereit.

1. Öffnen Sie ein Terminalfenster und navigieren Sie zu einem Verzeichnis, in das Sie den Vertical Pod Autoscaler-Quellcode herunterladen möchten.
2. Klonen Sie das [GitHub Kubernetes/Autoscaler-Repository](#).

```
git clone https://github.com/kubernetes/autoscaler.git
```

3. Wechseln Sie in das `vertical-pod-autoscaler`-Verzeichnis.

```
cd autoscaler/vertical-pod-autoscaler/
```

4. (Optional) Wenn Sie bereits eine andere Version des Vertical Pod Autoscalers bereitgestellt haben, entfernen Sie ihn mit dem folgenden Befehl.

```
./hack/vpa-down.sh
```

5. Wenn Ihre Knoten keinen Internetzugang zur `registry.k8s.io` Container-Registry haben, müssen Sie die folgenden Bilder abrufen und in Ihr eigenes privates Repository übertragen. Weitere Informationen zum Abrufen und Verschieben der Images in ein eigenes privates Repository finden Sie unter [the section called “Kopieren eines Images in ein Repository”](#).

```
registry.k8s.io/autoscaling/vpa-admission-controller:0.10.0
registry.k8s.io/autoscaling/vpa-recommender:0.10.0
registry.k8s.io/autoscaling/vpa-updater:0.10.0
```

Wenn Sie die Bilder in ein privates Amazon ECR-Repository übertragen, ersetzen Sie `registry.k8s.io` in den Manifesten durch Ihre Registrierung. Ersetzen Sie **111122223333** durch Ihre Konto-ID. **region-code** Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. Beim folgenden Befehl wird davon ausgegangen, dass Sie Ihr Repository genauso benannt haben wie das Repository im Manifest. Wenn Sie Ihrem Repository einen anderen Namen gegeben haben, müssen Sie ihn ebenfalls ändern.

```
sed -i.bak -e 's/registry.k8s.io/111122223333.dkr.ecr.region-code.amazonaws.com/' ./
deploy/admission-controller-deployment.yaml
sed -i.bak -e 's/registry.k8s.io/111122223333.dkr.ecr.region-code.amazonaws.com/' ./
deploy/recommender-deployment.yaml
sed -i.bak -e 's/registry.k8s.io/111122223333.dkr.ecr.region-code.amazonaws.com/' ./
deploy/updater-deployment.yaml
```

6. Stellen Sie den Vertical Pod Autoscaler mit dem folgenden Befehl für Ihren Cluster bereit.

```
./hack/vpa-up.sh
```

7. Stellen Sie sicher, dass die Vertical Pod Autoscaler-Pods erfolgreich erstellt wurden.

```
kubectl get pods -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                      | READY | STATUS  | RESTARTS | AGE |
|-------------------------------------------|-------|---------|----------|-----|
| [...]                                     |       |         |          |     |
| metrics-server-8459fc497-kfj8w            | 1/1   | Running | 0        | 83m |
| vpa-admission-controller-68c748777d-ppspd | 1/1   | Running | 0        | 7s  |
| vpa-recommender-6fc8c67d85-gljpl          | 1/1   | Running | 0        | 8s  |
| vpa-updater-786b96955c-bgp9d              | 1/1   | Running | 0        | 8s  |

## Testen der Installation von Vertical Pod Autoscaler

In diesem Abschnitt stellen Sie eine Beispielanwendung bereit, um zu überprüfen, ob der Vertical Pod Autoscaler funktioniert.

1. Stellen Sie das Vertical Pod Autoscaler-Beispiel `hamster.yaml` mit dem folgenden Befehl bereit.

```
kubectl apply -f examples/hamster.yaml
```

2. Holen Sie sich die Pods aus der `hamster` Beispielanwendung.

```
kubectl get pods -l app=hamster
```

Eine Beispielausgabe sieht wie folgt aus.

|                         |     |         |   |     |
|-------------------------|-----|---------|---|-----|
| hamster-c7d89d6db-rglf5 | 1/1 | Running | 0 | 48s |
| hamster-c7d89d6db-znvz5 | 1/1 | Running | 0 | 48s |

3. Beschreiben Sie einen der Pods, um ihn anzusehen, `cpu` und `memory` reservieren Sie ihn. `c7d89d6db-rglf5` Ersetzen Sie ihn durch einen der in Ihrer Ausgabe aus dem vorherigen Schritt IDs zurückgegebenen.

```
kubectl describe pod hamster-c7d89d6db-rglf5
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
Containers:
 hamster:
 Container ID: docker://
e76c2413fc720ac395c33b64588c82094fc8e5d590e373d5f818f3978f577e24
 Image: registry.k8s.io/ubuntu-slim:0.1
 Image ID: docker-pullable://registry.k8s.io/ubuntu-
slim@sha256:b6f8c3885f5880a4f1a7cf717c07242eb4858fdd5a84b5ffe35b1cf680ea17b1
 Port: <none>
 Host Port: <none>
 Command:
 /bin/sh
 Args:
 -c
 while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done
 State: Running
 Started: Fri, 27 Sep 2019 10:35:16 -0700
 Ready: True
 Restart Count: 0
 Requests:
 cpu: 100m
 memory: 50Mi
[...]
```

Sie können sehen, dass der ursprüngliche Pod 100 Milli-CPU an CPU und 50 Mebibyte Speicher reserviert. In dieser Beispielanwendung sind 100 Millicpu weniger, als der Pod zum Ausführen benötigt, weshalb er CPU-eingeschränkt ist. Außerdem reserviert er viel weniger Arbeitsspeicher, als er benötigt. Bei der `vpa-recommender` Bereitstellung von Vertical Pod Autoscaler werden die Hamster-Pods analysiert, um festzustellen, ob die CPU- und Speicheranforderungen angemessen sind. Wenn Anpassungen erforderlich sind, werden die Pods mit `vpa-updater` aktualisierten Werten neu gestartet.

4. Warten Sie, `vpa-updater` bis der neue Hamster-Pods gestartet hat. Dies sollte ein oder zwei Minuten dauern. Sie können die Pods mit dem folgenden Befehl überwachen.

#### Note

Wenn Sie sich nicht sicher sind, ob ein neuer Pod gestartet wurde, vergleichen Sie die Pod-Namen mit Ihrer vorherigen Liste. Wenn der neue Pod gestartet wird, siehst du einen neuen Pod-Namen.

```
kubectl get --watch Pods -l app=hamster
```

5. Wenn ein neuer Hamster-Pod gestartet wird, beschreibe ihn und sieh dir die aktualisierten CPU- und Speicherreservierungen an.

```
kubectl describe pod hamster-c7d89d6db-jxgfv
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
Containers:
 hamster:
 Container ID:
 docker://2c3e7b6fb7ce0d8c86444334df654af6fb3fc88aad4c5d710eac3b1e7c58f7db
 Image: registry.k8s.io/ubuntu-slim:0.1
 Image ID: docker-pullable://registry.k8s.io/ubuntu-
slim@sha256:b6f8c3885f5880a4f1a7cf717c07242eb4858fdd5a84b5ffe35b1cf680ea17b1
 Port: <none>
 Host Port: <none>
 Command:
 /bin/sh
 Args:
 -c
 while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done
 State: Running
 Started: Fri, 27 Sep 2019 10:37:08 -0700
 Ready: True
 Restart Count: 0
 Requests:
 cpu: 587m
 memory: 262144k
[...]
```

In der vorherigen Ausgabe können Sie feststellen, dass sich die cpu-Reservierung auf 587 Millicpu erhöht hat, was mehr als dem Fünffachen des ursprünglichen Werts entspricht. Der memory wurde auf 262.144 Kilobyte erhöht, was etwa 250 Megabyte bzw. dem Fünffachen des ursprünglichen Werts entspricht. Dieser Pod verfügte über unzureichende Ressourcen, und der Vertical Pod Autoscaler korrigierte die Schätzung mit einem viel geeigneteren Wert.

6. Beschreiben Sie die `hamster-vpa`-Ressource, um die neue Empfehlung anzuzeigen.

```
kubectl describe vpa/hamster-vpa
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name: hamster-vpa
Namespace: default
Labels: <none>
Annotations: kubectl.kubernetes.io/last-applied-configuration:
 {"apiVersion":"autoscaling.k8s.io/v1beta2","kind":"VerticalPodAutoscaler","metadata":{"annotations":{},"name":"hamster-
vpa","namespace":"d...
API Version: autoscaling.k8s.io/v1beta2
Kind: VerticalPodAutoscaler
Metadata:
 Creation Timestamp: 2019-09-27T18:22:51Z
 Generation: 23
 Resource Version: 14411
 Self Link: /apis/autoscaling.k8s.io/v1beta2/namespaces/default/
verticalpodautoscalers/hamster-vpa
 UID: d0d85fb9-e153-11e9-ae53-0205785d75b0
Spec:
 Target Ref:
 API Version: apps/v1
 Kind: Deployment
 Name: hamster
Status:
 Conditions:
 Last Transition Time: 2019-09-27T18:23:28Z
 Status: True
 Type: RecommendationProvided
 Recommendation:
 Container Recommendations:
 Container Name: hamster
 Lower Bound:
 Cpu: 550m
 Memory: 262144k
 Target:
 Cpu: 587m
 Memory: 262144k
 Uncapped Target:
 Cpu: 587m
 Memory: 262144k
```

```
Upper Bound:
 Cpu: 21147m
 Memory: 387863636
Events: <none>
```

7. Wenn Sie mit dem Experimentieren mit der Beispielanwendung fertig sind, können Sie sie mit dem folgenden Befehl löschen.

```
kubectl delete -f examples/hamster.yaml
```

## Skalieren Sie Pod-Bereitstellungen mit Horizontal Pod Autoscaler

Der Kubernetes [Horizontal Pod Autoscaler](#) skaliert automatisch die Anzahl der Pods in einer Bereitstellung, einem Replikationscontroller oder einem Replikatsatz basierend auf der CPU-Auslastung dieser Ressource. Auf diese Weise können Ihre Anwendungen aufskalieren, um den erhöhten Bedarf zu erfüllen, oder abskalieren, wenn Ressourcen nicht benötigt werden, sodass Ihre Knoten für andere Anwendungen freigegeben werden. Wenn Sie einen CPU-Auslastungsprozentsatz festlegen, skaliert der Horizontal Pod Autoscaler Ihre Anwendung in beide Richtungen, um zu versuchen, dieses Ziel zu erreichen.

Der Horizontal Pod Autoscaler ist eine Standard-API-Ressource in Kubernetes, die einfach erfordert, dass eine Metrikquelle (z. B. der Kubernetes-Metrikserver) auf Ihrem Amazon-EKS-Cluster installiert ist. Sie müssen den Horizontal Pod Autoscaler nicht auf Ihrem Cluster bereitstellen oder installieren, um mit der Skalierung Ihrer Anwendungen zu beginnen. Weitere Informationen finden Sie unter [Horizontal Pod Autoscaler](#) in der Kubernetes-Dokumentation.

Verwenden Sie dieses Thema, um den Horizontal Pod Autoscaler für Ihren Amazon-EKS-Cluster vorzubereiten und zu überprüfen, ob er mit einer Beispielanwendung funktioniert.

### Note

Dieses Thema basiert auf der exemplarischen Vorgehensweise für den [Horizontal Pod Autoscaler](#) in der Kubernetes-Dokumentation.

- Sie haben einen vorhandenen Amazon-EKS-Cluster. Falls nicht, finden Sie weitere Informationen unter [Erste Schritte](#)

- Sie haben den Kubernetes-Metrik-Server installiert. Weitere Informationen finden Sie unter [the section called “Kennzahlen-Server”](#).
- Sie verwenden einen `kubectl`-Client, der [für die Kommunikation mit Ihrem Amazon EKS-Cluster konfiguriert](#) ist.

## Ausführen einer Horizontal Pod Autoscaler-Testanwendung

In diesem Abschnitt stellen Sie eine Beispielanwendung bereit, um zu überprüfen, ob der Horizontal Pod Autoscaler funktioniert.

### Note

Dieses Beispiel basiert auf der Anleitung zur [automatischen Skalierung von Horizontal Pod in der Kubernetes-Dokumentation](#).

1. Stellen Sie mit dem folgenden Befehl eine einfache Apache-Webserveranwendung bereit.

```
kubectl apply -f https://k8s.io/examples/application/php-apache.yaml
```

Dieser Apache-Webserver-Pod hat ein CPU-Limit von 500 Milli-CPU und er wird auf Port 80 bedient.

2. Erstellen Sie eine Horizontal Pod Autoscaler-Ressource für die php-apache-Bereitstellung.

```
kubectl autoscale deployment php-apache --cpu-percent=50 --min=1 --max=10
```

Dieser Befehl erstellt ein Autoscaling, das für die Bereitstellung eine CPU-Auslastung von 50 Prozent anstrebt, mit mindestens einem Pod und maximal zehn Pods. Wenn die durchschnittliche CPU-Last unter 50 Prozent liegt, versucht das Autoscaling, die Anzahl der Pods in der Bereitstellung auf mindestens einen zu reduzieren. Wenn die Auslastung mehr als 50 Prozent beträgt, versucht das Autoscaling, die Anzahl der Pods in der Bereitstellung auf maximal zehn zu erhöhen. Weitere Informationen finden Sie unter [Wie funktioniert ein HorizontalPodAutoscaler ?](#) in der Kubernetes-Dokumentation.

3. Beschreiben Sie den Autoscaler mit dem folgenden Befehl, um seine Details anzuzeigen.

```
kubectl get hpa
```



Eine Beispielausgabe sieht wie folgt aus.

| NAME       | REFERENCE             | TARGETS | MINPODS | MAXPODS | REPLICAS | AGE |
|------------|-----------------------|---------|---------|---------|----------|-----|
| php-apache | Deployment/php-apache | 0%/50%  | 1       | 10      | 1        | 51s |

Wie Sie sehen können, liegt die aktuelle CPU-Last daran 0%, dass der Server noch nicht belastet ist. Die Pod-Anzahl hat bereits die niedrigste Grenze (eins) erreicht, sodass sie nicht skaliert werden kann.

- Erstellen Sie eine Last für den Webserver, indem Sie einen Container ausführen.

```
kubectl run -i \
 --tty load-generator \
 --rm --image=busybox \
 --restart=Never \
 -- /bin/sh -c "while sleep 0.01; do wget -q -O- http://php-apache; done"
```

- Um die Skalierung der Bereitstellung zu beobachten, führen Sie in regelmäßigen Abständen den folgenden Befehl in einem anderen Terminal als demjenigen aus, in dem Sie den vorherigen Schritt ausgeführt haben.

```
kubectl get hpa php-apache
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME       | REFERENCE             | TARGETS  | MINPODS | MAXPODS | REPLICAS | AGE   |
|------------|-----------------------|----------|---------|---------|----------|-------|
| php-apache | Deployment/php-apache | 250%/50% | 1       | 10      | 5        | 4m44s |

Es kann mehr als eine Minute dauern, bis die Anzahl der Replikate zunimmt. Solange der tatsächliche CPU-Prozentsatz höher als der Zielprozentsatz ist, erhöht sich die Replikanzahl auf bis zu 10. In diesem Fall ist es so 250%, also nimmt die Anzahl der REPLICAS weiter zu.

#### Note

Es kann einige Minuten dauern, bis die Replikanzahl ihr Maximum erreicht. Wenn beispielsweise nur 6 Replikate erforderlich sind, damit die CPU-Last bei oder unter 50% bleibt, kann die Auslastung nicht über 6 Replikate hinaus skaliert werden.

6. Stoppen Sie die Last. Halten Sie im Terminalfenster, in dem Sie die Last generieren, den Ladevorgang an, indem Sie die Tasten gedrückt halten. `Ctrl+C` Sie können beobachten, wie die Replikate auf 1 zurückskaliert werden, indem Sie den folgenden Befehl erneut in dem Terminal ausführen, in dem Sie die Skalierung beobachten.

```
kubectl get hpa
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME       | REFERENCE             | TARGETS | MINPODS | MAXPODS | REPLICAS | AGE |
|------------|-----------------------|---------|---------|---------|----------|-----|
| php-apache | Deployment/php-apache | 0%/50%  | 1       | 10      | 1        | 25m |

 Note

Der Standardzeitrahmen für das Zurückskalieren beträgt fünf Minuten. Es wird daher einige Zeit dauern, bis die Replikanzahl wieder 1 erreicht, selbst wenn der aktuelle CPU-Prozentsatz 0 Prozent beträgt. Der Zeitrahmen ist veränderbar. Weitere Informationen finden Sie unter [Horizontal Pod Autoscaler](#) in der Kubernetes-Dokumentation.

7. Wenn Sie mit dem Experimentieren mit Ihrer Beispielanwendung fertig sind, löschen Sie die php-apache-Ressourcen.

```
kubectl delete deployment.apps/php-apache service/php-apache
horizontalpodautoscaler.autoscaling/php-apache
```

## Weiterleiten von TCP- und UDP-Verkehr mit Network Load Balancers

 Note

Neu: Der automatische Modus von Amazon EKS automatisiert Routineaufgaben für den Lastenausgleich. Weitere Informationen finden Sie unter:

- [the section called “Stellen Sie den Load Balancer bereit”](#)
- [the section called “Service erstellen”](#)

Das Load Balancing des Netzwerkverkehrs erfolgt auf L4 des OSI-Modells. Um den Anwendungsdatenverkehr unter zu verteilenL7, stellen Sie ein Kubernetes bereit, das einen AWS Application Load Balancer bereitstellt. Weitere Informationen finden Sie unter [the section called “Application Load Balancing”](#). Weitere Informationen zu den Unterschieden zwischen den beiden Arten von Load Balancing finden Sie auf der AWS Website unter [Elastic Load Balancing Balancing-Funktionen](#).

[Wenn Sie einen Kubernetes-Typ erstellenLoadBalancer, erstellt Service der Load Balancer-Controller des AWS Cloud-Anbieters standardmäßig AWSClassic Load Balancer, kann aber auch Network Load Balancer erstellen AWS](#) . Dieser Controller erhält in Zukunft nur kritische Fehlerbehebungen. Weitere Informationen zur Verwendung des AWS Cloud-Provider-Loadbalancers finden Sie unter Cloud-Provider-Load Balancer-Controller in der [AWS Kubernetes-Dokumentation](#). Seine Verwendung wird in diesem Thema nicht behandelt.

Wir empfehlen, dass Sie Version 2.7.2 oder höher des [Load AWS Balancer Controllers](#) anstelle des AWS Cloud-Provider-Load Balancer-Controllers verwenden. Der Load AWS Balancer Controller erstellt AWS Network Load Balancer, aber keine AWS Classic Load Balancer. Der Rest dieses Themas befasst sich mit der Verwendung des Load AWS Balancer Controllers.

Ein AWS Network Load Balancer kann den Netzwerkverkehr auf Pods verteilen, die auf Amazon EC2 IP- und [Instance-Zielen](#) bereitgestellt werden, auf AWS Fargate-IP-Ziele oder auf Amazon EKS-Hybridknoten als IP-Ziele. Weitere Informationen finden Sie unter [AWS Load Balancer Controller](#) on GitHub.

## Voraussetzungen

Bevor Sie mit dem Load Balancer Controller einen AWS Lastenausgleich für den Netzwerkverkehr durchführen können, müssen Sie die folgenden Anforderungen erfüllen.

- Einen vorhandenen Cluster haben. Wenn Sie noch keinen Cluster haben, finden Sie weitere Informationen unter [Erste Schritte](#). Wenn Sie die Version eines vorhandenen Clusters aktualisieren müssen, finden Sie unter [the section called “Kubernetes-Version aktualisieren”](#).
- Lassen Sie den AWS Load Balancer Controller auf Ihrem Cluster bereitstellen. Weitere Informationen finden Sie unter [the section called “ AWS Load Balancer Balancer-Controller”](#). Wir empfehlen Version 2.7.2 oder höher.
- Mindestens ein Subnetz. Werden in einer Availability Zone mehrere markierte Subnetze gefunden, wählt der Controller das erste Subnetz, dessen Subnetz-ID lexikografisch an erster Stelle steht. Das Subnetz muss mindestens acht verfügbare IP-Adressen aufweisen.

- Wenn Sie die Load AWS Balancer Controller-Version 2.1.1 oder eine frühere Version verwenden, müssen Subnetze wie folgt gekennzeichnet werden. Bei Verwendung der Version 2.1.2 oder höher ist dieses Tag optional. Möglicherweise möchten Sie ein Subnetz taggen, wenn mehrere Cluster in derselben VPC ausgeführt werden, oder wenn mehrere AWS Dienste Subnetze in einer VPC gemeinsam nutzen, und Sie mehr Kontrolle darüber haben möchten, wo Load Balancer für jeden Cluster bereitgestellt werden. Wenn Sie das Subnetz explizit IDs als Anmerkung zu einem Serviceobjekt angeben, verwenden Kubernetes und der Load AWS Balancer Controller diese Subnetze direkt, um den Load Balancer zu erstellen. Subnetz-Tagging ist nicht erforderlich, wenn Sie diese Methode für die Bereitstellung von Load Balancern verwenden, und Sie können die folgenden Anforderungen an das Tagging von privaten und öffentlichen Subnetzen überspringen. Ersetzen Sie *my-cluster* mit Ihrem Clusternamen.
  - Schlüssel – `kubernetes.io/cluster/<my-cluster>`
  - Wert – `shared` oder `owned`
- Ihre öffentlichen und privaten Subnetze müssen die folgenden Anforderungen erfüllen, es sei denn, Sie geben das Subnetz explizit IDs als Anmerkung zu einem Dienst- oder Eingangsobjekt an. Wenn Sie Load Balancer bereitstellen, indem Sie das Subnetz explizit IDs als Anmerkung zu einem Service- oder Ingress-Objekt angeben, verwenden Kubernetes und der Load AWS Balancer Controller diese Subnetze direkt, um den Load Balancer zu erstellen, und die folgenden Tags sind nicht erforderlich.
  - Private Subnetze – Müssen im folgenden Format markiert sein. Auf diese Weise wissen Kubernetes und der Load AWS Balancer Controller, dass die Subnetze für interne Load Balancer verwendet werden können. Wenn Sie eine Amazon AWS CloudFormation EKS-Vorlage verwenden `eksctl`, um Ihre VPC nach dem 26. März 2020 zu erstellen, werden die Subnetze bei der Erstellung entsprechend gekennzeichnet. Weitere Informationen über die Amazon-EKS-AWS - AWS CloudFormation -VPC-Vorlagen finden Sie unter [the section called “Erstellen einer VPC”](#).
    - Schlüssel – `kubernetes.io/role/internal-elb`
    - Wert – `1`
  - Öffentliche Subnetze – Müssen im folgenden Format markiert sein. Auf diese Weise weiß Kubernetes, dass es nur diese Subnetze für externe Load Balancer verwenden muss, anstatt in jeder Availability Zone ein öffentliches Subnetz auszuwählen (basierend auf der lexikografischen Reihenfolge des Subnetzes). IDs Wenn Sie eine Amazon AWS CloudFormation EKS-Vorlage verwenden `eksctl`, um Ihre VPC nach dem 26. März 2020 zu erstellen, werden die Subnetze bei der Erstellung entsprechend gekennzeichnet. Weitere Informationen zu den Amazon AWS CloudFormation EKS-VPC-Vorlagen finden Sie unter [the section called “Erstellen einer VPC”](#).

- Schlüssel – `kubernetes.io/role/elb`
- Wert – 1

Wenn die Subnetz-Rollen-Tags nicht explizit hinzugefügt werden, untersucht der Kubernetes Service Controller die Routing-Tabelle Ihrer Cluster-VPC-Subnetze, um festzustellen, ob das Subnetz privat oder öffentlich ist. Wir empfehlen, dass Sie sich nicht auf dieses Verhalten verlassen und stattdessen die privaten oder öffentlichen Rollen-Tags explizit hinzufügen. Der Load AWS Balancer Controller untersucht keine Routing-Tabellen und setzt voraus, dass die privaten und öffentlichen Tags für eine erfolgreiche auto Erkennung vorhanden sind.

## Überlegungen

- Die Konfiguration Ihres Load Balancers wird durch Anmerkungen gesteuert, die zu dem Manifest für Ihren Service hinzugefügt werden. Dienstanmerkungen unterscheiden sich bei Verwendung des Load AWS Balancer Controllers von denen bei Verwendung des AWS Cloud-Provider-Load Balancer-Controllers. Stellen Sie sicher, dass Sie die [Anmerkungen](#) für den Load AWS Balancer Controller überprüfen, bevor Sie Dienste bereitstellen.
- Bei Verwendung des [Amazon VPC CNI-Plug-ins für Kubernetes](#) kann der Load Balancer Controller einen AWS Lastenausgleich auf Amazon EC2 IP- oder Instance-Ziele und Fargate-IP-Ziele durchführen. Wenn Sie [alternative kompatible CNI-Plug-ins](#) verwenden, kann der Controller nur einen Lastenausgleich auf Instance-Ziele durchführen, es sei denn, Sie führen einen Lastenausgleich auf Amazon EKS-Hybridknoten durch. Bei Hybridknoten kann der Controller den Lastenausgleich für IP-Ziele durchführen. Weitere Informationen zu Network-Load-Balancer-Zieltypen finden Sie unter [Zieltyp](#) im Benutzerhandbuch für Network Load Balancers.
- Wenn Sie dem Load Balancer bei oder nach seiner Erstellung Tags hinzufügen möchten, fügen Sie Ihrer Servicespezifikation die folgende Anmerkung hinzu. Weitere Informationen finden Sie unter [AWS Resource Tags](#) in der Load AWS Balancer Controller-Dokumentation.

```
service.beta.kubernetes.io/aws-load-balancer-additional-resource-tags
```

- Sie können [Elastic IP-Adressen](#) zum Network Load Balancer hinzufügen, indem Sie die folgende Anmerkung hinzufügen. Ersetzen Sie die *example values* mit den Allocation IDs Ihrer elastischen IP-Adressen. Die Anzahl der Allocation IDs muss mit der Anzahl der Subnetze übereinstimmen, die für den Load Balancer verwendet werden. Weitere Informationen finden Sie unter Ressourcen-Tags in der [AWS -Load-Balancer-Controller](#)-Dokumentation.

```
service.beta.kubernetes.io/aws-load-balancer-eip-allocations: eipalloc-
xxxxxxxxxxxxxxxxxxxxx,eipalloc-yyyyyyyyyyyyyyyyyyyy
```

- Amazon EKS fügt der Sicherheitsgruppe des Knotens eine Regel für eingehenden Datenverkehr und eine Regel für jedes Load Balancer-Subnetz in der VPC für Zustandsprüfungen für jeden von Ihnen erstellten Network Load Balancer hinzu. Bereitstellung eines Dienstes vom Typ Load Balancer kann fehlschlagen, wenn Amazon EKS versucht, Regeln zu erstellen, die das Kontingent für die maximal zulässige Anzahl von Regeln für eine Sicherheitsgruppe überschreiten. Weitere Informationen dazu finden Sie im Abschnitt [Sicherheitsgruppe](#) in Amazon VPC-Kontingenten im Amazon VPC-Benutzerhandbuch. Berücksichtigen Sie die folgenden Optionen, um die Wahrscheinlichkeit zu minimieren, dass die maximale Anzahl von Regeln für eine Sicherheitsgruppe überschritten wird:
  - Fordern Sie eine Erhöhung Ihrer Regeln pro Sicherheitsgruppenkontingent an. Weitere Informationen dazu finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Service-Quotas-Benutzerhandbuch.
  - Verwenden Sie IP-Ziele anstelle von Instance-Zielen. Mit IP-Zielen können Sie Regeln für dieselben Zielports freigeben. Sie können Load-Balancer-Subnetze manuell mit einer Anmerkung angeben. [Weitere Informationen finden Sie unter Anmerkungen zu.](#) GitHub
  - Verwenden Sie einen Eingang anstelle eines Services vom Typ Load Balancer, um Datenverkehr an Ihren Service zu senden. Der AWS Application Load Balancer benötigt weniger Regeln als Network Load Balancer. Sie können einen ALB für mehrere Eingänge freigeben. Weitere Informationen finden Sie unter [the section called “Application Load Balancing”](#). Sie können einen Network Load Balancer nicht für mehrere Dienste gemeinsam nutzen.
  - Stellen Sie Ihre Cluster für mehrere Konten bereit.
- Wenn Ihre Pods unter Windows in einem Amazon EKS-Cluster ausgeführt werden, kann ein einzelner Service mit einem Load Balancer bis zu 1024 Back-End-Pods unterstützen. Jeder Pod hat seine eigene eindeutige IP-Adresse.
- Wir empfehlen, nur neue Network Load Balancer mit dem Load AWS Balancer Controller zu erstellen. Der Versuch, vorhandene Network Load Balancer zu ersetzen, die mit dem Load Balancer-Controller des AWS Cloud-Anbieters erstellt wurden, kann zu mehreren Network Load Balancern führen, was zu Anwendungsausfällen führen kann.

## Erstellen eines Network Load Balancers

Sie können einen Netzwerk-Load-Balancer mit IP- oder Instance-Zielen erstellen.

## Netzwerk-Loadbalancer erstellen — IP-Ziele

- Sie können IP-Ziele mit Pods verwenden, die auf EC2 Amazon-Knoten, Fargate oder Amazon EKS-Hybridknoten bereitgestellt werden. Ihr Kubernetes-Service muss als Typ `LoadBalancer` erstellt werden. Weitere Informationen finden Sie `LoadBalancer` in der Kubernetes-Dokumentation unter [Type](#).

Um einen Load Balancer zu erstellen, der IP-Ziele verwendet, fügen Sie die folgende Anmerkung zu einem Service-Manifest hinzu und stellen Sie den Dienst bereit. Der `external aws-load-balancer-type` Wert für veranlasst den Load AWS Balancer Controller und nicht den Load Balancer Controller des AWS Cloud-Anbieters, den Network Load Balancer zu erstellen. Sie können ein [Beispiel-Service-Manifest](#) mit den Anmerkungen anzeigen.

```
service.beta.kubernetes.io/aws-load-balancer-type: "external"
service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: "ip"
```

### Note

Wenn Sie den Load Balancing für IPv6 Pods durchführen, fügen Sie die folgende Anmerkung hinzu. Load Balancing über IPv6 funktioniert nur auf IP-Ziele, nicht auf Instance-Ziele. Ohne diese Anmerkung verläuft das Load Balancing über IPv4.

```
service.beta.kubernetes.io/aws-load-balancer-ip-address-type: dualstack
```

Network Load Balancer werden standardmäßig mit dem `internal aws-load-balancer-scheme` erstellt. Sie können Network Load Balancers in jedem Subnetz in der VPC Ihres Clusters starten, einschließlich Subnetzen, die bei der Erstellung Ihres Clusters nicht angegeben wurden.

Kubernetes untersucht die Routing-Tabelle auf Ihre Subnetze, um zu identifizieren, ob sie öffentlich oder privat sind. Öffentliche Subnetze verfügen über einen direkten Zugang zum Internet über ein Internet-Gateway, nicht aber private Subnetze.

Wenn Sie einen Network Load Balancer in einem öffentlichen Subnetz für den Lastenausgleich auf EC2 Amazon-Knoten erstellen möchten (Fargate kann nur privat sein), geben Sie dies `internet-facing` mit der folgenden Anmerkung an:

```
service.beta.kubernetes.io/aws-load-balancer-scheme: "internet-facing"
```

#### Note

Aus Gründen der Abwärtskompatibilität wird `service.beta.kubernetes.io/aws-load-balancer-type: "nlb-ip"` weiterhin unterstützt. Wir empfehlen jedoch die Verwendung der vorherigen Anmerkungen für neue Load Balancer anstelle von `service.beta.kubernetes.io/aws-load-balancer-type: "nlb-ip"`.

#### Important

Bearbeiten Sie die Anmerkungen nicht, nachdem Sie Ihren Service erstellt haben. Wenn Sie es ändern müssen, löschen Sie das Service-Objekt und erstellen es erneut mit dem gewünschten Wert für diese Anmerkung.

## Netzwerk-Loadbalancer erstellen — Instance-Ziele

- Der Load Balancer-Controller des AWS Cloud-Anbieters erstellt Network Load Balancer nur mit Instanzzielen. Version 2.2.0 und höher des Load AWS Balancer Controllers erstellen auch Network Load Balancer mit Instanzzielen. Wir empfehlen, ihn anstelle des Load Balancer-Controllers des AWS Cloud-Anbieters zu verwenden, um neue Network Load Balancer zu erstellen. Sie können Network Load Balancer Balancer-Instance-Ziele mit Pods verwenden, die auf EC2 Amazon-Knoten, aber nicht auf Fargate bereitgestellt werden. Um den Netzwerkverkehr über Pods auszugleichen, die in Fargate bereitgestellt werden, müssen Sie IP-Ziele verwenden.

Um einen Network Load Balancer in einem privaten Subnetz bereitzustellen, muss Ihre Service-Spezifikation über die folgenden Anmerkungen verfügen. Sie können ein [Beispiel-Service-Manifest](#) mit den Anmerkungen anzeigen. Der `external aws-load-balancer-type` Wert für `external` veranlasst den Load AWS Balancer Controller und nicht den Load Balancer Controller des AWS Cloud-Anbieters, den Network Load Balancer zu erstellen.

```
service.beta.kubernetes.io/aws-load-balancer-type: "external"
service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: "instance"
```



Network Load Balancer werden standardmäßig mit dem `internal aws-load-balancer-scheme` erstellt. Für interne Network Load Balancer muss Ihr Amazon-EKS-Cluster so konfiguriert werden, dass er mindestens ein privates Subnetz in Ihrer VPC verwendet. Kubernetes untersucht die Routing-Tabelle auf Ihre Subnetze, um zu identifizieren, ob sie öffentlich oder privat sind. Öffentliche Subnetze verfügen über einen direkten Zugang zum Internet über ein Internet-Gateway, nicht aber private Subnetze.

Wenn Sie einen Network Load Balancer in einem öffentlichen Subnetz für den Lastenausgleich auf EC2 Amazon-Knoten erstellen möchten, geben Sie dies `internet-facing` mit der folgenden Anmerkung an:

```
service.beta.kubernetes.io/aws-load-balancer-scheme: "internet-facing"
```

#### Important

Bearbeiten Sie die Anmerkungen nicht, nachdem Sie Ihren Service erstellt haben. Wenn Sie es ändern müssen, löschen Sie das Service-Objekt und erstellen es erneut mit dem gewünschten Wert für diese Anmerkung.

## (Optional) Bereitstellen einer Beispielanwendung

- Mindestens ein öffentliches oder privates Subnetz in Ihrer Cluster-VPC.
  - Lassen Sie den AWS Load Balancer Controller auf Ihrem Cluster bereitstellen. Weitere Informationen finden Sie unter [the section called “AWS Load Balancer Balancer-Controller”](#). Wir empfehlen Version 2.7.2 oder höher.
1. Wenn Sie in Fargate bereitstellen, stellen Sie sicher, dass in Ihrer VPC ein privates Subnetz verfügbar ist, und erstellen Sie ein Fargate-Profil. Wenn Sie nicht in Fargate bereitstellen, überspringen Sie diesen Schritt. Sie können das Profil erstellen, indem Sie den folgenden Befehl ausführen oder in [AWS Management Console](#) die gleichen Werte für name und namespace verwenden, die im Befehl enthalten sind. Ersetzen Sie das *example values* durch Ihr eigenes.

```
eksctl create fargateprofile \
 --cluster my-cluster \
 --region region-code \
 --name nlb-sample-app \

```

```
--namespace nlb-sample-app
```

## 2. Bereitstellen einer Beispielanwendung

- a. Erstellen Sie einen Namespace für die Anwendung.

```
kubectl create namespace nlb-sample-app
```

- b. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `sample-deployment.yaml` auf Ihrem Computer.

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: nlb-sample-app
 namespace: nlb-sample-app
spec:
 replicas: 3
 selector:
 matchLabels:
 app: nginx
 template:
 metadata:
 labels:
 app: nginx
 spec:
 containers:
 - name: nginx
 image: public.ecr.aws/nginx/nginx:1.23
 ports:
 - name: tcp
 containerPort: 80
```

- c. Wenden Sie die Manifestdatei auf Ihren Cluster an.

```
kubectl apply -f sample-deployment.yaml
```

3. Erstellen Sie einen Service mit einem zum Internet offenen Network Load Balancer, der Load Balancing auf IP-Ziele vornimmt.

- a. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen `sample-service.yaml` auf Ihrem Computer. Wenn Sie auf Fargate-Knoten bereitstellen, entfernen Sie die

`service.beta.kubernetes.io/aws-load-balancer-scheme: internet-facing`  
Leitung.

```
apiVersion: v1
kind: Service
metadata:
 name: nlb-sample-service
 namespace: nlb-sample-app
 annotations:
 service.beta.kubernetes.io/aws-load-balancer-type: external
 service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: ip
 service.beta.kubernetes.io/aws-load-balancer-scheme: internet-facing
spec:
 ports:
 - port: 80
 targetPort: 80
 protocol: TCP
 type: LoadBalancer
 selector:
 app: nginx
```

b. Wenden Sie die Manifestdatei auf Ihren Cluster an.

```
kubectl apply -f sample-service.yaml
```

4. Stellen Sie sicher, dass der Dienst bereitgestellt wurde.

```
kubectl get svc nlb-sample-service -n nlb-sample-app
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME           | TYPE         | CLUSTER-IP     | EXTERNAL-IP                                                                       | AGE              |
|----------------|--------------|----------------|-----------------------------------------------------------------------------------|------------------|
| sample-service | LoadBalancer | 10.100.240.137 | k8s-nlbsampl-nlbsampl-xxxxxxxxxx-xxxxxxxxxxxxxxxxxx.elb.region-code.amazonaws.com | 80:32400/TCP 16h |

#### Note

Die Werte für **10.100.240.137** und **xxxxxxxxxx** - unterscheiden  
**xxxxxxxxxxxxxxxxxx** sich von der Beispielausgabe (sie gelten nur für Ihren Load

Balancer) und *us-west-2* können für Sie unterschiedlich sein, je nachdem, in welcher AWS Region sich Ihr Cluster befindet.

5. Öffne den [Amazon EC2 AWS Management Console](#). Wählen Sie Target Groups (Zielgruppen) unter Load Balancing (Lastausgleich) im linken Navigationsbereich aus. Wählen Sie in der Spalte Name den Namen der Zielgruppe aus, wobei der Wert in der Spalte Load Balancer einem Teil des Namens in der EXTERNAL-IP Spalte der Ausgabe im vorherigen Schritt entspricht. Sie würden beispielsweise die benannte Zielgruppe auswählen, *k8s-default-samplese-xxxxxxxxxx* wenn Ihre Ausgabe mit der vorherigen Ausgabe identisch wäre. Der Zieltyp ist IP, weil dies im Beispiel-Manifest des Services angegeben wurde.
6. Wählen Sie Ihre Zielgruppe und danach die Registerkarte Ziele aus. Unter Registrierte Ziele sollten Sie drei IP-Adressen der drei Replikate sehen, die in einem vorherigen Schritt bereitgestellt wurden. Warten Sie, bis der Status aller Ziele fehlerfrei ist, bevor Sie fortfahren. Möglicherweise dauert es ein paar Minuten, bis alle Ziele *healthy* sind. Die Ziele können sich in einem *unhealthy*-Zustand befinden, bevor sie in einen *healthy*-Zustand wechseln.
7. Senden Sie Datenverkehr an den Dienst, indem Sie *xxxxxxxxxx-xxxxxxxxxxxxxxxxxx* und *us-west-2* durch die Werte ersetzen, die in der Ausgabe für einen [vorherigen Schritt](#) für EXTERNAL-IP zurückgegeben wurden. Wenn Sie die Bereitstellung in einem privaten Subnetz durchgeführt haben, müssen Sie die Seite von einem Gerät in Ihrer VPC aus aufrufen, z. B. von einem Bastion-Host aus. Weitere Informationen finden Sie unter [Linux-Bastion-Hosts in AWS](#).

```
curl k8s-default-samplese-xxxxxxxxxx-xxxxxxxxxxxxxxxxxx.elb.region-code.amazonaws.com
```

Eine Beispielausgabe sieht wie folgt aus.

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
[...]
```

8. Wenn Sie mit der Beispielbereitstellung, dem Service und dem Namespace fertig sind, entfernen Sie sie.

```
kubectl delete namespace nlb-sample-app
```

# Weiterleiten von Anwendungs- und HTTP-Verkehr mit Application Load Balancers

## Note

Neu: Der automatische Modus von Amazon EKS automatisiert Routineaufgaben für den Lastenausgleich. Weitere Informationen finden Sie unter:

- [the section called “Stellen Sie den Load Balancer bereit”](#)
- [the section called “Ingress-Klasse erstellen”](#)

Wenn Sie ein Kubernetes erstellen `ingress`, wird ein AWS Application Load Balancer (ALB) bereitgestellt, der den Anwendungsdatenverkehr ausgleicht. Weitere Informationen finden Sie unter [Was ist ein Application Load Balancer?](#) im Application Load Balancers-Benutzerhandbuch und [Ingress](#) in der Kubernetes-Dokumentation. ALBs kann mit Pods verwendet werden, die auf Knoten oder in AWS Fargate bereitgestellt werden. Sie können einen ALB für öffentliche oder private Subnetze bereitstellen.

Der Anwendungsverkehr wird bei L7 des OSI-Modells ausgeglichen. Um den Netzwerkverkehr auf L4 auszugleichen, stellen Sie einen Kubernetes-service vom Typ `LoadBalancer` bereit. Dieser Typ stellt einen AWS Network Load Balancer bereit. Weitere Informationen finden Sie unter [the section called “Netzwerk-Load-Balancer”](#). Weitere Informationen zu den Unterschieden zwischen den beiden Arten von Load Balancing finden Sie auf der AWS Website unter [Elastic Load Balancing Balancing-Funktionen](#).

## Voraussetzungen

Bevor Sie den Anwendungsdatenverkehr auf eine Anwendung verteilen können, müssen Sie die folgenden Anforderungen erfüllen.

- Einen vorhandenen Cluster haben. Wenn Sie noch keinen Cluster haben, finden Sie weitere Informationen unter [Erste Schritte](#). Wenn Sie die Version eines vorhandenen Clusters aktualisieren müssen, finden Sie unter [the section called “Kubernetes-Version aktualisieren”](#).
- Lassen Sie den AWS Load Balancer Controller auf Ihrem Cluster bereitstellen. Weitere Informationen finden Sie unter [the section called “AWS Load Balancer Balancer-Controller”](#). Wir empfehlen Version 2.7.2 oder höher.

- Mindestens zwei Subnetze in verschiedenen Availability Zones. Der AWS Load Balancer Controller wählt aus jeder Availability Zone ein Subnetz aus. Wenn mehrere markierte Subnetze in einer Availability Zone gefunden werden, wählt der Controller das Subnetz aus, dessen Subnetz-ID lexikografisch an erster Stelle steht. Ein Subnetz muss jeweils mindestens acht verfügbare IP-Adressen aufweisen.

Wenn Sie mehrere Sicherheitsgruppen verwenden, die an den Worker-Knoten angehängt sind, muss genau eine Sicherheitsgruppe wie folgt gekennzeichnet werden. Ersetzen Sie *my-cluster* mit Ihrem Clusternamen.

- Schlüssel – `kubernetes.io/cluster/<my-cluster>`
- Wert – `shared` oder `owned`
- Wenn Sie die Load AWS Balancer Controller-Version 2.1.1 oder eine frühere Version verwenden, müssen Subnetze im folgenden Format gekennzeichnet werden. Wenn Sie Version 2.1.2 oder höher verwenden, ist das Taggen optional. Wir empfehlen jedoch, ein Subnetz zu markieren, falls einer der folgenden Fälle zutrifft. Sie haben mehrere Cluster, die in derselben VPC ausgeführt werden, oder haben mehrere AWS Dienste, die sich Subnetze in einer VPC teilen. Oder Sie möchten mehr Kontrolle darüber haben, wo Load Balancer für jeden Cluster bereitgestellt werden. Ersetzen Sie *my-cluster* durch Ihren Clusternamen.
  - Schlüssel – `kubernetes.io/cluster/<my-cluster>`
  - Wert – `shared` oder `owned`
- Ihre öffentlichen und privaten Subnetze müssen die folgenden Anforderungen erfüllen. Dies ist der Fall, es sei denn, Sie geben das Subnetz explizit IDs als Anmerkung zu einem Service- oder Eingangsobjekt an. Gehen Sie davon aus, dass Sie Load Balancer bereitstellen, indem Sie das Subnetz explizit IDs als Anmerkung zu einem Dienst- oder Eingangsobjekt angeben. In dieser Situation verwenden Kubernetes und der AWS Load Balancer-Controller diese Subnetze direkt, um den Load Balancer zu erstellen, und die folgenden Tags sind nicht erforderlich.
  - Private Subnetze – Müssen im folgenden Format markiert sein. Auf diese Weise wissen Kubernetes und der Load Balancer-Controller, dass die Subnetze für interne Load AWS Balancer verwendet werden können. Wenn Sie nach dem 26. März 2020 eine Amazon AWS CloudFormation EKS-Vorlage verwenden `eksctl`, um Ihre VPC zu erstellen, werden die Subnetze bei der Erstellung entsprechend gekennzeichnet. Weitere Informationen zu den Amazon AWS CloudFormation EKS-VPC-Vorlagen finden Sie unter [the section called “Erstellen einer VPC”](#).
    - Schlüssel – `kubernetes.io/role/internal-elb`
    - Wert – `1`

- Öffentliche Subnetze – Muss im folgenden Format markiert werden. So erkennt Kubernetes, dass nur die Subnetze verwendbar sind, die für externe Load Balancer angegeben wurden. Auf diese Weise wählt Kubernetes nicht in jeder Availability Zone ein öffentliches Subnetz aus (lexikografisch basierend auf ihrer Subnetz-ID). Wenn Sie nach dem 26. März 2020 eine Amazon AWS CloudFormation EKS-Vorlage verwenden<sup>1</sup>, um Ihre VPC zu erstellen, werden die Subnetze bei der Erstellung entsprechend gekennzeichnet. Weitere Informationen zu den Amazon AWS CloudFormation EKS-VPC-Vorlagen finden Sie unter [the section called “Erstellen einer VPC”](#).
- Schlüssel – `kubernetes.io/role/elb`
- Wert – `1`

Wenn die Subnetz-Rollen-Tags nicht explizit hinzugefügt werden, untersucht der Kubernetes Service Controller die Routentabelle Ihrer Cluster-VPC-Subnetze. Dadurch wird festgestellt, ob das Subnetz privat oder öffentlich ist. Wir empfehlen, dass Sie sich nicht auf dieses Verhalten verlassen. Fügen Sie stattdessen explizit die Rollen-Tags privat oder öffentlich hinzu. Der AWS Load Balancer Controller untersucht keine Routentabellen. Außerdem müssen die Tags privat und öffentlich für eine erfolgreiche automatische Erkennung vorhanden sein.

- Der [Load AWS Balancer Controller](#) erstellt ALBs und die erforderlichen unterstützenden AWS Ressourcen, wenn eine Kubernetes-Eingangsressource auf dem Cluster mit der Anmerkung erstellt wird. `kubernetes.io/ingress.class: alb` Die Ingress-Ressource konfiguriert den ALB so, dass er HTTP- oder HTTPS-Verkehr an verschiedene Pods innerhalb des Clusters weiterleitet. Um sicherzustellen, dass Ihre Ingress-Objekte den Load AWS Balancer Controller verwenden, fügen Sie Ihrer Kubernetes-Ingress-Spezifikation die folgende Anmerkung hinzu. Weitere Informationen finden Sie unter [Ingress-Spezifikation](#) auf GitHub.

```
annotations:
 kubernetes.io/ingress.class: alb
```

#### Note

Wenn Sie einen Load-Balancing für IPv6 Pods durchführen, fügen Sie Ihrer Ingress-Spezifikation die folgende Anmerkung hinzu. Load Balancing über IPv6 funktioniert nur auf IP-Ziele, nicht auf Instance-Ziele. Ohne diese Anmerkung verläuft das Load Balancing über IPv4.

```
alb.ingress.kubernetes.io/ip-address-type: dualstack
```

- Der AWS Load Balancer Controller unterstützt die folgenden Verkehrsmodi:
  - Instance – Registriert Knoten in Ihrem Cluster als Ziele für den ALB. Der Datenverkehr, der das ALB erreicht, wird NodePort für Ihren Dienst weitergeleitet und dann an Ihre Pods weitergeleitet. Dies ist der standardmäßige Datenverkehrsmodus. Sie können ihn auch explizit mit der `alb.ingress.kubernetes.io/target-type: instance`-Anmerkung angeben.

 Note

Ihr Kubernetes-Dienst muss den LoadBalancer Typ NodePort oder angeben, um diesen Verkehrsmodus zu verwenden.

- IP – Registriert Pods als Ziele für den ALB. Der Datenverkehr, der den ALB erreicht, wird für Ihren Service direkt an die Pods weitergeleitet. Sie müssen die `alb.ingress.kubernetes.io/target-type: ip`-Anmerkung angeben, um diesen Datenverkehrsmodus verwenden zu können. Der IP-Zieltyp ist erforderlich, wenn Ziel-Pods auf Fargate- oder Amazon EKS-Hybridknoten ausgeführt werden.
- Um ein vom Controller ALBs erstelltes Tag hinzuzufügen, fügen Sie dem Controller die folgende Anmerkung hinzu:`alb.ingress.kubernetes.io/tags`. Eine Liste aller verfügbaren Anmerkungen, die vom Load AWS Balancer Controller unterstützt werden, finden Sie unter [Ingress-Anmerkungen](#) auf GitHub
- Ein Upgrade oder Downgrade der ALB-Controller-Version kann zu einer Unterbrechung der Abwärtskompatibilität für Features führen, die darauf angewiesen sind. Weitere Informationen zu den Breaking Changes, die in jeder Version eingeführt werden, finden Sie in den Versionshinweisen zum [ALB-Controller](#) auf GitHub.

## Wiederverwendung mit Ingress-Gruppen ALBs

Sie können einen Application Load Balancer für mehrere Dienstressourcen gemeinsam nutzen, indem Sie `IngressGroups`

Um einen Ingress einer Gruppe hinzuzufügen, fügen Sie die folgende Anmerkung zu einer Kubernetes-Ingress-Ressourcenspezifikation hinzu.

```
alb.ingress.kubernetes.io/group.name: my-group
```



Der Gruppenname muss:

- Eine Länge von 63 oder weniger Zeichen haben.
- Aus Kleinbuchstaben, Zahlen, - und . bestehen
- Muss mit einer Zahl oder einem Buchstaben beginnen und enden.

Der Controller führt automatisch Ingress-Regeln für alle Ingresses in derselben Ingress-Gruppe zusammen. Es unterstützt sie mit einem einzigen ALB. Die meisten Anmerkungen, die auf einem Ingress definiert sind, gelten nur für die von diesem Ingress definierten Pfade. Standardmäßig gehören Eingangsressourcen keiner Eingangsgruppe an.

 Warning

Potenzielles Sicherheitsrisiko

Geben Sie nur dann eine Eingangsgruppe für einen Ingress an, wenn sich alle Kubernetes-Benutzer, die über die RBAC-Berechtigung zum Erstellen oder Ändern von Eingangsressourcen verfügen, innerhalb derselben Vertrauensgrenze befinden. Wenn Sie die Anmerkung mit einem Gruppennamen hinzufügen, können andere Kubernetes-Benutzer ihre Ingresses erstellen oder ändern, sodass sie derselben Ingress-Gruppe angehören. Dies kann zu unerwünschtem Verhalten führen, z. B. zum Überschreiben vorhandener Regeln durch Regeln mit höherer Priorität.

Sie können eine Reihenfolgennummer zu Ihrer Ingress-Ressource hinzufügen.

```
alb.ingress.kubernetes.io/group.order: '10'
```

Die Zahl kann 1-1000 sein. Die niedrigste Zahl für alle Ingresses in derselben Ingress-Gruppe wird zuerst ausgewertet. Alle Ingresses ohne diese Anmerkung werden mit dem Wert null bewertet. Doppelte Regeln mit einer höheren Nummer können Regeln mit einer niedrigeren Nummer überschreiben. Standardmäßig wird die Regelreihenfolge zwischen Ingressen innerhalb derselben Ingress-Gruppe lexikografisch basierend auf Namespace und Name bestimmt.

 **Important**

Stellen Sie sicher, dass jeder Ingress in derselben Ingress-Gruppe eine eindeutige Prioritätsnummer hat. Sie können keine doppelten Bestellnummern für mehrere Eingänge haben.

## (Optional) Bereitstellen einer Beispielanwendung

- Mindestens ein öffentliches oder privates Subnetz in Ihrer Cluster-VPC.
- Lassen Sie den AWS Load Balancer Controller auf Ihrem Cluster bereitstellen. Weitere Informationen finden Sie unter [the section called “AWS Load Balancer Balancer-Controller”](#). Wir empfehlen Version 2.7.2 oder höher.

Sie können die Beispielanwendung auf einem Cluster mit EC2 Amazon-Knoten, Fargate Pods oder beidem ausführen.

1. Wenn Sie nicht in Fargate bereitstellen, überspringen Sie diesen Schritt. Wenn Sie in Fargate bereitstellen, erstellen Sie ein Fargate-Profil. Sie können das Profil erstellen, indem Sie den folgenden Befehl ausführen oder in [AWS Management Console](#) die gleichen Werte für name und namespace verwenden, die im Befehl enthalten sind. Ersetzen Sie das *example values* durch Ihr eigenes.

```
eksctl create fargateprofile \
 --cluster my-cluster \
 --region region-code \
 --name alb-sample-app \
 --namespace game-2048
```

2. Stellen Sie das Spiel [2048](#) als Beispielanwendung bereit, um zu überprüfen, ob der Load AWS Balancer Controller als Ergebnis des AWS Eingangsobjekts eine ALB erstellt. Führen Sie die Schritte für den Subnetztyp aus, in dem Sie die Bereitstellung durchführen.
  - a. Wenn Sie die Bereitstellung auf Pods in einem Cluster durchführen, den Sie mit der IPv6 Familie erstellt haben, fahren Sie mit dem nächsten Schritt fort.
    - Öffentlich::

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/examples/2048/2048_full.yaml
```

- Privat::

A. Laden Sie das Manifest herunter.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/examples/2048/2048_full.yaml
```

B. Bearbeiten Sie die Datei und suchen Sie die Zeile mit der Aufschrift `alb.ingress.kubernetes.io/scheme: internet-facing`.

C. Ändern Sie *internet-facing* in `internal` und speichern Sie die Datei.

D. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f 2048_full.yaml
```

b. Wenn Sie die Bereitstellung auf Pods in einem Cluster durchführen, den Sie mit der [IPv6 Familie](#) erstellt haben, führen Sie die folgenden Schritte aus.

i. Laden Sie das Manifest herunter.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/examples/2048/2048_full.yaml
```

ii. Öffnen Sie die Datei in einem Editor und fügen Sie die folgende Zeile zu den Anmerkungen in der Ingress-Spezifikation hinzu.

```
alb.ingress.kubernetes.io/ip-address-type: dualstack
```

iii. Wenn Sie den Lastenausgleich für interne Pods und nicht für Pods mit Internetzugriff durchführen, ändern Sie die Zeile mit der `alb.ingress.kubernetes.io/scheme: internet-facing` Aufschrift `alb.ingress.kubernetes.io/scheme: internal`

iv. Speichern Sie die Datei.

v. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f 2048_full.yaml
```

- Überprüfen Sie nach ein paar Minuten mit dem folgenden Befehl, ob die Ressource für eingehenden Datenverkehr erstellt wurde.

```
kubectl get ingress/ingress-2048 -n game-2048
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME         | CLASS  | HOSTS | ADDRESS                                                                  |
|--------------|--------|-------|--------------------------------------------------------------------------|
|              |        | PORTS | AGE                                                                      |
| ingress-2048 | <none> | *     | k8s-game2048-ingress2-xxxxxxxxx-yyyyyyyyyy.region-code.elb.amazonaws.com |
|              |        | 80    | 2m32s                                                                    |

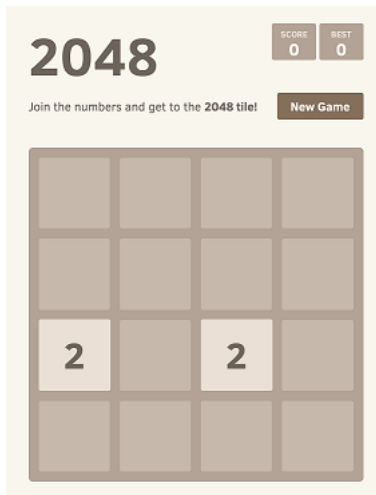
#### Note

Wenn Sie den Load Balancer in einem privaten Subnetz erstellt haben, wird dem Wert unter ADDRESS in der vorherigen Ausgabe `internal` - vorangestellt.

Wenn Ihr Ingress nach einigen Minuten nicht erfolgreich erstellt wurde, führen Sie den folgenden Befehl aus, um die Load AWS Balancer Controller-Protokolle anzuzeigen. Diese Protokolle können Fehlermeldungen enthalten, mit denen Sie Probleme mit Ihrer Bereitstellung diagnostizieren können.

```
kubectl logs -f -n kube-system -l app.kubernetes.io/instance=aws-load-balancer-controller
```

- Wenn Sie in einem öffentlichen Subnetz bereitgestellt haben, öffnen Sie einen Browser, und navigieren Sie zur ADDRESS-URL aus der vorherigen Befehlsausgabe, um die Beispielanwendung anzuzeigen. Wenn Sie nichts sehen, aktualisieren Sie Ihren Browser und versuchen Sie es erneut. Wenn Sie die Bereitstellung in einem privaten Subnetz durchgeführt haben, müssen Sie die Seite von einem Gerät in Ihrer VPC aus aufrufen, z. B. von einem Bastion-Host aus. Weitere Informationen finden Sie unter [Linux-Bastion-Hosts in AWS](#).



2. Wenn Sie mit dem Experimentieren mit Ihrer Beispielanwendung fertig sind, löschen Sie sie, indem Sie einen der folgenden Befehle ausführen.

- Wenn Sie das Manifest angewendet haben, anstatt eine heruntergeladene Kopie anzuwenden, verwenden Sie den folgenden Befehl.

```
kubectl delete -f https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.11.0/docs/examples/2048/2048_full.yaml
```

- Wenn Sie das Manifest heruntergeladen und bearbeitet haben, verwenden Sie den folgenden Befehl.

```
kubectl delete -f 2048_full.yaml
```

## Beschränken Sie externe IP-Adressen, die Diensten zugewiesen werden können

Kubernetes-Services können von innerhalb eines Clusters aus erreicht werden durch:

- Eine Cluster-IP-Adresse, die automatisch von Kubernetes zugewiesen wird
- Jede IP-Adresse, die Sie für die `externalIPs`-Eigenschaft in einer Service-Spezifikation festlegen. Externe IP-Adressen werden nicht von Kubernetes verwaltet und liegen in der Verantwortung des Cluster-Administrators. Externe IP-Adressen, die mit `externalIPs` festgelegt sind, unterscheiden sich von der externen IP-Adresse, die einem Service vom Typ `LoadBalancer` von einem Cloud-Anbieter zugewiesen ist.

Für weitere Informationen über Kubernetes Service, siehe [Service](#) in der Kubernetes-Dokumentation. Sie können die IP-Adressen einschränken, die für externalIPs in einer Service-Spezifikation festgelegt werden können.

1. Stellen Sie cert-manager bereit, um Webhook-Zertifikate zu verwalten. Weitere Informationen dazu finden Sie in der [cert-manager](#)-Dokumentation.

```
kubectl apply -f https://github.com/jetstack/cert-manager/releases/download/v1.5.4/cert-manager.yaml
```

2. Stellen Sie sicher, dass die cert-manager Pods laufen.

```
kubectl get pods -n cert-manager
```

Eine Beispielausgabe sieht wie folgt aus.

| NAME                                     | READY | STATUS  | RESTARTS | AGE |
|------------------------------------------|-------|---------|----------|-----|
| cert-manager-58c8844bb8-nlx7q            | 1/1   | Running | 0        | 15s |
| cert-manager-cainjector-745768f6ff-696h5 | 1/1   | Running | 0        | 15s |
| cert-manager-webhook-67cc76975b-4v4nk    | 1/1   | Running | 0        | 14s |

3. Überprüfen Sie Ihre vorhandenen Dienste, um sicherzustellen, dass keinem von ihnen externe IP-Adressen zugewiesen wurden, die nicht in dem CIDR-Block enthalten sind, auf den Sie die Adressen beschränken möchten.

```
kubectl get services -A
```

Eine Beispielausgabe sieht wie folgt aus.

| NAMESPACE                    | NAME                                  | TYPE      |
|------------------------------|---------------------------------------|-----------|
| CLUSTER-IP                   | EXTERNAL-IP                           | PORT(S)   |
| cert-manager                 | cert-manager                          | ClusterIP |
| 10.100.102.137               | <none>                                | 9402/TCP  |
| cert-manager                 | cert-manager-webhook                  | ClusterIP |
| 10.100.6.136                 | <none>                                | 443/TCP   |
| default                      | kubernetes                            | ClusterIP |
| 10.100.0.1                   | <none>                                | 443/TCP   |
| externalip-validation-system | externalip-validation-webhook-service | ClusterIP |
| 10.100.234.179               | <none>                                | 443/TCP   |

|               |             |               |      |           |
|---------------|-------------|---------------|------|-----------|
| kube-system   |             | kube-dns      |      | ClusterIP |
| 10.100.0.10   | <none>      | 53/UDP,53/TCP | 2d1h |           |
| my-namespace  |             | my-service    |      | ClusterIP |
| 10.100.128.10 | 192.168.1.1 | 80/TCP        | 149m |           |

Wenn es sich bei einem der Werte um IP-Adressen handelt, die sich nicht innerhalb des Blocks befinden, auf den Sie den Zugriff beschränken möchten, müssen Sie die Adressen so ändern, dass sie innerhalb des Blocks liegen, und die Dienste erneut bereitstellen. Dem my-service Dienst in der vorherigen Ausgabe wurde beispielsweise eine externe IP-Adresse zugewiesen, die nicht im CIDR-Blockbeispiel in Schritt 5 enthalten ist.

4. Laden Sie das externe IP-Webhook-Manifest herunter. Sie können auch den [Quellcode für Webhook](#) auf GitHub ansehen.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/docs/externalip-webhook.yaml
```

5. CIDR-Blöcke angeben. Öffnen Sie die heruntergeladene Datei in Ihrem Editor und entfernen Sie \# beim Start der folgenden Zeilen.

```
#args:
#- --allowed-external-ip-cidrs=10.0.0.0/8
```

Ersetzen Sie 10.0.0.0/8 mit Ihrem eigenen CIDR-Block. Sie können so viele Blöcke wie gewünscht festlegen. Wenn Sie mehrere Blöcke angeben, fügen Sie ein Komma zwischen Blöcken hinzu.

6. Wenn sich Ihr Cluster nicht in der us-west-2 AWS Region befindet, ersetzen Sie us-west-2602401143452, und amazonaws.com in der Datei durch die folgenden Befehle. Bevor Sie die Befehle ausführen, ersetzen Sie *region-code* und *111122223333* durch den Wert für Ihre AWS Region aus der Liste unter [Amazon Container-Image-Registries für Amazon EKS-Add-Ons anzeigen](#).

```
sed -i.bak -e 's|602401143452|111122223333|' externalip-webhook.yaml
sed -i.bak -e 's|us-west-2|region-code|' externalip-webhook.yaml
sed -i.bak -e 's|amazonaws.com||' externalip-webhook.yaml
```

7. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f externalip-webhook.yaml
```

Ein Versuch, in Ihrem Cluster einen Service mit einer angegebenen IP-Adresse bereitzustellen, scheitert, wenn die IP-Adresse nicht in den CIDR-Blöcken angegeben ist, die Sie im Schritt CIDR-Blöcke angeben angegeben haben, schlägt fehl.

## Kopieren eines Container-Images von einem Repository in ein anderes

In diesem Thema wird beschrieben, wie Sie ein Container-Image aus einem Repository abrufen, auf das Ihre Knoten keinen Zugriff haben, und das Image in ein Repository übertragen, auf das Ihre Knoten Zugriff haben. Das Image können Sie in Amazon ECR oder ein alternatives Repository verschieben, auf das die Knoten Zugriff haben.

- Die Docker-Engine ist auf Ihrem Computer installiert und konfiguriert. Weitere Informationen finden Sie unter [Installieren der Docker-Engine](#) in der Docker-Dokumentation.
- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie yumapt-get, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Ein VPC-Schnittstellen-Endpunkt für Amazon ECR, wenn Sie möchten, dass Ihre Knoten Container-Images aus einem privaten Amazon ECR-Repository über das Amazon-Netzwerk abrufen oder Container-Images in ein privates Amazon ECR-Repository übertragen. Weitere Informationen finden Sie unter [Erstellen der VPC Endpunkte für Amazon ECR](#) im Benutzerhandbuch von Amazon Elastic Container Registry.

Gehen Sie wie folgt vor, um ein Container-Image aus einem Repository abzurufen und es in ein eigenes Repository zu verschieben. In den folgenden Beispielen, die in diesem Thema bereitgestellt werden, wird das Image für den [Amazon VPC CNI-Plug-In für den Kubernetes-Metrik-Helper](#)



abgerufen. Ersetzen Sie beim Ausführen dieser Schritte die *example values* unbedingt durch eigene Werte.

1. Wenn Sie noch kein Amazon ECR-Repository oder ein anderes Repository haben, erstellen Sie eines, auf das Ihre Knoten Zugriff haben. Mit dem folgenden Befehl wird ein privates Amazon-ECR-Repository erstellt. Der Name eines privaten Amazon-ECR-Repositorys muss mit einem Buchstaben beginnen. Er darf nur Kleinbuchstaben, Zahlen, Bindestriche (-), Unterstriche (\_) und Schrägstriche (/) enthalten. Weitere Informationen finden Sie unter [Erstellen eines privaten Repositorys](#) im Benutzerhandbuch von Amazon Elastic Container Registry.

Sie können *cni-metrics-helper* mit einem beliebigen Namen ersetzen, den Sie wählen. Erstellen Sie – als bewährte Methode – ein separates Repository für jedes Image. Das wird empfohlen, weil Image-Tags in einem Repository eindeutig sein müssen. *region-code* Ersetzen Sie durch eine [AWS Region, die von Amazon ECR unterstützt wird](#).

```
aws ecr create-repository --region region-code --repository-name cni-metrics-helper
```

2. Bestimmen Sie die Registrierung, das Repository und das Tag (optional) des Images, das die Knoten abrufen müssen. Diese Informationen liegen im Format `registry/repository[:tag]` vor.

Bei vielen der Amazon-EKS-Themen zur Installation von Images müssen Sie eine Manifestdatei anwenden oder das Image mithilfe eines Helm-Charts installieren. Bevor Sie jedoch eine Manifestdatei anwenden oder ein Helm-Diagramm installieren, sollten Sie sich zunächst den Inhalt des Manifests oder der `values.yaml` Diagrammdatei ansehen. So können Sie die Registrierung, das Repository und das Tag für den Abrufvorgang bestimmen.

Sie finden beispielsweise die folgende Zeile in der [Manifestdatei](#) für den [Amazon VPC CNI-Plug-In für Kubernetes](#) Metrics Helper. Die Registrierung ist `602401143452.dkr.ecr.us-west-2.amazonaws.com`, eine private Amazon-ECR-Registrierung. Das Repository ist `cni-metrics-helper`.

```
image: "602401143452.dkr.ecr.us-west-2.amazonaws.com/cni-metrics-helper:v1.12.6"
```

Die folgenden Variationen sind bei einem Image-Speicherort möglich:

- Nur `repository-name:tag`. In diesem Fall ist in der Regel `docker.io` die Registrierung, aber nicht spezifiziert, da Kubernetes sie standardmäßig einem Repository-Namen voranstellt, wenn keine Registrierung angegeben ist.

- `repository-name/repository-namespace/repository:tag`. Ein Repository-Namespace ist optional, wird jedoch manchmal vom Repository-Besitzer zum Kategorisieren von Images angegeben. Beispielsweise verwenden alle [EC2 Amazon-Bilder in der Amazon ECR Public Gallery](#) den `aws-ec2` Namespace.

Zeigen Sie vor dem Installieren eines Images mit Helm die Helm-Datei `values.yaml` an, um den Image-Speicherort zu bestimmen. Die Datei [values.yaml](#) für den [Amazon VPC CNI Plugin for Kubernetes Metrics Helper](#) enthält beispielsweise die folgenden Zeilen.

```
image:
 region: us-west-2
 tag: v1.12.6
 account: "602401143452"
 domain: "amazonaws.com"
```

3. Rufen Sie das in der Manifestdatei angegebene Container-Image ab.
  - a. Wenn Sie Daten aus einer öffentlichen Registrierung abrufen, z. B. der [Amazon ECR Public Gallery](#), können Sie mit dem nächsten Unterschritt fortfahren, da keine Authentifizierung erforderlich ist. In diesem Beispiel authentifizieren Sie sich bei einer privaten Amazon-ECR-Registrierung, die das Repository für das Helper-Image für CNI-Kennzahlen enthält. Amazon EKS verwaltet das Image in jeder Registrierung, die unter [Amazon Container-Image-Registrierungen für Amazon EKS-Add-Ons anzeigen](#) aufgeführt ist. Die Authentifizierung ist bei jeder der Registrierungen möglich. Dazu ersetzen Sie `602401143452` und `region-code` durch die Informationen für eine andere Registrierung. Für jede [AWS Region, in der Amazon EKS unterstützt wird](#), gibt es eine separate Registrierung.

```
aws ecr get-login-password --region region-code | docker login --username AWS --password-stdin 602401143452.dkr.ecr.region-code.amazonaws.com
```

- b. Rufen Sie das Image ab. In diesem Beispiel erfolgt der Abruf aus der Registrierung, bei der Sie sich im letzten Unterschritt authentifiziert haben. Ersetzen Sie `602401143452` und `region-code` durch die Informationen, die Sie im vorherigen Unterschritt angegeben haben.

```
docker pull 602401143452.dkr.ecr.region-code.amazonaws.com/cni-metrics-helper:v1.12.6
```

4. Markieren Sie das abgerufene Image mit Ihrer Registrierung, Ihrem Repository und Ihrem Tag. Im folgenden Beispiel wird davon ausgegangen, dass Sie das Image über die Manifestdatei abgerufen haben und es in das private Amazon-ECR-Repository verschieben, das Sie im ersten

Schritt erstellt haben. Ersetzen Sie **111122223333** durch Ihre Konto-ID. **region-code** Ersetzen Sie es durch die AWS Region, in der Sie Ihr privates Amazon ECR-Repository erstellt haben.

```
docker tag cni-metrics-helper:v1.12.6 111122223333.dkr.ecr.region-code.amazonaws.com/cni-metrics-helper:v1.12.6
```

5. Authentifizieren Sie sich bei Ihrer Registrierung. In diesem Beispiel authentifizieren Sie sich bei der privaten Amazon-ECR-Registrierung, die Sie im ersten Schritt erstellt haben. Weitere Informationen finden Sie unter [Registrierungsauthentifizierung](#) im Benutzerhandbuch von Amazon Elastic Container Registry.

```
aws ecr get-login-password --region region-code | docker login --username AWS --password-stdin 111122223333.dkr.ecr.region-code.amazonaws.com
```

6. Verschieben Sie das Image in Ihr Repository. In diesem Beispiel verschieben Sie das Image in das private Amazon-ECR-Repository, das Sie im ersten Schritt erstellt haben. Weitere Informationen finden Sie unter [Verschieben eines Docker-Images](#) im Benutzerhandbuch von Amazon Elastic Container Registry.

```
docker push 111122223333.dkr.ecr.region-code.amazonaws.com/cni-metrics-helper:v1.12.6
```

7. Aktualisieren Sie die Manifestdatei, mit deren Hilfe Sie das Image in einem vorherigen Schritt bestimmt haben, mit den Werten `registry/repository:tag` für das verschobene Image. Wenn Sie mit einem Helm-Diagramm installieren, gibt es oft eine Option zur `registry/repository:tag` Angabe von. Geben Sie bei der Installation des Charts die Werte `registry/repository:tag` für das Image an, das Sie in das Repository verschoben haben.

## Amazon-Container-Image-Registrierungen für Amazon EKS-Add-Ons anzeigen

Wenn Sie [AWS Amazon-EKS-Add-Ons](#) in Ihrem Cluster bereitstellen, rufen Ihre Knoten die erforderlichen Container-Images aus der Registrierung ab, die im Installationsmechanismus für das Add-On angegeben ist, z. B. ein Installationsmanifest oder eine `values.yaml`-Helm-Datei. Die Images werden aus einem privaten Amazon-ECR-Repository abgerufen. Amazon EKS repliziert die Bilder in ein Repository in jeder von Amazon EKS unterstützten AWS Region. Die Knoten können das Container-Image über das Internet aus einer der folgenden Registrierungen abrufen. Alternativ können Ihre Knoten das Image über das Netzwerk von Amazon abrufen, wenn Sie in Ihrer

[VPC einen VPC-Schnittstellen-Endpunkt für Amazon ECR \(AWS PrivateLink\)](#) erstellt haben. Die Registries erfordern eine Authentifizierung mit einem IAM-Konto. AWS Ihre Knoten authentifizieren sich mithilfe der [Amazon EKS-Knoten-IAM-Rolle](#), der die Berechtigungen in der [Amazon EC2 ContainerRegistryReadOnly](#) Managed IAM-Richtlinie zugeordnet sind.

| AWS Region     | Registrierung                                     |
|----------------|---------------------------------------------------|
| af-south-1     | 877085696533.dkr.ecr.af-south-1.amazonaws.com     |
| ap-east-1      | 800184023465.dkr.ecr.ap-east-1.amazonaws.com      |
| ap-east-2      | 533267051163.dkr.ecr.ap-east-1.amazonaws.com      |
| ap-southeast-3 | 296578399912.dkr.ecr.ap-southeast-3.amazonaws.com |
| ap-south-2     | 900889452093.dkr.ecr.ap-south-2.amazonaws.com     |
| ap-southeast-4 | 491585149902.dkr.ecr.ap-southeast-4.amazonaws.com |
| ap-south-1     | 602401143452.dkr.ecr.ap-south-1.amazonaws.com     |
| ap-northeast-3 | 602401143452.dkr.ecr.ap-northeast-3.amazonaws.com |
| ap-northeast-2 | 602401143452.dkr.ecr.ap-northeast-2.amazonaws.com |
| ap-southeast-1 | 602401143452.dkr.ecr.ap-southeast-1.amazonaws.com |
| ap-southeast-2 | 602401143452.dkr.ecr.ap-southeast-2.amazonaws.com |

| AWS Region     | Registrierung                                            |
|----------------|----------------------------------------------------------|
| ap-southeast-7 | 121268973566.dkr.ecr.ap-southeast-7.<br>amazonaws.com    |
| ap-northeast-1 | 602401143452.dkr.ecr.ap-northeast-1.<br>amazonaws.com    |
| cn-north-1     | 918309763551.dkr.ecr.cn-north-1.amaz<br>onaws.com.cn     |
| cn-northwest-1 | 961992271922.dkr.ecr.cn-northwest-1.<br>amazonaws.com.cn |
| eu-central-1   | 602401143452.dkr.ecr.eu-central-1.am<br>azonaws.com      |
| eu-west-1      | 602401143452.dkr.ecr.eu-west-1.amazo<br>naws.com         |
| eu-west-2      | 602401143452.dkr.ecr.eu-west-2.amazo<br>naws.com         |
| eu-south-1     | 590381155156.dkr.ecr.eu-south-1.amaz<br>onaws.com        |
| eu-west-3      | 602401143452.dkr.ecr.eu-west-3.amazo<br>naws.com         |
| eu-south-2     | 455263428931.dkr.ecr.eu-south-2.amaz<br>onaws.com        |
| eu-north-1     | 602401143452.dkr.ecr.eu-north-1.amaz<br>onaws.com        |
| eu-central-2   | 900612956339.dkr.ecr.eu-central-2.am<br>azonaws.com      |
| il-central-1   | 066635153087.dkr.ecr.il-central-1.am<br>azonaws.com      |

| AWS Region    | Registrierung                                    |
|---------------|--------------------------------------------------|
| mx-central-1  | 730335286997.dkr.ecr.mx-central-1.amazonaws.com  |
| me-south-1    | 558608220178.dkr.ecr.me-south-1.amazonaws.com    |
| me-central-1  | 759879836304.dkr.ecr.me-central-1.amazonaws.com  |
| us-east-1     | 602401143452.dkr.ecr.us-east-1.amazonaws.com     |
| us-east-2     | 602401143452.dkr.ecr.us-east-2.amazonaws.com     |
| us-west-1     | 602401143452.dkr.ecr.us-west-1.amazonaws.com     |
| us-west-2     | 602401143452.dkr.ecr.us-west-2.amazonaws.com     |
| ca-central-1  | 602401143452.dkr.ecr.ca-central-1.amazonaws.com  |
| ca-west-1     | 761377655185.dkr.ecr.ca-west-1.amazonaws.com     |
| sa-east-1     | 602401143452.dkr.ecr.sa-east-1.amazonaws.com     |
| us-gov-east-1 | 151742754352.dkr.ecr.us-gov-east-1.amazonaws.com |
| us-gov-west-1 | 013241004608.dkr.ecr.us-gov-west-1.amazonaws.com |

# Amazon-EKS-Add-ons

Ein Add-on ist eine Software, die unterstützende Betriebsfunktionen für Kubernetes-Anwendungen bereitstellt, aber nicht anwendungsspezifisch ist. Dazu gehören Software wie Observability-Agenten oder Kubernetes-Treiber, die es dem Cluster ermöglichen, mit den zugrunde liegenden AWS Ressourcen für Netzwerke, Berechnungen und Speicher zu interagieren. Zusatzsoftware wird in der Regel von der Kubernetes-Community, Cloud-Anbietern oder Drittanbietern entwickelt und verwaltet. AWS Amazon EKS installiert automatisch selbstverwaltete Add-Ons wie das Amazon VPC CNI-Plugin für Kubernetes und CoreDNS für kube-proxy jeden Cluster. Beachten Sie, dass das VPC CNI-Add-On nicht mit Amazon EKS-Hybridknoten kompatibel ist und nicht auf Hybridknoten bereitgestellt werden kann. Sie können die Standardkonfiguration der Add-ons ändern und sie bei Bedarf aktualisieren.

Amazon-EKS-Add-ons bieten die Installation und Verwaltung eines ausgewählten Satzes von Add-ons für Amazon-EKS-Cluster. Alle Amazon EKS-Add-Ons enthalten die neuesten Sicherheitspatches und Bugfixes und sind für die Verwendung AWS mit Amazon EKS validiert. Mit Amazon-EKS-Add-ons können Sie konsequent sicherstellen, dass Ihre Amazon-EKS-Cluster sicher und stabil sind und den Arbeitsaufwand reduzieren, den Sie für die Installation, Konfiguration und Aktualisierung von Add-ons benötigen. Wenn ein selbstverwaltetes Add-on wie kube-proxy bereits auf Ihrem Cluster ausgeführt wird und als Amazon-EKS-Add-on verfügbar ist, können Sie das Amazon-EKS-Add-on kube-proxy installieren, um die Vorteile der Funktionen von Amazon-EKS-Add-ons zu nutzen.

Sie können bestimmte von Amazon EKS verwaltete Konfigurationsfelder für Amazon-EKS-Add-ons über die Amazon EKS API aktualisieren. Sie können auch Konfigurationsfelder, die nicht von Amazon EKS verwaltet werden, direkt im Kubernetes-Cluster ändern, sobald das Add-on gestartet wird. Dazu gehört das Definieren spezifischer Konfigurationsfelder für ein Add-on, falls zutreffend. Diese Änderungen werden von Amazon EKS nicht überschrieben, sobald sie vorgenommen wurden. Dies ist möglich mit der serverseitigen Anwendungsfunktion von Kubernetes. Weitere Informationen finden Sie unter [the section called “Felder, die Sie anpassen können”](#).

Sie können Amazon-EKS-Add-Ons mit allen Amazon-EKS-Knotentypen verwenden. Weitere Informationen finden Sie unter [Rechenleistung verwalten](#).

Sie können Amazon EKS-Add-Ons mithilfe der Amazon EKS-API, AWS CLI und hinzufügen AWS Management Console, aktualisieren oder löschen `kubectl`. Sie können Amazon-EKS-Add-ons auch mit [AWS CloudFormation](#) erstellen.

# Überlegungen

Beachten Sie Folgendes, wenn Sie Amazon EKS-Add-Ons verwenden:

- Um Add-ons für den Cluster zu konfigurieren, muss der [IAM-Prinzipal](#) über IAM-Berechtigungen verfügen, um mit Add-ons zu arbeiten. Weitere Informationen finden Sie in den Aktionen mit Addon in ihrem Namen in [Von Amazon Elastic Kubernetes Service definierte Aktionen](#).
- Amazon-EKS-Add-ons werden auf den Knoten ausgeführt, die Sie für Ihren Cluster bereitstellen oder konfigurieren. Zu den Knotentypen gehören EC2 Amazon-Instances, Fargate und Hybridknoten.
- Sie können Felder ändern, die nicht von Amazon EKS verwaltet werden, um die Installation eines Amazon EKS-Add-ons anzupassen. Weitere Informationen finden Sie unter [the section called “Felder, die Sie anpassen können”](#).
- Wenn Sie einen Cluster mit den Add-Ons Amazon EKS AWS Management Console kube-proxy, Amazon VPC CNI für Kubernetes und CoreDNS erstellen, werden Amazon EKS Add-Ons automatisch zu Ihrem Cluster hinzugefügt. Wenn Sie `config` verwenden, um Ihren Cluster mit einer `eksctl`-Datei zu erstellen, kann `eksctl` den Cluster auch mit Amazon-EKS-Add-ons erstellen. Wenn Sie Ihren Cluster `eksctl` ohne `config` Datei oder mit einem anderen Tool erstellen, werden das selbstverwaltete kube-proxy Amazon VPC CNI-Plug-In für Kubernetes und die CoreDNS-Add-Ons installiert und nicht die Amazon EKS-Add-Ons. Sie können sie entweder selbst verwalten oder die Amazon-EKS-Add-ons nach der Clustererstellung manuell hinzufügen. Unabhängig von der Methode, mit der Sie Ihren Cluster erstellen, wird das VPC CNI-Add-on nicht auf Hybridknoten installiert.
- Das `eks:addon-cluster-admin ClusterRoleBinding` bindet die an die `cluster-admin ClusterRole` Kubernetes-Identität. `eks:addon-manager` Die Rolle verfügt über die erforderlichen Berechtigungen für die `eks:addon-manager` Identität, um Kubernetes-Namespaces zu erstellen und Add-Ons in Namespaces zu installieren. Wenn `eks:addon-cluster-admin ClusterRoleBinding` entfernt wird, funktioniert der Amazon-EKS-Cluster weiterhin, Amazon EKS kann jedoch keine Add-Ons mehr verwalten. Alle Cluster ab den folgenden Plattformversionen verwenden das neue `ClusterRoleBinding`.
- Eine Teilmenge der EKS-Add-Ons von AWS wurde auf ihre Kompatibilität mit Amazon EKS Hybrid Nodes überprüft. Weitere Informationen finden Sie in der Kompatibilitätstabelle unter [the section called “ AWS Add-Ons”](#).



# Überlegungen zum Amazon EKS Auto Mode

Der Amazon EKS Auto-Modus umfasst Funktionen, die wichtige Cluster-Funktionen bereitstellen, darunter:

- Pod-Netzwerke
- Servicenetzwerke
- Cluster-DNS
- Auto Scaling
- Blockspeicher
- Loadbalancer-Controller
- Pod-Identitätsagent
- Agent zur Knotenüberwachung

Mit Compute im automatischen Modus werden viele häufig verwendete EKS-Add-Ons überflüssig, wie z. B.:

- Amazon VPC CNI
- kube-proxy
- CoreDNS
- Amazon EBS CSI-Treiber
- EKS Pod Identity Agent

Wenn Ihr Cluster den automatischen Modus jedoch mit anderen Rechenoptionen wie selbstverwalteten EC2 Instances, Managed Node Groups oder AWS Fargate kombiniert, bleiben diese Add-Ons weiterhin erforderlich. AWS hat EKS-Add-Ons um Anti-Affinitätsregeln erweitert, die automatisch sicherstellen, dass Add-On-Pods nur für unterstützte Compute-Typen geplant werden. Darüber hinaus können Benutzer jetzt die `DescribeAddonVersions` EKS-Add-Ons-API nutzen, um die unterstützten ComputeTypes für jedes Add-on und seine spezifischen Versionen zu überprüfen. Darüber hinaus laufen die oben aufgeführten Controller im EKS-Auto-Modus auf der AWS eigenen Infrastruktur. Sie werden sie also möglicherweise nicht einmal in Ihren Konten sehen, es sei denn, Sie verwenden den EKS-Automodus mit anderen Rechenarten. In diesem Fall werden Ihnen die Controller angezeigt, die Sie auf Ihrem Cluster installiert haben.

Wenn Sie planen, den automatischen EKS-Modus auf einem vorhandenen Cluster zu aktivieren, müssen Sie möglicherweise die Version bestimmter Addons aktualisieren. Weitere Informationen finden Sie unter [the section called “Erforderliche Zusatzversionen”](#) EKS Auto Mode.

## Support

AWS veröffentlicht mehrere Arten von Add-Ons mit unterschiedlichen Unterstützungsstufen.

- **AWS Add-Ons:** Diese Add-Ons wurden von entwickelt und werden vollständig unterstützt von AWS.
  - Verwenden Sie ein AWS Add-on, um mit anderen AWS Diensten wie Amazon EFS zu arbeiten.
  - Weitere Informationen finden Sie unter [the section called “ AWS Add-Ons”](#).
- **AWS Marketplace-Add-Ons:** Diese Add-Ons werden von einem unabhängigen AWS Partner gescannt AWS und von diesem unterstützt.
  - Verwenden Sie ein Marketplace-Add-on, um Ihrem Cluster wertvolle und anspruchsvolle Funktionen hinzuzufügen, wie z. B. die Überwachung mit Splunk.
  - Weitere Informationen finden Sie unter [the section called “Marketplace-Add-ons”](#).
- **Community-Add-ons:** Diese Add-Ons werden von der Open-Source-Community gescannt, AWS aber von ihr unterstützt.
  - Verwenden Sie ein Community-Add-on, um die Komplexität der Installation gängiger Open-Source-Software wie Kubernetes Metrics Server zu reduzieren.
  - Community-Add-Ons werden von erstellt. AWS AWS validiert nur Community-Add-Ons auf Versionskompatibilität.
  - Weitere Informationen finden Sie unter [the section called “Community-Erweiterungen”](#).

In der folgenden Tabelle wird der Umfang der Unterstützung für jeden Add-On-Typ detailliert beschrieben:

| Kategorie   | Funktion       | AWS Add-Ons | AWS Marketplace-Add-ons | Erweiterungen für die Community |
|-------------|----------------|-------------|-------------------------|---------------------------------|
| Entwicklung | Gebaut von AWS | Ja          | Nein                    | Ja                              |

| Kategorie    | Funktion                                        | AWS Add-Ons | AWS Marketplace-Add-ons | Erweiterungen für die Community |
|--------------|-------------------------------------------------|-------------|-------------------------|---------------------------------|
| Entwicklung  | Validiert von AWS                               | Ja          | Nein                    | Ja*                             |
| Entwicklung  | Vom AWS Partner validiert                       | Nein        | Ja                      | Nein                            |
| Wartung      | Gescannt von AWS                                | Ja          | Ja                      | Ja                              |
| Wartung      | Gepatcht von AWS                                | Ja          | Nein                    | Ja                              |
| Wartung      | Vom Partner gepatcht AWS                        | Nein        | Ja                      | Nein                            |
| Distribution | Herausgegeben von AWS                           | Ja          | Nein                    | Ja                              |
| Distribution | Herausgegeben von AWS Partner                   | Nein        | Ja                      | Nein                            |
| Support      | Grundlegende Installationsunterstützung von AWS | Ja          | Ja                      | Ja                              |
| Support      | Umfassender AWS Support                         | Ja          | Nein                    | Nein                            |
| Support      | AWS Umfassender Partner-Support                 | Nein        | Ja                      | Nein                            |

\*: Die Validierung für Community-Add-Ons beinhaltet nur die Kompatibilität mit der Kubernetes-Version. Wenn Sie beispielsweise ein Community-Add-on auf einem Cluster installieren, wird AWS geprüft, ob es mit der Kubernetes-Version Ihres Clusters kompatibel ist.

AWS Marketplace-Add-Ons können zusätzliche Softwareabhängigkeiten von externen Quellen außerhalb von heruntergeladenen AWS. Diese externen Abhängigkeiten werden von nicht gescannt oder validiert AWS. Berücksichtigen Sie Ihre Sicherheitsanforderungen bei der Bereitstellung von AWS Marketplace-Add-Ons, die externe Abhängigkeiten abrufen.

## AWS Add-Ons

Die folgenden Amazon-EKS-Add-Ons können in Ihrem Cluster erstellt werden. Sie können die aktuelle Liste der verfügbaren Add-Ons mithilfe `eksctl` der AWS Management Console oder der AWS CLI anzeigen. Informationen zu allen verfügbaren Add-Ons oder zur Installation eines Add-Ons finden Sie unter [the section called “Erstellen Sie ein Add-on”](#). Wenn für ein Add-on IAM-Berechtigungen erforderlich sind, benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen verfügen oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#). Sie können ein Add-on erstellen oder löschen, nachdem Sie es installiert haben. Weitere Informationen finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#) oder [the section called “Entfernen Sie ein Add-On”](#). Weitere Informationen zu Überlegungen, die speziell für die Ausführung von EKS-Add-Ons mit Amazon EKS-Hybridknoten gelten, finden Sie unter [the section called “Add-Ons konfigurieren”](#).

Sie können jedes der folgenden Amazon EKS-Add-Ons verwenden.

| Beschreibung                                                                        | Weitere Informationen                                                      | Kompatible Compute-Typen                           |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------|
| Stellen Sie native VPC-Netzwerke für Ihren Cluster bereit                           | <a href="#">the section called “Amazon-VPC-CNI-Plug-In für Kubernetes”</a> | EC2                                                |
| Ein flexibler, erweiterbarer DNS-Server, der als Kubernetes-Cluster-DNS dienen kann | <a href="#">the section called “CoreDNS”</a>                               | EC2, Fargate, EKS-Automatikmodus, EKS-Hybridknoten |

| Beschreibung                                                                                                            | Weitere Informationen                                                     | Kompatible Compute-Typen                           |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------|
| Pflegen Sie die Netzwerkeinstellungen auf jedem EC2 Amazon-Knoten                                                       | <a href="#">the section called “Kube-proxy ”</a>                          | EC2, EKS-Hybridknoten                              |
| Stellen Sie Amazon EBS-Speicher für Ihren Cluster bereit                                                                | <a href="#">the section called “Amazon-EBS-CSI-Treiber”</a>               | EC2                                                |
| Stellen Sie Amazon EFS-Speicher für Ihren Cluster bereit                                                                | <a href="#">the section called “Amazon EFS-CSI-Treiber”</a>               | EC2, Automatischer EKS-Modus                       |
| Stellen Sie Amazon FSx for Lustre-Speicher für Ihren Cluster bereit                                                     | <a href="#">the section called “Amazon FSx CSI-Treiber”</a>               | EC2, EKS-Automatikmodus                            |
| Stellen Sie Amazon S3 S3-Speicher für Ihren Cluster bereit                                                              | <a href="#">the section called “Mountpoint für Amazon S3 CSI-Treiber”</a> | EC2, EKS-Automatikmodus                            |
| Erkennen Sie weitere Probleme mit dem Zustand des Knotens                                                               | <a href="#">the section called “Agent zur Knotenüberwachung”</a>          | EC2, EKS-Hybridknoten                              |
| Aktivieren Sie die Verwendung der Snapshot-Funktionalität in kompatiblen CSI-Treibern, z. B. dem Amazon EBS CSI-Treiber | <a href="#">the section called “CSI-Snapshot-Controller”</a>              | EC2, Fargate, EKS-Automatikmodus, EKS-Hybridknoten |

| Beschreibung                                                                                                                                                                                                                                 | Weitere Informationen                                                                    | Kompatible Compute-Typen                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------|
| SageMaker HyperPod Task Governance optimiert die Zuweisung und Nutzung von Rechenressourcen durch Teams in Amazon EKS-Clustern und behebt damit Ineffizienzen bei der Priorisierung von Aufgaben und der gemeinsamen Nutzung von Ressourcen. | <a href="#">the section called “SageMaker HyperPod Amazon-Aufgabenverwaltung”</a>        | EC2, Automatischer EKS-Modus,                      |
| Amazon SageMaker HyperPod Observability AddOn bietet umfassende Überwachungs- und Beobachtbarkeitsfunktionen für HyperPod Cluster.                                                                                                           | <a href="#">the section called “Amazon SageMaker HyperPod Observability-Zusatzmodul”</a> | EC2, Automatischer EKS-Modus,                      |
| Ein Kubernetes-Agent, der Netzwerkflussdaten sammelt und an Amazon CloudWatch meldet und so eine umfassende Überwachung von TCP-Verbindungen zwischen Clusterknoten ermöglicht.                                                              | <a href="#">the section called “AWS Network Flow Monitor-Agent”</a>                      | EC2, EKS-Automatikmodus                            |
| Sicherer, produktionsreifer, AWS unterstützter Vertrieb des Projekts OpenTelemetry                                                                                                                                                           | <a href="#">the section called “AWS Distribution für OpenTelemetry”</a>                  | EC2, Fargate, EKS-Automatikmodus, EKS-Hybridknoten |

| Beschreibung                                                                                                                                                                                                                                                     | Weitere Informationen                                                         | Kompatible Compute-Typen                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|----------------------------------------------------|
| Sicherheitsüberwachungsservice, der grundlegende Datenquellen analysiert und verarbeitet, darunter AWS CloudTrail Verwaltungsereignisse und Amazon VPC-Flow-Logs. Amazon verarbeitet GuardDuty auch Funktionen wie Kubernetes-Audit-Logs und Laufzeitüberwachung | <a href="#">the section called “GuardDuty Amazon-Vertreter”</a>               | EC2, EKS-Automatikmodus                            |
| Überwachungs- und Beobachtbarkeitservice von AWS. Dieses Add-on installiert den CloudWatch Agenten und aktiviert sowohl CloudWatch Application Signals als auch CloudWatch Container Insights mit verbesserter Observability für Amazon EKS                      | <a href="#">the section called “Amazon CloudWatch Observability-Agent”</a>    | EC2, EKS-Automatikmodus, EKS-Hybridknoten          |
| Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie EC2 Instanzprofile Anmeldeinformationen für EC2 Instanzen bereitstellen                                                                                                         | <a href="#">the section called “EKS Pod Identity Agent”</a>                   | EC2, EKS-Hybridknoten                              |
| Aktivieren Sie den Cert-Manager, um X.509-Zertifikate von AWS einer privaten CA auszustellen. Erfordert den Cert-Manager.                                                                                                                                        | <a href="#">the section called “AWS Privater CA-Connector für Kubernetes”</a> | EC2, Fargate, EKS-Automatikmodus, EKS-Hybridknoten |

## Amazon-VPC-CNI-Plug-In für Kubernetes

Das Amazon VPC CNI-Plug-In für Kubernetes Amazon EKS ist ein Kubernetes Container Network Interface (CNI) -Plugin, das native VPC-Netzwerke für Ihren Cluster bereitstellt. Der selbstverwaltete oder verwaltete Typ dieses Add-ons ist standardmäßig auf jedem EC2 Amazon-Knoten installiert. Weitere Informationen finden Sie unter [Kubernetes Container Network Interface \(CNI\) -Plugin](#).

### Note

Sie müssen dieses Add-on nicht auf Amazon EKS Auto Mode-Clustern installieren. Weitere Informationen finden Sie unter [the section called “Überlegungen zum Amazon EKS Auto Mode”](#).

Der Name des Amazon EKS-Add-ons lautet `vpccni`.

### Erforderliche IAM-Berechtigungen

Dieses Add-on verwendet die Funktion IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#).

Wenn Ihr Cluster die IPv4-Familie verwendet, sind die Berechtigungen in der [AmazonEKS\\_CNI\\_Policy](#) erforderlich. [Wenn Ihr Cluster die IPv6 Familie verwendet, müssen Sie eine IAM-Richtlinie mit den Berechtigungen im IPv6 Modus erstellen](#). Sie können eine IAM-Rolle erstellen, ihr eine der Richtlinien zuordnen und das vom Add-on verwendete Kubernetes-Dienstkonto mit dem folgenden Befehl mit Anmerkungen versehen.

Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *AmazonEKSVPCCNIRole* durch den Namen Ihrer Rolle. Wenn der Cluster die IPv6-Familie verwendet, ersetzen Sie *AmazonEKS\_CNI\_Policy* durch den Namen der Richtlinie, die Sie erstellt haben. Dieser Befehl setzt voraus, dass Sie [eksctl auf Ihrem Gerät installiert](#) haben. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle zu erstellen, die Richtlinie daran anzuhängen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#).

```
eksctl create iamserviceaccount --name aws-node --namespace kube-system --cluster my-cluster --role-name AmazonEKSVPCCNIRole \
 --role-only --attach-policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy --approve
```



## Informationen aktualisieren

Sie können jeweils nur eine Nebenversion aktualisieren. Wenn Ihre aktuelle Version beispielsweise `1.28.x-eksbuild.y` ist und Sie auf `1.30.x-eksbuild.y` aktualisieren möchten, müssen Sie zuerst ihre aktuelle Version auf `1.29.x-eksbuild.y` und dann auf `1.30.x-eksbuild.y` aktualisieren. Weitere Informationen zum Aktualisieren des Add-ons finden Sie unter [the section called “Aktualisieren \(EKS-Add-on\)”](#).

## CoreDNS

Das CoreDNS Amazon EKS Add-on ist ein flexibler, erweiterbarer DNS-Server, der als Kubernetes-Cluster-DNS dienen kann. Der selbstverwaltete oder verwaltete Typ dieses Add-Ons wurde standardmäßig installiert, als Sie Ihren Cluster erstellt haben. Wenn Sie einen Amazon-EKS-Cluster mit mindestens einem Knoten starten, werden standardmäßig zwei Replikate des CoreDNS-Image bereitgestellt, unabhängig von der Anzahl der in Ihrem Cluster bereitgestellten Knoten. Die CoreDNS-Pods bieten eine Namensauflösung für alle Pods im Cluster. Sie können die CoreDNS-Pods auf Fargate-Knoten bereitstellen, wenn Ihr Cluster ein Fargate-Profil mit einem Namespace enthält, der dem Namespace für die CoreDNS-Bereitstellung entspricht. Weitere Informationen finden Sie unter [the section called “Definieren Sie Profile”](#).

### Note

Sie müssen dieses Add-on nicht auf Amazon EKS Auto Mode-Clustern installieren. Weitere Informationen finden Sie unter [the section called “Überlegungen zum Amazon EKS Auto Mode”](#).

Der Name des Amazon EKS-Add-ons lautet `coredns`.

## Erforderliche IAM-Berechtigungen

Für dieses Add-on sind keine Berechtigungen erforderlich.

## Zusätzliche Informationen

Weitere Informationen zu CoreDNS finden Sie in der [Kubernetes-Dokumentation unter CoreDNS for Service Discovery](#) und [Customizing DNS Service](#).

## Kube-proxy

Das Kube-proxy Amazon EKS-Add-on verwaltet die Netzwerkregeln auf jedem EC2 Amazon-Knoten. Es ermöglicht die Netzwerkkommunikation mit Ihren Pods. Der selbstverwaltete oder verwaltete Typ dieses Add-ons ist standardmäßig auf jedem EC2 Amazon-Knoten in Ihrem Cluster installiert.

### Note

Sie müssen dieses Add-on nicht auf Amazon EKS Auto Mode-Clustern installieren. Weitere Informationen finden Sie unter [the section called “Überlegungen zum Amazon EKS Auto Mode”](#).

Der Name des Amazon EKS-Add-ons lautet kube-proxy.

Erforderliche IAM-Berechtigungen

Für dieses Add-on sind keine Berechtigungen erforderlich.

Informationen aktualisieren

Bevor Sie Ihre aktuelle Version aktualisieren, sollten Sie die folgenden Anforderungen berücksichtigen:

- Kube-proxy hat auf einem Amazon EKS-Cluster dieselbe [Kompatibilitäts- und Schrägstellungsrichtlinie wie Kubernetes](#).

Zusätzliche Informationen

Weitere Informationen kube-proxy finden Sie unter [kube-proxy in der Kubernetes-Dokumentation](#).

## Amazon-EBS-CSI-Treiber

Das Amazon EBS CSI-Treiber Amazon EKS-Add-on ist ein Kubernetes Container Storage Interface (CSI) -Plugin, das Amazon EBS-Speicher für Ihren Cluster bereitstellt.

 Note

Sie müssen dieses Add-on nicht auf Amazon EKS Auto Mode-Clustern installieren. Der automatische Modus beinhaltet eine Blockspeicherfunktion. Weitere Informationen finden Sie unter [the section called “Stellen Sie einen statusbehafteten Work”](#).

Der Name des Amazon EKS-Add-ons lautet `aws-ebs-csi-driver`.

### Erforderliche IAM-Berechtigungen

Dieses Add-on nutzt die IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#). Die Berechtigungen in der von [Amazon EBSCSIDriver Policy](#) AWS verwalteten Richtlinie sind erforderlich. Sie können eine IAM-Rolle erstellen und ihr die verwaltete Richtlinie mit dem folgenden Befehl anfügen. Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *AmazonEKS\_EBS\_CSI\_DriverRole* durch den Namen Ihrer Rolle. Dieser Befehl setzt voraus, dass Sie [eksctl](#) auf Ihrem Gerät installiert haben. Wenn Sie ein anderes Tool oder einen benutzerdefinierten [KMS-Schlüssel](#) für die Verschlüsselung verwenden müssen, finden Sie weitere Informationen unter [the section called “Schritt 1: Erstellen einer IAM-Rolle”](#).

```
eksctl create iamserviceaccount \
 --name ebs-csi-controller-sa \
 --namespace kube-system \
 --cluster my-cluster \
 --role-name AmazonEKS_EBS_CSI_DriverRole \
 --role-only \
 --attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \
 --approve
```

### Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie unter [the section called “Amazon EBS”](#)

### Amazon EFS-CSI-Treiber

Das Amazon EKS-Add-on für den Amazon EFS-CSI-Treiber ist ein Kubernetes Container Storage Interface (CSI) -Plugin, das Amazon EFS-Speicher für Ihren Cluster bereitstellt.

Der Name des Amazon EKS-Add-ons lautet `aws-efs-csi-driver`.

## Erforderliche IAM-Berechtigungen

Erforderliche IAM-Berechtigungen — Dieses Add-on nutzt die IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#). Die Berechtigungen in der von [Amazon EFSCSIDriver Policy](#) AWS verwalteten Richtlinie sind erforderlich. Sie können eine IAM-Rolle erstellen und ihr die verwaltete Richtlinie mit dem folgenden Befehl anfügen. Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *AmazonEKS\_EFS\_CSI\_DriverRole* durch den Namen Ihrer Rolle. Diese Befehle setzen voraus, dass Sie [eksctl](#) auf Ihrem Gerät installiert haben. Wenn Sie ein anderes Tool verwenden müssen, finden Sie Informationen unter [the section called “Schritt 1: Erstellen einer IAM-Rolle”](#).

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
eksctl create iamserviceaccount \
 --name efs-csi-controller-sa \
 --namespace kube-system \
 --cluster $cluster_name \
 --role-name $role_name \
 --role-only \
 --attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
 --approve
TRUST_POLICY=$(aws iam get-role --output json --role-name $role_name --query
 'Role.AssumeRolePolicyDocument' | \
 sed -e 's/efs-csi-controller-sa/efs-csi-*/' -e 's/StringEquals/StringLike/')
aws iam update-assume-role-policy --role-name $role_name --policy-document
"$TRUST_POLICY"
```

## Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie unter [the section called “Amazon EFS”](#)

## Amazon FSx CSI-Treiber

Das Amazon EKS-Add-on für Amazon FSx CSI-Treiber ist ein Kubernetes Container Storage Interface (CSI) -Plugin, das Amazon FSx for Lustre-Speicher für Ihren Cluster bereitstellt.

Der Name des Amazon EKS-Add-ons lautet `aws-fsx-csi-driver`.

 Note

- Bereits vorhandene Amazon FSx CSI-Treiberinstallationen im Cluster können zu Fehlern bei der Installation von Add-Ons führen. Wenn Sie versuchen, die Amazon EKS-Add-On-Version zu installieren, während ein FSx Nicht-EKS-CSI-Treiber vorhanden ist, schlägt die Installation aufgrund von Ressourcenkonflikten fehl. Verwenden Sie die **OVERWRITE** Markierung während der Installation, um dieses Problem zu beheben:

```
aws eks create-addon --addon-name aws-fsx-csi-driver --cluster-name my-cluster
--resolve-conflicts OVERWRITE
```

- Das Amazon FSx CSI Driver EKS-Add-On benötigt den EKS Pod Identity-Agenten für die Authentifizierung. Ohne diese Komponente schlägt das Add-on mit dem Fehler `Amazon EKS Pod Identity agent is not installed in the cluster` und verhindert Volume-Operationen. Installieren Sie den Pod Identity-Agenten vor oder nach der Bereitstellung des FSx CSI-Treiber-Add-ons. Weitere Informationen finden Sie unter [the section called “Richten Sie den Agenten ein”](#).

## Erforderliche IAM-Berechtigungen

Dieses Add-on nutzt die IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#). Die Berechtigungen in der von [Amazon FSx FullAccess](#) AWS verwalteten Richtlinie sind erforderlich. Sie können eine IAM-Rolle erstellen und ihr die verwaltete Richtlinie mit dem folgenden Befehl anfügen. Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *AmazonEKS\_FSx\_CSI\_DriverRole* durch den Namen Ihrer Rolle. Dieser Befehl setzt voraus, dass Sie [eksctl](#) auf Ihrem Gerät installiert haben.

```
eksctl create iamserviceaccount \
 --name fsx-csi-controller-sa \
 --namespace kube-system \
 --cluster my-cluster \
 --role-name AmazonEKS_FSx_CSI_DriverRole \
 --role-only \
 --attach-policy-arn arn:aws: iam::aws:policy/AmazonFSxFullAccess \
 --approve
```

## Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie unter [the section called “Amazon FSx für Lustre”](#)

## Mountpoint für Amazon S3 CSI-Treiber

Das Amazon EKS-Add-on Mountpoint for Amazon S3 CSI Driver ist ein Kubernetes Container Storage Interface (CSI) -Plugin, das Amazon S3 S3-Speicher für Ihren Cluster bereitstellt.

Der Name des Amazon EKS-Add-ons lautet `aws-mountpoint-s3-csi-driver`.

### Erforderliche IAM-Berechtigungen

Dieses Add-on verwendet die Funktion IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#).

Für die erstellte IAM-Rolle ist eine Richtlinie erforderlich, die Zugriff auf S3 gewährt. Folgen Sie bei der [Erstellung der Richtlinie den Empfehlungen für Mountpoint IAM-Berechtigungen](#). Alternativ können Sie den Link für AWS verwaltete Richtlinien verwenden: `iam/home?#/policies/arn:aws:iam::aws:policy/amazons3 FullAccess` `$jsonEditor [amazonS3, type="console "],` aber diese verwaltete Richtlinie gewährt mehr Berechtigungen `FullAccess`, als für Mountpoint benötigt werden.

Sie können eine IAM-Rolle erstellen und ihr Ihre Richtlinie mit dem folgenden Befehl anfügen. *my-cluster* Ersetzen Sie es durch den Namen Ihres Clusters, *region-code* durch den richtigen AWS Regionalcode, *AmazonEKS\_S3\_CSI\_DriverRole* durch den Namen für Ihre Rolle und *AmazonEKS\_S3\_CSI\_DriverRole\_ARN* durch den Rollen-ARN. Für diese Befehle muss [eksctl auf Ihrem Gerät](#) installiert sein. Anweisungen zur Verwendung der IAM-Konsole oder AWS CLI finden Sie unter [the section called “Schritt 2: Erstellen einer IAM-Rolle”](#).

```
CLUSTER_NAME=my-cluster
REGION=region-code
ROLE_NAME=AmazonEKS_S3_CSI_DriverRole
POLICY_ARN=AmazonEKS_S3_CSI_DriverRole_ARN
eksctl create iamserviceaccount \
 --name s3-csi-driver-sa \
 --namespace kube-system \
 --cluster $CLUSTER_NAME \
 --attach-policy-arn $POLICY_ARN \
 --approve \
 --role-name $ROLE_NAME \
 --region $REGION \
```

```
--role-only
```

## Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie unter [the section called “Mountpoint für Amazon S3”](#).

## CSI-Snapshot-Controller

Der Container Storage Interface (CSI) -Snapshot-Controller ermöglicht die Verwendung der Snapshot-Funktionalität in kompatiblen CSI-Treibern, wie dem Amazon EBS CSI-Treiber.

Der Name des Amazon EKS-Add-ons lautet `snapshot-controller`.

## Erforderliche IAM-Berechtigungen

Für dieses Add-on sind keine Berechtigungen erforderlich.

## Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie unter [the section called “CSI-Snapshot-Controller”](#).

## SageMaker HyperPod Amazon-Aufgabenverwaltung

SageMaker HyperPod Task Governance ist ein robustes Managementsystem, das entwickelt wurde, um die Ressourcenzuweisung zu optimieren und eine effiziente Nutzung der Rechenressourcen durch Teams und Projekte für Ihre Amazon EKS-Cluster sicherzustellen. Dies bietet Administratoren die Möglichkeit, Folgendes festzulegen:

- Prioritätsstufen für verschiedene Aufgaben
- Berechne die Zuteilung für jedes Team
- Wie jedes Team ungenutzte Rechenleistung leiht und ausleiht
- Wenn ein Team seinen eigenen Aufgaben zuvorkommt

HyperPod Task Governance bietet auch Amazon EKS-Cluster-Observability und bietet so Echtzeiteinblicke in die Clusterkapazität. Dazu gehören die Verfügbarkeit und Nutzung von Rechenleistung, Teamzuweisung und -auslastung sowie Informationen zur Ausführung und Wartezeit von Aufgaben, sodass Sie fundierte Entscheidungen treffen und Ihre Ressourcen proaktiv verwalten können.

Der Name des Amazon EKS-Add-ons lautet `amazon-sagemaker-hyperpod-taskgovernance`.

### Erforderliche IAM-Berechtigungen

Für dieses Add-on sind keine Berechtigungen erforderlich.

### Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie unter [SageMaker HyperPod Task-Governance](#)

## Amazon SageMaker HyperPod Observability-Zusatzmodul

Das Amazon SageMaker HyperPod Observability Add-on bietet umfassende Überwachungs- und Beobachtbarkeitsfunktionen für HyperPod Cluster. Dieses Add-on implementiert und verwaltet automatisch wichtige Überwachungskomponenten wie den Node-Exporter, den DCGM-Exporter und den EFA-Exporter. kube-state-metrics Es sammelt Metriken und leitet sie an eine vom Kunden angegebene Amazon Managed Prometheus (AMP) -Instance weiter und stellt einen OTLP-Endpunkt für benutzerdefinierte Metriken und die Erfassung von Ereignissen aus Kundens Schulungen zur Verfügung.

Das Add-on lässt sich in das breitere HyperPod Ökosystem integrieren, indem es Metriken aus verschiedenen Komponenten wie dem HyperPod Task Governance-Add-on, Training Operator, Kubeflow und KEDA abrufen. HyperPod Alle gesammelten Metriken sind in Amazon Managed Prometheus zentralisiert, sodass Kunden über Amazon Managed Grafana-Dashboards eine einheitliche Beobachtbarkeitsansicht erhalten. Dies bietet end-to-end Einblick in den Zustand des Clusters, die Ressourcennutzung und die Leistung der Trainingsaufgaben in der gesamten Umgebung. HyperPod

Der Name des Amazon EKS-Add-ons lautet `amazon-sagemaker-hyperpod-observability`.

### Erforderliche IAM-Berechtigungen

Dieses Add-on verwendet die Funktion IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called “Referenzen bei IRSA”](#). Die folgenden verwalteten Richtlinien sind erforderlich:

- `AmazonPrometheusRemoteWriteAccess`— für das Schreiben von Metriken aus dem Cluster per Fernzugriff auf AMP
- `CloudWatchAgentServerPolicy`- für das Remote-Schreiben der Logs vom Cluster in CloudWatch



## Zusätzliche Informationen

Weitere Informationen über das Add-on und seine Funktionen finden Sie unter [SageMaker HyperPod Observability](#).

## AWS Network Flow Monitor-Agent

Der Amazon CloudWatch Network Flow Monitor Agent ist eine Kubernetes-Anwendung, die TCP-Verbindungsstatistiken von allen Knoten in einem Cluster sammelt und Netzwerkflussberichte für Amazon CloudWatch Network Flow Monitor Ingestion veröffentlicht. APIs

Der Name des Amazon EKS-Add-ons lautet `aws-network-flow-monitoring-agent`.

### Erforderliche IAM-Berechtigungen

Für dieses Add-on sind IAM-Berechtigungen erforderlich.

Sie müssen die `CloudWatchNetworkFlowMonitorAgentPublishPolicy` verwaltete Richtlinie an das Add-on anhängen.

Weitere Informationen zum erforderlichen IAM-Setup finden Sie unter [IAM-Richtlinie](#) im Amazon CloudWatch Network Flow Monitor GitHub Agent-Repository.

Weitere Informationen zur verwalteten Richtlinie finden Sie [CloudWatchNetworkFlowMonitorAgentPublishPolicy](#) im CloudWatch Amazon-Benutzerhandbuch.

## Zusätzliche Informationen

Weitere Informationen über das Add-on finden Sie im [Amazon CloudWatch Network Flow Monitor Agent GitHub Repo](#).

## Agent zur Knotenüberwachung

Das Amazon EKS-Add-on für den Knotenüberwachungsagenten kann zusätzliche Probleme mit dem Knotenstatus erkennen. Diese zusätzlichen Gesundheitssignale können auch durch die optionale Funktion zur auto Reparatur von Knoten genutzt werden, um Knoten bei Bedarf automatisch auszutauschen.

 Note

Sie müssen dieses Add-on nicht auf Amazon EKS Auto Mode-Clustern installieren. Weitere Informationen finden Sie unter [the section called “Überlegungen zum Amazon EKS Auto Mode”](#).

Der Name des Amazon EKS-Add-ons lautet `eks-node-monitoring-agent`.

Erforderliche IAM-Berechtigungen

Für dieses Add-on sind keine zusätzlichen Berechtigungen erforderlich.

Zusätzliche Informationen

Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).

## AWS Distribution für OpenTelemetry

Das Add-on AWS Distro for OpenTelemetry Amazon EKS ist eine sichere, produktionsbereite und AWS unterstützte Distribution des Projekts. OpenTelemetry Weitere Informationen finden Sie unter [AWS Distro](#) for on. OpenTelemetry GitHub

Der Name des Amazon EKS-Add-ons lautet `adot`.

Erforderliche IAM-Berechtigungen

Für dieses Add-on sind nur IAM-Berechtigungen erforderlich, wenn Sie eine der vorkonfigurierten benutzerdefinierten Ressourcen verwenden, für die Sie sich über die erweiterte Konfiguration anmelden können.

Zusätzliche Informationen

Weitere Informationen finden Sie in der Dokumentation unter [Erste Schritte mit AWS Distro für die OpenTelemetry Verwendung von EKS-Add-Ons](#) in der AWS Distro. OpenTelemetry

[ADOT setzt voraus, dass das cert-manager Add-on auf dem Cluster bereitgestellt wird. Andernfalls funktioniert dieses Add-on nicht, wenn es direkt über `https://registry.terraform.io/modules/terraform-aws-modules/eks/aws/latest` bereitgestellt wird.](#) Weitere Anforderungen finden Sie in der Dokumentation unter [Anforderungen für die ersten Schritte mit AWS Distro für die OpenTelemetry Verwendung von EKS-Add-Ons](#) in der AWS Distro. OpenTelemetry

## GuardDuty Amazon-Vertreter

Das Amazon EKS-Add-on für GuardDuty Agenten sammelt [Laufzeitereignisse](#) (Dateizugriff, Prozessausführung, Netzwerkverbindungen) von Ihren EKS-Clusterknoten zur Analyse durch GuardDuty Runtime Monitoring. GuardDuty selbst (nicht der Agent) ist der Sicherheitsüberwachungsdienst, der [grundlegende Datenquellen](#) wie AWS CloudTrail Verwaltungsereignisse und Amazon VPC-Flow-Logs sowie [Funktionen](#) wie Kubernetes-Auditprotokolle und Laufzeitüberwachung analysiert und verarbeitet.

Der Name des Amazon EKS-Add-ons lautet `aws-guardduty-agent`.

### Erforderliche IAM-Berechtigungen

Für dieses Add-on sind keine Berechtigungen erforderlich.

### Zusätzliche Informationen

Weitere Informationen finden Sie unter [Laufzeitüberwachung für Amazon EKS-Cluster in Amazon GuardDuty](#).

- Um potenzielle Sicherheitsbedrohungen in Ihren Amazon EKS-Clustern zu erkennen, aktivieren Sie Amazon GuardDuty Runtime Monitoring und stellen Sie den GuardDuty Security Agent auf Ihren Amazon EKS-Clustern bereit.

## Amazon CloudWatch Observability-Agent

Der Amazon CloudWatch Observability-Agent Amazon EKS erweitert den Überwachungs- und Observabilitätsservice von AWS. Dieses Add-on installiert den CloudWatch Agenten und aktiviert sowohl CloudWatch Application Signals als auch CloudWatch Container Insights mit verbesserter Observability für Amazon EKS. Weitere Informationen finden Sie unter [Amazon CloudWatch Agent](#).

Der Name des Amazon EKS-Add-ons lautet `amazon-cloudwatch-observability`.

### Erforderliche IAM-Berechtigungen

Dieses Add-on verwendet die Funktion IAM-Rollen für Dienstkonten von Amazon EKS. Weitere Informationen finden Sie unter [the section called "Referenzen bei IRSA"](#). Die Berechtigungen in den vom Link `iam/home#/policies/arn:aws:iam:::aws:arn:aws:iam::policy/AWSXrayWriteOnlyAccess[AWSXrayWriteOnlyAccess,type="console"]` and `link:iam/home#`

policies :aws:policy/ CloudWatchAgentServerPolicy [CloudWatchAgentServerPolicy, type="console"] verwalteten Richtlinien sind erforderlich. AWS Sie können eine IAM-Rolle erstellen, ihr die verwalteten Richtlinien zuordnen und das vom Add-on verwendete Kubernetes-Dienstkonto mit dem folgenden Befehl mit Anmerkungen versehen. Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *AmazonEKS\_Observability\_role* durch den Namen Ihrer Rolle. Dieser Befehl setzt voraus, dass Sie [eksctl auf Ihrem Gerät installiert](#) haben. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle zu erstellen, die Richtlinie daran anzuhängen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie unter [the section called “Weisen Sie eine IAM-Rolle zu”](#)

```
eksctl create iamserviceaccount \
 --name cloudwatch-agent \
 --namespace amazon-cloudwatch \
 --cluster my-cluster \
 --role-name AmazonEKS_Observability_Role \
 --role-only \
 --attach-policy-arn arn:aws: iam::aws:policy/AWSXrayWriteOnlyAccess \
 --attach-policy-arn arn:aws: iam::aws:policy/CloudWatchAgentServerPolicy \
 --approve
```

## Zusätzliche Informationen

Weitere Informationen finden Sie unter Den Agenten [installieren](#). CloudWatch

## AWS Privater CA-Connector für Kubernetes

Der AWS Private CA Connector for Kubernetes ist ein Add-on für Cert-Manager, mit dem Benutzer Zertifikate von einer AWS privaten Zertifizierungsstelle (Private CA) erhalten können.AWS

- Der Name des Amazon EKS-Add-ons lautetaws-privateca-connector-for-kubernetes.
- Der Add-On-Namespace istaws-privateca-issuer.

Dieses Add-on erfordertcert-manager. cert-managerist auf Amazon EKS als Community-Add-on verfügbar. Weitere Informationen zu diesem Add-on finden Sie unter[the section called “Zertifikatsmanager”](#). Weitere Informationen zur Installation von Add-Ons finden Sie unter[the section called “Erstellen Sie ein Add-on”](#).

## Erforderliche IAM-Berechtigungen

Für dieses Add-on sind IAM-Berechtigungen erforderlich.

Verwenden Sie EKS Pod Identities, um die `AWSPrivateCAConnectorForKubernetesPolicy` IAM-Richtlinie an das `aws-privateca-issuer` Kubernetes-Dienstkonto anzuhängen. Weitere Informationen finden Sie unter [the section called “Verwenden Sie Pod-Identitäten”](#).

Informationen zu den erforderlichen Berechtigungen finden Sie [AWSPrivateCAConnectorForKubernetesPolicy](#) in der Referenz zu verwalteten AWS Richtlinien.

## Zusätzliche Informationen

Weitere Informationen finden Sie im Repository [AWS Private CA Issuer for Kubernetes GitHub](#).

Weitere Informationen zur Konfiguration des Add-ons finden Sie unter [values.yaml](#) im Repo. `aws-privateca-issuer` GitHub Vergewissern Sie sich, dass die Version von `values.yaml` mit der Version des auf Ihrem Cluster installierten Add-ons übereinstimmt.

Dieses Add-on toleriert den `CriticalAddonsOnly` Makel, der vom EKS Auto Mode verwendet wird. `system NodePool` Weitere Informationen finden Sie unter [the section called “Führen Sie wichtige Add-Ons aus”](#).

## EKS Pod Identity Agent

Das Amazon EKS Pod Identity Agent Amazon EKS Add-on bietet die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie EC2 Instance-Profile Anmeldeinformationen für EC2 Instances bereitstellen.

### Note

Sie müssen dieses Add-on nicht auf Amazon EKS Auto Mode-Clustern installieren. Amazon EKS Auto Mode ist in EKS Pod Identity integriert. Weitere Informationen finden Sie unter [the section called “Überlegungen zum Amazon EKS Auto Mode”](#).

Der Name des Amazon EKS-Add-ons lautet `eks-pod-identity-agent`.

## Erforderliche IAM-Berechtigungen

Für das Pod Identity Agent-Add-On selbst ist keine IAM-Rolle erforderlich. Es verwendet die Berechtigungen der [Amazon EKS-Knoten-IAM-Rolle](#), um zu funktionieren, benötigt jedoch keine dedizierte IAM-Rolle für das Add-on.

## Informationen aktualisieren

Sie können jeweils nur eine Nebenversion aktualisieren. Wenn Ihre aktuelle Version beispielsweise 1.28.x-eksbuild.y ist und Sie auf 1.30.x-eksbuild.y aktualisieren möchten, müssen Sie zuerst ihre aktuelle Version auf 1.29.x-eksbuild.y und dann auf 1.30.x-eksbuild.y aktualisieren. Weitere Informationen zum Aktualisieren des Add-ons finden Sie unter [the section called “Aktualisieren Sie ein Add-on”](#).

## Community-Erweiterungen

Sie können AWS APIs Community-Add-Ons wie den Kubernetes Metrics Server installieren. Sie können sich dafür entscheiden, Community-Add-Ons als Amazon EKS-Add-Ons zu installieren, um die Komplexität der Wartung der Software auf mehreren Clustern zu reduzieren.

Sie können beispielsweise die AWS API, CLI oder die Management Console verwenden, um Community-Add-Ons zu installieren. Sie können ein Community-Add-on während der Clustererstellung installieren.

Sie verwalten Community-Add-Ons genauso wie bestehende Amazon EKS-Add-Ons. Community-Add-Ons unterscheiden sich von bestehenden Add-Ons dadurch, dass sie über einen einzigartigen Unterstützungsumfang verfügen.

### Note

Die Verwendung von Community-Add-Ons liegt in Ihrem Ermessen. Im Rahmen des [Modells der gemeinsamen Verantwortung](#) zwischen Ihnen und Ihnen wird von Ihnen erwartet AWS, dass Sie wissen, was Sie für diese Drittanbieter-Plugins in Ihrem Cluster installieren. Sie sind auch für die Community-Add-Ons verantwortlich, die Ihren Cluster-Sicherheitsanforderungen entsprechen. Weitere Informationen finden Sie unter [the section called “Support für Software, die auf EKS bereitgestellt wird”](#).

Community-Add-Ons werden von gepackt AWS. AWS validiert nur Community-Add-Ons auf Versionskompatibilität. Wenn Sie beispielsweise ein Community-Add-on auf einem Cluster installieren, wird AWS geprüft, ob es mit der Kubernetes-Version Ihres Clusters kompatibel ist.

Wichtig ist, dass Community-Add-Ons AWS nicht vollständig unterstützt werden. AWS unterstützt nur Lebenszyklusvorgänge, die mithilfe von Add-Ons ausgeführt werden AWS APIs, z. B. das Installieren von Add-Ons oder das Löschen von Add-Ons

Wenn Sie Unterstützung für ein Community-Add-on benötigen, nutzen Sie die vorhandenen Projektressourcen. Sie können beispielsweise ein GitHub Problem im Repo für das Projekt erstellen.

## Ermitteln Sie den Add-On-Typ

Sie können die AWS CLI verwenden, um den Typ eines Amazon EKS-Add-ons zu bestimmen.

Verwenden Sie den folgenden CLI-Befehl, um Informationen zu einem Add-on abzurufen. Sie können es `metrics-server` durch den Namen eines beliebigen Add-Ons ersetzen.

```
aws eks describe-addon-versions --addon-name metrics-server
```

Überprüfen Sie die CLI-Ausgabe für das `owner` Feld.

```
{
 "addons": [
 {
 "addonName": "metrics-server",
 "type": "observability",
 "owner": "community",
 "addonVersions": [
```

Wenn der Wert von `owner` `community` ist, handelt es sich bei dem Add-On um ein Community-Add-On. AWS bietet nur Unterstützung für die Installation, Aktualisierung und Deinstallation des Add-ons. Wenn Sie Fragen zur Funktionalität und zum Betrieb des Add-ons selbst haben, nutzen Sie Community-Ressourcen wie GitHub Issues.

## Installieren oder aktualisieren Sie das Community-Add-on

Sie installieren oder aktualisieren Community-Add-Ons auf die gleiche Weise wie andere Amazon EKS-Add-Ons.

- [the section called “Erstellen Sie ein Add-on”](#)
- [the section called “Aktualisieren Sie ein Add-on”](#)
- [the section called “Entfernen Sie ein Add-On”](#)

## Verfügbare Community-Add-Ons

Die folgenden Community-Add-Ons sind bei Amazon EKS erhältlich.

- [the section called “Kubernetes Metrics Server”](#)
- [the section called “kube-state-metrics”](#)
- [the section called “Prometheus-Knotenexporteur”](#)
- [the section called “Zertifikatsmanager”](#)
- [the section called “Externes DNS”](#)
- [the section called “Fluent Bit”](#)

## Kubernetes Metrics Server

Der Kubernetes Metrics Server ist eine skalierbare und effiziente Quelle für Container-Ressourcenmetriken für die integrierten Autoscaling-Pipelines von Kubernetes. Er sammelt Ressourcenmetriken von Kubelets und stellt sie im Kubernetes-Apiserver über die Metrics-API zur Verwendung durch Horizontal Pod Autoscaler und Vertical Pod Autoscaler zur Verfügung.

| Eigenschaft                           | Wert                          |
|---------------------------------------|-------------------------------|
| Name des Add-ons                      | metrics-server                |
| Namespace                             | kube-system                   |
| Dokumentation                         | <a href="#">GitHub Readme</a> |
| Servicekonto-Name                     | Keine                         |
| Verwaltete IAM-Richtlinie             | Keine                         |
| Benutzerdefinierte IAM-Berechtigungen | Keine                         |

## kube-state-metrics

Zusatzagent zum Generieren und Bereitstellen von Metriken auf Clusterebene.

Der Status von Kubernetes-Objekten in der Kubernetes-API kann als Metriken angezeigt werden. Ein aufgerufener Zusatzagent kube-state-metrics kann eine Verbindung zum Kubernetes-API-Server herstellen und einen HTTP-Endpunkt mit Metriken bereitstellen, die aus dem Status einzelner Objekte im Cluster generiert werden. Er stellt verschiedene Informationen über den Status von Objekten wie Labels und Anmerkungen, Start- und Endzeiten, Status oder die Phase, in der sich das Objekt gerade befindet, zur Verfügung.



| Eigenschaft                           | Wert                                                                    |
|---------------------------------------|-------------------------------------------------------------------------|
| Name des Add-ons                      | kube-state-metrics                                                      |
| Namespace                             | kube-state-metrics                                                      |
| Dokumentation                         | <a href="#">Metriken für Kubernetes-Objektstatus in Kubernetes Docs</a> |
| Servicekonto-Name                     | Keine                                                                   |
| Verwaltete IAM-Richtlinie             | Keine                                                                   |
| Benutzerdefinierte IAM-Berechtigungen | Keine                                                                   |

### Prometheus-Knotenexporteur

Prometheus-Exporter für Hardware- und Betriebssystemmetriken, bereitgestellt durch \*NIX-Kernel, geschrieben in Go mit austauschbaren Metrik-Kollektoren. Der Prometheus Node Exporter bietet eine Vielzahl von Hardware- und Kernel-Metriken.

| Eigenschaft                           | Wert                                                                                         |
|---------------------------------------|----------------------------------------------------------------------------------------------|
| Name des Add-ons                      | prometheus-node-exporter                                                                     |
| Namespace                             | prometheus-node-exporter                                                                     |
| Dokumentation                         | <a href="#">Überwachung von Linux-Host-Metriken mit dem Node Exporter</a> in Prometheus Docs |
| Servicekonto-Name                     | Keine                                                                                        |
| Verwaltete IAM-Richtlinie             | Keine                                                                                        |
| Benutzerdefinierte IAM-Berechtigungen | Keine                                                                                        |

## Zertifikatsmanager

Cert Manager kann verwendet werden, um die Erstellung und Erneuerung von Zertifikaten zu verwalten.

| Eigenschaft                           | Wert                                   |
|---------------------------------------|----------------------------------------|
| Name des Add-ons                      | cert-manager                           |
| Namespace                             | cert-manager                           |
| Dokumentation                         | <a href="#">Cert Manager-Dokumente</a> |
| Servicekonto-Name                     | Keine                                  |
| Verwaltete IAM-Richtlinie             | Keine                                  |
| Benutzerdefinierte IAM-Berechtigungen | Keine                                  |

## Externes DNS

Das External DNS EKS-Add-On kann verwendet werden, um Route53-DNS-Einträge über Kubernetes-Ressourcen zu verwalten.

Externe DNS-Berechtigungen können auf, und `route53:ListResourceRecordSets` auf die gehosteten Zonen reduziert werden  
`route53:ChangeResourceRecordSets``route53:ListHostedZones`, die Sie verwalten möchten.

| Eigenschaft       | Wert                          |
|-------------------|-------------------------------|
| Name des Add-ons  | external-dns                  |
| Namespace         | external-dns                  |
| Dokumentation     | <a href="#">GitHub Readme</a> |
| Servicekonto-Name | external-dns                  |

| Eigenschaft                           | Wert                                             |
|---------------------------------------|--------------------------------------------------|
| Verwaltete IAM-Richtlinie             | arn:aws: iam::aws:policy/AmazonRoute53FullAccess |
| Benutzerdefinierte IAM-Berechtigungen | Keine                                            |

## Fluent Bit

Fluent Bit ist ein leichter und leistungsstarker Protokollprozessor und Forwarder. Es ermöglicht Ihnen, Daten data/logs aus verschiedenen Quellen zu sammeln, zu vereinheitlichen und an mehrere Ziele zu senden, darunter Amazon CloudWatch Logs, Amazon S3 und Amazon Kinesis Data Firehose. Fluent Bit wurde unter Berücksichtigung von Leistung und Ressourceneffizienz entwickelt und eignet sich daher ideal für Kubernetes-Umgebungen.

Für dieses Add-on sind in der Standardkonfiguration keine IAM-Berechtigungen erforderlich. Möglicherweise müssen Sie diesem Add-on jedoch IAM-Berechtigungen gewähren, wenn Sie einen AWS Ausgabespeicherort konfigurieren. Weitere Informationen finden Sie unter [the section called “Verwenden Sie Pod-Identitäten”](#).

| Eigenschaft                           | Wert                                     |
|---------------------------------------|------------------------------------------|
| Name des Add-ons                      | fluent-bit                               |
| Namespace                             | fluent-bit                               |
| Dokumentation                         | <a href="#">Fluent Bit-Dokumentation</a> |
| Servicekonto-Name                     | fluent-bit                               |
| Verwaltete IAM-Richtlinie             | Keine                                    |
| Benutzerdefinierte IAM-Berechtigungen | Keine                                    |

## Zuschreibungen anzeigen

Sie können die Open-Source-Quellenangaben und Lizenzinformationen für Community-Add-Ons herunterladen.

1. Ermitteln Sie den Namen und die Version des Add-ons, für das Sie Attributionen herunterladen möchten.
2. Aktualisieren Sie den folgenden Befehl mit dem Namen und der Version:

```
curl -O https://amazon-eks-docs.s3.amazonaws.com/attributions/<add-on-name>/<add-on-version>/attributions.zip
```

Zum Beispiel:

```
curl -O https://amazon-eks-docs.s3.amazonaws.com/attributions/kube-state-metrics/v2.14.0-eksbuild.1/attributions.zip
```

3. Verwenden Sie den Befehl, um die Datei herunterzuladen.

Verwenden Sie diese ZIP-Datei, um Informationen zu den Lizenzzuweisungen anzuzeigen.

## AWS Marketplace-Add-ons

Zusätzlich zur vorherigen Liste der Amazon-EKS-Add-Ons können Sie auch eine große Auswahl an Amazon-EKS-Add-Ons für Betriebssoftware von unabhängigen Softwareanbietern hinzufügen. Wählen Sie ein Add-on aus, um mehr darüber und seine Installationsanforderungen zu erfahren.

### Accuknox

Der Name des Add-ons ist `accuknox_kubearmor` und der Namespace ist `kubearmor`. Accuknox veröffentlicht das Add-on.

Informationen zum Add-on finden Sie KubeArmor in der [Dokumentation unter Erste Schritte mit KubeArmor](#)

Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Akuity

Der Name des Add-ons ist `akuity_agent` und der Namespace ist `akuity`. Akuity veröffentlicht das Add-on.

Informationen zur Funktionsweise des Add-ons finden Sie unter [Installation des Akuity Agents auf Amazon EKS mit dem Akuity EKS-Add-on in der Akuity-Plattform-Dokumentation](#).

### Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Calyptia

Der Name des Add-ons ist `calyptia_fluent-bit` und der Namespace ist `calyptia-fluentbit`. Calyptia veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Getting Started with Calyptia Core Agent](#) auf der Calyptia-Dokumentationswebsite.

### Servicekonto-Name

Der Name des Dienstkontos lautet `calyptia-fluentbit`.

### AWS verwaltete IAM-Richtlinie

Dieses Add-on verwendet die `AWSMarketplaceMeteringRegisterUsage` verwaltete Richtlinie. Weitere Informationen finden Sie [AWSMarketplaceMeteringRegisterUsage](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

## Befehl zum Erstellen der erforderlichen IAM-Rolle

Der folgende Befehl setzt voraus, dass Sie über einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster verfügen. Um festzustellen, ob Sie über einen solchen verfügen oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#). Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *my-calyptia-role* durch den Namen Ihrer Rolle. Für diesen Befehl muss [eksctl](#) auf Ihrem Gerät installiert sein. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle zu erstellen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie weitere Informationen unter [the section called “Weisen Sie eine IAM-Rolle zu”](#)

```
eksctl create iamserviceaccount --name service-account-name --namespace calyptia-
fluentbit --cluster my-cluster --role-name my-calyptia-role \
--role-only --attach-policy-arn arn:aws:iam::aws:policy/
AWSMarketplaceMeteringRegisterUsage --approve
```

## Cisco Observability Collector

Der Name des Add-ons lautet `cisco_cisco-cloud-observability-collectors` und der Namespace ist `appdynamics`. Cisco veröffentlicht das Add-On.

Informationen zum Add-on finden Sie unter [Verwenden der Cisco Cloud Observability AWS Marketplace-Add-Ons](#) in der AppDynamics Cisco-Dokumentation.

### Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

### Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Cisco Observability Operator

Der Name des Add-ons lautet `cisco_cisco-cloud-observability-operators` und der Namespace ist `appdynamics`. Cisco veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Verwenden der Cisco Cloud Observability AWS Marketplace-Add-Ons](#) in der AppDynamics Cisco-Dokumentation.

## Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## CLOUDSOFT

Der Name des Add-ons ist `cloudsoft_cloudsoft-amp` und der Namespace ist `cloudsoft-amp`. CLOUDSOFT veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Amazon EKS ADDON](#) in der CLOUDSOFT-Dokumentation.

## Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Cribl

Der Name des Add-ons ist `cribl_cribledge` und der Namespace ist `cribledge`. Cribl veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in der [Cribl-Dokumentation unter Installation des Cribl Amazon EKS Add-ons für Edge](#)

## Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Dynatrace

Der Name des Add-ons ist `dynatrace_dynatrace-operator` und der Namespace ist. `dynatrace` Dynatrace veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Kubernetes-Monitoring](#) in der Dynatrace-Dokumentation.

## Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Datree

Der Name des Add-ons ist `datree_engine-pro` und der Namespace ist. `datree` Datree veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Amazon EKS-Integration in der Datree-Dokumentation](#).

## Servicekonto-Name

Der Name des Dienstkontos lautet. `datree-webhook-server-awsm`

## AWS verwaltete IAM-Richtlinie

Die verwaltete Richtlinie ist `AWSLicenseManagerConsumptionPolicy`. Weitere Informationen finden Sie [AWSLicenseManagerConsumptionPolicy](#) im Referenzhandbuch für AWS verwaltete Richtlinien..



## Befehl zum Erstellen der erforderlichen IAM-Rolle

Der folgende Befehl setzt voraus, dass Sie über einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster verfügen. Um festzustellen, ob Sie über einen solchen verfügen oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#). Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *my-datree-role* durch den Namen Ihrer Rolle. Für diesen Befehl muss [eksctl](#) auf Ihrem Gerät installiert sein. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle zu erstellen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie weitere Informationen unter [the section called “Weisen Sie eine IAM-Rolle zu”](#)

```
eksctl create iamserviceaccount --name datree-webhook-server-awsmp --namespace datree
--cluster my-cluster --role-name my-datree-role \
--role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/
AWSLicenseManagerConsumptionPolicy --approve
```

## Benutzerdefinierte Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Datadog

Der Name des Add-Ons ist `datadog_operator` und der Namespace ist `datadog-agent`. Datadog veröffentlicht das Add-On.

Informationen zum Add-on finden Sie unter [Installation des Datadog Agent auf Amazon EKS mit dem Datadog Operator Add-on in der Datadog-Dokumentation](#).

## Servicekonto-Name

Für dieses Add-on wird kein Servicekonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Bodendecker

Der Name des Add-ons lautet `groundcover_agent` und der Namespace ist `groundcover`. Groundcover veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Installation des Groundcover Amazon EKS Add-ons](#) in der Groundcover-Dokumentation.

#### Servicekonto-Name

Für dieses Add-on wird kein Servicekonto verwendet.

#### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

#### Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

### Grafana-Labore

Der Name des Add-ons ist `grafana-labs_kubernetes-monitoring` und der Namespace ist `monitoring`. Grafana Labs veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Konfiguration von Kubernetes Monitoring als Add-on mit Amazon EKS](#) in der Grafana Labs-Dokumentation.

#### Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

#### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

#### Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

### Guance

- Herausgeber — GUANCE
- Name (Name – `guance_datakit`)
- Namespace – `datakit`
- Name des Dienstkontos — Bei diesem Add-on wird kein Dienstkonto verwendet.
- AWS verwaltete IAM-Richtlinie — Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

- Benutzerdefinierte IAM-Berechtigungen — Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.
- Anweisungen zur Einrichtung und Verwendung — Weitere Informationen finden Sie [unter Amazon EKS-Add-on](#) verwenden in der Guance-Dokumentation.

## HA-Proxy

Der Name ist haproxy-technologies\_kubernetes-ingress-ee und der Namespace ist haproxy-controller. HA Proxy veröffentlicht das Add-On.

Informationen zum Add-on finden Sie unter [Amazon EKS-Integration in der Datree-Dokumentation](#).

### Servicekonto-Name

Der Name des Dienstkontos lautet. customer defined

### AWS verwaltete IAM-Richtlinie

Die verwaltete Richtlinie ist AWSLicenseManagerConsumptionPolicy. Weitere Informationen finden Sie [AWSLicenseManagerConsumptionPolicy](#) im Referenzhandbuch für AWS verwaltete Richtlinien..

### Befehl zum Erstellen der erforderlichen IAM-Rolle

Der folgende Befehl setzt voraus, dass Sie über einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster verfügen. Um festzustellen, ob Sie über einen solchen verfügen oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#). Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *my-haproxy-role* durch den Namen Ihrer Rolle. Für diesen Befehl muss [eksctl](#) auf Ihrem Gerät installiert sein. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle zu erstellen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie weitere Informationen unter. [the section called “Weisen Sie eine IAM-Rolle zu”](#)

```
eksctl create iamserviceaccount --name service-account-name --namespace haproxy-
controller --cluster my-cluster --role-name my-haproxy-role \
--role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/
AWSLicenseManagerConsumptionPolicy --approve
```

## Benutzerdefinierte Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Kow

Der Name des Add-ons ist `factorhouse_kpow` und der Namespace ist `factorhouse`. Factorhouse veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [AWS Marketplace LM](#) in der Kpow-Dokumentation.

### Servicekonto-Name

Der Name des Dienstkontos lautet `kpow`.

### AWS verwaltete IAM-Richtlinie

Die verwaltete Richtlinie ist `AWSLicenseManagerConsumptionPolicy`. Weitere Informationen finden Sie [AWSLicenseManagerConsumptionPolicy](#) im Referenzhandbuch für AWS verwaltete Richtlinien..

### Befehl zum Erstellen der erforderlichen IAM-Rolle

Der folgende Befehl setzt voraus, dass Sie über einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster verfügen. Um festzustellen, ob Sie über einen solchen verfügen oder um einen zu erstellen, lesen Sie [the section called "IAM OIDC-Anbieter"](#). Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *my-kpow-role* durch den Namen Ihrer Rolle. Für diesen Befehl muss [eksctl](#) auf Ihrem Gerät installiert sein. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle zu erstellen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie weitere Informationen unter [the section called "Weisen Sie eine IAM-Rolle zu"](#)

```
eksctl create iamserviceaccount --name kpow --namespace factorhouse --cluster my-cluster --role-name my-kpow-role \
 --role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy --approve
```

### Benutzerdefinierte Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Kubecost

Der Name des Add-ons lautet `kubecost_kubecost` und der Namespace ist `kubecost`. Kubecost veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [AWS Cloud Billing Integration](#) in der Kubecost-Dokumentation.

Sie müssen die [Store Kubernetes-Volumes mit Amazon EBS](#) auf Ihrem Cluster installiert haben. Andernfalls erhalten Sie eine Fehlermeldung.

### Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

### Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Kasten

Der Name des Add-ons ist `kasten_k10` und der Namespace ist `kasten-io`. Kasten by Veeam veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Installation von K10 unter AWS Verwendung des Amazon EKS Add-ons](#) in der Kasten-Dokumentation.

Sie müssen den Amazon EBS CSI-Treiber auf Ihrem Cluster mit einem Standard `StorageClass` installiert haben.

### Servicekonto-Name

Der Name des Dienstkontos lautet `k10-k10`.

### AWS verwaltete IAM-Richtlinie

Die verwaltete Richtlinie ist `AWSLicenseManagerConsumptionPolicy`. Weitere Informationen finden Sie [AWSLicenseManagerConsumptionPolicy](#) im Referenzhandbuch für AWS verwaltete Richtlinien..

### Befehl zum Erstellen der erforderlichen IAM-Rolle

Der folgende Befehl setzt voraus, dass Sie über einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster verfügen. Um festzustellen, ob Sie über einen solchen verfügen oder um einen zu erstellen, lesen Sie [the section called "IAM OIDC-Anbieter"](#). Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *my-kasten-role* durch den Namen Ihrer Rolle. Für diesen Befehl muss [eksctl](#) auf Ihrem Gerät installiert sein. Wenn Sie ein anderes Tool verwenden müssen, um die Rolle

zu erstellen und das Kubernetes-Dienstkonto mit Anmerkungen zu versehen, finden Sie weitere Informationen unter. [the section called “Weisen Sie eine IAM-Rolle zu”](#)

```
eksctl create iamserviceaccount --name k10-k10 --namespace kasten-io --cluster my-cluster --role-name my-kasten-role \
 --role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy --approve
```

## Benutzerdefinierte Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Kong

Der Name des Add-ons lautet `kong_konnect-ri` und der Namespace ist `kong`. Kong veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in [der Kong-Dokumentation unter Installation des Kong Gateway EKS Add-ons](#).

Sie müssen die [Store Kubernetes-Volumes mit Amazon EBS](#) auf Ihrem Cluster installiert haben. Andernfalls erhalten Sie eine Fehlermeldung.

## Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## LeakSignal

Der Name des Add-ons lautet `leaksignal_leakagent` und der Namespace ist `leakagent`. LeakSignal veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in der Dokumentation unter <https://www.leaksignal.com/docs/LeakAgent/Deployment/> AWS%20EKS%20Addon/ [Das Add-on installieren] LeakAgent LeakSignal

Sie müssen die [Store Kubernetes-Volumes mit Amazon EBS](#) auf Ihrem Cluster installiert haben. Andernfalls erhalten Sie eine Fehlermeldung.

### Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

### Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## NetApp

Der Name des Add-ons lautet `netapp_trident-operator` und der Namespace ist `trident`. NetApp veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in der NetApp Dokumentation unter [Konfiguration des Trident EKS-Add-ons](#).

### Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

### AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

### Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## New Relic

Der Name des Add-ons lautet `new-relic_kubernetes-operator` und der Namespace ist `newrelic`. New Relic veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in der New [Relic-Dokumentation unter Installation des New Relic Add-ons für EKS](#).

## Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Rafay

Der Name des Add-ons ist `rafay-systems_rafay-operator` und der Namespace ist `rafay-system`. Rafay veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Installation des Rafay Amazon EKS Add-ons](#) in der Rafay-Dokumentation.

## Servicekonto-Name

Für dieses Add-on wird kein Servicekonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Sicherheit lesen

- Herausgeber — RAD SECURITY
- Name (Name – `rad-security_rad-security`)
- Namespace – `ksoc`
- Name des Dienstkontos — Bei diesem Add-on wird kein Dienstkonto verwendet.
- AWS verwaltete IAM-Richtlinie — Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.
- Benutzerdefinierte IAM-Berechtigungen — Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.



- Anweisungen zur Einrichtung und Verwendung — Weitere Informationen finden Sie unter [Installation von Rad Through The AWS Marketplace](#) in der Rad Security-Dokumentation.

## SolarWinds

- Herausgeber — SOLARWINDS
- Name (Name – solarwinds\_swo-k8s-collector-addon
- Namespace – solarwinds
- Name des Dienstkontos — Mit diesem Add-on wird kein Dienstkonto verwendet.
- AWS verwaltete IAM-Richtlinie — Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.
- Benutzerdefinierte IAM-Berechtigungen — Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.
- Anweisungen zur Einrichtung und Verwendung — siehe [Überwachen eines Amazon EKS-Clusters](#) in der SolarWinds Dokumentation.

## Solo

Der Name des Add-ons lautet solo-io\_istio-distro und der Namespace ist istio-system. Solo veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Installation von Istio](#) in der Solo.io-Dokumentation.

Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Snyk

- Herausgeber — SNYK
- Name (Name – snyk\_runtime-sensor

- Namespace – `snyk_runtime-sensor`
- Name des Dienstkontos — Ein Dienstkonto wird mit diesem Add-on nicht verwendet.
- AWS verwaltete IAM-Richtlinie — Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.
- Benutzerdefinierte IAM-Berechtigungen — Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.
- Anweisungen zur Einrichtung und Verwendung — Weitere Informationen finden Sie unter [Snyk Runtime Sensor](#) in den Snyk-Benutzerdokumenten.

## Stormforge

Der Name des Add-ons ist `stormforge_optimize-Live` und der Namespace ist `stormforge-system`. Stormforge veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in [der Dokumentation unter Installation des StormForge Agenten](#). StormForge

Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Splunk

Der Name des Add-ons ist `splunk_splunk-otel-collector-chart` und der Namespace ist `splunk-monitoring`. Splunk veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Installieren des Splunk-Add-ons für Amazon EKS](#) in der Splunk-Dokumentation.

Servicekonto-Name

Für dieses Add-on wird kein Servicekonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Teleport

Der Name des Add-ons ist `teleport_teleport` und der Namespace ist `teleport`. Teleport veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in der [Teleport-Dokumentation unter So funktioniert Teleport](#).

## Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Tetrate

Der Name des Add-ons ist `tetrate-io_istio-distro` und der Namespace ist `istio-system`. Tetrate Io veröffentlicht das Add-on.

Informationen zum Add-on finden Sie auf der [Tetrate Istio](#) Distro-Website.

## Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

## AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

## Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Universal Crossplane für unterwegs

Der Name des Add-ons lautet `upbound_universal-crossplane` und der Namespace ist `upbound-system`. Upbound veröffentlicht das Add-on.

Informationen zum Add-on finden Sie unter [Upbound Universal Crossplane \(UXP\)](#) in der Upbound-Dokumentation.

Servicekonto-Name

Ein Dienstkonto wird mit diesem Add-on nicht verwendet.

AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Aufwind

Der Name des Add-ons ist `upwind` und der Namespace ist `upwind`. Upwind veröffentlicht das Add-on.

Informationen zum Add-on finden Sie in der [Upwind-Dokumentation](#).

Servicekonto-Name

Für dieses Add-on wird kein Dienstkonto verwendet.

AWS verwaltete IAM-Richtlinie

Eine verwaltete Richtlinie wird mit diesem Add-on nicht verwendet.

Benutzerdefinierte IAM-Berechtigungen

Benutzerdefinierte Berechtigungen werden mit diesem Add-on nicht verwendet.

## Ein Amazon EKS-Add-on erstellen

Amazon EKS-Add-ons sind Zusatzsoftware für Amazon EKS-Cluster. Alle Amazon-EKS-Add-ons:

- Fügen Sie die neuesten Sicherheitspatches und Bugfixes hinzu.
- Sind für die Verwendung AWS mit Amazon EKS validiert.
- Reduzieren Sie den Arbeitsaufwand für die Verwaltung der Zusatzsoftware.

Sie können ein Amazon EKS-Add-on mithilfe `eksctl` der AWS Management Console oder der AWS CLI erstellen. Wenn für das Add-on eine IAM-Rolle erforderlich ist, finden Sie in den Details für das jeweilige Add-on in [Amazon EKS-Add-Ons](#) weitere Informationen zur Erstellung der Rolle.

## Voraussetzungen

Gehen Sie wie folgt vor, bevor Sie ein Add-on erstellen:

- Der Cluster muss vorhanden sein, bevor Sie ein Add-On dafür erstellen können. Weitere Informationen finden Sie unter [the section called “Erstellen eines -Clusters”](#).
- Prüfen Sie, ob Ihr Add-on eine IAM-Rolle benötigt. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die Kompatibilität”](#).
- Stellen Sie sicher, dass die Amazon EKS-Add-On-Version mit Ihrem Cluster kompatibel ist. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die Kompatibilität”](#).
- Vergewissern Sie sich, dass Version 0.190.0 oder höher des `eksctl` Befehlszeilentools auf Ihrem Computer installiert ist oder. AWS CloudShell Weitere Informationen finden Sie unter [Installation](#) auf der `eksctl`-Website.

## Verfahren

Sie können ein Amazon EKS-Add-on mithilfe `eksctl` der AWS Management Console oder der AWS CLI erstellen. Wenn für das Add-on eine IAM-Rolle erforderlich ist, finden Sie in den Details für das jeweilige Add-on unter [Verfügbare Amazon EKS-Add-Ons von](#) weitere Informationen AWS zur Erstellung der Rolle.

### Add-on erstellen (eksctl)

1. Zeigen Sie die Namen der Add-Ons an, die für eine Cluster-Version verfügbar sind. Ersetzen Sie **1.33** durch die Version Ihres Clusters.

```
eksctl utils describe-addon-versions --kubernetes-version 1.33 | grep AddonName
```

Eine Beispielausgabe sieht wie folgt aus.

```
"AddonName": "aws-ebs-csi-driver",
 "AddonName": "coredns",
 "AddonName": "kube-proxy",
 "AddonName": "vpc-cni",
 "AddonName": "adot",
 "AddonName": "dynatrace_dynatrace-operator",
 "AddonName": "upbound_universal-crossplane",
 "AddonName": "teleport_teleport",
 "AddonName": "factorhouse_kpow",
 [...]
```

2. Zeigen Sie die Versionen des Add-Ons an, die für das Add-On verfügbar sind, das Sie erstellen möchten. Ersetzen Sie **1.33** durch die Version Ihres Clusters. Ersetzen Sie *name-of-addon* mit dem Namen des Add-Ons, für das Sie die Versionen anzeigen möchten. Der Name muss einer der Namen sein, die im vorherigen Schritt zurückgegeben wurden.

```
eksctl utils describe-addon-versions --kubernetes-version 1.33 --name name-of-addon |
grep AddonVersion
```

Die folgende Ausgabe ist ein Beispiel dafür, was für das Add-On mit dem Namen `vpc-cni` zurückgegeben wird. Sie können sehen, dass das Add-On in mehreren Versionen verfügbar ist.

```
"AddonVersions": [
 "AddonVersion": "v1.12.0-eksbuild.1",
 "AddonVersion": "v1.11.4-eksbuild.1",
 "AddonVersion": "v1.10.4-eksbuild.1",
 "AddonVersion": "v1.9.3-eksbuild.1",
```

- a. Stellen Sie fest, ob es sich bei dem Add-on, das Sie erstellen möchten, um ein Amazon EKS- oder AWS Marketplace-Add-On handelt. Der AWS Marketplace enthält Add-Ons von Drittanbietern, für die Sie zusätzliche Schritte ausführen müssen, um das Add-on zu erstellen.

```
eksctl utils describe-addon-versions --kubernetes-version 1.33 --name name-of-
addon | grep ProductUrl
```

Wenn keine Ausgabe zurückgegeben wird, handelt es sich bei dem Add-On um ein Amazon EKS. Wenn die Ausgabe zurückgegeben wird, handelt es sich bei dem Add-On um ein AWS Marketplace-Add-On. Die folgende Ausgabe bezieht sich auf ein Add-On mit dem Namen `teleport_teleport`.

```
"ProductUrl": "https://aws.amazon.com/marketplace/pp?sku=3bda70bb-566f-4976-806c-f96faef18b26"
```

Sie können mehr über das Add-on im AWS Marketplace mit der zurückgegebenen URL erfahren. Wenn für das Add-on ein Abonnement erforderlich ist, können Sie das Add-on über den AWS Marketplace abonnieren. Wenn Sie ein Add-on im AWS Marketplace erstellen möchten, muss der [IAM-Principal](#), den Sie zum Erstellen des Add-ons verwenden, über die Berechtigung verfügen, die [AWSServiceRoleForAWSLicenseManagerRoles](#) serviceverknüpfte Rolle zu erstellen. Weitere Informationen zum Zuweisen von Berechtigungen zu einer IAM-Entität finden Sie unter [Hinzufügen und Entfernen von IAM-Identitäts-Berechtigungen](#) im IAM-Benutzerhandbuch.

3. Erstellen Sie ein Amazon-EKS-Add-On. Kopieren Sie den Befehl und ersetzen Sie ihn *user-data* wie folgt:

- Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
- Ersetzen Sie *name-of-addon* durch den Namen des Add-Ons, das Sie erstellen möchten.
- Wenn Sie eine Version des Add-ons verwenden möchten, die älter als die neueste Version ist, *latest* ersetzen Sie sie durch die Versionsnummer, die in der Ausgabe eines vorherigen Schritts zurückgegeben wurde, den Sie verwenden möchten.
- Wenn das Add-On eine Servicekonto-Rolle verwendet, ersetzen Sie *111122223333* durch Ihre Konto-ID und *role-name* durch den Namen der Rolle. Anweisungen zum Erstellen einer Rolle für Ihr Dienstkonto finden Sie in der Dokumentation für das Add-on, das Sie erstellen. Eine Liste der Add-Ons finden Sie unter [the section called "AWS Add-Ons"](#). Für die Angabe einer Dienstkontorolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called "IAM OIDC-Anbieter"](#).

Wenn das Add-on keine Dienstkontorolle verwendet, löschen Sie es. `--service-account-role-arn arn:aws:iam::111122223333:role/role-name`

- Dieser Beispielbefehl überschreibt die Konfiguration aller vorhandenen selbstverwalteten Versionen des Add-Ons, falls es eine gibt. Wenn Sie die Konfiguration eines vorhandenen selbstverwalteten Add-ons nicht überschreiben möchten, entfernen Sie die *--force* Option. Wenn Sie die Option entfernen und das Amazon-EKS-Add-On die Konfiguration eines vorhandenen selbstverwalteten Add-Ons benötigt, scheitert die Erstellung des Amazon-EKS-Add-Ons mit einer Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt. Bevor Sie diese Option angeben, stellen Sie sicher, dass das Amazon EKS-Add-on keine Einstellungen

verwaltet, die Sie verwalten müssen, da diese Einstellungen mit dieser Option überschrieben werden.

```
eksctl create addon --cluster my-cluster --name name-of-addon --version latest \
 --service-account-role-arn arn:aws:iam::111122223333:role/role-name --force
```

Sie finden eine Liste mit allen verfügbaren Optionen für den Befehl.

```
eksctl create addon --help
```

Weitere Informationen zu verfügbaren Optionen finden Sie unter [Add-Ons](#) in der eksctl-Dokumentation.

## Add-on erstellen (AWS Konsole)

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster aus.
3. Wählen Sie den Namen des Clusters, für den Sie das Add-on erstellen möchten.
4. Wählen Sie die Registerkarte Add-ons.
5. Wählen Sie Weitere Add-Ons erhalten.
6. Wählen Sie auf der Seite Select add-ons (Add-Ons auswählen) die Add-Ons aus, die Sie Ihrem Cluster hinzufügen möchten. Sie können so viele Amazon EKS-Add-Ons und AWS Marketplace-Add-Ons hinzufügen, wie Sie benötigen.

Für AWS Marketplace-Add-Ons muss der [IAM-Principal](#), den Sie zum Erstellen des Add-ons verwenden, über Berechtigungen zum Lesen von Berechtigungen für das Add-on aus dem verfügen. AWS LicenseManager AWS LicenseManager erfordert eine [AWSServiceRoleForAWSLicenseManagerRole](#) serviceverknüpfte Rolle (SLR), die es AWS Ressourcen ermöglicht, Lizenzen in Ihrem Namen zu verwalten. Die SLR ist eine einmalige Anforderung pro Konto, und Sie müssen weder für jedes Add-On noch für jeden Cluster separate Spiegelreflexkameras erstellen. Weitere Informationen zum Zuweisen von Berechtigungen zu einem [IAM-Prinzipal](#) finden Sie unter [Hinzufügen und Entfernen von IAM-Identitäts-Berechtigungen](#) im IAM-Benutzerhandbuch.

Wenn die AWS Marketplace-Add-Ons, die Sie installieren möchten, nicht aufgeführt sind, können Sie auf die Seitennummerierung klicken, um zusätzliche Seitenergebnisse anzuzeigen, oder



im Suchfeld suchen. In den Filtering options (Filteroptionen) können Sie auch nach category (Kategorie), vendor (Anbieter) oder pricing model (Preismodell) filtern und dann die Add-ons aus den Suchergebnissen auswählen. Nachdem Sie die Add-Ons ausgewählt haben, die Sie installieren möchten, wählen Sie Weiter.

7. Gehen Sie auf der Seite Konfigurieren ausgewählter Add-Ons-Einstellungen wie folgt vor:

- a. Wählen Sie View subscription options (Abonnementoptionen anzeigen), um das Formular Subscription options (Abonnementoptionen) zu öffnen. Lesen Sie die Abschnitte Pricing details (Preisinformationen) und Legal (Rechtliche Hinweise) und klicken Sie dann auf Subscribe (Abonnieren), um fortzufahren.
- b. Wählen Sie unter Version die Version aus, die Sie installieren möchten. Wir empfehlen die als neueste Version markierte Version, es sei denn, das einzelne Add-on, das Sie erstellen, empfiehlt eine andere Version. Um festzustellen, ob es für ein Add-On eine empfohlene Version gibt, lesen Sie in der Dokumentation zu dem Add-on, das Sie erstellen. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#).
- c. Sie haben zwei Möglichkeiten, Rollen für Add-Ons zu konfigurieren: die IAM-Rolle von EKS Pod Identities und IAM-Rollen für Dienstkonten (IRSA). Folgen Sie den entsprechenden Schritten unten für Ihre bevorzugte Option. Wenn für alle von Ihnen ausgewählten Add-Ons unter Status die Option Abonnement erforderlich steht, wählen Sie Weiter aus. Sie können [diese Add-Ons erst weiter konfigurieren](#), wenn Sie sie nach der Erstellung Ihres Clusters abonniert haben. Gehen Sie für die Add-Ons, für die unter Status nicht die Option Abonnement erforderlich ist, wie folgt vor:
  - i. Für die Pod Identity-IAM-Rolle für das Dienstkonto können Sie entweder eine vorhandene EKS Pod Identity-IAM-Rolle verwenden oder über die Schaltfläche „Empfohlene Rolle erstellen“ eine erstellen. Dieses Feld enthält nur Optionen mit der entsprechenden Vertrauensrichtlinie. Wenn es keine Rolle zur Auswahl gibt, haben Sie keine bestehende Rolle mit einer passenden Vertrauensrichtlinie. Um eine EKS Pod Identity IAM-Rolle für Dienstkonten des ausgewählten Add-ons zu konfigurieren, wählen Sie Empfohlene Rolle erstellen aus. Der Assistent zur Rollenerstellung wird in einem separaten Fenster geöffnet. Der Assistent füllt die Rolleninformationen automatisch wie folgt aus. Führen Sie für jedes Add-On, für das Sie die IAM-Rolle EKS Pod Identity erstellen möchten, die Schritte im IAM-Assistenten wie folgt aus.
    - Im Schritt Vertrauenswürdige Entität auswählen sind die AWS Serviceoption für EKS und der Anwendungsfall für EKS — Pod Identity vorausgewählt, und die entsprechende Vertrauensrichtlinie wird automatisch für das Add-on ausgefüllt. Beispielsweise wird die Rolle mit der entsprechenden Vertrauensrichtlinie erstellt, die den IAM-Prinzipal

pods.eks.amazonaws.com enthält, wie unter beschrieben. [the section called “Vorteile von EKS-Pod-Identitäten”](#) Wählen Sie Weiter aus.

- Im Schritt Berechtigungen hinzufügen wird die entsprechende verwaltete Richtlinie für die Rollenrichtlinie für das Add-on vorausgewählt. Für das Amazon VPC CNI-Add-on wird die Rolle beispielsweise mit der verwalteten Richtlinie erstellt, AmazonEKS\_CNI\_Policy wie unter beschrieben. [the section called “Amazon-VPC-CNI-Plug-In für Kubernetes”](#) Wählen Sie Weiter aus.
- Im Schritt Name, Überprüfung und Erstellung im Feld Rollenname wird der Standardrollenname für das Add-on automatisch aufgefüllt. Für das Amazon VPC CNI-Add-on wird die Rolle beispielsweise mit dem Namen AmazonEKSPodIdentityAmazonVPCCNIRole Unter Beschreibung wird die Standardbeschreibung automatisch mit der entsprechenden Beschreibung für das Add-on aufgefüllt. Für das Amazon VPC CNI-Add-on wird die Rolle beispielsweise mit der Beschreibung Erlaubt Pods, die im Amazon EKS-Cluster ausgeführt werden, den Zugriff auf AWS Ressourcen erstellt. Sehen Sie sich unter Vertrauensrichtlinie die ausgefüllte Vertrauensrichtlinie für das Add-on an. Wählen Sie Rolle erstellen aus.

HINWEIS: Durch Beibehaltung des Standardrollennamens kann EKS die Rolle für Add-Ons in neuen Clustern oder beim Hinzufügen von Add-Ons zu vorhandenen Clustern vorab auswählen. Sie können diesen Namen immer noch überschreiben und die Rolle wird für das Add-on in Ihren Clustern verfügbar sein, aber die Rolle muss manuell aus der Drop-down-Liste ausgewählt werden.

- Informationen zu Add-Ons, für die unter Status nicht „Abonnement erforderlich“ steht und bei denen Sie Rollen mithilfe von IRSA konfigurieren möchten, finden Sie in der Dokumentation zu dem Add-on, das Sie erstellen, um eine IAM-Richtlinie zu erstellen und sie einer Rolle zuzuordnen. Eine Liste der Add-Ons finden Sie unter. [the section called “ AWS Add-Ons”](#) Für die Auswahl einer IAM-Rolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).
- Wählen Sie Optional configuration settings (Optionale Konfigurationseinstellungen) aus.
- Wenn für das Add-On eine Konfiguration erforderlich ist, geben Sie diese in das Feld Configuration values (Konfigurationswerte) ein. Informationen darüber, ob für das Add-on Konfigurationsinformationen erforderlich sind, finden Sie in der Dokumentation zu dem Add-on, das Sie erstellen. Eine Liste der Add-Ons finden Sie unter [the section called “ AWS Add-Ons”](#).

- v. Wählen Sie eine der verfügbaren Optionen für die Konfliktlösungsmethode. Wenn Sie Override für die Konfliktlösungsmethode wählen, können eine oder mehrere Einstellungen für das bestehende Add-on mit den Amazon EKS-Add-On-Einstellungen überschrieben werden. Wenn Sie diese Option nicht aktivieren und ein Konflikt mit Ihren vorhandenen Einstellungen besteht, schlägt der Vorgang fehl. Sie können die sich daraus ergebende Fehlermeldung heranziehen, um den Konflikt zu beheben. Bevor Sie diese Option wählen, stellen Sie sicher, dass das Amazon EKS-Add-on keine Einstellungen verwaltet, die Sie selbst verwalten müssen.
  - vi. Wählen Sie Weiter aus.
8. Wählen Sie auf der Seite Überprüfen und hinzufügen die Option Erstellen aus. Nachdem die Installation der Add-Ons abgeschlossen ist, werden Ihre installierten Add-Ons angezeigt.
9. Wenn für eines der von Ihnen installierten Add-Ons ein Abonnement erforderlich ist, gehen Sie wie folgt vor:
- a. Wählen Sie die Schaltfläche Subscribe (Abonnieren) in der unteren rechten Ecke für das Add-On. Sie werden auf die Seite für das Add-on im AWS Marketplace weitergeleitet. Lesen Sie die Informationen zum Add-On, z. B. die Product Overview (Produktübersicht) und die Pricing Information (Preisinformationen).
  - b. Wählen Sie oben rechts auf der Add-on-Seite die Schaltfläche Continue to Subscribe (Mit dem Abonnement fortfahren) aus.
  - c. Lesen Sie sich die (Allgemeinen Geschäftsbedingungen) durch. Wenn Sie damit einverstanden sind, wählen Sie Accept Terms (Bedingungen akzeptieren) aus. Die Bearbeitung des Abonnements kann mehrere Minuten dauern. Während das Abonnement bearbeitet wird, ist die Schaltfläche Return to Amazon EKS Console (Zurück zur Amazon-EKS-Konsole) ausgegraut.
  - d. Sobald die Bearbeitung des Abonnements abgeschlossen ist, ist die Schaltfläche Return to Amazon EKS Console (Zurück zur Amazon-EKS-Konsole) nicht mehr ausgegraut. Wählen Sie die Schaltfläche aus, um zur Registerkarte Add-ons (Add-Ons) der Amazon-EKS-Konsole für Ihren Cluster zurückzukehren.
  - e. Wählen Sie für das Add-On, das Sie abonniert haben, Remove and reinstall (Entfernen und erneut installieren) und dann Reinstall add-on (Add-On erneut installieren) aus. Die Installation des Add-Ons kann einige Minuten dauern. Wenn die Installation abgeschlossen ist, können Sie das Add-On konfigurieren.

## Add-on erstellen (AWS CLI)

1. Sie müssen Version 2.12.3 oder höher oder Version 1.27.160 oder höher der AWS Befehlszeilenschnittstelle (AWS CLI) auf Ihrem Gerät installiert und konfiguriert haben oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yumapt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
2. Bestimmen Sie, welche Add-Ons verfügbar sind. Sie können alle verfügbaren Add-Ons, ihren Typ und ihren Publisher anzeigen. Sie können auch die URL für Add-Ons sehen, die über den AWS Marketplace erhältlich sind. Ersetzen Sie **1.33** durch die Version Ihres Clusters.

```
aws eks describe-addon-versions --kubernetes-version 1.33 \
 --query 'addons[].{MarketplaceProductId: marketplaceInformation.productId,
 Name: addonName, Owner: owner Publisher: publisher, Type: type}' --output table
```

Eine Beispielausgabe sieht wie folgt aus.

```

|
| DescribeAddonVersions
|
+-----+
+-----+
+-----+
| MarketplaceProductId | Name
| Owner | Publisher | Type |
+-----+
+-----+
+-----+
| None | aws | eks | storage | aws-ebs-csi-driver
| None | aws | eks | networking | coredns
| None | aws | eks | networking | kube-proxy
| None | aws | eks | networking |
```

```

| None | aws | eks | networking | vpc-cni
| None | aws | eks | observability | adot
| https://aws.amazon.com/marketplace/pp/prodview-brb73nceicv7u | dynatrace_dynatrace-operator | aws-marketplace | dynatrace | monitoring
| https://aws.amazon.com/marketplace/pp/prodview-uhc2iwi5xysoc | upbound_universal-crossplane | aws-marketplace | upbound | infra-management
| https://aws.amazon.com/marketplace/pp/prodview-hd2ydsrgqy4li | teleport_teleport | aws-marketplace | teleport | policy-management
| https://aws.amazon.com/marketplace/pp/prodview-vgghgqdsplhvc | factorhouse_kpow | aws-marketplace | factorhouse | monitoring
| [...] | [...] | [...] | [...] | [...]
+-----+
+-----+-----+-----+
+-----+

```

Ihre Ausgabe ist möglicherweise anders. In dieser Beispielausgabe sind drei verschiedene Add-Ons vom Typ `networking` und fünf Add-Ons mit einem Publisher vom Typ `eks` verfügbar. Für die Add-Ons `aws-marketplace` in der `Owner` Spalte ist möglicherweise ein Abonnement erforderlich, bevor Sie sie installieren können. Sie können die URL besuchen, um mehr über das Add-On zu erfahren und es zu abonnieren.

- Sie können anzeigen, welche Versionen für jedes Add-On verfügbar sind. Ersetzen Sie **1.33** durch die Version Ihres Clusters und **`vpc-cni`** durch den Namen eines Add-Ons, das im vorherigen Schritt zurückgegeben wurde.

```
aws eks describe-addon-versions --kubernetes-version 1.33 --addon-name vpc-cni \
 --query 'addons[].addonVersions[].{Version: addonVersion, Defaultversion:
 compatibilities[0].defaultVersion}' --output table
```

Eine Beispielausgabe sieht wie folgt aus.

```

| DescribeAddonVersions |
+-----+-----+
| Defaultversion | Version |
+-----+-----+
| False | v1.12.0-eksbuild.1 |
| True | v1.11.4-eksbuild.1 |

```

|               |       |  |                    |  |
|---------------|-------|--|--------------------|--|
|               | False |  | v1.10.4-eksbuild.1 |  |
|               | False |  | v1.9.3-eksbuild.1  |  |
| +-----+-----+ |       |  |                    |  |

Die Version True in der Defaultversion-Spalte ist standardmäßig die Version, mit der das Add-On erstellt wurde.

4. (Optional) Finden Sie die Konfigurationsoptionen für das von Ihnen gewählte Add-On, indem Sie den folgenden Befehl ausführen:

```
aws eks describe-addon-configuration --addon-name vpc-cni --addon-version v1.12.0-eksbuild.1
```

```
{
 "addonName": "vpc-cni",
 "addonVersion": "v1.12.0-eksbuild.1",
 "configurationSchema": "{ \"$ref\": \"#/definitions/VpcCni\", \"$schema\": \"http://json-schema.org/draft-06/schema#\", \"definitions\": { \"Cri\": { \"additionalProperties\": false, \"properties\": { \"hostPath\": { \"$ref\": \"#/definitions/HostPath\" } }, \"title\": \"Cri\", \"type\": \"object\" }, \"Env\": { \"additionalProperties\": false, \"properties\": { \"ADDITIONAL_ENI_TAGS\": { \"type\": \"string\" }, \"AWS_VPC_CNI_NODE_PORT_SUPPORT\": { \"format\": \"boolean\", \"type\": \"string\" }, \"AWS_VPC_ENI_MTU\": { \"format\": \"integer\", \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_CONFIGURE_RPFILTER\": { \"format\": \"boolean\", \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG\": { \"format\": \"boolean\", \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_EXTERNALSNAT\": { \"format\": \"boolean\", \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_LOGLEVEL\": { \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_LOG_FILE\": { \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_RANDOMIZESNAT\": { \"type\": \"string\" }, \"AWS_VPC_K8S_CNI_VETHPREFIX\": { \"type\": \"string\" }, \"AWS_VPC_K8S_PLUGIN_LOG_FILE\": { \"type\": \"string\" }, \"AWS_VPC_K8S_PLUGIN_LOG_LEVEL\": { \"type\": \"string\" }, \"DISABLE_INTROSPECTION\": { \"format\": \"boolean\", \"type\": \"string\" }, \"DISABLE_METRICS\": { \"format\": \"boolean\", \"type\": \"string\" }, \"DISABLE_NETWORK_RESOURCE_PROVISIONING\": { \"format\": \"boolean\", \"type\": \"string\" }, \"ENABLE_POD_ENI\": { \"format\": \"boolean\", \"type\": \"string\" }, \"ENABLE_PREFIX_DELEGATION\": { \"format\": \"boolean\", \"type\": \"string\" }, \"WARM_ENI_TARGET\": { \"format\": \"integer\", \"type\": \"string\" }, \"WARM_PREFIX_TARGET\": { \"format\": \"integer\", \"type\": \"string\" } }, \"title\": \"Env\", \"type\": \"object\" }, \"HostPath\": { \"additionalProperties\": false, \"properties\": { \"path\": { \"type\": \"string\" } }, \"title\": \"HostPath\", \"type\": \"object\" }, \"Limits\": { \"additionalProperties\": false, \"properties\": { \"cpu\": { \"type\": \"string\" }, \"memory\": { \"type\": \"string\" } }, \"title\": \"Limits\", \"type\": \"object\" }, \"Resources\": { \"additionalProperties\": false, \"properties\": { \"limits\": { \"$ref\": \"#/definitions/Limits\" }, \"requests\": { \"$ref\": \"#/definitions/Limits\" } }, \"title
```

```
\":\\"Resources\\",\\"type\\":\\"object\\"},\\"VpcCni\\":{\\"additionalProperties\\":false,
\\"properties\\":{\\"cri\\":{\\"$ref\\":\\"#/definitions/Cri\\"},\\"env\\":{\\"$ref\\":\\"#/
definitions/Env\\"},\\"resources\\":{\\"$ref\\":\\"#/definitions/Resources\\"}},\\"title\\":
\\"VpcCni\\",\\"type\\":\\"object\\"}}}"
}
```

Die Ausgabe ist ein standardmäßiges JSON-Schema.

Hier ist ein Beispiel für gültige Konfigurationswerte im JSON-Format, die mit dem obigen Schema funktionieren.

```
{
 "resources": {
 "limits": {
 "cpu": "100m"
 }
 }
}
```

Hier ist ein Beispiel für gültige Konfigurationswerte im YAML-Format, die mit dem obigen Schema funktionieren.

```
resources:
 limits:
 cpu: 100m
```

5. Stellen Sie fest, ob für das Add-on IAM-Berechtigungen erforderlich sind. Wenn ja, müssen Sie (1) ermitteln, ob Sie EKS Pod Identities oder IAM Roles for Service Accounts (IRSA) verwenden möchten, (2) den ARN der IAM-Rolle bestimmen, die mit dem Add-on verwendet werden soll, und (3) den Namen des Kubernetes-Dienstkontos bestimmen, das vom Add-on verwendet wird. Weitere Informationen finden Sie unter [the section called “IAM-Informationen abrufen”](#).
  - Amazon EKS schlägt vor, EKS Pod Identities zu verwenden, sofern das Add-on dies unterstützt. Dies setzt voraus, dass der [Pod Identity Agent auf Ihrem Cluster installiert ist](#). Weitere Informationen zur Verwendung von Pod-Identitäten mit Add-Ons finden Sie unter [the section called “IAM-Rollen”](#).
  - Wenn das Add-on oder Ihr Cluster nicht für EKS Pod Identities eingerichtet ist, verwenden Sie IRSA. [Vergewissern Sie sich, dass IRSA auf Ihrem Cluster eingerichtet ist](#).

- [Lesen Sie in der Dokumentation zu Amazon EKS Add-ons nach, ob für das Add-on IAM-Berechtigungen erforderlich sind, und geben Sie den Namen des zugehörigen Kubernetes-Servicekontos an.](#)
    - a. Erstellen Sie ein Amazon-EKS-Add-On. Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor und führen Sie anschließend den geänderten Befehl aus:
  - Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
  - Ersetzen Sie *vpc-cni* durch einen Add-On-Namen, der in der Ausgabe des vorherigen Schritts zurückgegeben wurde, den Sie erstellen möchten.
  - Ersetzen Sie *version-number* durch die in der Ausgabe des vorherigen Schritts zurückgegebene Version, die Sie verwenden möchten.
  - Wenn für das Add-on keine IAM-Berechtigungen erforderlich sind, löschen Sie es. *<service-account-configuration>*
  - Führen Sie eine der folgenden Aktionen aus:
    - Wenn für das Add-on (1) IAM-Berechtigungen erforderlich sind und (2) Ihr Cluster EKS-Pod-Identitäten verwendet, *<service-account-configuration>* ersetzen Sie es durch die folgende Pod-Identitätszuordnung. Ersetzen Sie es *<service-account-name>* durch den Namen des Dienstkontos, der vom Add-on verwendet wird. Durch *<role-arn>* den ARN einer IAM-Rolle ersetzen. Die Rolle muss über die von EKS Pod Identities geforderte Vertrauensrichtlinie verfügen.
- ```
--pod-identity-associations 'serviceAccount=<service-account-name>,roleArn=<role-arn>'
```
- Wenn für das Add-on (1) IAM-Berechtigungen erforderlich sind und (2) Ihr Cluster IRSA verwendet, *<service-account-configuration>* ersetzen Sie es durch die folgende IRSA-Konfiguration. *111122223333* Ersetzen Sie es durch Ihre Konto-ID und *role-name* den Namen einer vorhandenen IAM-Rolle, die Sie erstellt haben. Anweisungen zum Erstellen der Rolle finden Sie in der Dokumentation für das Add-on, das Sie erstellen. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#). Für die Angabe einer Dienstkontorolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).

```
--service-account-role-arn arn:aws::iam::111122223333:role/role-name
```


- Diese Beispielbefehle überschreiben die Option `--configuration-values` von gegebenenfalls vorhandenen selbstverwalteten Versionen des Add-Ons. Ersetzen Sie diese durch die gewünschten Konfigurationswerte, z. B. eine Zeichenfolge oder eine Dateieingabe. Wenn Sie keine Konfigurationswerte angeben möchten, löschen Sie die Option `--configuration-values`. Wenn Sie nicht möchten, dass die AWS CLI die Konfiguration eines vorhandenen selbstverwalteten Add-Ons überschreibt, entfernen Sie die `--resolve-conflicts OVERWRITE` Option. Wenn Sie die Option entfernen und das Amazon-EKS-Add-On die Konfiguration eines vorhandenen selbstverwalteten Add-Ons benötigt, scheitert die Erstellung des Amazon-EKS-Add-Ons mit einer Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt. Bevor Sie diese Option angeben, stellen Sie sicher, dass das Amazon EKS-Add-on keine Einstellungen verwaltet, die Sie verwalten müssen, da diese Einstellungen mit dieser Option überschrieben werden.

```
aws eks create-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version
version-number \
    <service-account-configuration> --configuration-values '{"resources":
{"limits":{"cpu":"100m"}}}' --resolve-conflicts OVERWRITE
```

```
aws eks create-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version
version-number \
    <service-account-configuration> --configuration-values 'file://example.yaml' --
resolve-conflicts OVERWRITE
```

Eine vollständige Liste der verfügbaren Optionen finden Sie unter [create-addon](#) in der Amazon-EKS-Befehlszeilenreferenz. Wenn das von Ihnen erstellte Add-On in der Owner Spalte eines vorherigen Schritts `aws-marketplace` aufgeführt wurde, schlägt die Erstellung möglicherweise fehl und Sie erhalten möglicherweise eine Fehlermeldung, die der folgenden ähnelt.

```
{
  "addon": {
    "addonName": "addon-name",
    "clusterName": "my-cluster",
    "status": "CREATE_FAILED",
    "addonVersion": "version",
    "health": {
      "issues": [
        {
          "code": "AddonSubscriptionNeeded",
```

```
        "message": "You are currently not subscribed to this add-on. To  
subscribe, visit the AWS Marketplace console, agree to the seller EULA, select the  
pricing type if required, then re-install the add-on"  
    }  
]  
}  
}
```

Wenn Sie einen Fehler erhalten, der dem Fehler in der vorherigen Ausgabe ähnelt, besuchen Sie die URL in der Ausgabe eines vorherigen Schritts, um das Add-On zu abonnieren. Führen Sie den `create-addon`-Befehl nach dem Abonnieren erneut aus.

Ein Amazon EKS-Add-on aktualisieren

Amazon EKS aktualisiert ein Add-on nicht automatisch, wenn neue Versionen veröffentlicht werden oder nachdem Sie Ihren Cluster auf eine neue Kubernetes-Nebenversion aktualisiert haben. Um ein Add-On für einen vorhandenen Cluster zu aktualisieren, müssen Sie das Update initiieren. Nachdem Sie das Update initiiert haben, aktualisiert Amazon EKS das Add-On für Sie. Lesen Sie vor dem Aktualisieren eines Add-Ons die aktuelle Dokumentation für das Add-On. Eine Liste der verfügbaren Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#). Wenn für das Add-on eine IAM-Rolle erforderlich ist, finden Sie in den Details für das jeweilige Add-on unter [Verfügbare Amazon EKS-Add-Ons von](#) weitere Informationen AWS zur Erstellung der Rolle.

Voraussetzungen

Gehen Sie wie folgt vor, bevor Sie ein Add-on erstellen:

- Prüfen Sie, ob für Ihr Add-on eine IAM-Rolle erforderlich ist. Weitere Informationen finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).
- Stellen Sie sicher, dass die Amazon EKS-Add-On-Version mit Ihrem Cluster kompatibel ist. Weitere Informationen finden Sie unter [the section called “Überprüfen Sie die Kompatibilität”](#).

Verfahren

Sie können ein Amazon EKS-Add-on mithilfe `eksctl` der AWS Management Console oder der AWS CLI aktualisieren.

Add-on aktualisieren (eksctl)

1. Bestimmen Sie die aktuellen Add-Ons und Add-On-Versionen, die auf Ihrem Cluster installiert sind. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
eksctl get addon --cluster my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	VERSION	STATUS	ISSUES	IAMROLE	UPDATE AVAILABLE
coredns	v1.8.7-eksbuild.2	ACTIVE	0		
kube-proxy	v1.23.7-eksbuild.1	ACTIVE	0		v1.23.8-eksbuild.2
vpc-cni	v1.10.4-eksbuild.1	ACTIVE	0		v1.12.0-eksbuild.1,v1.11.4-eksbuild.1,v1.11.3-eksbuild.1,v1.11.2-eksbuild.1,v1.11.0-eksbuild.1

Ihre Ausgabe sieht möglicherweise anders aus, je nachdem, welche Add-Ons und Versionen Sie auf Ihrem Cluster haben. Sie können sehen, dass in der vorherigen Beispielausgabe für zwei vorhandene Add-Ons auf dem Cluster neuere Versionen in der UPDATE AVAILABLE-Spalte verfügbar sind.

2. Aktualisieren Sie das Add-On.

- a. Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie nach Bedarf die folgenden Änderungen am Befehl vor:
 - Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
 - *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet.
 - Ersetzen Sie *vpc-cni* durch den Namen eines Add-Ons, das in der Ausgabe des vorherigen Schritts zurückgegeben wurde, das Sie aktualisieren möchten.
 - Wenn Sie eine ältere Version als die neueste verfügbare Version aktualisieren möchten, dann ersetzen Sie *latest* durch die Versionsnummer, die in der Ausgabe des vorherigen Schritts zurückgegeben wurde, die Sie verwenden möchten. Für einige Add-Ons gibt es empfohlene Versionen. Weitere Informationen finden Sie in der Dokumentation für das Add-on, das Sie aktualisieren. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#). * Wenn das Add-on ein Kubernetes-Dienstkonto und eine IAM-Rolle verwendet, *111122223333* ersetzen Sie es durch Ihre Konto-ID und *role-name* durch den Namen einer vorhandenen IAM-Rolle, die Sie erstellt haben. Anweisungen zur Erstellung der Rolle finden Sie in der Dokumentation für das Add-on, das Sie erstellen. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#). Für die Angabe einer

Dienstkontorolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).

Wenn das Add-on kein Kubernetes-Dienstkonto und keine IAM-Rolle verwendet, löschen Sie die Zeile `serviceAccountRoleARN: arn:aws: iam::111122223333:role/role-name`

- Die *preserve* Option behält die vorhandenen Werte für das Add-on bei. Wenn Sie benutzerdefinierte Werte für Add-On-Einstellungen festgelegt haben und diese Option nicht verwenden, überschreibt Amazon EKS Ihre Werte mit den Standardwerten. Wenn Sie diese Option verwenden, empfehlen wir, dass Sie alle Feld- und Wertänderungen auf einem Nicht-Produktionscluster testen, bevor Sie das Add-on auf Ihrem Produktionscluster aktualisieren. Wenn Sie diesen Wert auf *overwrite* ändern, werden alle Einstellungen auf die Amazon-EKS-Standardwerte geändert. Wenn Sie benutzerdefinierte Werte für Einstellungen festgelegt haben, werden diese möglicherweise mit den Amazon EKS-Standardwerten überschrieben. Wenn Sie diesen Wert auf *ändernnone*, ändert Amazon EKS den Wert keiner Einstellungen, aber das Update schlägt möglicherweise fehl. Wenn das Update fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt.

```
cat >update-addon.yaml <<EOF
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: my-cluster
  region: region-code

addons:
- name: vpc-cni
  version: latest
  serviceAccountRoleARN: arn:aws: iam::111122223333:role/role-name
  resolveConflicts: preserve
EOF
```

- Führen Sie den bearbeiteten Befehl aus, um die `update-addon.yaml`-Datei zu erstellen.
- Wenden Sie die Konfigurationsdatei auf Ihren Cluster an.

```
eksctl update addon -f update-addon.yaml
```

Weitere Informationen zum Aktualisieren von Add-Ons finden Sie in der eksctl Dokumentation unter [Aktualisieren von Addons](#).

Add-on aktualisieren (AWS Konsole)

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster aus.
3. Wählen Sie den Namen des Clusters, für den Sie das Add-on aktualisieren möchten.
4. Wählen Sie die Registerkarte Add-ons.
5. Wählen Sie das Add-on aus, das Sie aktualisieren möchten.
6. Wählen Sie Bearbeiten aus.
7. Gehen Sie auf der *name of addon* Seite „Konfigurieren“ wie folgt vor:
 - a. Wählen Sie die Version aus, die Sie verwenden möchten. Das Add-On verfügt möglicherweise über eine empfohlene Version. Weitere Informationen finden Sie in der Dokumentation für das Add-on, das Sie aktualisieren. Eine Liste der Add-Ons finden Sie unter [the section called “ AWS Add-Ons”](#).
 - b. Sie haben zwei Möglichkeiten, Rollen für Add-Ons zu konfigurieren: die IAM-Rolle von EKS Pod Identities und IAM-Rollen für Dienstkonten (IRSA). Folgen Sie den entsprechenden Schritten unten für Ihre bevorzugte Option. Wenn für alle von Ihnen ausgewählten Add-Ons unter Status die Option Abonnement erforderlich steht, wählen Sie Weiter aus. Gehen Sie für die Add-Ons, für die unter Status nicht „Abonnement erforderlich“ nicht angezeigt wird, wie folgt vor:
 - i. Für die Pod Identity-IAM-Rolle für das Dienstkonto können Sie entweder eine vorhandene EKS Pod Identity-IAM-Rolle verwenden oder über die Schaltfläche „Empfohlene Rolle erstellen“ eine erstellen. Dieses Feld enthält nur Optionen mit der entsprechenden Vertrauensrichtlinie. Wenn es keine Rolle zur Auswahl gibt, haben Sie keine bestehende Rolle mit einer passenden Vertrauensrichtlinie. Um eine EKS Pod Identity IAM-Rolle für Dienstkonten des ausgewählten Add-ons zu konfigurieren, wählen Sie Empfohlene Rolle erstellen aus. Der Assistent zur Rollenerstellung wird in einem separaten Fenster geöffnet. Der Assistent füllt die Rolleninformationen automatisch wie folgt aus. Führen Sie für jedes Add-On, für das Sie die IAM-Rolle EKS Pod Identity erstellen möchten, die Schritte im IAM-Assistenten wie folgt aus.
 - Im Schritt Vertrauenswürdige Entität auswählen sind die AWS Serviceoption für EKS und der Anwendungsfall für EKS — Pod Identity vorausgewählt, und die entsprechende Vertrauensrichtlinie wird automatisch für das Add-on ausgefüllt. Beispielsweise wird

die Rolle mit der entsprechenden Vertrauensrichtlinie erstellt, die den IAM-Prinzipal `pods.eks.amazonaws.com` enthält, wie unter beschrieben. [the section called “Vorteile von EKS-Pod-Identitäten”](#) Wählen Sie Weiter aus.

- Im Schritt „Berechtigungen hinzufügen“ wird die entsprechende verwaltete Richtlinie für die Rollenrichtlinie für das Add-on vorausgewählt. Für das Amazon VPC CNI-Add-on wird die Rolle beispielsweise mit der verwalteten Richtlinie erstellt, `AmazonEKS_CNI_Policy` wie unter beschrieben. [the section called “Amazon-VPC-CNI-Plug-In für Kubernetes”](#) Wählen Sie Weiter aus.
- Im Schritt Name, Überprüfung und Erstellung im Feld Rollenname wird der Standardrollenname für das Add-on automatisch aufgefüllt. Für das Amazon VPC CNI-Add-on wird die Rolle beispielsweise mit dem Namen `AmazonEKSCNIRole` erstellt. Unter Beschreibung wird die Standardbeschreibung automatisch mit der entsprechenden Beschreibung für das Add-on aufgefüllt. Für das Amazon VPC CNI-Add-on wird die Rolle beispielsweise mit der Beschreibung `Erlaubt Pods, die im Amazon EKS-Cluster ausgeführt werden, den Zugriff auf AWS Ressourcen` erstellt. Sehen Sie sich unter Vertrauensrichtlinie die ausgefüllte Vertrauensrichtlinie für das Add-on an. Wählen Sie Rolle erstellen aus.

 Note

Durch Beibehaltung des Standardrollennamens kann EKS die Rolle für Add-Ons in neuen Clustern oder beim Hinzufügen von Add-Ons zu vorhandenen Clustern vorab auswählen. Sie können diesen Namen immer noch überschreiben und die Rolle wird für das Add-on in Ihren Clustern verfügbar sein, aber die Rolle muss manuell aus der Drop-down-Liste ausgewählt werden.

- Informationen zu Add-Ons, für die unter Status nicht „Abonnement erforderlich“ steht und bei denen Sie Rollen mithilfe von IRSA konfigurieren möchten, finden Sie in der Dokumentation zu dem Add-on, das Sie erstellen, um eine IAM-Richtlinie zu erstellen und sie einer Rolle zuzuordnen. Eine Liste der Add-Ons finden Sie unter. [the section called “AWS Add-Ons”](#) Für die Auswahl einer IAM-Rolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).
- Erweitern Sie Optionale Konfigurationseinstellungen.
 - Geben Sie im Feld Konfigurationswerte alle zusätzlichen spezifischen Konfigurationsinformationen ein. Weitere Informationen finden Sie in der Dokumentation für

das Add-on, das Sie aktualisieren. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#)... Wählen Sie unter Konfliktlösungsmethode eine der Optionen aus. Wenn Sie benutzerdefinierte Werte für Add-On-Einstellungen festgelegt haben, empfehlen wir die Option Preserve (Beibehalten). Wenn Sie diese Option nicht wählen, überschreibt Amazon EKS Ihre Werte mit den Standardwerten. Wenn Sie diese Option verwenden, empfehlen wir, dass Sie alle Feld- und Wertänderungen auf einem Nicht-Produktionscluster testen, bevor Sie das Add-on auf Ihrem Produktionscluster aktualisieren. Wenn Sie diesen Wert auf Überschreiben ändern, werden alle Einstellungen auf Amazon EKS-Standardwerte geändert. Wenn Sie benutzerdefinierte Werte für Einstellungen festgelegt haben, werden diese möglicherweise mit den Amazon EKS-Standardwerten überschrieben. Wenn Sie diesen Wert auf None ändern, ändert Amazon EKS den Wert aller Einstellungen nicht, aber das Update schlägt möglicherweise fehl. Wenn das Update fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt.

8. Wählen Sie Änderungen speichern aus.

Add-on aktualisieren (AWS CLI)

1. Sie müssen Version 2.12.3 oder höher oder Version 1.27.160 oder höher der AWS Befehlszeilenschnittstelle (AWS CLI) auf Ihrem Gerät installiert und konfiguriert haben oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum`/`apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
2. Hier finden Sie eine Liste der installierten Add-Ons. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks list-addons --cluster-name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "addons": [
```

```

        "coredns",
        "kube-proxy",
        "vpc-cni"
    ]
}

```

3. Zeigen Sie die aktuelle Version des Add-Ons an, die Sie aktualisieren möchten. Ersetzen Sie *my-cluster* mit Ihrem Clusternamen und *vpc-cni* mit dem Namen des Add-Ons, das Sie aktualisieren möchten.

```

aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query
  "addon.addonVersion" --output text

```

Eine Beispielausgabe sieht wie folgt aus.

```
v1.10.4-eksbuild.1
```

4. Ermitteln Sie, welche Versionen des Add-ons für die Version Ihres Clusters verfügbar sind. *1.33* Ersetzen Sie es durch die Version Ihres Clusters und *vpc-cni* durch den Namen des Add-ons, das Sie aktualisieren möchten.

```

aws eks describe-addon-versions --kubernetes-version 1.33 --addon-name vpc-cni \
  --query 'addons[].addonVersions[].{Version: addonVersion, Defaultversion:
    compatibilities[0].defaultVersion}' --output table

```

Eine Beispielausgabe sieht wie folgt aus.

```

-----
|           DescribeAddonVersions           |
+-----+-----+
| Defaultversion |           Version           |
+-----+-----+
| False         | v1.12.0-eksbuild.1 |
| True          | v1.11.4-eksbuild.1 |
| False         | v1.10.4-eksbuild.1 |
| False         | v1.9.3-eksbuild.1  |
+-----+-----+

```

Die Version True in der Defaultversion-Spalte ist standardmäßig die Version, mit der das Add-On erstellt wurde.

5. Aktualisieren Sie Ihr Add-on. Kopieren Sie den folgenden Befehl auf Ihr Gerät. Nehmen Sie bei Bedarf die folgenden Änderungen am Befehl vor, und führen Sie dann den geänderten Befehl aus. Weitere Informationen zu diesem Befehl finden Sie unter [update-addon](#) in der Amazon EKS-Befehlszeilenreferenz.
- Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.
 - Ersetzen Sie *vpc-cni* durch den Namen des Add-Ons, das Sie aktualisieren möchten und das in der Ausgabe eines vorherigen Schritts zurückgegeben wurde.
 - Ersetzen Sie *version-number* durch die in der Ausgabe des vorherigen Schritts zurückgegebene Version, auf die Sie aktualisieren möchten. Für einige Add-Ons gibt es empfohlene Versionen. Weitere Informationen finden Sie in der Dokumentation für das Add-on, das Sie aktualisieren. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#). * Wenn das Add-on ein Kubernetes-Dienstkonto und eine IAM-Rolle verwendet, *111122223333* ersetzen Sie es durch Ihre Konto-ID und *role-name* durch den Namen einer vorhandenen IAM-Rolle, die Sie erstellt haben. Anweisungen zur Erstellung der Rolle finden Sie in der Dokumentation für das Add-on, das Sie erstellen. Eine Liste der Add-Ons finden Sie unter [the section called “AWS Add-Ons”](#). Für die Angabe einer Dienstkontorolle benötigen Sie einen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Um festzustellen, ob Sie über einen solchen für Ihren Cluster verfügen, oder um einen zu erstellen, lesen Sie [the section called “IAM OIDC-Anbieter”](#).

Wenn das Add-on kein Kubernetes-Dienstkonto und keine IAM-Rolle verwendet, löschen Sie die Zeile. `serviceAccountRoleARN: arn:aws:iam::111122223333:role/role-name`

- Die `--resolve-conflicts PRESERVE` Option behält die vorhandenen Werte für das Add-on bei. Wenn Sie benutzerdefinierte Werte für Add-On-Einstellungen festgelegt haben und diese Option nicht verwenden, überschreibt Amazon EKS Ihre Werte mit den Standardwerten. Wenn Sie diese Option verwenden, empfehlen wir, dass Sie alle Feld- und Wertänderungen auf einem Nicht-Produktionscluster testen, bevor Sie das Add-on auf Ihrem Produktionscluster aktualisieren. Wenn Sie diesen Wert auf `OVERWRITE` ändern, werden alle Einstellungen auf die Amazon-EKS-Standardwerte geändert. Wenn Sie benutzerdefinierte Werte für Einstellungen festgelegt haben, werden diese möglicherweise mit den Amazon EKS-Standardwerten überschrieben. Wenn Sie diesen Wert auf `ändernNONE` ändern, ändert Amazon EKS den Wert keiner Einstellungen, aber das Update schlägt möglicherweise fehl. Wenn das Update fehlschlägt, erhalten Sie eine Fehlermeldung, die Sie bei der Behebung des Konflikts unterstützt.
- Wenn Sie die gesamte benutzerdefinierte Konfiguration entfernen möchten, führen Sie das Update mit der `--configuration-values '{}'`-Option durch. Dadurch werden alle benutzerdefinierten Konfigurationen auf die Standardwerte zurückgesetzt. Wenn Sie Ihre

benutzerdefinierte Konfiguration nicht ändern möchten, geben Sie das `--configuration-values` Kennzeichen nicht an. Wenn Sie eine benutzerdefinierte Konfiguration anpassen möchten, ersetzen Sie `{}` durch die neuen Parameter.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version
version-number \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name --
configuration-values '{}' --resolve-conflicts PRESERVE
```

6. Überprüfen Sie den Status des Updates. `my-cluster` Ersetzen Sie es durch den Namen Ihres Clusters und `vpc-cni` durch den Namen des Add-ons, das Sie aktualisieren.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "addon": {
    "addonName": "vpc-cni",
    "clusterName": "my-cluster",
    "status": "UPDATING",
  }
}
```

Das Update ist abgeschlossen, wenn der Status ACTIVE ist.

Überprüfen Sie die Kompatibilität der Amazon EKS-Add-On-Version mit einem Cluster

Bevor Sie ein Amazon EKS-Add-on erstellen, müssen Sie überprüfen, ob die Amazon EKS-Add-On-Version mit Ihrem Cluster kompatibel ist.

Verwenden Sie die [describe-addon-versions API](#), um die verfügbaren Versionen von EKS-Add-Ons aufzulisten und aufzulisten, welche Kubernetes-Versionen jede Addon-Version unterstützt.

1. Stellen Sie sicher, dass die AWS CLI installiert ist und mit ihr funktioniert `aws sts get-caller-identity`. Wenn dieser Befehl nicht funktioniert, erfahren Sie, wie [Sie mit der AWS CLI beginnen können](#).

2. Ermitteln Sie den Namen des Add-Ons, für das Sie Informationen zur Versionskompatibilität abrufen möchten, z. `amazon-cloudwatch-observability` B.
3. Ermitteln Sie die Kubernetes-Version Ihres Clusters, z. B. `1.33`
4. Verwenden Sie die AWS CLI, um die Addon-Versionen abzurufen, die mit der Kubernetes-Version Ihres Clusters kompatibel sind.

```
aws eks describe-addon-versions --addon-name amazon-cloudwatch-observability --  
kubernetes-version 1.33
```

Eine Beispielausgabe sieht wie folgt aus.

```
{  
  "addons": [  
    {  
      "addonName": "amazon-cloudwatch-observability",  
      "type": "observability",  
      "addonVersions": [  
        {  
          "addonVersion": "vX.X.X-eksbuild.X",  
          "architecture": [  
            "amd64",  
            "arm64"  
          ],  
          "computeTypes": [  
            "ec2",  
            "auto",  
            "hybrid"  
          ],  
          "compatibilities": [  
            {  
              "clusterVersion": "1.33",  
              "platformVersions": [  
                "*"   
              ],  
              "defaultVersion": true  
            }  
          ],  
        }  
      ],  
    }  
  ]  
}
```

```
}
```

Diese Ausgabe zeigt, dass die Addon-Version mit der `vX.X.X-eksbuild.X` Kubernetes-Cluster-Version kompatibel ist. 1.33

Kompatibilität des Add-ons mit Compute-Typen

Das `computeTypes` Feld in der `describe-addon-versions` Ausgabe gibt die Kompatibilität eines Add-ons mit EKS Auto Mode Managed Nodes oder Hybrid Nodes an. Die markierten Add-Ons `auto` funktionieren mit der cloudbasierten, AWS verwalteten Infrastruktur von EKS Auto Mode, während die markierten Add-Ons auf lokalen Knoten ausgeführt werden `hybrid` können, die mit der EKS-Cloud-Steuerebene verbunden sind.

Weitere Informationen finden Sie unter [the section called “Überlegungen zum Amazon EKS Auto Mode”](#).

Ein Amazon EKS-Add-on aus einem Cluster entfernen

Sie können ein Amazon EKS-Add-on mithilfe `eksctl` oder der AWS Management Console AWS CLI aus Ihrem Cluster entfernen.

Wenn Sie ein Amazon EKS-Add-on aus einem Cluster entfernen:

- Es gibt keine Ausfallzeit für die Funktionalität, die das Add-On bereitstellt.
- Wenn Sie IAM-Rollen für Servicekonten (IRSA) verwenden und dem Add-on eine IAM-Rolle zugeordnet ist, wird die IAM-Rolle nicht entfernt.
- Wenn Sie Pod-Identitäten verwenden, werden alle Pod-Identitätszuordnungen, die dem Add-on gehören, entfernt. Wenn Sie die `--preserve` Option für die AWS CLI angeben, werden die Verknüpfungen beibehalten.
- Amazon EKS beendet die Verwaltung der Einstellungen für das Add-On.
- Die Konsole benachrichtigt Sie nicht mehr, wenn neue Versionen verfügbar sind.
- Sie können das Add-On nicht mit irgendwelchen AWS Tools oder aktualisieren APIs.
- Sie können die Add-On-Software auf Ihrem Cluster beibehalten, damit Sie sie selbst verwalten können, oder Sie können die Add-On-Software aus Ihrem Cluster entfernen. Sie sollten die Add-On-Software nur dann aus Ihrem Cluster entfernen, wenn keine Ressourcen in Ihrem Cluster von der Funktionalität abhängen, die das Add-On bereitstellt.

Voraussetzungen

Gehen Sie wie folgt vor, bevor Sie ein Add-on erstellen:

- Ein vorhandener Amazon-EKS-Cluster. Informationen zum Bereitstellen finden Sie unter [Erste Schritte](#).
- Prüfen Sie, ob für Ihr Add-on eine IAM-Rolle erforderlich ist. Weitere Informationen finden Sie unter [IAM-Rollen](#).
- Version 0.210.0 oder höher des eksctl-Befehlszeilen-Tools, das auf Ihrem Computer oder in der AWS CloudShell installiert ist. Informationen zur Installation oder Aktualisierung eksctl finden Sie in der eksctl Dokumentation unter [Installation](#).

Verfahren

Sie haben zwei Möglichkeiten, ein Amazon EKS-Add-on zu entfernen.

- Beibehalten von Add-on-Software auf Ihrem Cluster - Diese Option entfernt die Amazon-EKS-Verwaltung aller Einstellungen. Amazon EKS wird außerdem die Möglichkeit aufgehoben, Sie über Updates zu informieren und das Amazon-EKS-Add-on automatisch zu aktualisieren, nachdem Sie ein Update eingeleitet haben. Es behält jedoch die Add-on-Software auf Ihrem Cluster bei. Diese Option macht das Add-on zu einem selbstverwalteten Add-on statt einem Amazon-EKS-Add-on. Mit dieser Option gibt es keine Ausfallzeiten für das Add-on.
- Entfernen Sie die Add-on-Software vollständig aus Ihrem Cluster – Wir empfehlen, dass Sie das Amazon-EKS-Add-on nur aus Ihrem Cluster entfernen, wenn auf Ihrem Cluster keine Ressourcen vorhanden sind, die davon abhängig sind.

Sie können ein Amazon EKS-Add-on mithilfe eksctl der AWS Management Console oder der AWS CLI entfernen.

Add-On entfernen (eksctl)

1. Bestimmen Sie die aktuell auf Ihrem Cluster installierten Add-Ons. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
eksctl get addon --cluster my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	VERSION	STATUS	ISSUES	IAMROLE	UPDATE AVAILABLE
coredns	v1.8.7-eksbuild.2	ACTIVE	0		
kube-proxy	v1.23.7-eksbuild.1	ACTIVE	0		
vpc-cni	v1.10.4-eksbuild.1	ACTIVE	0		
[...]					

Ihre Ausgabe sieht möglicherweise anders aus, je nachdem, welche Add-Ons und Versionen Sie auf Ihrem Cluster haben.

- Entfernen Sie das Add-on. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters und *name-of-add-on* mit dem Namen des Add-Ons, das in der Ausgabe des vorherigen Schritts zurückgegeben wurde. Wenn Sie die *--preserve* Option entfernen, wird die Zusatzsoftware nicht mehr von Amazon EKS verwaltet, sondern auch aus Ihrem Cluster gelöscht.

```
eksctl delete addon --cluster my-cluster --name name-of-addon --preserve
```

Weitere Informationen zum Entfernen von Add-Ons finden Sie in der `eksctl` Dokumentation unter [Löschen von Addons](#).

Add-on entfernen (AWS Konsole)

- Öffnen Sie die [Amazon-EKS-Konsole](#).
- Wählen Sie im linken Navigationsbereich Cluster aus.
- Wählen Sie den Namen des Clusters, für den Sie das Amazon EKS-Add-on entfernen möchten.
- Wählen Sie die Registerkarte Add-ons.
- Wählen Sie das Add-On aus, das Sie entfernen möchten.
- Wählen Sie Remove (Entfernen) aus.
- Gehen Sie im **name of addon** Bestätigungsdialogfeld Entfernen: wie folgt vor:
 - Wenn Amazon EKS die Verwaltung von Einstellungen für das Add-on einstellen soll, wählen Sie Auf dem Cluster beibehalten. Tun Sie dies, wenn Sie die Add-on-Software auf Ihrem Cluster behalten möchten. Auf diese Weise können Sie alle Einstellungen des Add-ons selbst verwalten.
 - Geben Sie den Namen des Add-ons ein.
 - Wählen Sie Remove (Entfernen) aus.

Add-on entfernen (AWS CLI)

1. Sie benötigen eine Version 0.210.0 oder eine neuere Version des eksctl Befehlszeilentools, das auf Ihrem Gerät installiert ist oder AWS CloudShell. Informationen zum Installieren und Aktualisieren von eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).
2. Hier finden Sie eine Liste der installierten Add-Ons. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks list-addons --cluster-name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "addons": [
    "coredns",
    "kube-proxy",
    "vpc-cni",
    "name-of-addon"
  ]
}
```

3. Entfernen Sie das installierte Add-On. Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und *name-of-add-on* durch den Namen des Add-Ons, das Sie entfernen. Durch das Entfernen *--preserve* wird die Zusatzsoftware aus Ihrem Cluster gelöscht.

```
aws eks delete-addon --cluster-name my-cluster --addon-name name-of-addon --preserve
```

Die gekürzte Beispielausgabe lautet wie folgt.

```
{
  "addon": {
    "addonName": "name-of-add-on",
    "clusterName": "my-cluster",
    "status": "DELETING",
  }
}
```

4. Überprüfen Sie den Status der Deinstallation. *my-cluster* Ersetzen Sie ihn durch den Namen Ihres Clusters und *name-of-addon* durch den Namen des Add-ons, das Sie entfernen möchten.

```
aws eks describe-addon --cluster-name my-cluster --addon-name name-of-addon
```

Nachdem das Add-on entfernt wurde, sieht die Beispielausgabe wie folgt aus.

```
An error occurred (ResourceNotFoundException) when calling the DescribeAddon operation: No addon: name-of-addon found in cluster: my-cluster
```

IAM-Rollen für Amazon EKS-Add-Ons

Bestimmte Amazon EKS-Add-Ons benötigen zum Aufrufen AWS APIs IAM-Rollen und -Berechtigungen. Beispielsweise ruft das Amazon VPC CNI-Add-on bestimmte Netzwerkressourcen in Ihrem AWS APIs Konto auf, um sie zu konfigurieren. Diese Add-Ons müssen mithilfe von IAM autorisiert werden. Insbesondere muss das Dienstkonto des Pods, auf dem das Add-on ausgeführt wird, einer IAM-Rolle mit einer bestimmten IAM-Richtlinie zugeordnet sein.

Die empfohlene Methode zur Erteilung von AWS Berechtigungen für Cluster-Workloads ist die Verwendung der Amazon EKS-Funktion Pod Identities. Sie können eine Pod Identity Association verwenden, um das Dienstkonto eines Add-ons einer IAM-Rolle zuzuordnen. Wenn ein Pod ein Servicekonto mit einer Zuordnung verwendet, legt Amazon EKS Umgebungsvariablen in den Containern des Pods fest. Die Umgebungsvariablen konfigurieren die AWS SDKs, einschließlich der AWS CLI, für die Verwendung der EKS Pod Identity-Anmeldeinformationen. Weitere Informationen finden Sie unter [the section called "Pod-Identität"](#)

Amazon EKS-Add-Ons können dabei helfen, den Lebenszyklus von Pod-Identitätszuordnungen zu verwalten, die dem Add-on entsprechen. Sie können beispielsweise ein Amazon EKS-Add-on und die erforderliche Pod-Identitätszuordnung in einem einzigen API-Aufruf erstellen oder aktualisieren. Amazon EKS bietet auch eine API zum Abrufen von vorgeschlagenen IAM-Richtlinien.

1. Vergewissern Sie sich, dass der [Amazon EKS Pod Identity Agent](#) auf Ihrem Cluster eingerichtet ist.
2. Ermitteln Sie mithilfe des `describe-addon-versions` AWS CLI-Vorgangs, ob für das Add-on, das Sie installieren möchten, IAM-Berechtigungen erforderlich sind. Wenn das `requiresIamPermissions` Kennzeichen aktiviert ist `true`, sollten Sie den `describe-addon-configurations` Vorgang verwenden, um die für das Addon benötigten Berechtigungen zu ermitteln. Die Antwort enthält eine Liste der vorgeschlagenen verwalteten IAM-Richtlinien.

3. Rufen Sie den Namen des Kubernetes-Dienstkontos und die IAM-Richtlinie mithilfe der `describe-addon-configuration` CLI-Operation ab. Vergleichen Sie den Umfang der vorgeschlagenen Richtlinie anhand Ihrer Sicherheitsanforderungen.
4. Erstellen Sie eine IAM-Rolle mithilfe der vorgeschlagenen Berechtigungsrichtlinie und der von Pod Identity geforderten Vertrauensrichtlinie. Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Pod Identity-Zuordnung \(Konsole\)AWS”](#).
5. Erstellen oder aktualisieren Sie ein Amazon EKS-Add-on mithilfe der CLI. Geben Sie mindestens eine Pod-Identitätszuordnung an. Eine Pod-Identitätszuordnung ist der Name eines Kubernetes-Dienstkontos und der ARN der IAM-Rolle.
 - Mit dem Add-on erstellte Pod-Identitätszuordnungen APIs gehören dem jeweiligen Add-on. Wenn Sie das Add-on löschen, wird auch die Pod-Identitätszuordnung gelöscht. Sie können dieses kaskadierende Löschen verhindern, indem Sie die `preserve` Option beim Löschen eines Add-ons über die AWS CLI oder API verwenden. Sie können die Pod-Identitätszuordnung bei Bedarf auch direkt aktualisieren oder löschen. Add-Ons können nicht das Eigentum an bestehenden Pod-Identitätszuordnungen übernehmen. Sie müssen die bestehende Zuordnung löschen und sie mithilfe eines Add-On-Vorgangs zum Erstellen oder Aktualisieren neu erstellen.
 - Amazon EKS empfiehlt die Verwendung von Pod-Identitätszuordnungen zur Verwaltung von IAM-Berechtigungen für Add-Ons. Die vorherige Methode, IAM-Rollen für Dienstkonten (IRSA), wird weiterhin unterstützt. Sie können für ein Add-On sowohl eine `IRSA serviceAccountRoleArn` - als auch eine Pod-Identitätszuordnung angeben. Wenn der EKS-Pod-Identitätsagent auf dem Cluster installiert ist, `serviceAccountRoleArn` wird er ignoriert und EKS verwendet die bereitgestellte Pod-Identitätszuordnung. Wenn Pod Identity nicht aktiviert ist, `serviceAccountRoleArn` wird verwendet.
 - Wenn Sie die Pod-Identitätszuordnungen für ein vorhandenes Add-on aktualisieren, leitet Amazon EKS einen fortlaufenden Neustart der Add-On-Pods ein.

Rufen Sie IAM-Informationen zu einem Amazon EKS-Add-on ab

Bevor Sie ein Add-on erstellen, verwenden Sie die AWS CLI, um Folgendes zu ermitteln:

- Wenn das Add-on IAM-Berechtigungen benötigt
- Die empfohlene zu verwendende IAM-Richtlinie

Verfahren

1. Ermitteln Sie den Namen des Add-ons, das Sie installieren möchten, und die Kubernetes-Version Ihres Clusters. Weitere Informationen zu Add-ons finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).
2. Ermitteln Sie mithilfe der AWS CLI, ob für das Add-on IAM-Berechtigungen erforderlich sind.

```
aws eks describe-addon-versions \
--addon-name <addon-name> \
--kubernetes-version <kubernetes-version>
```

Zum Beispiel:

```
aws eks describe-addon-versions \
--addon-name aws-ebs-csi-driver \
--kubernetes-version 1.30
```

Sehen Sie sich die folgende Beispielausgabe an. Beachten Sie, dass `requiresIamPermissions` `true` und die Standard-Add-On-Version sind. Sie müssen die Add-On-Version angeben, wenn Sie die empfohlene IAM-Richtlinie abrufen.

```
{
  "addons": [
    {
      "addonName": "aws-ebs-csi-driver",
      "type": "storage",
      "addonVersions": [
        {
          "addonVersion": "v1.31.0-eksbuild.1",
          "architecture": [
            "amd64",
            "arm64"
          ],
          "compatibilities": [
            {
              "clusterVersion": "1.30",
              "platformVersions": [
                "*"
              ],
              "defaultVersion": true
            }
          ]
        }
      ]
    }
  ]
}
```

```

    ],
    "requiresConfiguration": false,
    "requiresIamPermissions": true
  },
  [...]

```

3. Wenn das Add-on IAM-Berechtigungen benötigt, verwenden Sie die AWS CLI, um eine empfohlene IAM-Richtlinie abzurufen.

```

aws eks describe-addon-configuration \
--query podIdentityConfiguration \
--addon-name <addon-name> \
--addon-version <addon-version>

```

Zum Beispiel:

```

aws eks describe-addon-configuration \
--query podIdentityConfiguration \
--addon-name aws-ebs-csi-driver \
--addon-version v1.31.0-eksbuild.1

```

Überprüfen Sie die folgende Ausgabe. Beachten Sie den `recommendedManagedPolicies`.

```

[
  {
    "serviceAccount": "ebs-csi-controller-sa",
    "recommendedManagedPolicies": [
      "arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy"
    ]
  }
]

```

4. Erstellen Sie eine IAM-Rolle und fügen Sie die empfohlene verwaltete Richtlinie hinzu. Sie können auch die verwaltete Richtlinie überprüfen und den Umfang der Berechtigungen entsprechend einschränken. Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Pod Identity-Zuordnung \(Konsole\)AWS”](#).

Referenz zur Support von Pod Identity

Die folgende Tabelle zeigt, ob bestimmte Amazon EKS-Add-Ons EKS Pod Identity unterstützen.

Name des Add-ons	Unterstützung für Pod-Identitäten	Mindestversion erforderlich
Amazon EBS CSI-Treiber	Ja	v1.26.0-eksbuild.1
Amazon VPC CNI	Ja	v1.15.5-eksbuild.1
Amazon EFS-CSI-Treiber	Ja	v2.0.5-eksbuild.1
AWS Distribution für OpenTelemetry	Ja	v0.94.1-eksbuild.1
Mountpoint für Amazon S3 CSI-Treiber	Nein	N/A
Amazon CloudWatch Observability-Agent	Ja	v3.1.0-eksbuild.1

Diese Tabelle wurde zuletzt am 28. Oktober 2024 aktualisiert.

Verwenden Sie Pod Identities, um einem Amazon EKS-Add-on eine IAM-Rolle zuzuweisen

Bestimmte Amazon EKS-Add-Ons benötigen IAM-Rollen und -Berechtigungen. Bevor Sie ein Amazon EKS-Add-on zur Verwendung einer Pod Identity-Zuordnung aktualisieren, überprüfen Sie die zu verwendende Rolle und Richtlinie. Weitere Informationen finden Sie unter [the section called “IAM-Informationen abrufen”](#).

1. Ermitteln Sie:

- `cluster-name`— Der Name des Clusters, auf dem das Add-on installiert werden soll.
- `addon-name`— Der Name des Add-Ons, das installiert werden soll.
- `service-account-name`— Der Name des Kubernetes-Dienstkontos, das vom Add-on verwendet wird.
- `iam-role-arn`— Der ARN einer IAM-Rolle mit ausreichenden Berechtigungen für das Add-on. Die Rolle muss über die erforderliche Vertrauensrichtlinie für EKS Pod Identity verfügen. Weitere Informationen finden Sie unter [the section called “Erstellen Sie eine Pod Identity-Zuordnung \(Konsole\)AWS”](#).

2. Aktualisieren Sie das Add-on mit der AWS CLI. Sie können beim Erstellen eines Add-Ons auch Pod Identity-Zuordnungen angeben, indem Sie dieselbe `--pod-identity-associations` Syntax verwenden. Beachten Sie, dass, wenn Sie beim Aktualisieren eines Add-ons Pod-Identitätszuordnungen angeben, alle vorherigen Pod-Identitätszuordnungen überschrieben werden.

```
aws eks update-addon --cluster-name <cluster-name> \
--addon-name <addon-name> \
--pod-identity-associations 'serviceAccount=<service-account-name>,roleArn=<role-arn>'
```

Zum Beispiel:

```
aws eks update-addon --cluster-name mycluster \
--addon-name aws-ebs-csi-driver \
--pod-identity-associations 'serviceAccount=ebs-csi-controller-sa,roleArn=arn:aws:iam::123456789012:role/StorageDriver'
```

3. Stellen Sie sicher, dass die Pod-Identity-Zuordnung erstellt wurde:

```
aws eks list-pod-identity-associations --cluster-name <cluster-name>
```

Wenn Sie erfolgreich waren, sollte die Ausgabe folgendermaßen oder ähnlich aussehen. Notieren Sie sich den OwnerARN des EKS-Add-Ons.

```
{
  "associations": [
    {
      "clusterName": "mycluster",
      "namespace": "kube-system",
      "serviceAccount": "ebs-csi-controller-sa",
      "associationArn": "arn:aws:eks:us-west-2:123456789012:podidentityassociation/mycluster/a-4wvljrezsukshq1bv",
      "associationId": "a-4wvljrezsukshq1bv",
      "ownerArn": "arn:aws:eks:us-west-2:123456789012:addon/mycluster/aws-ebs-csi-driver/9cc7ce8c-2e15-b0a7-f311-426691cd8546"
    }
  ]
}
```

Pod Identity-Verknüpfungen aus einem Amazon EKS-Add-on entfernen

Entfernen Sie die Pod Identity-Verknüpfungen aus einem Amazon EKS-Add-on.

1. Ermitteln Sie:

- `cluster-name`- Der Name des EKS-Clusters, auf dem das Add-on installiert werden soll.
- `addon-name`- Der Name des zu installierenden Amazon EKS-Add-ons.

2. Aktualisieren Sie das Addon, um ein leeres Array von Pod-Identitätszuordnungen anzugeben.

```
aws eks update-addon --cluster-name <cluster-name> \
--addon-name <addon-name> \
--pod-identity-associations "[]"
```

Problembehandlung bei Pod-Identitäten für EKS-Add-Ons

Wenn bei Ihren Add-Ons beim Versuch von AWS API-, SDK- oder CLI-Vorgängen Fehler auftreten, überprüfen Sie Folgendes:

- Der Pod Identity Agent ist in Ihrem Cluster installiert.
 - Informationen zur Installation des Pod Identity Agent finden Sie unter [the section called “Richten Sie den Agenten ein”](#).
- Das Add-on hat eine gültige Pod Identity-Zuordnung.
 - Verwenden Sie die AWS CLI, um die Verknüpfungen für den vom Add-on verwendeten Dienstkontonamen abzurufen.

```
aws eks list-pod-identity-associations --cluster-name <cluster-name>
```

- Die IAM-Rolle verfügt über die erforderliche Vertrauensrichtlinie für Pod-Identitäten.
 - Verwenden Sie die AWS CLI, um die Vertrauensrichtlinie für ein Add-on abzurufen.

```
aws iam get-role --role-name <role-name> --query Role.AssumeRolePolicyDocument
```

- Die IAM-Rolle verfügt über die erforderlichen Berechtigungen für das Add-on.
 - Wird AWS CloudTrail zur Überprüfung AccessDenied von UnauthorizedOperation Ereignissen verwendet.
- Der Dienstkontoname in der Pod-Identitätszuordnung entspricht dem vom Add-on verwendeten Dienstkontonamen.

- Informationen zu den verfügbaren Add-Ons finden Sie unter [the section called “ AWS Add-Ons”](#).
- Überprüfen Sie die Konfiguration von MutatingWebhookConfiguration named pod-identity-webhook
 - admissionReviewVersionsdes Webhooks muss v1beta1 und funktioniert nicht. v1

Ermitteln Sie Felder, die Sie für Amazon EKS-Add-Ons anpassen können

Amazon-EKS-Add-ons werden in Ihrem Cluster unter Verwendung von bewährten Standardkonfigurationen installiert. Weitere Informationen zum Hinzufügen eines Amazon-EKS-Add-ons zu Ihrem Cluster finden Sie unter [the section called “Amazon-EKS-Add-ons”](#).

Möglicherweise möchten Sie die Konfiguration eines Amazon-EKS-Add-ons anpassen, um erweiterte Funktionen zu aktivieren. Amazon EKS verwendet die serverseitige Anwendungsfunktion von Kubernetes, um die Verwaltung eines Add-ons durch Amazon EKS zu ermöglichen, ohne Ihre Konfiguration für Einstellungen zu überschreiben, die nicht von Amazon EKS verwaltet werden. Weitere Informationen dazu finden Sie unter [Serverseitiges Anwenden](#) in der Kubernetes-Dokumentation. Um dies zu erreichen, verwaltet Amazon EKS einen Minimalsatz von Feldern für jedes Add-on, das installiert wird. Sie können alle Felder, die nicht von Amazon EKS oder einem anderen Kubernetes-Steuerebenenprozess verwaltet werden kube-controller-manager, problemlos ändern.

Important

Das Ändern eines von Amazon EKS verwalteten Felds verhindert, dass Amazon EKS das Add-on verwaltet und kann dazu führen, dass Ihre Änderungen überschrieben werden, wenn ein Add-on aktualisiert wird.

Syntax für die Feldverwaltung

Wenn Sie Details für ein Kubernetes-Objekt anzeigen, werden sowohl verwaltete als auch nicht verwaltete Felder in der Ausgabe zurückgegeben. Verwaltete Felder können einer der folgenden Typen sein:

- Vollständig verwaltet – Alle Schlüssel für das Feld werden von Amazon EKS verwaltet. Änderungen an einem beliebigen Wert verursachen einen Konflikt.

- Teilweise verwaltet – Einige Schlüssel für das Feld werden von Amazon EKS verwaltet. Nur Änderungen an den Schlüsseln, die explizit von Amazon EKS verwaltet werden, verursachen einen Konflikt.

Beide Arten von Feldern sind gekennzeichnet mit `manager: eks`.

Jeder Schlüssel ist entweder ein `.`, welches das Feld darstellt, das immer einem leeren Satz zugeordnet wird, oder eine Zeichenfolge, die ein Unterfeld oder Element darstellt. Die Ausgabe für die Feldverwaltung besteht aus folgenden Angabetypen:

- `f: name` , wobei *name* der Name eines Feldes in einer Liste ist.
- `k: keys` , wo *keys* sich eine Zuordnung der Felder eines Listenelements befindet.
- `v: value` , wobei *value* der exakte JSON-formatierte Wert eines Listenelements ist.
- `i: index` , wobei *index* die Position eines Elements in der Liste ist.

Die folgenden Ausgabeteile für das CoreDNS Add-on veranschaulichen die vorherigen Angaben:

- Vollständig verwaltete Felder – Wenn ein verwaltetes Feld ein `f: (Feld)` festgelegt hat, aber keinen `k: (Schlüssel)`, dann wird das gesamte Feld verwaltet. Änderungen an Werten in diesem Feld verursachen einen Konflikt.

In der folgenden Ausgabe sehen Sie, dass der Container mit dem Namen `coredns` verwaltet von `eks`. Die `args`, `image` und `imagePullPolicy` Unterfelder werden auch verwaltet von `eks`. Änderungen an Werten in diesen Feldern verursachen einen Konflikt.

```
[...]
f:containers:
  k:{"name":"coredns"}:
    .: {}
    f:args: {}
    f:image: {}
    f:imagePullPolicy: {}
[...]
manager: eks
[...]
```

- Teilweise verwaltete Felder – Wenn für einen verwalteten Schlüssel ein Wert angegeben ist, werden die angegebenen Schlüssel für dieses Feld verwaltet. Das Ändern der angegebenen Schlüssel führt zu einem Konflikt.

In der folgenden Ausgabe sehen Sie, dass eks die config-volume und tmp Volumes verwaltet, welche mit dem name-Schlüssel eingestellt wurden.

```
[...]
f:volumes:
  k:{"name":"config-volume"}:
    .: {}
    f:configMap:
      f:items: {}
      f:name: {}
    f:name: {}
  k:{"name":"tmp"}:
    .: {}
    f:name: {}
[...]
manager: eks
[...]
```

- Hinzufügen von Schlüsseln zu teilweise verwalteten Feldern – Wenn nur ein bestimmter Schlüsselwert verwaltet wird, können Sie sicher zusätzliche Schlüssel wie Argumente zu einem Feld hinzufügen, ohne einen Konflikt zu verursachen. Wenn Sie zusätzliche Schlüssel hinzufügen, stellen Sie sicher, dass das Feld nicht zuerst verwaltet wird. Das Hinzufügen oder Ändern eines verwalteten Werts verursacht einen Konflikt.

In der folgenden Ausgabe sehen Sie, dass sowohl der Schlüssel name als auch das Feld name verwaltet werden. Das Hinzufügen oder Ändern eines Containernamens verursacht einen Konflikt mit diesem verwalteten Schlüssel.

```
[...]
f:containers:
  k:{"name":"coredns"}:
[...]\n    f:name: {}
[...]\nmanager: eks
[...]
```

Verfahren

Sie können `kubectl` verwenden, um zu sehen, welche Felder von Amazon EKS für ein Amazon EKS Add-on verwaltet werden.

Sie können alle Felder, die nicht von Amazon EKS oder einem anderen Kubernetes-Steuerebenenprozess verwaltet werden `kube-controller-manager`, problemlos ändern.

1. Bestimmen Sie das Add-on, das Sie überprüfen möchten. Informationen zu allen in Ihrem Cluster DaemonSets bereitgestellten Daten finden Sie unter `deployments` [the section called “Auf Cluster-Ressourcen zugreifen”](#)
2. Führen Sie den folgenden Befehl aus, um die verwalteten Felder für ein Add-on anzuzeigen:

```
kubectl get type/add-on-name -n add-on-namespace -o yaml
```

Sie können beispielsweise die verwalteten Felder für das CoreDNS Add-on mit dem folgenden Befehl sehen.

```
kubectl get deployment/coredns -n kube-system -o yaml
```

Die Feldverwaltung wird im folgenden Abschnitt in der zurückgegebenen Ausgabe aufgeführt.

```
[...]
managedFields:
  - apiVersion: apps/v1
    fieldsType: FieldsV1
    fieldsV1:
[...]
```

Note

Wenn Sie `managedFields` in der Ausgabe nichts sehen, ergänzen Sie `--show-managed-fields` den Befehl und führen Sie ihn erneut aus. Die Version `kubectl`, die Sie verwenden, bestimmt, ob verwaltete Felder standardmäßig zurückgegeben werden.

Nächste Schritte

Passen Sie die Felder an, die nicht AWS Ihrem Add-on gehören.

Überprüfen Sie Container-Image-Signaturen während der Bereitstellung

Wenn Sie [AWS Signer](#) verwenden und signierte Container-Images zum Zeitpunkt der Bereitstellung verifizieren möchten, können Sie eine der folgenden Lösungen verwenden:

- [Gatekeeper und Ratify](#) — Verwenden Sie Gatekeeper als Zugangscontroller und Ratify, konfiguriert mit einem AWS Signer-Plugin, als Webhook für die Überprüfung von Signaturen.
- [Kyverno](#) — Eine Kubernetes-Policy-Engine, die mit einem Signer-Plugin zur Validierung von Signaturen konfiguriert ist. AWS

Note

Bevor Sie die Signaturen von Container-Images verifizieren, müssen Sie den Trust Store und die Vertrauensrichtlinie für die [Notation](#) entsprechend den Anforderungen des ausgewählten Zugangscontrollers konfigurieren.

Cluster-Ressourcen organisieren und überwachen

In diesem Kapitel finden Sie die folgenden Themen, die Ihnen beim Verwalten Ihres Clusters helfen. Sie können auch Informationen zu Ihren [Kubernetes-Ressourcen](#) mit dem anzeigen. AWS Management Console

- Das Kubernetes-Dashboard ist eine allgemeine, webbasierte Benutzeroberfläche für Kubernetes-Cluster. Es ermöglicht Benutzern, im Cluster ausgeführte Anwendungen zu verwalten und Fehler zu beheben sowie den Cluster selbst zu verwalten. [Weitere Informationen finden Sie unter Das Kubernetes-Dashboard-Repository](#). GitHub
- [the section called “Kennzahlen-Server”](#) Der Kubernetes-Metrik-Server ist ein Aggregator für Ressourcenverbrauchsdaten in Ihrem Cluster. Es wird nicht standardmäßig in Ihrem Cluster bereitgestellt, sondern von Kubernetes-Add-Ons wie dem Kubernetes-Dashboard und verwendet. [the section called “Horizontal Pod Autoscaler”](#) In diesem Thema erfahren Sie, wie der Metrics Server installiert wird.
- [the section called “Stellen Sie Apps mit Helm bereit”](#) Der Helm-Paketmanager für Kubernetes unterstützt Sie bei der Installation und Verwaltung von Anwendungen in Ihrem Kubernetes-Cluster. Dieses Thema hilft Ihnen bei der Installation und Ausführung der Helm-Binärdateien, sodass Sie Charts mit der Helm-CLI auf Ihrem lokalen Computer installieren und verwalten können.
- [the section called “Markieren Ihrer -Ressourcen”](#) - Um Sie bei der Verwaltung Ihrer Amazon EKS-Ressourcen zu unterstützen, können Sie jeder Ressource eigene Metadaten in Form von Tags zuweisen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.
- [the section called “Servicekontingente”](#)— Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden Dienst. AWS erfahren Sie mehr über Amazon EKS-Ressourcenkontingente, und wie Sie sie erhöhen.

Überwachen und optimieren Sie die Amazon EKS-Clusterkosten

Die Kostenüberwachung ist ein wesentlicher Aspekt der Verwaltung Ihrer Kubernetes-Cluster auf Amazon EKS. Indem Sie sich einen Überblick über Ihre Cluster-Kosten verschaffen, können Sie die Ressourcennutzung optimieren, Budgets festlegen und datengestützte Entscheidungen über Ihre Bereitstellungen treffen. Amazon EKS bietet zwei Kostenüberwachungslösungen mit jeweils eigenen Vorteilen, mit denen Sie Ihre Kosten effektiv verfolgen und zuordnen können:

AWS Daten zur Aufteilung der Fakturierungskosten für Amazon EKS — Diese native Funktion lässt sich nahtlos in die AWS Billing Console integrieren, sodass Sie Kosten mit derselben vertrauten Oberfläche und denselben Workflows analysieren und zuordnen können, die Sie für andere AWS Services verwenden. Mit der geteilten Kostenzuweisung können Sie direkt neben Ihren anderen AWS Ausgaben auch Einblicke in Ihre Kubernetes-Kosten gewinnen, was es einfacher macht, die Kosten in Ihrer gesamten Umgebung ganzheitlich zu optimieren. AWS Sie können auch bestehende AWS Abrechnungsfunktionen wie Cost Categories und Erkennung von Kostenanomalien nutzen, um Ihre Kostenmanagementfunktionen weiter zu verbessern. Weitere Informationen finden Sie unter [Grundlegendes zu Daten zur geteilten Kostenzuweisung](#) im AWS Billing User Guide.

Kubecost — Amazon EKS unterstützt Kubecost, ein Tool zur Kostenüberwachung von Kubernetes. Kubecost bietet einen funktionsreichen, Kubernetes-nativen Ansatz zur Kostenüberwachung, der detaillierte Kostenaufschlüsselungen nach Kubernetes-Ressourcen, Empfehlungen zur Kostenoptimierung sowie Dashboards und Berichte bietet. out-of-the-box Kubecost ruft durch die Integration in den AWS Kosten- und Nutzungsbericht auch genaue Preisdaten ab, sodass Sie einen genauen Überblick über Ihre Amazon EKS-Kosten erhalten. [Erfahren Sie, wie Sie Kubecost installieren.](#) Informationen zu einem kostenlosen [Kubecost AWS Abonnement finden Sie auf der Kubecost Marketplace-Seite.](#)

Kosten pro Pod in der AWS Abrechnung mit geteilter Kostenzuweisung anzeigen

Kostenüberwachung mithilfe von Daten zur AWS geteilten Kostenzuweisung für Amazon EKS

Sie können Daten zur AWS geteilten Kostenzuweisung für Amazon EKS verwenden, um eine detaillierte Kostentransparenz für Ihre Amazon EKS-Cluster zu erhalten. Auf diese Weise können Sie die Kosten und die Nutzung Ihrer Kubernetes-Anwendungen analysieren, optimieren und rückbuchen. Sie weisen die Anwendungskosten einzelnen Geschäftseinheiten und Teams auf der Grundlage der EC2 CPU- und Speicherressourcen von Amazon zu, die von Ihrer Kubernetes-Anwendung verbraucht werden. Geteilte Kostenzuweisungsdaten für Amazon EKS bieten Einblick in die Kosten pro Pod und ermöglichen es Ihnen, die Kostendaten pro Pod mithilfe von Namespace, Cluster und anderen Kubernetes-Primitiven zu aggregieren. Im Folgenden finden Sie Beispiele für Kubernetes-Primitive, mit denen Sie Amazon EKS-Kostenzuordnungsdaten analysieren können.

- Clustername
- Bereitstellung

- Namespace
- Knoten
- Name der Workload
- Workload-Typ

[Benutzerdefinierte Kostenzuweisungs-Tags](#) werden ebenfalls unterstützt. Weitere Informationen zur Verwendung von Daten zur geteilten Kostenzuweisung finden Sie unter [Grundlegendes zu Daten zur geteilten Kostenzuweisung](#) im AWS Billing User Guide.

Richten Sie Kosten- und Nutzungsberichte ein

Sie können Split Cost Allocation Data für EKS in der Cost Management Console, der AWS Befehlszeilenschnittstelle oder im aktivieren AWS SDKs.

Verwenden Sie Folgendes für geteilte Kostenzuordnungsdaten:

1. Entscheiden Sie sich für das Teilen von Kostenverrechnungsdaten. Weitere Informationen finden Sie unter [Aktivieren von Daten zur geteilten Kostenzuweisung](#) im Benutzerhandbuch AWS für Kosten- und Nutzungsberichte.
2. Nehmen Sie die Daten in einen neuen oder vorhandenen Bericht auf.
3. Den Bericht anzeigen. Sie können die Konsole Fakturierung und Kostenmanagement verwenden oder die Berichtsdateien in Amazon Simple Storage Service anzeigen.

Installieren Sie Kubecost

Amazon EKS unterstützt Kubecost, mit dem Sie Ihre Kosten, aufgeschlüsselt nach Kubernetes-Ressourcen wie Pods, Knoten, Namespaces und Labels, überwachen können. Dieses Thema behandelt die Installation von Kubecost und den Zugriff auf das Kubecost-Dashboard.

Amazon EKS bietet ein AWS optimiertes Kubecost-Paket für die Transparenz der Cluster-Kosten. Sie können Ihre bestehenden AWS Supportverträge verwenden, um Support zu erhalten. Weitere Informationen zu den verfügbaren Versionen von Kubecost finden Sie unter [the section called "Erfahre mehr über Kubecost"](#)

 Note

Kubecost v2 führt mehrere wichtige neue Funktionen ein. [Erfahren Sie mehr über Kubecost v2.](#)

[Weitere Informationen zu Kubecost finden Sie in der Kubecost-Dokumentation und in den häufig gestellten Fragen.](#)

Installieren Sie das für Amazon EKS optimierte Kubecost-Paket

Sie können eines der folgenden Verfahren verwenden, um das für Amazon EKS optimierte Kubecost-Paket zu installieren:

- Bevor Sie beginnen, wird empfohlen, [Kubecost — Architecture Overview](#) zu lesen, um zu verstehen, wie Kubecost auf Amazon EKS funktioniert.
- Wenn Sie Amazon EKS noch nicht kennen, empfehlen wir Ihnen, Helm für die Installation zu verwenden, da dies die für Amazon EKS optimierte Kubecost-Bundle-Installation vereinfacht. Weitere Informationen finden Sie unter [Bereitstellen von Kubecost auf einem Amazon EKS-Cluster mithilfe des Amazon EKS-Add-ons](#).
- Um die Installation anzupassen, können Sie Ihr für Amazon EKS optimiertes Kubecost-Paket mit Helm konfigurieren. Weitere Informationen finden Sie unter [Bereitstellen von Kubecost auf einem Amazon EKS-Cluster mithilfe von Helm](#) in der Kubecost-Dokumentation.

Rufen Sie das Kubecost-Dashboard auf

Sobald die Einrichtung des für Amazon EKS optimierten Kubecost-Bundles abgeschlossen ist, sollten Sie Zugriff auf das Kubecost-Dashboard haben. Weitere Informationen finden Sie unter [the section called “Greifen Sie auf das Kubecost Dashboard zu”](#).

Greifen Sie auf das Kubecost Dashboard zu

Voraussetzungen

1. Stellen Sie sicher, dass der Status der kubecost-bezogenen Pods auf „Running“ eingestellt ist.

```
kubectl get pods --namespace kubecost
```

Greifen Sie auf das Kubecost Dashboard zu

1. Aktivieren Sie auf Ihrem Gerät die Portweiterleitung, um das Kubecost-Dashboard verfügbar zu machen.

```
kubectl port-forward deployment/kubecost-cost-analyzer 9090 --namespace kubecost
```

Alternativ können Sie den [Load AWS Balancer Controller](#) verwenden, um Kubecost verfügbar zu machen, und Amazon Cognito für Authentifizierung, Autorisierung und Benutzerverwaltung verwenden. Weitere Informationen finden Sie unter [So verwenden Sie Application Load Balancer und Amazon Cognito, um Benutzer für Ihre Kubernetes-Web-Apps zu authentifizieren](#).

2. Öffnen Sie auf demselben Gerät, auf dem Sie den vorherigen Schritt ausgeführt haben, einen Webbrowser und geben Sie die folgende Adresse ein.

```
http://localhost:9090
```

Sie sehen die Kubecost-Übersichtsseite in Ihrem Browser. Abhängig von Ihrer Clustergröße kann es 5—10 Minuten (oder länger) dauern, bis Kubecost Metriken erfasst hat. Sie können Ihre Amazon EKS-Ausgaben einsehen, einschließlich der kumulierten Cluster-Kosten, der zugehörigen Kubernetes-Asset-Kosten und der monatlichen aggregierten Ausgaben.

3. Um die Kosten auf Clusterebene zu verfolgen, kennzeichnen Sie Ihre Amazon-EKS-Ressourcen für die Abrechnung mit Tags. Weitere Informationen finden Sie unter [the section called “Markieren von Ressourcen für die Fakturierung”](#).
 - Cost allocation (Kostenzuordnung) – Zeigen Sie die monatlichen Amazon-EKS-Kosten und kumulierten Kosten für jeden Ihrer Namespaces und andere Dimensionen der letzten sieben Tage an. Dies ist hilfreich, um zu verstehen, welche Teile Ihrer Anwendung zu den Amazon-EKS-Ausgaben beitragen.
 - Anlagen — Sehen Sie sich die Kosten der AWS Infrastrukturressourcen an, die Ihren Amazon EKS-Ressourcen zugeordnet sind.

Erfahre mehr über Kubecost

Amazon EKS bietet ein AWS optimiertes Kubecost-Paket für die Transparenz der Cluster-Kosten. Amazon EKS unterstützt Kubecost, mit dem Sie Ihre Kosten, aufgeschlüsselt nach Kubernetes-Ressourcen wie Pods, Knoten, Namespaces und Labels, überwachen können.

In diesem Thema werden die verfügbaren Versionen von Kubecost und die Unterschiede zwischen den verfügbaren Stufen behandelt. EKS unterstützt Kubecost Version 1 und Version 2. Jede Version ist in verschiedenen Stufen erhältlich. Sie können das für Amazon EKS optimierte Kubecost Bundle ohne zusätzliche Kosten für Ihre Amazon EKS-Cluster verwenden. Möglicherweise wird Ihnen die Nutzung verbundener AWS Dienste wie Amazon Managed Service für Prometheus in Rechnung gestellt. Sie können auch Ihre bestehenden AWS Supportverträge verwenden, um Support zu erhalten.

Als Kubernetes-Plattformadministrator und Finanzleiter können Sie Kubecost verwenden, um eine Aufschlüsselung der Amazon EKS-Gebühren zu visualisieren, Kosten zuzuweisen und Organisationseinheiten wie Anwendungsteams zu belasten. Sie können Ihren internen Teams und Geschäftseinheiten transparente und genaue Kostendaten zur Verfügung stellen, die auf der tatsächlichen Abrechnung basieren. AWS Darüber hinaus können Sie angepasste Empfehlungen für die Kostenoptimierung erhalten, die auf der Infrastrukturumgebung und den Nutzungsmustern innerhalb ihrer Cluster basieren. Weitere Informationen zu Kubecost finden Sie in der [Kubecost-Dokumentation](#).

Was ist der Unterschied zwischen dem benutzerdefinierten Paket von Kubecost und der kostenlosen Version von Kubecost (auch bekannt als)? OpenCost

AWS und Kubecost haben zusammengearbeitet, um eine maßgeschneiderte Version von Kubecost anzubieten. Diese Version enthält eine Teilmenge kommerzieller Features ohne zusätzliche Kosten. In den folgenden Tabellen finden Sie Funktionen, die im benutzerdefinierten Paket von Kubecost enthalten sind.

Kubecost v2

Was ist der Unterschied zwischen Kubecost v1 und v2?

Kubecost 2.0 ist ein wichtiges Upgrade gegenüber früheren Versionen und beinhaltet wichtige neue Funktionen, darunter ein brandneues API-Backend. Beachten Sie, dass [Allocation](#) und [Assets vollständig APIs abwärtskompatibel](#) sind. [Bitte lesen Sie die Kubecost-Dokumentation, um einen reibungslosen Übergang zu gewährleisten. Die vollständige Liste der Verbesserungen finden Sie in der Ankündigung von Kubecost v2.0 und in den vollständigen Versionshinweisen.](#)

Important

[Lesen Sie vor dem Upgrade die Kubecost-Dokumentation.](#) Ein Upgrade kann sich auf die Verfügbarkeit von Berichten auswirken.

Vergleich der wichtigsten Funktionen:

Funktion	Kostenloses Kontingent 2.0 von Kubecost	Für Amazon EKS optimiertes Kubecost Bundle 2.0	Kubecost Enterprise 2.0
Transparenz der Cluster-Kosten	Unbegrenzte Anzahl von Clustern bis zu 250 Kernen	Einheitlicher Multi-Cluster ohne Kernbeschränkungen bei Integration mit Amazon Managed Service für Prometheus	Einheitliche und unbegrenzte Anzahl von Clustern in einer unbegrenzten Anzahl von Umgebungen (d. h. Multi-Cloud)
Bereitstellung	Vom Benutzer gehostet	Vom Benutzer gehostet	Vom Benutzer gehostet, Kubecost gehostet (dedizierter Mandant), SaaS
Unterstützte Datenbanken	Lokaler Prometheus	Amazon Managed Service für Prometheus oder Local Prometheus	Beliebige Prometheus-Varianten und benutzerdefinierte Datenbanken
Unterstützung für die Aufbewahrung von Datenbanken (Rohmetriken)	15 Tage	Unbegrenzte historische Daten	Unbegrenzte historische Daten
Aufbewahrung von Kubecost API und UI (ETL)	15 Tage	15 Tage	Unbegrenzt
Sichtbarkeit in der Hybrid Cloud	-	Amazon EKS und Amazon-EKS-Anywhere-Cluster	Multi-Cloud und Hybrid-Cloud

Funktion	Kostenloses Kontingent 2.0 von Kubecost	Für Amazon EKS optimiertes Kubecost Bundle 2.0	Kubecost Enterprise 2.0
Benachrichtigungen und wiederkehrende Berichte	Wird nur auf dem primären Cluster unterstützt, begrenzt auf 250 Kerne	Effizienzwarnungen , Budgetwarnungen, Benachrichtigungen über Ausgabenänderungen und mehr werden in allen Clustern unterstützt	Effizienzwarnungen , Budgetwarnungen, Benachrichtigungen über Ausgabenänderungen und mehr werden in allen Clustern unterstützt
Gespeicherte Berichte	-	Berichte, die Messwerte von 15 Tagen verwenden	Berichte mit unbegrenzten historischen Daten und Metriken
Integration der Cloud-Abrechnung	Wird nur auf dem primären Cluster unterstützt, begrenzt auf 250 Kerne	Unterstützung bei kundenspezifischen Preisen für AWS (einschließlich mehrerer Cluster und mehrerer Konten)	Unterstützung bei der individuellen Preisgestaltung für jede Cloud
Empfehlungen für Einsparungen	Wird nur auf dem primären Cluster unterstützt, begrenzt auf 250 Kerne	Einblicke in den primären Cluster, aber es gibt kein Limit von 250 Kernen	Erkenntnisse aus mehreren Clustern
Unternehmensführung: Prüfungen	-	-	Prüfen Sie historische Kostenereignisse
Unterstützung von Single Sign-On (SSO)	-	Unterstützung von Amazon Cognito	Okta, Auth0, PingID und alles KeyCloak andere benutzerdefinierte

Funktion	Kostenloses Kontingent 2.0 von Kubecost	Für Amazon EKS optimiertes Kubecost Bundle 2.0	Kubecost Enterprise 2.0
Rollenbasierte Zugriffskontrolle (RBAC) mit SAML 2.0	-	-	Okta, Auth0, PingID und alles andere benutzerdefinierte KeyCloak
Training und Onboarding für Unternehmen	-	-	Schulung und Onboarding mit umfassendem Service FinOps
Teams	-	-	Ja

Neue Funktionen:

Für die folgenden Funktionen gelten metrische Grenzwerte:

- Kubecost Aggregator
- Netzwerk-Überwachung
- Kubecost-Aktionen
- Sammlungen
- Anomalie-Erkennung
- Richtige Größe der Container-Anfrage
- Kubecost-Prognose
- Autocomplete für Filterung und Aggregation

Metrische Grenzwerte:

Metrik	Kostenloses Kontingent 2.0 von Kubecost	Für Amazon EKS optimiertes Kubecost Bundle 2.0	Kubecost Enterprise 2.0
Cluster-Größe	Unbegrenzte Anzahl von Clustern bis zu 250 Kernen	Unbegrenzt	Unbegrenzt
Aufbewahrung metrischer Daten	15 Tage	15 Tage	Unbegrenzt
Unterstützung mehrerer Cluster	Nicht verfügbar	Verfügbar	Verfügbar
Kerngrenzen	250 Kerne pro Cluster	Keine Core-Limits	Keine Kerngrenzen

Kubecost v1

Funktion	Kostenloses Kontingent für Kubecost	Für Amazon EKS optimiertes Kubecost-Paket	Kubecost Enterprise
Bereitstellung	Vom Benutzer gehostet	Vom Benutzer gehostet	Vom Benutzer gehostet oder von Kubecost gehostet (SaaS)
Anzahl der unterstützten Cluster	Unbegrenzt	Unbegrenzt	Unbegrenzt
Unterstützte Datenbanken	Lokaler Prometheus	Lokaler Prometheus- oder Amazon Managed Service für Prometheus	Prometheus, Amazon Managed Service für Prometheus, Cortex oder Thanos

Funktion	Kostenloses Kontingent für Kubecost	Für Amazon EKS optimiertes Kubecost-Paket	Kubecost Enterprise
Unterstützung für die Aufbewahrung von Datenbanken	15 Tage	Unbegrenzte historische Daten	Unbegrenzte historische Daten
Aufbewahrung der Kubecost API (ETL)	15 Tage	15 Tage	Unbegrenzte historische Daten
Transparenz der Cluster-Kosten	Einzelne Cluster	Einheitliches Multi-Cluster	Einheitliches Multi-Cluster
Sichtbarkeit in der Hybrid Cloud	-	Amazon EKS und Amazon-EKS-Anywhere-Cluster	Multi-Cloud- und Hybrid-Cloud-Unterstützung
Benachrichtigungen und wiederkehrende Berichte	-	Unterstützung von Effizienzwarnungen, Budgetwarnungen, Ausgabenänderungswarnungen und mehr	Unterstützung von Effizienzwarnungen, Budgetwarnungen, Ausgabenänderungswarnungen und mehr
Gespeicherte Berichte	-	Berichte mit Daten aus 15 Tagen	Berichte mit unbegrenzten historischen Daten
Integration der Cloud-Abrechnung	Für jeden einzelnen Cluster erforderlich	Unterstützung bei kundenspezifischen Preisen für AWS (einschließlich mehrerer Cluster und mehrerer Konten)	Unterstützung bei kundenspezifischen Preisen für AWS (einschließlich mehrerer Cluster und mehrerer Konten)
Empfehlungen für Einsparungen	Erkenntnisse aus einzelnen Clustern	Erkenntnisse aus einzelnen Clustern	Erkenntnisse aus mehreren Clustern

Funktion	Kostenloses Kontingent für Kubecost	Für Amazon EKS optimiertes Kubecost-Paket	Kubecost Enterprise
Unternehmensführung: Prüfungen	-	-	Prüfen Sie historische Kostenereignisse
Unterstützung von Single Sign-On (SSO)	-	Unterstützung von Amazon Cognito	Okta, Auth0, PingID, KeyCloak
Rollenbasierte Zugriffskontrolle (RBAC) mit SAML 2.0	-	-	Okta, Auth0, PingID, Keycloak
Training und Onboarding für Unternehmen	-	-	Schulung und FinOps Onboarding mit umfassendem Service

Häufig gestellte Fragen

Sehen Sie sich die folgenden häufig gestellten Fragen und Antworten zur Verwendung von Kubecost mit Amazon EKS an.

Was ist die Kubecost API Retention (ETL) -Funktion?

Die ETL-Funktion von Kubecost aggregiert und organisiert Metriken, um die Kosten auf verschiedenen Granularitätsebenen (wie, und) transparent zu machen. namespace-level pod-level deployment-level Für das für Amazon EKS optimierte Kubecost Bundle erhalten Kunden Daten und Erkenntnisse aus Kennzahlen der letzten 15 Tage.

Was ist die Funktion für Benachrichtigungen und wiederkehrende Berichte? Welche Benachrichtigungen und Berichte beinhaltet sie?

Kubecost Alerts ermöglichen es Teams, Updates zu Kubernetes-Ausgaben und Cloud-Ausgaben in Echtzeit zu erhalten. Durch wiederkehrende Berichte erhalten Teams maßgeschneiderte Ansichten der bisherigen Kubernetes- und Cloud-Ausgaben. Beide können mithilfe der Kubecost UI- oder Helm-Werte konfiguriert werden. Sie unterstützen E-Mail, Slack und Microsoft Teams.

Was beinhalten gespeicherte Berichte?

Bei den gespeicherten Berichten von Kubecost handelt es sich um vordefinierte Ansichten von Kosten- und Effizienzkennzahlen. Sie beinhalten die Kosten nach Cluster, Namespace, Label und mehr.

Was ist Cloud-Abrechnungsintegration?

Durch die Integration mit der AWS Abrechnung APIs kann Kubecost out-of-cluster Kosten anzeigen (z. B. Amazon S3). Darüber hinaus ermöglicht es Kubecost, die Cluster-Prognosen von Kubecost mit den tatsächlichen Abrechnungsdaten abzugleichen, um die Spot-Nutzung, Sparpläne und Unternehmensrabatte zu berücksichtigen.

Was beinhalten Sparempfehlungen?

Kubecost bietet Einblicke und Automatisierung, um Benutzern dabei zu helfen, ihre Kubernetes-Infrastruktur und ihre Ausgaben zu optimieren.

Fallen für diese Funktionalität Gebühren an?

Nein. Sie können das für Amazon EKS optimierte Kubecost Bundle ohne zusätzliche Kosten nutzen. Wenn Sie zusätzliche Kubecost-Funktionen wünschen, die nicht enthalten sind, können Sie eine Enterprise-Lizenz von Kubecost über den AWS Marketplace oder direkt bei Kubecost erwerben.

Ist Support für das Amazon EKS-optimierte Kubecost-Paket verfügbar?

Ja, nur wenn Sie das für Amazon EKS optimierte Kubecost-Paket verwenden.

Wie erhalte ich Support für das für Amazon EKS optimierte Kubecost Bundle?

Sie können einen Support-Fall beim AWS Support-Team unter [Kontakt](#) eröffnen AWS.

Benötige ich eine Lizenz, um die von der Amazon EKS-Integration bereitgestellten Kubecost-Funktionen nutzen zu können?

Nein.

Kann ich Kubecost in den AWS Kosten- und Nutzungsbericht integrieren, um genauere Berichte zu erhalten?

Ja. Sie können Kubecost so konfigurieren, dass Daten aus dem AWS Kosten- und Nutzungsbericht aufgenommen werden, um eine genaue Kostentransparenz zu erhalten, einschließlich Rabatte, Spot-

Preise, Preise für Reserved Instances und andere. Weitere Informationen finden Sie unter [AWS Cloud Billing Integration](#) in der Kubecost-Dokumentation.

Unterstützt diese Version das Kostenmanagement von selbstverwalteten Kubernetes-Clustern auf Amazon? EC2

Nein. Das für Amazon EKS optimierte Kubecost-Paket ist nur mit Amazon EKS-Clustern kompatibel.

Kann Kubecost die Kosten für Amazon EKS auf AWS Fargate verfolgen?

Kubecost bietet beste Möglichkeiten, die Cluster-Kosten für Amazon EKS auf Fargate sichtbar zu machen, jedoch mit geringerer Genauigkeit als mit Amazon EKS auf Amazon. EC2 Dies ist in erster Linie auf die unterschiedliche Art und Weise zurückzuführen, wie Ihnen Ihre Nutzung in Rechnung gestellt wird. Mit Amazon EKS auf Fargate werden Ihnen verbrauchte Ressourcen in Rechnung gestellt. Mit Amazon EKS auf EC2 Amazon-Knoten werden Ihnen die bereitgestellten Ressourcen in Rechnung gestellt. Kubecost berechnet die Kosten eines EC2 Amazon-Knotens auf der Grundlage der Knotenspezifikation, die CPU, RAM und kurzlebigen Speicher umfasst. Bei Fargate werden die Kosten auf der Grundlage der angeforderten Ressourcen für die Fargate Pods berechnet.

Wie kann ich Updates und neue Versionen von Kubecost erhalten?

Sie können Ihre Kubecost-Version mithilfe der Standard-Helm-Upgrade-Verfahren aktualisieren. Die neuesten Versionen sind in der [Amazon ECR Public Gallery](#).

Wird die **kubect1-cost** CLI unterstützt? Wie installiere ich es?

Ja. **kubect1-cost** ist ein Open-Source-Tool von Kubecost (Apache 2.0-Lizenz), das CLI-Zugriff auf Kubernetes-Kostenzuweisungsmetriken bietet. [Informationen zur Installation finden Sie unter Installation kubect1-cost am.](#) GitHub

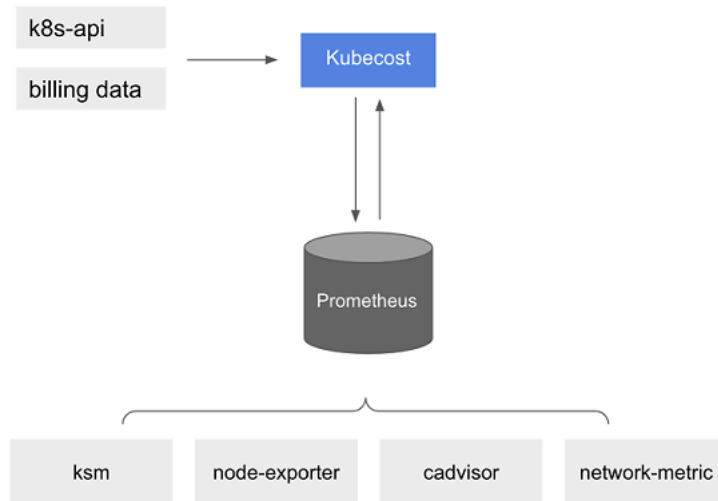
Wird die Kubecost Benutzerschnittstelle unterstützt? Wie greife ich darauf zu?

Kubecost bietet ein Web-Dashboard, auf das Sie über **kubect1** Portweiterleitung, Ingress oder Load Balancer zugreifen können. Sie können auch den Load AWS Balancer Controller verwenden, um Kubecost verfügbar zu machen, und Amazon Cognito für Authentifizierung, Autorisierung und Benutzerverwaltung verwenden. Weitere Informationen finden Sie im Blog unter [So verwenden Sie Application Load Balancer und Amazon Cognito zur Authentifizierung von Benutzern für Ihre Kubernetes-Web-Apps.](#) AWS

Zusätzliche Funktionen von Kubecost

- Die folgenden Funktionen sind sowohl in Kubecost v1 als auch in Kubecost v2 verfügbar.

- **Kostenkennzahlen exportieren** — Die optimierte Kostenüberwachung von Amazon EKS wird mit Kubecost und Prometheus, einem Open-Source-Überwachungssystem und einer Zeitreihendatenbank, bereitgestellt. Kubecost liest Metriken aus Prometheus, führt dann Berechnungen zur Kostenzuweisung durch und schreibt die Metriken zurück in Prometheus. Das Kubecost Frontend liest Metriken aus Prometheus und zeigt sie auf der Kubecost Benutzeroberfläche an. Das folgende Diagramm veranschaulicht die Architektur.



Wenn [Prometheus](#) vorinstalliert ist, können Sie Abfragen schreiben, um Kubecost-Daten zur weiteren Analyse in Ihr aktuelles Business Intelligence-System aufzunehmen. Sie können es auch als Datenquelle für Ihr aktuelles [Grafana-Dashboard](#) verwenden, um die Amazon EKS-Clusterkosten anzuzeigen, mit denen Ihre internen Teams vertraut sind. [Weitere Informationen zum Schreiben von Prometheus-Abfragen finden Sie unter <https://opencost.io/docs/installation/prometheus/>](#)readmeDatei auf GitHub oder verwende die Grafana-JSON-Beispielmodelle im [Kubecost Github-Repository](#) als Referenz.

- **AWS Integration von Kosten- und Nutzungsberichten** — Um Berechnungen der Kostenzuweisung für Ihren Amazon EKS-Cluster durchzuführen, ruft Kubecost die öffentlichen Preisinformationen für AWS Dienste und AWS Ressourcen aus der AWS Preislisten-API ab. Sie können Kubecost auch in den AWS Kosten- und Nutzungsbericht integrieren, um die Genauigkeit der für Ihr Konto spezifischen Preisinformationen zu verbessern. AWS Zu diesen Informationen gehören Rabattprogramme für Unternehmen, Nutzung von reservierten Instances, Savings Plans und Spot-Nutzung. Weitere Informationen zur Funktionsweise der Integration von AWS Kosten- und Nutzungsberichten finden Sie unter [AWS Cloud Billing Integration](#) in der Kubecost-Dokumentation.

Ressourcennutzung mit dem Kubernetes Metrics Server anzeigen

Der Kubernetes Metrics Server ist ein Aggregator von Ressourcennutzungsdaten in Ihrem Cluster und wird nicht standardmäßig in Amazon EKS-Clustern bereitgestellt. Weitere Informationen finden Sie unter [Kubernetes Metrics Server](#) unter. GitHub [Der Metrics Server wird häufig von anderen Kubernetes-Add-Ons verwendet, z. B. von den Scale-Pod-Bereitstellungen mit Horizontal Pod Autoscaler oder dem Kubernetes-Dashboard](#). Weitere Informationen finden Sie unter [Ressourcenmetrikpipeline](#) in der Kubernetes-Dokumentation. In diesem Thema wird erläutert, wie Sie den Kubernetes-Metrik-Server in Ihrem Amazon EKS-Cluster bereitstellen.

Important

Die Metriken sind für Analysen gedacht und stellen keine point-in-time genaue Quelle für historische Analysen dar. Sie können nicht als Überwachungslösung oder für andere Zwecke verwendet werden, die nicht zur auto Skalierung gehören. Weitere Informationen zu Überwachungstools finden Sie unter [Überwachen Sie Cluster](#).

Überlegungen

- Wenn Sie Kubernetes Metrics Server mithilfe des Manifests manuell auf Fargate-Knoten bereitstellen, konfigurieren Sie die `metrics-server` Bereitstellung so, dass ein anderer Port als der Standardport verwendet wird. 10250 Dieser Port ist für Fargate reserviert. Die Amazon EKS-Add-On-Version von Metrics Server ist für die Verwendung von Ports 10251 vorkonfiguriert.
- Stellen Sie sicher, dass Sicherheitsgruppen und Netzwerk 10250 den Port zwischen den `metrics-server` Pods und allen anderen Knoten und Pods ACLs zulassen. Der Kubernetes Metrics Server verwendet weiterhin den Port 10250, um Metriken von anderen Endpunkten im Cluster zu sammeln. Wenn Sie auf Fargate-Knoten bereitstellen, lassen Sie sowohl den konfigurierten alternativen Metrics Server-Port als auch den Port 10250 zu.

Als Community-Add-on mit Amazon EKS Add-ons bereitstellen

Neu: Sie können Metrics Server jetzt über die AWS Konsole oder Amazon EKS als Community-Add-on bereitstellen APIs.

Mit der AWS Konsole bereitstellen

1. Öffnen Sie Ihren EKS-Cluster in der AWS Konsole
2. Wählen Sie auf der Registerkarte „Add-Ons“ die Option Weitere Add-Ons abrufen aus.
3. Wählen Sie im Bereich „Community-Add-Ons“ die Option Metrics Server und dann Weiter
4. EKS bestimmt die passende Version des Add-ons für Ihren Cluster. Sie können die Version mithilfe des Dropdownmenüs Version ändern.
5. Wählen Sie Weiter und dann Erstellen aus, um das Add-on zu installieren.

Weitere Ressourcen

Weitere Informationen zu [the section called “Community-Erweiterungen”](#).

Sie installieren oder aktualisieren Community-Add-Ons auf die gleiche Weise wie andere Amazon EKS-Add-Ons.

- [the section called “Erstellen Sie ein Add-on”](#)
- [the section called “Aktualisieren Sie ein Add-on”](#)
- [the section called “Entfernen Sie ein Add-On”](#)

Mit Manifest bereitstellen

Neu: Sie können Metrics Server jetzt über die AWS Konsole oder Amazon EKS als Community-Add-on bereitstellen APIs. Diese Anweisungen zur Installation des Manifests werden archiviert.

1. Stellen Sie den Metrics Server mit dem folgenden Befehl bereit:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml
```

Wenn Sie Fargate verwenden, müssen Sie diese Datei ändern. In der Standardkonfiguration verwendet der Metrikserver Port 10250. Dieser Port ist auf Fargate reserviert. Ersetzen Sie Verweise auf Port 10250 in components.yaml durch einen anderen Port, z. B. 10251.

2. Stellen Sie mit dem folgenden Befehl sicher, dass die metrics-server Bereitstellung die gewünschte Anzahl von Pods ausführt.

```
kubectl get deployment metrics-server -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
metrics-server	1/1	1	1	6m

3. Testen Sie, ob der Metrikserver funktioniert, indem Sie die Ressourcennutzung (CPU/Arbeitsspeicher) der Knoten anzeigen.

```
kubectl top nodes
```

4. Wenn Sie die Fehlermeldung erhalten `Error from server (Forbidden)`, müssen Sie Ihre Kubernetes-RBAC-Konfiguration aktualisieren. Ihre Kubernetes-RBAC-Identität benötigt ausreichende Berechtigungen, um Cluster-Metriken zu lesen. Informieren Sie sich über die [mindestens erforderlichen Kubernetes-API-Berechtigungen](#) zum Lesen von Metriken. GitHub Erfahren Sie, wie Sie [AWS IAM-Identitäten wie Rollen Zugriff auf Kubernetes gewähren](#). APIs

Stellen Sie Anwendungen mit Helm auf Amazon EKS bereit

Der Helm-Paketmanager für Kubernetes unterstützt Sie bei der Installation und Verwaltung von Anwendungen in Ihrem Kubernetes-Cluster. Weitere Informationen finden Sie in der [Helm-Dokumentation](#). Dieses Thema hilft Ihnen bei der Installation und Ausführung der Helm-Binärdateien, sodass Sie Charts mit der Helm-CLI auf Ihrem lokalen System installieren und verwalten können.

Important

Bevor Sie Helm-Charts in Ihrem Amazon-EKS-Cluster installieren können, müssen Sie `kubectl` so konfigurieren, dass es für Amazon EKS funktioniert. Wenn Sie dies noch nicht getan haben, lesen Sie [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#), bevor Sie fortfahren. Wenn der folgende Befehl für Ihren Cluster erfolgreich ist, sind Sie richtig konfiguriert.

```
kubectl get svc
```

1. Führen Sie den entsprechenden Befehl für das Client-Betriebssystem aus.

- Wenn Sie macOS mit [Homebrew](#) verwenden, installieren Sie die Binärdateien mit dem folgenden Befehl.

```
brew install helm
```

- Weitere Installationsoptionen finden Sie unter [Helm installieren](#) in den Helm-Dokumenten.

 Note

Wenn Sie eine Nachricht bekommen, dass zunächst openssl installiert werden muss, können Sie es mit dem folgenden Befehl installieren.

```
sudo yum install openssl
```

1. Um die neue Binärdatei in Ihren PATH aufzunehmen, schließen Sie Ihr aktuelles Terminalfenster und öffnen Sie ein neues.
2. Sehen Sie die Version von Helm, die Sie installiert haben.

```
helm version --template='{{ .Version }}{{ "\n" }}'
```

Eine Beispielausgabe sieht wie folgt aus.

```
v3.17.2
```

3. Stellen Sie sicher, dass die installierte Version mit Ihrer Cluster-Version kompatibel ist. Weitere Informationen finden Sie [unter Unterstützte Version Skew](#). Wenn Sie beispielsweise mit der unterstützten Kubernetes-Version arbeiten 3.17.x, sollte sie nicht außerhalb des Bereichs von ~ liegen. 1.29.x 1.32.x
4. An dieser Stelle können Sie beliebige Helm-Befehle ausführen (z. B. `helm install chart-name`), um Helm-Charts in Ihrem Cluster zu installieren, zu ändern, zu löschen oder abzufragen. Wenn Sie Helm noch nicht kennen und kein bestimmtes Diagramm installieren müssen, können Sie:
 - Experimentieren, indem Sie ein Beispiel-Chart installieren. [Ein Beispiel-Chart installieren](#) in der Helm- [Schnellstartanleitung](#) lesen.

- Erstellen Sie ein Beispieldiagramm und übertragen Sie es an Amazon ECR. Weitere Informationen finden Sie unter [Übertragen eines Helm-Diagramms](#) im Amazon-Elastic-Container-Registry-Benutzerhandbuch.
- Installieren Sie ein Amazon EKS-Diagramm aus dem [GitHub eks-charts-Repo](#) oder von [ArtifactHub](#)

Organisieren Sie Amazon EKS-Ressourcen mit Tags

Sie können Tags verwenden, die Sie bei der Verwaltung Ihrer Amazon-EKS-Ressourcen unterstützen. Dieses Thema bietet einen Überblick über die Tags -Funktion und zeigt, wie Sie Tags erstellen können.

Themen

- [Grundlagen zu Tags \(Markierungen\)](#)
- [Markieren Ihrer -Ressourcen](#)
- [Tag-Einschränkungen](#)
- [Markieren von Ressourcen für die Fakturierung](#)
- [Arbeiten mit Tags über die Konsole](#)
- [Arbeiten mit Tags mittels CLI, API oder eksctl](#)

Note

Bei Tags handelt es sich um eine Art von Metadaten, die von Kubernetes-Labels und -Annotationen getrennt sind. Weitere Informationen zu diesen anderen Metadatentypen finden Sie in folgenden Abschnitten der Kubernetes-Dokumentation:

- [Labels und Selektoren](#)
- [Anmerkungen](#)

Grundlagen zu Tags (Markierungen)

Ein Tag ist ein Label, das Sie einer Ressource zuweisen. AWS Jedes Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert.

Mit Tags können Sie Ihre AWS Ressourcen kategorisieren. Sie können Ressourcen beispielsweise nach Zweck, Inhaber oder Umgebung kategorisieren. Wenn Sie viele Ressourcen desselben Typs haben, können Sie die Tags, die Sie einer bestimmten Ressource zugewiesen haben, verwenden, um diese Ressource schnell zu identifizieren. Sie können beispielsweise eine Reihe von Tags für Ihre Amazon EKS-Cluster definieren, um Ihnen zu helfen, den Besitzer und die Stack-Ebene jedes Clusters zu verfolgen. Sie sollten für jeden Ressourcentyp einen konsistenten Satz von Tag-Schlüsseln entwickeln. Anschließend können Sie die Ressourcen basierend auf den hinzugefügten Tags suchen und filtern.

Nachdem Sie ein Tag hinzugefügt haben, können Sie jederzeit Tag-Schlüssel und -Werte bearbeiten oder Tags aus einer Ressource entfernen. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Tags haben für Amazon EKS keine semantische Bedeutung und werden ausschließlich als Zeichenfolge interpretiert. Sie können den Wert eines Tags auf eine leere Zeichenfolge setzen. Sie können den Wert eines Tags jedoch nicht auf Null setzen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben.

Wenn Sie AWS Identity and Access Management (IAM) verwenden, können Sie steuern, welche Benutzer in Ihrem AWS Konto berechtigt sind, Tags zu verwalten.

Markieren Ihrer -Ressourcen

Die folgenden Amazon-EKS-Ressourcen unterstützen Tags:

- Cluster
- Verwaltete Knotengruppen
- Fargate-Profil

So wenden Sie Tags auf Ressourcen an:

- Wenn Sie die Amazon EKS-Konsole verwenden, können Sie jederzeit Tags auf neue oder bestehende Ressourcen anwenden. Dies können Sie über das Tags auf der entsprechenden Ressourcenseite. Weitere Informationen finden Sie unter [the section called “Arbeiten mit Tags über die Konsole”](#).
- Wenn Sie die Option `eksctl` verwenden, können Sie Tags auf Ressourcen anwenden, wenn sie mit dieser `--tags` Option erstellt werden.

- Wenn Sie die AWS CLI, die Amazon EKS-API oder ein AWS SDK verwenden, können Sie mithilfe des `tags` Parameters für die entsprechende API-Aktion Tags auf neue Ressourcen anwenden. Sie können auch über die `TagResource`-API Tags auf Ressourcen anwenden. Weitere Informationen finden Sie unter [TagResource](#).

Wenn Sie einige Aktionen zur Erstellung von Ressourcen verwenden, können Sie gleichzeitig mit der Erstellung auch Tags für die Ressource angeben. Wenn Tags nicht angewendet werden können, während die Ressource erstellt wird, kann die Ressource nicht erstellt werden. Dieser Mechanismus stellt sicher, dass Ressourcen, die Sie mit Tags versehen möchten, entweder mit den von Ihnen angegebenen Tags oder gar nicht erstellt werden. Wenn Sie Ressourcen bei ihrer Erstellung taggen, müssen Sie nach der Erstellung der Ressource keine benutzerdefinierten Tagging-Skripts ausführen.

Tags werden nicht auf andere Ressourcen übertragen, die mit der von Ihnen erstellten Ressource verknüpft sind. Fargate-Profil-Tags werden beispielsweise nicht auf andere Ressourcen übertragen, die mit dem Fargate-Profil verknüpft sind, wie z. B. die Pods, die mit dem Fargate-Profil geplant sind.

Tag-Einschränkungen

Für Tags gelten die folgenden Einschränkungen:

- Maximal 50 Tags können einer Ressource zugeordnet werden.
- Tag-Schlüssel können nicht für eine Ressource wiederholt werden. Jeder Tag-Schlüssel muss eindeutig sein, und jeder Schlüssel darf nur einen Wert besitzen.
- Schlüssel können aus bis zu 128 Zeichen im UTF-8-Format bestehen.
- Werte können aus bis zu 256 Zeichen im UTF-8-Format bestehen.
- Wenn mehrere AWS Dienste und Ressourcen Ihr Tagging-Schema verwenden, beschränken Sie die verwendeten Zeichentypen. Einige Services haben möglicherweise Einschränkungen für zulässige Zeichen. Allgemein erlaubte Zeichen sind: Buchstaben, Zahlen, Leerzeichen und die folgenden Sonderzeichen: `+ - = . _ : / @`.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Verwenden Sie `aws:` weder für Schlüssel noch für Werte ein Präfix `AWS:`, noch eine Kombination aus Groß- oder Kleinbuchstaben. Diese sind nur für den AWS Gebrauch reserviert. Sie können Tag-Schlüssel oder -Werte mit diesem Präfix nicht bearbeiten oder löschen. Tags mit diesem Präfix werden nicht auf dein `tags-per-resource` Limit angerechnet.

Markieren von Ressourcen für die Fakturierung

Wenn Sie Tags auf Amazon-EKS-Cluster anwenden, können Sie sie für die Kostenzuweisung in Ihren Kosten- und Nutzungsberichten verwenden. Die Messdaten in Ihren Kosten- und Nutzungsberichten zeigen die Nutzung für alle Ihre Amazon-EKS-Cluster an. Weitere Informationen finden Sie im [AWS Kosten- und Nutzungsbericht](#) im AWS Billing User Guide.

Insbesondere `aws:eks:cluster-name` mit dem AWS generierten Kostenzuweisungs-Tag können Sie die EC2 Amazon-Instance-Kosten im Cost Explorer nach einzelnen Amazon EKS-Clustern aufschlüsseln. Dieses Tag erfasst jedoch nicht die Kosten für die Kontrollebene. Das Tag wird automatisch zu EC2 Amazon-Instances hinzugefügt, die Teil eines Amazon EKS-Clusters sind. Dieses Verhalten tritt unabhängig davon auf, ob die Instances mithilfe von Amazon EKS-verwalteten Knotengruppen, Karpenter oder direkt bei Amazon bereitgestellt werden. EC2 Dieses spezielle Tag wird nicht auf das Limit von 50 Tags angerechnet. Um das Tag verwenden zu können, muss der Kontoinhaber es in der AWS Abrechnungskonsolle oder mithilfe der API aktivieren. Wenn ein Inhaber eines AWS Organisationsverwaltungskontos das Tag aktiviert, wird es auch für alle Mitgliedskonten der Organisation aktiviert.

Sie können Ihre Rechnungsinformationen auch auf der Grundlage von Ressourcen organisieren, die dieselben Tag-Schlüsselwerte haben. Beispielsweise können Sie mehrere Ressourcen mit einem bestimmten Anwendungsnamen taggen und dann Ihre Fakturierungsinformationen organisieren. Auf diese Weise können Sie die Gesamtkosten dieser Anwendung über mehrere Services hinweg sehen. Weitere Informationen zum Einrichten eines Kostenzuordnungsberichts mit Stichwörtern finden Sie unter [Der monatliche Kostenzuordnungsbericht](#) im AWS Billing User Guide.

Note

Wenn Sie die Berichterstellung gerade erst aktiviert haben, werden die Daten für den aktuellen Monat nach 24 Stunden bereitgestellt.

Cost Explorer ist ein Berichtstool, das im Rahmen des AWS kostenlosen Kontingents verfügbar ist. Sie können Cost Explorer verwenden, um Diagramme Ihrer Amazon-EKS-Ressourcen der letzten 13 Monate anzuzeigen. Sie können auch prognostizieren, wie viel Sie in den nächsten drei Monaten voraussichtlich ausgeben werden. Sie können Muster darin erkennen, wie viel Sie im Laufe der Zeit für AWS Ressourcen ausgeben. Sie können es zum Beispiel verwenden, um Bereiche zu identifizieren, die eine genauere Untersuchung erfordern, sowie um Trends auszumachen, die Ihnen

helfen, Ihre Kosten zu verstehen. Sie können auch Zeitbereiche für die Daten angeben und die Daten nach Tagen oder Monate anzeigen lassen.

Arbeiten mit Tags über die Konsole

Mithilfe der Amazon-EKS-Konsole können Sie die Tags im Zusammenhang mit neuen oder vorhandenen Clustern und verwalteten Knotengruppen verwalten.

Wenn Sie eine ressourcenspezifische Seite in der Amazon-EKS-Konsole auswählen, wird auf der Seite eine Liste der Ressourcen angezeigt. Wenn Sie beispielsweise Clusters (Cluster) im Navigationsbereich auswählen, zeigt die Konsole eine Liste der Amazon EKS-Cluster an. Wenn Sie eine Ressource aus einer dieser Listen auswählen (z. B. einen bestimmten Cluster) und die Ressource Tags unterstützt, können Sie deren Tags auf der Registerkarte Tags anzeigen und verwalten.

Sie können auch den Tag-Editor in der verwendeten AWS Management Console, der eine einheitliche Methode zur Verwaltung Ihrer Tags bietet. Weitere Informationen finden Sie unter [Taggen Ihrer AWS Ressourcen mit dem Tag-Editor](#) im AWS Tag-Editor-Benutzerhandbuch.

Hinzufügen von Tags zu einer Ressource bei der Erstellung

Sie können Tags zu Amazon EKS-Clustern und verwalteten Knotengruppen hinzufügen, wenn Sie sie erstellen. Weitere Informationen finden Sie unter [the section called “Erstellen eines -Clusters”](#).

Hinzufügen und Löschen von Tags für eine Ressource

Sie können die Tags, die Ihren Clustern zugeordnet sind, direkt auf der Seite der Ressource hinzufügen oder löschen.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie in der Navigationsleiste die AWS Region aus, die Sie verwenden möchten.
3. Wählen Sie im linken Navigationsbereich die Option Cluster aus.
4. Wählen Sie einen bestimmten Cluster aus.
5. Wählen Sie die Registerkarte Tags und dann Manage tags (Tags verwalten).
6. Fügen Sie auf der Seite Manage tags (Tags verwalten) Ihre Tags bei Bedarf hinzu oder löschen Sie sie.
 - Um einen Tag hinzuzufügen, wählen Sie Add tag (Tag hinzufügen). Geben Sie dann den Schlüssel und den Wert für jedes Tag an.

- Um ein Tag zu entfernen, wählen Sie Remove tag (Tag entfernen) aus.
7. Wiederholen Sie diesen Vorgang für jedes Tag, das Sie hinzufügen oder löschen möchten.
 8. Wählen Sie zum Abschluss Update (Aktualisieren) aus.

Arbeiten mit Tags mittels CLI, API oder **eksctl**

Verwenden Sie die folgenden AWS CLI-Befehle oder Amazon EKS-API-Operationen, um die Tags für Ihre Ressourcen hinzuzufügen, zu aktualisieren, aufzulisten und zu löschen. Sie können **eksctl** nur dann zum Hinzufügen von Tags verwenden, wenn Sie gleichzeitig neue Ressourcen mit einem Befehl erstellen.

Aufgabe	AWS CLI	AWS Tools für Windows PowerShell	API-Aktion
Fügen Sie einen oder mehrere Tags hinzu oder überschreiben Sie sie.	tag-resource	EKSResourceTag hinzufügen	TagResource
Löschen Sie ein oder mehrere Tags.	untag-resource	Entfernen — EKSResource Tag	UntagResource

Die folgenden Beispiele zeigen, wie Ressourcen mithilfe der AWS CLI markiert oder deren Markierung aufgehoben werden.

Beispiel 1: Markieren eines bestehenden Clusters

Der folgende Befehl markiert einen vorhandenen Cluster.

```
aws eks tag-resource --resource-arn resource_ARN --tags team=devs
```

Beispiel 2: Entfernen von Tags von einem bestehenden Cluster

Der folgende Befehl löscht ein Tag von einem bestehenden Cluster.

```
aws eks untag-resource --resource-arn resource_ARN --tag-keys tag_key
```

Beispiel 3: Tags für eine Ressource auflisten

Der folgende Befehl listet die Tags auf, die einer vorhandenen Ressource zugeordnet sind.

```
aws eks list-tags-for-resource --resource-arn resource_ARN
```

Wenn Sie einige Aktionen zur Erstellung von Ressourcen verwenden, können Sie gleichzeitig mit der Erstellung der Ressource auch Tags angeben. Die folgenden Aktionen unterstützen das Taggen beim Erstellen einer Ressource.

Aufgabe	AWS CLI	AWS Tools für Windows PowerShell	API-Aktion	eksctl
Erstellen eines - Clusters	create-cluster	Neu- EKSCluster	CreateCluster	create cluster
Erstellen einer verwalteten Knotengruppe	create-nodegroup	Neu- EKSCluster Nodegroup	CreateNodegroup	create nodegroup
Erstellen eines Fargate-Profiles	create-fargate-profile	Neu- EKSFargate Profil	CreateFargateProfile.html	create fargateprofile

- Wenn Sie die EC2 Amazon-Instances bei der Erstellung einer verwalteten Knotengruppe auch taggen möchten, erstellen Sie die verwaltete Knotengruppe mithilfe einer Startvorlage. Weitere Informationen finden Sie unter [the section called “ EC2 Amazon-Instances taggen”](#). Wenn Ihre Instances bereits vorhanden sind, können Sie die Instanzen manuell mit Tags versehen. Weitere Informationen finden Sie unter [Taggen Ihrer Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

Servicekontingente für Amazon EKS und Fargate anzeigen und verwalten

Amazon EKS hat Service Quotas integriert, einen AWS Service, mit dem Sie Ihre Kontingente von einem zentralen Ort aus einsehen und verwalten können. Weitere Informationen zu Service

Quotas finden Sie unter [Was sind Service Quotas](#) im Benutzerhandbuch für Service Quotas. Mit der Integration von Service Quotas können Sie mithilfe der und AWS CLI schnell den Wert Ihrer Amazon EKS- und AWS Fargate-Servicekontingenten AWS Management Console ermitteln.

EKS-Servicekontingente finden Sie in der AWS Management Console

1. Öffnen Sie die [Service Quotas-Konsole](#).
2. Wählen Sie im linken Navigationsbereich **AWS Dienste** aus.
3. Suchen Sie in der **AWS Serviceliste** nach **Amazon Elastic Kubernetes Service (Amazon EKS)** oder **AWS Fargate** und wählen Sie diese aus.

In der Liste der Service-Kontingente sehen Sie den Namen des Service-Kontingents, den angewendeten Wert (falls verfügbar), das AWS Standardkontingent und ob der Kontingentwert anpassbar ist.

4. Wählen Sie den Kontingentnamen, um zusätzliche Informationen zu einem Service Quota anzuzeigen, z. B. seine Beschreibung.
5. (Optional) Um eine Kontingenterhöhung zu beantragen, wählen Sie das Kontingent, das Sie erhöhen möchten, und dann **Request quota increase** (Kontingenterhöhung beantragen) aus, geben Sie die erforderlichen Informationen ein, und wählen Sie dann **Request** (Beantragen) aus.

Weitere Informationen zum Umgang mit Servicekontingenten mithilfe von finden Sie im [Service Quotas User Guide](#). AWS Management Console Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Service-Quotas-Benutzerhandbuch.

EKS-Dienstkontingente mit der AWS CLI anzeigen

Führen Sie den folgenden Befehl aus, um Ihre Amazon-EKS-Kontingente anzuzeigen.

```
aws service-quotas list-aws-default-service-quotas \
  --query 'Quotas[*]'.
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
  --service-code eks \
  --output table
```

Führen Sie den folgenden Befehl aus, um Ihre Fargate-Kontingente anzuzeigen.

```
aws service-quotas list-aws-default-service-quotas \
```

```
--query 'Quotas[*].  
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \  
--service-code fargate \  
--output table
```

Note

Das zurückgegebene Kontingent ist die Anzahl der Amazon ECS-Aufgaben oder Amazon EKS-Pods, die in diesem Konto in der aktuellen AWS Region gleichzeitig auf Fargate ausgeführt werden können.

Weitere Informationen zum Arbeiten mit Servicekontingenten mithilfe der AWS CLI finden Sie unter [service-quota](#) in der AWS CLI-Befehlsreferenz. Informationen zum Anfordern einer Erhöhung des Kontingents finden Sie unter dem [request-service-quota-increase](#)Befehl in der AWS CLI-Befehlsreferenz.

Amazon-EKS-Service-Quotas

AWS empfiehlt die Verwendung von AWS Management Console , um Ihre aktuellen Kontingente einzusehen. Weitere Informationen finden Sie unter [the section called “EKS-Servicekontingente finden Sie in der AWS Management Console”](#).

Die standardmäßigen EKS-Servicekontingente finden Sie unter [Amazon Elastic Kubernetes Service Service-Endpunkte und Kontingente](#) in der AWS Allgemeinen Referenz.

Diese Servicekontingente werden unter Amazon Elastic Kubernetes Service (Amazon EKS) in der Service-Quotas-Konsole aufgeführt. Informationen zum Anfordern einer Kontingenterhöhung für Werte, die als anpassbar angezeigt werden, finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Benutzerhandbuch von Service Quotas.

Note

Anpassungen an den folgenden Komponenten werden in Service Quotas nicht unterstützt: * Pod Identity-Zuordnungen pro Cluster. Grenzwerte finden Sie unter [the section called “Pod-Identität”](#). * CIDRs für Remote Node Networks oder Remote Pod Networks für Hybridknoten. Grenzwerte finden Sie unter [the section called “Hybridknoten”](#).

AWS Fargate-Servicekontingente

Der AWS Fargate-Dienst in der Service Quotas-Konsole listet mehrere Service Quotas auf. Sie können Alarme konfigurieren, mit denen Sie benachrichtigt werden, wenn sich Ihre Nutzung einem Servicekontingent nähert. Weitere Informationen finden Sie unter [the section called “Einen CloudWatch Alarm zur Überwachung der Fargate-Ressourcennutzungsmetriken erstellen”](#).

Neue AWS Konten haben möglicherweise niedrigere anfängliche Kontingente, die sich im Laufe der Zeit erhöhen können. Fargate überwacht ständig die Kontonutzung in jeder AWS Region und erhöht dann automatisch die Kontingente je nach Nutzung. Außerdem können Sie eine Kontingenterhöhung für Werte anfordern, die als anpassbar angezeigt werden. Weitere Informationen finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Service-Quotas-Benutzerhandbuch.

AWS empfiehlt, sie zu verwenden, um Ihre aktuellen AWS Management Console Kontingente einzusehen. Weitere Informationen finden Sie unter [the section called “EKS-Servicekontingente finden Sie in der AWS Management Console”](#).

Die standardmäßigen AWS Fargate on EKS-Dienstkontingente finden Sie unter [Fargate-Dienstkontingente](#) in der AWS Allgemeinen Referenz.

Note

Fargate setzt außerdem Amazon ECS-Aufgaben und Startquoten für Amazon EKS Pods durch. Weitere Informationen finden Sie unter [AWS Fargate-Drosselungsquoten](#) im Amazon ECS-Handbuch.

Sicherheit in Amazon EKS

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS ist für Amazon EKS für die Kubernetes-Steuerebene verantwortlich, die die Knoten und etcd die Datenbank der Kontrollebene umfasst. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS - Compliance-Programme](#) regelmäßig. Informationen zu den Compliance-Programmen, die für Amazon EKS gelten, finden Sie unter [AWS -Services im Geltungsbereich nach Compliance-Programm](#).
- Sicherheit in der Cloud – Ihre Verantwortlichkeit umfasst die folgenden Bereiche.
 - Die Sicherheitskonfiguration der Datenebene, einschließlich der Konfiguration der Sicherheitsgruppen, die den Durchgang des Datenverkehrs aus der Amazon-EKS-Steuerebene in die VPC des Kunden zulassen.
 - Die Konfiguration der Knoten und der Container selbst.
 - Das Betriebssystem des Knotens (einschließlich Updates und Sicherheitspatches)
 - Andere zugehörige Anwendungssoftware:
 - Einrichten und Verwalten von Kontrollelementen für das Netzwerk (wie beispielsweise Firewall-Regeln)
 - Verwalten des Identity and Access Management auf Plattformebene, entweder mit oder zusätzlich zu IAM
 - Die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und geltende Gesetze und Vorschriften

Amazon EKS ist durch mehrere Compliance-Programme für regulierte und sensible Anwendungen zertifiziert. [Amazon EKS entspricht SOC, PCI, ISO, FedRAMP-Moderate, IRAP, C5, K-ISMS, ENS High, OSPAR und HITRUST CSF und ist ein HIPAA-fähiger Service](#). Weitere Informationen finden Sie unter [Zugriff verwalten](#).

Diese Dokumentation zeigt Ihnen, wie Sie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Amazon EKS einsetzen können. Die folgenden Themen zeigen Ihnen, wie Sie Amazon EKS konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Services nutzen können, mit denen Sie Ihre Amazon EKS-Ressourcen überwachen und sichern können.

Note

Linux-Container bestehen aus Kontrollgruppen (Cgroups) und Namespaces, die dazu beitragen, den Zugriff eines Containers einzuschränken, aber alle Container verwenden denselben Linux-Kernel wie die Host-Amazon-Instance. EC2 Es wird dringend davon abgeraten, einen Container als Root-Benutzer (UID 0) auszuführen oder einem Container Zugriff auf Hostressourcen oder Namespaces wie das Hostnetzwerk oder den Host-PID-Namespace zu gewähren, da dies die Effektivität der von Containern bereitgestellten Isolation verringert.

Themen

- [Schützen Sie Amazon EKS-Cluster mit Best Practices](#)
- [Analysieren Sie Sicherheitslücken in Amazon EKS](#)
- [Konformitätsprüfung für Amazon EKS-Cluster](#)
- [Sicherheitsüberlegungen für Amazon Elastic Kubernetes Service](#)
- [Sicherheitsüberlegungen für Kubernetes](#)
- [Sicherheitsüberlegungen für den Amazon EKS Auto Mode](#)
- [Identitäts- und Zugriffsverwaltung für Amazon EKS](#)

Schützen Sie Amazon EKS-Cluster mit Best Practices

Die bewährten Sicherheitsmethoden von Amazon EKS finden Sie in den [Best Practices for Security](#) im Amazon EKS Best Practices Guide.

Analysieren Sie Sicherheitslücken in Amazon EKS

Sicherheit ist ein wichtiger Aspekt bei der Konfiguration und Wartung von Kubernetes-Clustern und -Anwendungen. Im Folgenden sind Ressourcen aufgeführt, mit denen Sie die Sicherheitskonfiguration

Ihrer EKS-Cluster analysieren können, Ressourcen, mit denen Sie nach Schwachstellen suchen können, und Integrationen mit AWS Services, die diese Analyse für Sie durchführen können.

Der Benchmark des Center for Internet Security (CIS) für Amazon EKS

Der [Kubernetes-Benchmark des Center for Internet Security \(CIS\)](#) bietet Anleitungen für Amazon EKS-Sicherheitskonfigurationen. Die Benchmark:

- Gilt für EC2 Amazon-Knoten (sowohl verwaltete als auch selbstverwaltete), bei denen Sie für die Sicherheitskonfigurationen der Kubernetes-Komponenten verantwortlich sind.
- Bietet eine von der Community genehmigte Standardmethode, um sicherzustellen, dass Sie Ihren Kubernetes-Cluster und Ihre Knoten sicher konfiguriert haben, wenn Sie Amazon EKS verwenden.
- Besteht aus vier Abschnitten; Protokollierungskonfiguration der Steuerebene, Knotensicherheitskonfigurationen, Richtlinien und verwaltete Services.
- Unterstützt alle Kubernetes-Versionen, die derzeit in Amazon EKS verfügbar sind und können mit [kube-bench](#), ein Standard-Open-Source-Tool zur Überprüfung der Konfiguration mit dem CIS-Benchmark auf Kubernetes-Clustern.

Weitere Informationen hierzu finden Sie unter [Einführung des CIS Amazon EKS Benchmark](#) aus.

Eine automatisierte aws-sample Pipeline zur Aktualisierung Ihrer Knotengruppe mit einem CIS-Benchmark-AMI finden Sie unter [EKS-Optimized AMI](#) Hardening Pipeline.

Amazon-EKS-Plattformversionen

Die Amazon EKS-Plattformversionen stellen die Funktionen der Cluster-Steuerebene dar, einschließlich der aktivierten Kubernetes-API-Serverflugs und der aktuellen Kubernetes-Patch-Version. Neue Cluster werden mit der neuesten Plattformversion bereitgestellt. Details hierzu finden Sie unter [the section called "Plattformversionen"](#).

Sie können einen [Amazon EKS-Cluster](#) auf neuere Kubernetes-Versionen aktualisieren. Wenn neue Kubernetes-Versionen in Amazon EKS verfügbar werden, empfehlen wir Ihnen, Ihre Cluster proaktiv auf die neueste verfügbare Version zu aktualisieren. Weitere Informationen zu Kubernetes-Versionen in EKS finden Sie unter [the section called "Kubernetes-Versionen"](#).

Liste der Sicherheitslücken im Betriebssystem

AL2023 Liste der Sicherheitslücken

Verfolgen Sie Sicherheits- oder Datenschutzereignisse für Amazon Linux 2023 im [Amazon Linux Security Center](#) oder abonnieren Sie den zugehörigen [RSS-Feed](#). Sicherheits- und Datenschutzereignisse enthalten eine Übersicht über das Problem sowie Pakete und Anweisungen zum Aktualisieren Ihrer Instances, um das Problem zu beheben.

Liste der Sicherheitslücken in Amazon Linux 2

Sie können Sicherheits- oder Datenschutzereignisse für Amazon Linux 2 im [Amazon Linux-Sicherheitszentrum](#) verfolgen oder den zugehörigen [RSS-Feed](#) abonnieren. Sicherheits- und Datenschutzereignisse enthalten eine Übersicht über das Problem sowie Pakete und Anweisungen zum Aktualisieren Ihrer Instances, um das Problem zu beheben.

Knotenerkennung mit Amazon Inspector

Sie können [Amazon Inspector](#) verwenden, um Ihre Knoten auf unbeabsichtigten Netzwerkzugriff und auf Sicherheitslücken in diesen EC2 Amazon-Instances zu überprüfen.

Cluster- und Knotenerkennung mit Amazon GuardDuty

Der GuardDuty Bedrohungserkennungsservice von Amazon, der Ihnen hilft, Ihre Konten, Container, Workloads und die Daten in Ihrer AWS Umgebung zu schützen. GuardDuty Bietet unter anderem die folgenden beiden Funktionen zur Erkennung potenzieller Bedrohungen für Ihre EKS-Cluster: EKS-Schutz und Runtime Monitoring.

Weitere Informationen finden Sie unter [the section called “Amazon GuardDuty”](#).

Konformitätsprüfung für Amazon EKS-Cluster

Um zu erfahren, ob ein AWS Service in den Geltungsbereich bestimmter Compliance-Programme fällt, sehen Sie sich die [AWS Services unter Umfang nach Compliance-Programmen an und wählen Sie das Compliance-Programm](#) aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS -Compliance-Programme](#).

Mit AWS Artifact können Sie Prüfberichte von Drittanbietern herunterladen. Weitere Informationen finden Sie unter [Berichte in AWS Artifact herunterladen](#).

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung von AWS Diensten hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Compliance und Governance im Bereich Sicherheit](#) – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- [Referenz für berechnete HIPAA-Services](#) – Listet berechnete HIPAA-Services auf. Nicht alle AWS Dienste sind HIPAA-fähig.
- [AWS Ressourcen zur Einhaltung](#) von Vorschriften — Diese Sammlung von Arbeitsmapen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. Die Leitfäden fassen die bewährten Verfahren zur Sicherung von AWS Diensten zusammen und ordnen die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI) und International Organization for Standardization (ISO)) zu.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Developer Guide — Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#) — Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS Ressourcen zu bewerten und Ihre Einhaltung der Sicherheitsstandards und Best Practices der Sicherheitsbranche zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerelementreferenz](#).
- [Amazon GuardDuty](#) — Dieser AWS Service erkennt potenzielle Bedrohungen für Ihre AWS Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem wir die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllen.
- [AWS Audit Manager](#) — Mit diesem AWS Service können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um Ihr Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Sicherheitsüberlegungen für Amazon Elastic Kubernetes Service

Im Folgenden finden Sie Überlegungen zur Sicherheit der Cloud, da sie sich auf Amazon EKS auswirken.

Themen

- [Infrastruktursicherheit in Amazon EKS](#)
- [Verstehen Sie die Resilienz in Amazon EKS-Clustern](#)

Infrastruktursicherheit in Amazon EKS

Als verwalteter Service ist Amazon Elastic Kubernetes Service durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon EKS zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Oder Sie können den [AWS Security Token Service](#) (AWS STS) verwenden, um temporäre Sicherheitsanmeldeinformationen zum Signieren von Anfragen zu generieren.

Wenn Sie einen Amazon-EKS-Cluster erstellen, geben Sie die VPC-Subnetze an, die Ihr Cluster verwenden soll. Amazon EKS erfordert Subnetze in mindestens zwei Availability Zones. Wir empfehlen eine VPC mit öffentlichen und privaten Subnetzen, damit Kubernetes öffentliche Load Balancer in den öffentlichen Subnetzen einrichten kann, die den Traffic auf Pods ausgleichen, die auf Knoten laufen, die sich in privaten Subnetzen befinden.

Weitere Informationen zu Überlegungen bezüglich der VPC finden Sie unter [the section called “VPC- und Subnetz-Anforderungen”](#).

Wenn Sie Ihre VPC- und Knotengruppen mit den AWS CloudFormation Vorlagen erstellen, die in der Anleitung [Erste Schritte mit Amazon EKS](#) bereitgestellt werden, werden Ihre Kontrollebene und Ihre Knotensicherheitsgruppen mit unseren empfohlenen Einstellungen konfiguriert.

Weitere Informationen zu Überlegungen bezüglich Sicherheitsgruppen finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#).

Wenn Sie einen neuen Cluster erstellen, erstellt Amazon EKS einen Endpunkt für den verwalteten Kubernetes-API-Server, über den Sie mit Ihrem Cluster kommunizieren (mit Kubernetes-Verwaltungswerkzeugen wie `kubectl`). Standardmäßig ist dieser API-Serverendpunkt im Internet öffentlich, und der Zugriff auf den API-Server wird mithilfe einer Kombination aus AWS Identity and Access Management (IAM) und nativer Kubernetes [Role Based Access Control](#) (RBAC) gesichert.

Sie können den privaten Zugriff auf den Kubernetes-API-Server aktivieren, sodass die gesamte Kommunikation zwischen Ihren Knoten und dem API-Server innerhalb Ihrer VPC bleibt. Sie können die IP-Adressen einschränken, die über das Internet auf Ihren API-Server zugreifen können, oder den Internetzugriff auf den API-Server vollständig deaktivieren.

Weitere Informationen zum Ändern des Zugriffs auf Cluster-Endpunkte finden Sie unter [the section called “Ändern des Cluster-Endpunktzugriffs”](#).

[Sie können Kubernetes-Netzwerkrichtlinien mit dem Amazon VPC CNI oder Tools von Drittanbietern wie Project Calico implementieren.](#) Weitere Informationen zur Verwendung von Amazon VPC CNI für Netzwerkrichtlinien finden Sie unter [the section called “Kubernetes-Richtlinien”](#). Project Calico ist ein Open-Source-Projekt eines Drittanbieters. Weitere Informationen finden Sie in der [Dokumentation zu Project Calico](#).

Greifen Sie auf Amazon EKS zu mit AWS PrivateLink

Sie können AWS PrivateLink verwenden, um eine private Verbindung zwischen Ihrer VPC und Amazon Elastic Kubernetes Service herzustellen. Sie können auf Amazon EKS zugreifen, als wäre es in Ihrer VPC, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung verwenden zu müssen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf Amazon EKS zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellenendpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem

Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für Amazon EKS bestimmt ist.

Weitere Informationen finden Sie unter [Access AWS services through AWS PrivateLink](#) im AWS PrivateLink Handbuch.

Bevor Sie beginnen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Aufgaben ausgeführt haben:

- Lesen Sie [den Artikel Zugriff auf einen AWS Dienst über einen VPC-Endpunkt mit einer Schnittstelle](#) im AWS PrivateLink Handbuch.

Überlegungen

- Support und Einschränkungen: Amazon EKS-Schnittstellenendpunkte ermöglichen den sicheren Zugriff auf alle Amazon EKS-API-Aktionen von Ihrer VPC aus, unterliegen jedoch bestimmten Einschränkungen: Sie unterstützen keinen Zugriff auf Kubernetes APIs, da diese über einen separaten privaten Endpunkt verfügen. Sie können Amazon EKS nicht so konfigurieren, dass nur über den Schnittstellenendpunkt zugegriffen werden kann.
- Preisgestaltung: Für die Nutzung von Schnittstellenendpunkten für Amazon EKS AWS PrivateLink fallen Standardgebühren an: Stundengebühren für jeden in jeder Availability Zone bereitgestellten Endpunkt, Datenverarbeitungsgebühren für den Datenverkehr über den Endpunkt. Weitere Informationen finden Sie auf der Seite über [AWS PrivateLink – Preise](#).
- Sicherheit und Zugriffskontrolle: Wir empfehlen, die Sicherheit zu verbessern und den Zugriff mit diesen zusätzlichen Konfigurationen zu kontrollieren. Verwenden Sie VPC-Endpunktrichtlinien, um den Zugriff auf Amazon EKS über den Schnittstellenendpunkt zu kontrollieren, Ordnen Sie Sicherheitsgruppen den Endpunkt-Netzwerkschnittstellen zu, um den Verkehr zu verwalten, verwenden Sie VPC-Flussprotokolle, um den IP-Verkehr zu und von den Schnittstellenendpunkten zu erfassen und zu überwachen, wobei die Protokolle auf Amazon oder Amazon S3 veröffentlicht werden können. CloudWatch Weitere Informationen finden Sie unter [Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien](#) und [Protokollieren von IP-Verkehr mithilfe von VPC Flow Logs](#).
- Konnektivitätsoptionen: Schnittstellenendpunkte bieten flexible Konnektivitätsoptionen über lokalen Zugriff (verbinden Sie Ihr lokales Rechenzentrum mit einer VPC mit dem Schnittstellenendpunkt über AWS Direct Connect oder AWS Site-to-Site VPN) oder über Inter-VPC-Konnektivität

(verwenden Sie AWS Transit Gateway oder VPC-Peering, um andere mit der VPC über den Schnittstellenendpunkt zu verbinden und so den Verkehr im Netzwerk VPCs zu halten). AWS

- **IP-Versionsunterstützung:** Endpunkte, die vor August 2024 erstellt wurden, unterstützen nur die IPv4 Verwendung von `eks.region.amazonaws.com`. Neue Endpunkte, die nach August 2024 erstellt wurden, unterstützen Dual-Stack IPv4 und (z. B. `eks.region.amazonaws.com`, `eks.region.api.aws`). IPv6
- **Regionale Verfügbarkeit:** AWS PrivateLink Die EKS-API ist in den Regionen Asien-Pazifik (Malaysia) (`ap-southeast-5`), Asien-Pazifik (Thailand) (`ap-southeast-7`), Mexiko (Central) (`mx-central-1`) und Asien-Pazifik (Taipeh) (`ap-east-2`) nicht verfügbar. AWS PrivateLink Unterstützung für `eks-auth` (EKS Pod Identity) ist in der Region Asien-Pazifik (Malaysia) (`ap-Southeast-5`) verfügbar.

Erstellen eines Schnittstellen-Endpunkts für Amazon EKS

Sie können einen Schnittstellenendpunkt für Amazon EKS entweder mit der Amazon VPC-Konsole oder der AWS Befehlszeilschnittstelle (AWS CLI) erstellen. Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter [Erstellen eines VPC-Endpunkts](#).

Erstellen Sie einen Schnittstellenendpunkt für Amazon EKS mit den folgenden Servicenamen:

EKS-API

- `com.amazonaws.region-code.eks`
- `com.amazonaws.region-code.eks-fips` (für FIPS-konforme Endpunkte)

EKS-Authentifizierungs-API (EKS-Pod-Identität)

- `com.amazonaws.region-code.eks-auth`

Private DNS-Funktion für Amazon EKS-Schnittstellenendpunkte

Die private DNS-Funktion, die standardmäßig für Schnittstellenendpunkte von Amazon EKS und anderen AWS Diensten aktiviert ist, ermöglicht sichere und private API-Anfragen mit standardmäßigen regionalen DNS-Namen. Diese Funktion stellt sicher, dass API-Aufrufe über den Schnittstellenendpunkt über das private AWS Netzwerk weitergeleitet werden, wodurch Sicherheit und Leistung verbessert werden.

Die private DNS-Funktion wird automatisch aktiviert, wenn Sie einen Schnittstellenendpunkt für Amazon EKS oder andere AWS Dienste erstellen. Zur Aktivierung müssen Sie Ihre VPC korrekt konfigurieren, indem Sie bestimmte Attribute festlegen:

- `enableDnsHostnames`: Ermöglicht Instances innerhalb der VPC, DNS-Hostnamen zu haben.
- `enableDnsSupport`: Aktiviert die DNS-Auflösung in der gesamten VPC.

step-by-stepAnweisungen zum Überprüfen oder Ändern dieser Einstellungen finden Sie unter [DNS-Attribute für Ihre VPC anzeigen und aktualisieren](#).

DNS-Namen und IP-Adresstypen

Wenn die private DNS-Funktion aktiviert ist, können Sie bestimmte DNS-Namen verwenden, um eine Verbindung zu Amazon EKS herzustellen. Diese Optionen entwickeln sich im Laufe der Zeit:

- `eks.region.amazonaws.com`: Der traditionelle DNS-Name, der nur für Adressen vor August 2024 aufgelöst wird. IPv4 Bei bestehenden Endpunkten, die auf Dual-Stack aktualisiert wurden, wird dieser Name in Adressen sowohl als auch aufgelöst. IPv4 IPv6
- `eks.region.api.aws`: Dieser Dual-Stack-DNS-Name ist für neue Endpunkte verfügbar, die nach August 2024 erstellt wurden. Er wird in Adressen sowohl als auch aufgelöst. IPv4 IPv6

Nach August 2024 verfügen neue Schnittstellenendpunkte über zwei DNS-Namen, und Sie können sich für den Dual-Stack-IP-Adresstyp entscheiden. Bei bestehenden Endpunkten wird durch die Aktualisierung auf Dual-Stack `eks.region.amazonaws.com` so geändert, dass sowohl als auch unterstützt werden. IPv4 IPv6

Verwendung der privaten DNS-Funktion

Nach der Konfiguration kann die private DNS-Funktion in Ihre Workflows integriert werden und bietet die folgenden Funktionen:

- **API-Anfragen**: Verwenden Sie die standardmäßigen regionalen DNS-Namen, entweder `eks.region.amazonaws.com` oder `eks.region.api.aws`, je nach Einrichtung Ihres Endpunkts, um API-Anfragen an Amazon EKS zu stellen.
- **Anwendungskompatibilität**: Ihre vorhandenen Anwendungen, die EKS aufrufen, APIs müssen nicht geändert werden, um diese Funktion nutzen zu können.

- AWS CLI mit Dual-Stack: Informationen zur Verwendung der Dual-Stack-Endpunkte mit der AWS CLI finden Sie in der Konfiguration von [Dual-Stack- und FIPS-Endpunkten im Referenzhandbuch](#) und im Tools-Referenzhandbuch. AWS SDKs
- Automatisches Routing: Jeder Anruf an den Amazon EKS-Standard-Serviceendpunkt wird automatisch über den Schnittstellenendpunkt geleitet, wodurch eine private und sichere Konnektivität gewährleistet ist.

Verstehen Sie die Resilienz in Amazon EKS-Clustern

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Amazon EKS betreibt und skaliert die Kubernetes-Steuerebene über mehrere AWS Availability Zones hinweg, um eine hohe Verfügbarkeit zu gewährleisten. Amazon EKS skaliert Steuerebene-Instances automatisch basierend auf der Last, erkennt und ersetzt fehlerhafte Steuerebene-Instances und patcht die Steuerebene automatisch. Nachdem Sie ein Versionsupdate eingeleitet haben, aktualisiert Amazon EKS Ihre Steuerebene für Sie und behält die hohe Verfügbarkeit der Steuerebene während des Updates bei.

Diese Kontrollebene besteht aus mindestens zwei API-Server-Instances und drei etcd Instances, die in drei Availability Zones innerhalb einer AWS Region ausgeführt werden. Amazon EKS:

- überwacht aktiv die Last auf Steuerebenen-Instances und skaliert sie automatisch, um eine hohe Leistung sicherzustellen;
- Erkennt und ersetzt automatisch fehlerhafte Instanzen der Kontrollebene und startet sie bei Bedarf in allen Availability Zones innerhalb der AWS Region neu.
- Nutzt die Architektur der AWS Regionen, um eine hohe Verfügbarkeit aufrechtzuerhalten. Deshalb kann Amazon EKS ein [SLA für die Verfügbarkeit von API-Server-Endpunkten](#) anbieten.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Sicherheitsüberlegungen für Kubernetes

Im Folgenden finden Sie Überlegungen zur Sicherheit in der Cloud, da sie sich auf Kubernetes in Amazon EKS-Clustern auswirken. Einen ausführlichen Überblick über die Sicherheitskontrollen und -praktiken in Kubernetes finden Sie unter [Cloud Native Security und Kubernetes in der Kubernetes-Dokumentation](#).

Themen

- [Sichere Workloads mit Kubernetes-Zertifikaten](#)
- [Verstehen Sie die von Amazon EKS erstellten RBAC-Rollen und -Benutzer](#)
- [Verschlüsseln Sie Kubernetes-Geheimnisse mit KMS auf vorhandenen Clustern](#)
- [AWS Secrets Manager Manager-Geheimnisse mit Amazon EKS Pods verwenden](#)
- [Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten](#)

Sichere Workloads mit Kubernetes-Zertifikaten

[Die Kubernetes-Zertifikats-API automatisiert die Bereitstellung von X.509-Anmeldeinformationen.](#)

Die API bietet eine Befehlszeilenschnittstelle für Kubernetes-API-Clients, um [X.509-Zertifikate](#) von einer Zertifizierungsstelle (CA) anzufordern und zu erhalten. Sie können die `CertificateSigningRequest` (CSR)-Ressource verwenden, um anzufordern, dass ein benannter Unterzeichner das Zertifikat signiert. Ihre Anfragen werden entweder genehmigt oder abgelehnt, bevor sie signiert werden. Kubernetes unterstützt sowohl integrierte Unterzeichner als auch benutzerdefinierte Unterzeichner mit klar definiertem Verhalten. Auf diese Weise können Kunden vorhersagen, was mit ihnen passiert. CSRs Weitere Informationen zur Zertifikatsignatur finden Sie unter [Signieren von Anforderungen](#).

Einer der integrierten Unterzeichner ist `kubernetes.io/legacy-unknown`. Die `v1beta1`-API der CSR-Ressource berücksichtigte diesen Unterzeichnertyp „legacy-unknown“. Die stabile `v1` API von CSR erlaubt es jedoch nicht, auf eingestellt `signerName` zu `kubernetes.io/legacy-unknown` werden.

Wenn Sie Amazon EKS CA zum Generieren von Zertifikaten verwenden möchten, müssen Sie einen benutzerdefinierten Unterzeichner verwenden. Um die CSR-`v1`-API-Version zu verwenden und ein neues Zertifikat zu generieren, müssen Sie alle vorhandenen Manifeste und API-Clients migrieren. Bestehende Zertifikate, die mit der vorhandenen `v1beta1`-API erstellt wurden, sind gültig und funktionieren, bis sie ablaufen. Diese umfasst die folgenden Funktionen:

- Vertrauensverteilung: keine. In einem Kubernetes-Cluster gibt es keine Standardvertrauensstellung oder -verteilung für diesen Unterzeichner.
- Zulässige Themen: beliebig
- Zulässige x509-Erweiterungen: Zeichnet Nutzungserweiterungen zu `subjectAltName` und verwirft andere Erweiterungen
- Zulässige Schlüsselnutzung: Darf keine anderen Nutzungen als [„Schlüsselverschlüsselung“, „digitale Signatur“, „Serverauth“] enthalten

 Note

Das Signieren von Clientzertifikaten wird nicht unterstützt.

- Ablauf/Zertifikatslebensdauer: 1 Jahr (Standard und Maximum)
- CA-Bit zulässig/unzulässig: unzulässig

Beispiel CSR-Erstellung mit `signerName`

Diese Schritte veranschaulichen, wie Sie ein Bereitstellungszertifikat für DNS-Namen `myserver.default.svc` mit `signerName: beta.eks.amazonaws.com/app-serving` erstellen. Verwenden Sie dies als Leitfaden für Ihre eigene Umgebung.

1. Führen Sie den Befehl `openssl genrsa -out myserver.key 2048` aus, um einen privaten RSA-Schlüssel zu erzeugen.

```
openssl genrsa -out myserver.key 2048
```

2. Führen Sie den folgenden Befehl aus, um eine Zertifikatsanforderung zu erstellen.

```
openssl req -new -key myserver.key -out myserver.csr -subj "/CN=myserver.default.svc"
```

3. Generieren Sie einen base64-Wert für die CSR-Variablen für die Verwendung in einem späteren Schritt.

```
base_64=$(cat myserver.csr | base64 -w 0 | tr -d "  
")
```

4. Führen Sie den folgenden Befehl aus, um eine Datei mit dem Namen `mycsr.yaml` zu erstellen. Im folgenden Beispiel ist `beta.eks.amazonaws.com/app-serving` der `signerName`.

```
cat >mycsr.yaml <<EOF
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  name: myserver
spec:
  request: $base_64
  signerName: beta.eks.amazonaws.com/app-serving
  usages:
    - digital signature
    - key encipherment
    - server auth
EOF
```

5. Reichen Sie die CSR ein.

```
kubectl apply -f mycsr.yaml
```

6. Genehmigen Sie das Bereitstellungszertifikat.

```
kubectl certificate approve myserver
```

7. Stellen Sie sicher, dass das Zertifikat ausgestellt wurde.

```
kubectl get csr myserver
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	AGE	SIGNERNAME	REQUESTOR	CONDITION
myserver	3m20s	beta.eks.amazonaws.com/app-serving	kubernetes-admin	Approved, Issued

8. Exportieren Sie das ausgestellte Zertifikat.

```
kubectl get csr myserver -o jsonpath='{.status.certificate}' | base64 -d >
myserver.crt
```

Verstehen Sie die von Amazon EKS erstellten RBAC-Rollen und -Benutzer

Wenn Sie einen Kubernetes-Cluster erstellen, werden auf diesem Cluster mehrere Standard-Kubernetes-Identitäten erstellt, damit Kubernetes ordnungsgemäß funktioniert. Amazon EKS erstellt Kubernetes-Identitäten für jede seiner Standardkomponenten. Die Identitäten bieten eine rollenbasierte Autorisierungssteuerung (RBAC) von Kubernetes für die Cluster-Komponenten. Weitere Informationen finden Sie unter [Using RBAC Authorization](#) in der Kubernetes-Dokumentation.

Wenn Sie optionale [Add-Ons](#) für Ihren Cluster installieren, werden Ihrem Cluster möglicherweise zusätzliche Kubernetes-Identitäten hinzugefügt. Weitere Informationen zu Identitäten, die in diesem Thema nicht behandelt werden, finden Sie in der Dokumentation des Add-Ons.

Sie können die Liste der von Amazon EKS erstellten Kubernetes-Identitäten auf Ihrem Cluster mit dem `kubectl` Befehlszeilentool, der AWS Management Console oder anzeigen. Alle Benutzeridentitäten erscheinen in den kube Audit-Logs, die Ihnen über Amazon CloudWatch zur Verfügung stehen.

AWS Management Console

Voraussetzung

Der von Ihnen [verwendete IAM-Principal](#) muss über die unter [Erforderliche](#) Berechtigungen beschriebenen Berechtigungen verfügen.

Um von Amazon EKS erstellte Identitäten anzuzeigen, verwenden Sie den AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie in der Liste Clusters (Cluster) den Cluster aus, der die anzuzeigenden Identitäten enthält.
3. Wählen Sie die Registerkarte Resources (Ressourcen) aus.
4. Wählen Sie unter Resource types (Ressourcentypen) die Option Authorization (Autorisierung) aus.
5. Wählen Sie ClusterRoles, ClusterRoleBindings, Rollen oder RoleBindings. Alle Ressourcen, denen eks vorangestellt ist, wurden von Amazon EKS erstellt. Weitere von Amazon EKS erstellte Identitätsressourcen sind:
 - Der ClusterRole und ClusterRoleBinding benannte `aws-node`. Die `aws-node`-Ressourcen unterstützen das [Amazon VPC CNI-Plugin für Kubernetes](#), das Amazon EKS auf allen Clustern installiert.

- Ein benannter und ein benannter. `ClusterRoleVPCResourceController` `roleClusterRoleBindingVPCResourceController` Diese Ressourcen unterstützen den [Amazon-VPC-Ressourcencontroller](#), den Amazon EKS auf allen Clustern installiert.

Zusätzlich zu den Ressourcen, die Sie in der Konsole sehen, gibt es in Ihrem Cluster die folgenden speziellen Benutzeridentitäten, die jedoch in der Clusterkonfiguration nicht sichtbar sind:

- **eks:cluster-bootstrap**— Wird für `kubectl` Operationen beim Cluster-Bootstrap verwendet.
 - **eks:support-engineer**— Wird für Clusterverwaltungsvorgänge verwendet.
6. Wählen Sie eine bestimmte Ressource aus, um Details dazu anzuzeigen. Standardmäßig werden Ihnen Informationen in der Strukturierten Ansicht angezeigt. In der oberen rechten Ecke der Detailseite können Sie die Raw view (Rohansicht) auswählen, um alle Informationen für die Ressource anzuzeigen.

Kubectl

Voraussetzung

Die Entität, die Sie verwenden (AWS Identity and Access Management (IAM) oder OpenID Connect (OIDC)), um die Kubernetes-Ressourcen auf dem Cluster aufzulisten, muss von IAM oder Ihrem OIDC-Identitätsanbieter authentifiziert werden. Der Entität müssen Berechtigungen zur Verwendung von Kubernetes `get` und `list` Verben für die, und Ressourcen in Ihrem Cluster erteilt werden `Role` `ClusterRole` `RoleBinding`, mit denen die Entität arbeiten soll. `ClusterRoleBinding` Weitere Informationen zum Gewähren von Zugriff auf IAM-Entitäten auf Ihren Cluster finden Sie unter [the section called "Kubernetes-API-Zugriff"](#). Weitere Informationen darüber, wie Sie Entitäten, die von Ihrem eigenen OIDC-Anbieter authentifiziert wurden, Zugriff auf Ihren Cluster gewähren, finden Sie unter [the section called "OIDC-Anbieter verknüpfen"](#)

So zeigen Sie von Amazon EKS erstellte Identitäten mit dem **kubectl** an

Führen Sie den Region aus, die Sie anzeigen möchten. Alle zurückgegebenen Ressourcen, denen `eks` vorangestellt ist, wurden von Amazon EKS erstellt. Zusätzlich zu den Ressourcen, die in der Ausgabe der Befehle zurückgegeben wurden, sind die folgenden speziellen Benutzeridentitäten in Ihrem Cluster vorhanden, obwohl sie in der Clusterkonfiguration nicht sichtbar sind:

- **eks:cluster-bootstrap**— Wird für `kubectl` Operationen beim Cluster-Bootstrap verwendet.
- **eks:support-engineer**— Wird für Clusterverwaltungsvorgänge verwendet.

ClusterRoles— ClusterRoles sind auf Ihren Cluster beschränkt, sodass alle einer Rolle erteilten Berechtigungen für Ressourcen in jedem Kubernetes-Namespace auf dem Cluster gelten.

Der folgende Befehl gibt alle von Amazon EKS erstellten Kubernetes ClusterRoles auf Ihrem Cluster zurück.

```
kubectl get clusterroles | grep eks
```

Zusätzlich zu dem in der Ausgabe zurückgegebenen ClusterRoles, dem etwas vorangestellt ist, sind die folgenden ClusterRoles vorhanden.

- **aws-node**— Dies ClusterRole unterstützt das [Amazon VPC CNI-Plugin für Kubernetes](#), das Amazon EKS auf allen Clustern installiert.
- **vpc-resource-controller-role**— Dies ClusterRole unterstützt den [Amazon VPC Resource Controller](#), den Amazon EKS auf allen Clustern installiert.

Um die Spezifikation für a zu sehenClusterRole, ersetzen Sie *eks:k8s-metrics* den folgenden Befehl durch einen, der in der Ausgabe des vorherigen Befehls ClusterRole zurückgegeben wurde. Das folgende Beispiel gibt die Spezifikation für die zurück *eks:k8s-metrics*ClusterRole.

```
kubectl describe clusterrole eks:k8s-metrics
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name:          eks:k8s-metrics
Labels:        <none>
Annotations:   <none>
PolicyRule:
  Resources      Non-Resource URLs  Resource Names  Verbs
  -----
  endpoints      [ ]                  [ ]             [list]
  nodes          [ ]                  [ ]             [list]
  pods           [ ]                  [ ]             [list]
  deployments.apps [ ]                  [ ]             [list]
```

ClusterRoleBindings— ClusterRoleBindings sind auf Ihren Cluster beschränkt.

Der folgende Befehl gibt alle von Amazon EKS erstellten Kubernetes ClusterRoleBindings auf Ihrem Cluster zurück.

```
kubectl get clusterrolebindings | grep eks
```

Zusätzlich zu dem in der Ausgabe zurückgegebenen ClusterRoleBindings, sind die folgenden ClusterRoleBindings vorhanden.

- **aws-node**— Dies ClusterRoleBinding unterstützt das [Amazon VPC CNI-Plugin für Kubernetes](#), das Amazon EKS auf allen Clustern installiert.
- **vpc-resource-controller-rolebinding**— Dies ClusterRoleBinding unterstützt den [Amazon VPC Resource Controller](#), den Amazon EKS auf allen Clustern installiert.

Um die Spezifikation für a zu sehenClusterRoleBinding, ersetzen Sie *eks:k8s-metrics* den folgenden Befehl durch einen, der in der Ausgabe des vorherigen Befehls ClusterRoleBinding zurückgegeben wurde. Das folgende Beispiel gibt die Spezifikation für die zurück *eks:k8s-metrics*ClusterRoleBinding.

```
kubectl describe clusterrolebinding eks:k8s-metrics
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name:          eks:k8s-metrics
Labels:        <none>
Annotations:   <none>
Role:
  Kind: ClusterRole
  Name:  eks:k8s-metrics
Subjects:
  Kind  Name          Namespace
  ----  -
  User  eks:k8s-metrics
```

Rollen — Roles sind auf einen Kubernetes-Namespace beschränkt. Alle mit Roles erstellten Amazon EKS sind auf den kube-system-Namespace beschränkt.

Der folgende Befehl gibt alle von Amazon EKS erstellten Kubernetes Roles auf Ihrem Cluster zurück.

```
kubectl get roles -n kube-system | grep eks
```

Um die Spezifikation für `a` zu sehen, ersetzen Sie `eks:k8s-metrics` den folgenden Befehl durch den Namen von `a`, der in der Ausgabe des vorherigen Befehls zurückgegeben wurde. Das folgende Beispiel gibt die Spezifikation für die zurück `eks:k8s-metrics` Rolle.

```
kubectl describe role eks:k8s-metrics -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name:          eks:k8s-metrics
Labels:        <none>
Annotations:   <none>
PolicyRule:
  Resources      Non-Resource URLs  Resource Names      Verbs
  -----
  daemonsets.apps  []                  [aws-node]          [get]
  deployments.apps  []                  [vpc-resource-controller] [get]
```

RoleBindings— RoleBindings sind auf einen Kubernetes-Namespace beschränkt. Alle mit RoleBindings erstellten Amazon EKS sind auf den `kube-system`-Namespace beschränkt.

Der folgende Befehl gibt alle von Amazon EKS erstellten Kubernetes RoleBindings auf Ihrem Cluster zurück.

```
kubectl get rolebindings -n kube-system | grep eks
```

Um die Spezifikation für `a` zu sehen, ersetzen Sie `eks:k8s-metrics` den folgenden Befehl durch einen, der in der Ausgabe des vorherigen Befehls zurückgegeben wurde. Das folgende Beispiel gibt die Spezifikation für die zurück `eks:k8s-metrics` RoleBinding.

```
kubectl describe rolebinding eks:k8s-metrics -n kube-system
```

Eine Beispielausgabe sieht wie folgt aus.

```
Name:          eks:k8s-metrics
Labels:        <none>
Annotations:   <none>
Role:
  Kind:  Role
  Name:  eks:k8s-metrics
```

Subjects:

Kind	Name	Namespace
----	----	-----
User	eks:k8s-metrics	

Verschlüsseln Sie Kubernetes-Geheimnisse mit KMS auf vorhandenen Clustern

Important

Dieses Verfahren gilt nur für EKS-Cluster, auf denen Kubernetes Version 1.27 oder niedriger ausgeführt wird. Wenn Sie Kubernetes Version 1.28 oder höher ausführen, sind Ihre Kubernetes-Secrets standardmäßig mit Envelope-Verschlüsselung geschützt. Weitere Informationen finden Sie unter [the section called “Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten”](#).

Wenn Sie die [Verschlüsselung von Geheimnissen](#) aktivieren, werden die Kubernetes-Secrets mit dem von Ihnen ausgewählten KMS-Schlüssel verschlüsselt. AWS Der KMS-Schlüssel muss die folgenden Bedingungen erfüllen:

- Symmetrisch
- Kann Daten verschlüsseln und entschlüsseln
- In derselben AWS Region wie der Cluster erstellt
- Wenn der KMS-Schlüssel in einem anderen Konto erstellt wurde, muss der [IAM-Prinzipal](#) Zugriff auf den KMS-Schlüssel haben.

Weitere Informationen finden Sie unter [Zulassen, dass IAM-Prinzipale in anderen Konten einen KMS-Schlüssel verwenden können im AWS Key Management Service Developer Guide](#).

Warning

Sie können die Verschlüsselung von Geheimnissen nicht mehr deaktivieren, nachdem Sie sie aktiviert haben. Diese Aktion ist unumkehrbar.

eksctl

Dieses Verfahren gilt nur für EKS-Cluster, auf denen Kubernetes Version 1.27 oder niedriger ausgeführt wird. Weitere Informationen finden Sie unter [the section called “Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten”](#).

Sie können die Verschlüsselung auf zwei Arten aktivieren:

- Fügen Sie Ihrem Cluster mit einem einzigen Befehl Verschlüsselung hinzu.

Um Ihre Secrets automatisch erneut zu verschlüsseln, führen Sie den folgenden Befehl aus.

```
eksctl utils enable-secrets-encryption \
  --cluster my-cluster \
  --key-arn arn:aws:kms:region-code:account:key/key
```

Um die automatische Neuverschlüsselung Ihrer Secrets zu deaktivieren, führen Sie den folgenden Befehl aus.

```
eksctl utils enable-secrets-encryption
  --cluster my-cluster \
  --key-arn arn:aws:kms:region-code:account:key/key \
  --encrypt-existing-secrets=false
```

- Fügen Sie Ihrem Cluster eine Verschlüsselung mit einer `kms-cluster.yaml`-Datei hinzu.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: region-code

secretsEncryption:
  keyARN: arn:aws:kms:region-code:account:key/key
```

Um Ihre Secrets automatisch erneut zu verschlüsseln, führen Sie den folgenden Befehl aus.

```
eksctl utils enable-secrets-encryption -f kms-cluster.yaml
```

Um die automatische Neuverschlüsselung Ihrer Secrets zu deaktivieren, führen Sie den folgenden Befehl aus.

```
eksctl utils enable-secrets-encryption -f kms-cluster.yaml --encrypt-existing-secrets=false
```

AWS Management Console

- Dieses Verfahren gilt nur für EKS-Cluster, auf denen Kubernetes Version 1.27 oder niedriger ausgeführt wird. Weitere Informationen finden Sie unter [the section called “Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten”](#).
- Öffnen Sie die [Amazon-EKS-Konsole](#).
- Wählen Sie den Cluster aus, dem Sie die KMS-Verschlüsselung hinzufügen möchten.
- Wählen Sie die Registerkarte Overview (Übersicht) aus (sie ist standardmäßig ausgewählt).
- Scrollen Sie nach unten zum Abschnitt Secrets encryption (Secrets-Verschlüsselung) und wählen Sie Enable (Aktivieren) aus.
- Wählen Sie einen Schlüssel in der Dropdown-Liste und dann die Schaltfläche Enable (Aktivieren) aus. Wenn keine Schlüssel aufgeführt sind, müssen Sie zuerst einen erstellen. Weitere Informationen finden Sie unter [Erstellen von Schlüsseln](#)
- Wählen Sie die Schaltfläche Confirm (Bestätigen) aus, um den ausgewählten Schlüssel zu verwenden.

AWS CLI

- Dieses Verfahren gilt nur für EKS-Cluster, auf denen Kubernetes Version 1.27 oder niedriger ausgeführt wird. Weitere Informationen finden Sie unter [the section called “Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten”](#).
- Ordnen Sie die [Secrets-Verschlüsselungskonfiguration](#) mithilfe des folgenden AWS CLI-Befehls Ihrem Cluster zu. Ersetzen Sie das *example values* durch Ihr eigenes.

```
aws eks associate-encryption-config \
  --cluster-name my-cluster \
  --encryption-config '[{"resources":["secrets"],"provider":
{"keyArn":"arn:aws:kms:region-code:account:key/key"}]'
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
```

```

"update": {
  "id": "3141b835-8103-423a-8e68-12c2521ffa4d",
  "status": "InProgress",
  "type": "AssociateEncryptionConfig",
  "params": [
    {
      "type": "EncryptionConfig",
      "value": "[{\"resources\": [\"secrets\"], \"provider\": {\"keyArn\": \"arn:aws:kms:region-code:account:key/key\"}}]"
    }
  ],
  "createdAt": 1613754188.734,
  "errors": []
}
}

```

- c. Sie können den Status Ihrer Verschlüsselungsaktualisierung mit dem folgenden Befehl überwachen. Verwenden Sie den `cluster name` und die `update ID`, die in der vorherigen Ausgabe zurückgegeben wurden. Wenn der Status `Successful` angezeigt wird, ist das Update abgeschlossen.

```

aws eks describe-update \
  --region region-code \
  --name my-cluster \
  --update-id 3141b835-8103-423a-8e68-12c2521ffa4d

```

Eine Beispielausgabe sieht wie folgt aus.

```

{
  "update": {
    "id": "3141b835-8103-423a-8e68-12c2521ffa4d",
    "status": "Successful",
    "type": "AssociateEncryptionConfig",
    "params": [
      {
        "type": "EncryptionConfig",
        "value": "[{\"resources\": [\"secrets\"], \"provider\": {\"keyArn\": \"arn:aws:kms:region-code:account:key/key\"}}]"
      }
    ],
    "createdAt": 1613754188.734>,
    "errors": []
  }
}

```

```
}  
}
```

- d. Führen Sie den Befehl `describe-cluster` aus, um zu überprüfen, ob die Verschlüsselung in Ihrem Cluster aktiviert ist. Die Antwort enthält eine `EncryptionConfig`-Zeichenfolge.

```
aws eks describe-cluster --region region-code --name my-cluster
```

Nachdem Sie die Verschlüsselung in Ihrem Cluster aktiviert haben, müssen Sie alle vorhandenen Secrets mit dem neuen Schlüssel verschlüsseln:

 Note

Wenn Sie `eksctl` verwenden, ist die Ausführung des folgenden Befehls nur dann erforderlich, wenn Sie die automatische Neuverschlüsselung Ihrer Secrets deaktivieren.

```
kubectl get secrets --all-namespaces -o json | kubectl annotate --overwrite -f - kms-  
encryption-timestamp="time value"
```

 Warning

Wenn Sie die [Verschlüsselung von Geheimnissen](#) für einen vorhandenen Cluster aktivieren und der von Ihnen verwendete KMS-Schlüssel jemals gelöscht wird, gibt es keine Möglichkeit, den Cluster wiederherzustellen. Wenn Sie den KMS-Schlüssel löschen, wird der Cluster dauerhaft auf einen degradierten Zustand festgelegt. Weitere Informationen finden Sie unter [Löschen von AWS KMS-Schlüsseln](#).

 Note

Standardmäßig erstellt der `create-key` Befehl einen [KMS-Schlüssel mit symmetrischer Verschlüsselung und einer Schlüsselrichtlinie](#), die dem Konto Root-Administratorzugriff auf AWS KMS-Aktionen und -Ressourcen gewährt. Wenn Sie die Berechtigungen begrenzen möchten, müssen Sie sicherstellen, dass die Aktionen `kms:DescribeKey` und `kms:CreateGrant` für die Richtlinie für den Prinzipal zulässig sind, der die API `create-cluster` aufruft.

Für Cluster, die KMS-Umschlagverschlüsselung verwenden, sind `kms:CreateGrant`-Berechtigungen erforderlich. Die Bedingung `kms:GrantIsForAWSResource` wird für die `CreateCluster` Aktion nicht unterstützt und sollte nicht in KMS-Richtlinien zur Steuerung der `kms:CreateGrant` Berechtigungen von Benutzern verwendet werden, die diese Aktion ausführen `CreateCluster`.

AWS Secrets Manager Manager-Geheimnisse mit Amazon EKS Pods verwenden

Um Geheimnisse aus Secrets Manager und Parameter aus dem Parameter Store als in Amazon EKS-Pods gemountete Dateien anzuzeigen, können Sie den AWS Secrets and Configuration Provider (ASCP) für den [Kubernetes Secrets Store](#) CSI-Treiber verwenden.

Mit dem ASCP können Sie Ihre Secrets in Secrets Manager speichern und verwalten und diese dann über Ihre auf Amazon EKS ausgeführten Workloads abrufen. Sie können IAM-Rollen und -Richtlinien verwenden, um den Zugriff auf Ihre Geheimnisse auf bestimmte Kubernetes-Pods in einem Cluster zu beschränken. Das ASCP ruft die Pod-Identität ab und tauscht die Identität gegen eine IAM-Rolle aus. ASCP übernimmt die IAM-Rolle des Pods und kann dann Secrets aus Secrets Manager abrufen, die für diese Rolle autorisiert sind.

Wenn Sie in Secrets Manager die automatische Rotation für Ihre Secrets verwenden, können Sie auch die Secrets-Store-CSI-Treiberrotation verwenden, um sicherzustellen, dass Sie das neueste Secret aus Secrets Manager abrufen.

Note

AWS Fargate (Fargate) -Knotengruppen werden nicht unterstützt.

Weitere Informationen finden Sie unter [Verwenden von Secrets Manager Manager-Geheimnissen in Amazon EKS](#) im AWS Secrets Manager Manager-Benutzerhandbuch.

Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten

Amazon Elastic Kubernetes Service (Amazon EKS) bietet eine Standard-Envelope-Verschlüsselung für alle Kubernetes-API-Daten in EKS-Clustern, auf denen Kubernetes Version 1.28 oder höher ausgeführt wird.

Die Envelope-Verschlüsselung schützt die Daten, die Sie auf dem Kubernetes-API-Server speichern. Die Envelope-Verschlüsselung gilt beispielsweise für die Konfiguration Ihres Kubernetes-Clusters, wie z. ConfigMaps. Die Envelope-Verschlüsselung gilt nicht für Daten auf Knoten oder EBS-Volumes. EKS unterstützte zuvor die Verschlüsselung von Kubernetes-Geheimnissen, und jetzt erstreckt sich diese Envelope-Verschlüsselung auf alle Kubernetes-API-Daten.

Dies bietet eine verwaltete Standarderfahrung, die defense-in-depth für Ihre Kubernetes-Anwendungen implementiert wird und keine weiteren Maßnahmen Ihrerseits erfordert.

Amazon EKS verwendet AWS [Key Management Service \(KMS\)](#) mit [Kubernetes KMS Provider v2](#) für diese zusätzliche Sicherheitsebene mit einem [Amazon Web Services Services-eigenen Schlüssel](#) und der Option, dass Sie Ihren eigenen vom [Kunden verwalteten Schlüssel](#) (CMK) von KMS verwenden können. AWS

Umschlagverschlüsselung verstehen

Bei der Umschlagverschlüsselung werden Klartextdaten mit einem Datenverschlüsselungsschlüssel (DEK) verschlüsselt, bevor sie an den Datenspeicher (etcd) gesendet werden. Anschließend werden die DEK mit einem KMS-Stammschlüssel verschlüsselt, der in einem zentral verwalteten Remote-KMS-System (KMS) gespeichert ist. AWS Dies ist eine defense-in-depth Strategie, da sie die Daten mit einem Verschlüsselungsschlüssel (DEK) schützt und dann eine weitere Sicherheitsebene hinzufügt, indem dieser DEK mit einem separaten, sicher gespeicherten Verschlüsselungsschlüssel geschützt wird, der als Key Encryption Key (KEK) bezeichnet wird.

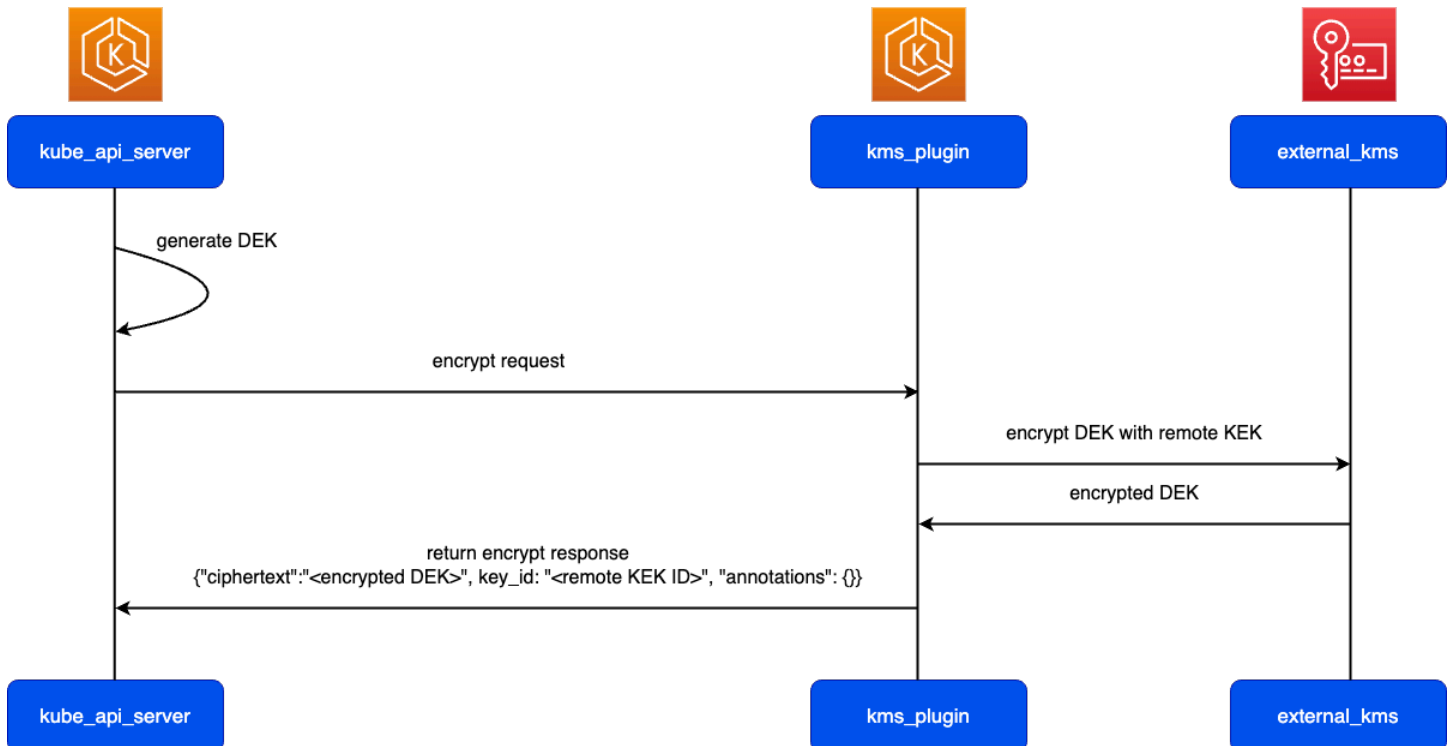
So ermöglicht Amazon EKS die standardmäßige Umschlagverschlüsselung mit KMS v2 und AWS KMS

[Amazon EKS verwendet KMS v2, um die Standard-Envelope-Verschlüsselung für alle API-Daten in der verwalteten Kubernetes-Steuerebene zu implementieren, bevor sie in der etcd-Datenbank gespeichert werden.](#) Beim Start generiert der Cluster-API-Server einen Datenverschlüsselungsschlüssel (DEK) aus einem geheimen Seed in Kombination mit zufällig generierten Daten. Außerdem ruft der API-Server beim Start das KMS-Plug-In auf, um den DEK-Seed mithilfe eines Remote Key Encryption Key (KEK) von AWS KMS zu verschlüsseln. Dies ist ein einmaliger Aufruf, der beim Start des API-Servers und bei der KEK-Rotation ausgeführt wird. Der API-Server speichert dann den verschlüsselten DEK-Seed zwischen. Danach verwendet der API-Server den zwischengespeicherten DEK-Seed, um auf der DEKs Grundlage einer Key Derivation Function (KDF) einen weiteren einmaligen Verwendungszweck zu generieren. Jede dieser generierten Ressourcen DEKs wird dann nur einmal verwendet, um eine einzelne Kubernetes-

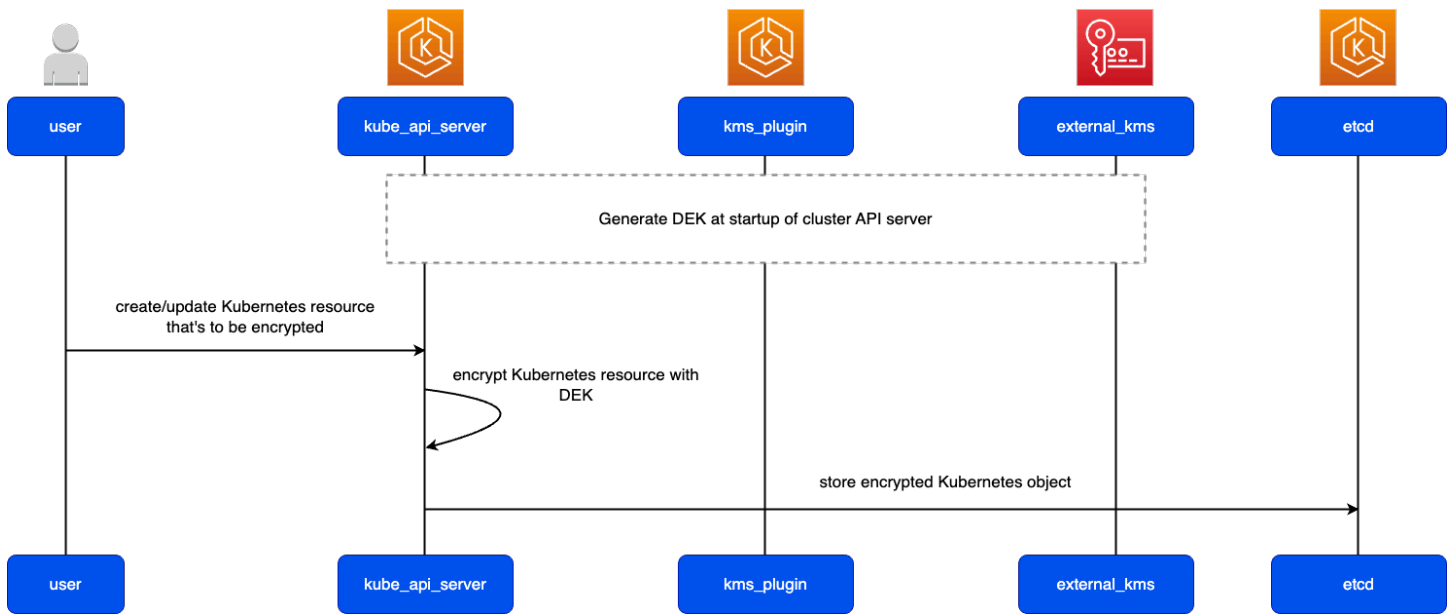
Ressource zu verschlüsseln, bevor sie in etcd gespeichert wird. Durch die Verwendung eines verschlüsselten zwischengespeicherten DEK-Seeds in KMS v2 ist der Prozess der Verschlüsselung von Kubernetes-Ressourcen im API-Server sowohl leistungsfähiger als auch kostengünstiger.

Standardmäßig gehört dieser KEK AWS, aber Sie können optional Ihren eigenen von KMS mitbringen. AWS

Das folgende Diagramm zeigt die Generierung und Verschlüsselung eines DEK beim Start des API-Servers.



Das folgende Diagramm auf hoher Ebene zeigt die Verschlüsselung einer Kubernetes-Ressource, bevor sie in etcd gespeichert wird.



Häufig gestellte Fragen

Wie verbessert die Standard-Envelope-Verschlüsselung den Sicherheitsstatus meines EKS-Clusters?

Diese Funktion reduziert die Oberfläche und den Zeitraum, in dem Metadaten und Kundeneinhalte unverschlüsselt sind. Bei der standardmäßigen Envelope-Verschlüsselung befinden sich Metadaten und Kundeneinhalte immer nur vorübergehend unverschlüsselt im Speicher des Kube-Apiservers, bevor sie in etcd gespeichert werden. [Der Speicher des Kube-Apiservers ist durch das Nitro-System gesichert](#). Amazon EKS verwendet nur [Nitro-basierte EC2 Instances](#) für die verwaltete Kubernetes-Steuerebene. Diese Instances verfügen über Sicherheitskontrollen, die verhindern, dass Systeme oder Personen auf ihren Speicher zugreifen.

Welche Version von Kubernetes muss ich ausführen, um diese Funktion nutzen zu können?

Damit die Standard-Envelope-Verschlüsselung aktiviert werden kann, muss auf Ihrem Amazon EKS-Cluster Kubernetes Version 1.28 oder höher ausgeführt werden.

Sind meine Daten immer noch sicher, wenn ich eine Kubernetes-Cluster-Version verwende, die diese Funktion nicht unterstützt?

Ja. [Sicherheit hat für uns höchste Priorität](#). AWS Wir stützen unsere gesamte digitale Transformation und Innovation auf die höchsten Sicherheitsstandards und setzen uns auch weiterhin dafür ein, diese Messlatte höher zu legen.

Alle in der etcd gespeicherten Daten werden auf Festplattenebene für jeden EKS-Cluster verschlüsselt, unabhängig davon, welche Kubernetes-Version ausgeführt wird. EKS verwendet Root-

Schlüssel, die Volume-Verschlüsselungsschlüssel generieren, die vom EKS-Dienst verwaltet werden. Darüber hinaus wird jeder Amazon EKS-Cluster in einer isolierten VPC mit clusterspezifischen virtuellen Maschinen ausgeführt. Aufgrund dieser Architektur und unserer Praktiken im Bereich der Betriebssicherheit hat Amazon EKS [mehrere Compliance-Bewertungen und Standards](#) erhalten, darunter SOC 1,2,3, PCI-DSS, ISO und HIPAA-Eignung. Diese Einstufungen und Standards werden für alle EKS-Cluster mit oder ohne standardmäßige Envelope-Verschlüsselung beibehalten.

Wie funktioniert die Umschlagverschlüsselung in Amazon EKS?

Beim Start generiert der Cluster-API-Server einen Datenverschlüsselungsschlüssel (DEK) aus einem geheimen Ausgangswert in Kombination mit zufällig generierten Daten. Außerdem ruft der API-Server beim Start das KMS-Plug-In auf, um den DEK mit einem Remote Key Encryption Key (KEK) von AWS KMS zu verschlüsseln. Dies ist ein einmaliger Aufruf, der beim Start des API-Servers und bei der KEK-Rotation ausgeführt wird. Der API-Server speichert dann den verschlüsselten DEK-Seed zwischen. Danach verwendet der API-Server den zwischengespeicherten DEK-Seed, um auf der DEKs Grundlage einer Key Derivation Function (KDF) einen weiteren einmaligen Verwendungszweck zu generieren. Jede dieser generierten Ressourcen DEKs wird dann nur einmal verwendet, um eine einzelne Kubernetes-Ressource zu verschlüsseln, bevor sie in etcd gespeichert wird.

Es ist wichtig zu beachten, dass vom API-Server zusätzliche Aufrufe getätigt werden, um den Zustand und die normale Funktionalität der KMS-Integration zu überprüfen. AWS Diese zusätzlichen Gesundheitschecks sind in Ihrem sichtbar AWS CloudTrail.

Muss ich irgendetwas tun oder irgendwelche Berechtigungen ändern, damit diese Funktion in meinem EKS-Cluster funktioniert?

Nein, Sie müssen keine Maßnahmen ergreifen. Die Envelope-Verschlüsselung in Amazon EKS ist jetzt eine Standardkonfiguration, die in allen Clustern aktiviert ist, auf denen Kubernetes Version 1.28 oder höher ausgeführt wird. Die AWS KMS-Integration wird durch den Kubernetes-API-Server eingerichtet, der von verwaltet wird. AWS Das bedeutet, dass Sie keine Berechtigungen konfigurieren müssen, um mit der Verwendung der KMS-Verschlüsselung für Ihren Cluster zu beginnen.

Woher weiß ich, ob die Standard-Envelope-Verschlüsselung auf meinem Cluster aktiviert ist?

Wenn Sie zur Verwendung Ihres eigenen CMK migrieren, wird Ihnen der ARN des KMS-Schlüssels angezeigt, der Ihrem Cluster zugeordnet ist. Darüber hinaus können Sie die AWS CloudTrail Ereignisprotokolle einsehen, die mit der Verwendung des CMK Ihres Clusters verknüpft sind.

Wenn Ihr Cluster einen AWS eigenen Schlüssel verwendet, wird dies in der EKS-Konsole detailliert beschrieben (mit Ausnahme des ARN des Schlüssels).

Kann ich AWS auf den AWS eigenen Schlüssel zugreifen, der für die Standard-Umschlagverschlüsselung in Amazon EKS verwendet wird?

Nein. AWS verfügt über strenge Sicherheitskontrollen in Amazon EKS, die verhindern, dass Personen auf Klartext-Verschlüsselungsschlüssel zugreifen, die zur Sicherung von Daten in der etcd-Datenbank verwendet werden. Diese Sicherheitsmaßnahmen werden auch auf den AWS eigenen KMS-Schlüssel angewendet.

Ist die Standard-Envelope-Verschlüsselung in meinem vorhandenen EKS-Cluster aktiviert?

Wenn Sie einen Amazon EKS-Cluster mit Kubernetes Version 1.28 oder höher ausführen, ist die Envelope-Verschlüsselung aller Kubernetes-API-Daten aktiviert. Für bestehende Cluster verwendet Amazon EKS den `eks:kms-storage-migrator` RBAC, ClusterRole um Daten, die zuvor nicht in etcd umhüllt waren, in diesen neuen Verschlüsselungsstatus zu migrieren.

Was bedeutet das, wenn ich die Envelope-Verschlüsselung für Secrets in meinem EKS-Cluster bereits aktiviert habe?

Wenn Sie bereits über einen vom Kunden verwalteten Schlüssel (CMK) in KMS verfügen, der zur Envelope-Verschlüsselung Ihrer Kubernetes-Geheimnisse verwendet wurde, wird derselbe Schlüssel als KEK für die Envelope-Verschlüsselung aller Kubernetes-API-Datentypen in Ihrem Cluster verwendet.

Fallen zusätzliche Kosten für den Betrieb eines EKS-Clusters mit standardmäßiger Envelope-Verschlüsselung an?

Für die verwaltete Kubernetes-Steuerebene fallen keine zusätzlichen Kosten an, wenn Sie einen [Amazon Web Services Services-eigenen Schlüssel](#) für die Standard-Envelope-Verschlüsselung verwenden. Standardmäßig verwendet jeder EKS-Cluster, auf dem Kubernetes Version 1.28 oder höher ausgeführt wird, einen [Amazon Web Service-eigenen Schlüssel](#). Wenn Sie jedoch Ihren eigenen AWS KMS-Schlüssel verwenden, gelten die normalen [KMS-Preise](#).

Wie viel kostet es, meinen eigenen AWS KMS-Schlüssel zur Verschlüsselung von Kubernetes-API-Daten in meinem Cluster zu verwenden?

Sie zahlen 1\$ pro Monat, um jeden benutzerdefinierten Schlüssel zu speichern, den Sie erstellen oder in KMS importieren. KMS berechnet Gebühren für Verschlüsselungs- und Entschlüsselungsanfragen. Es gibt ein kostenloses Kontingent von 20.000 Anfragen pro Monat und Konto. Darüber hinaus zahlen Sie 0,03\$ pro 10.000 Anfragen. Dies gilt für die gesamte KMS-Nutzung für ein Konto, sodass die Kosten für die Verwendung Ihres eigenen AWS KMS-Schlüssels in

Ihrem Cluster durch die Verwendung dieses Schlüssels in anderen Clustern oder AWS Ressourcen innerhalb Ihres Kontos beeinflusst werden.

Werden meine KMS-Gebühren jetzt höher sein, da mein vom Kunden verwalteter Schlüssel (CMK) für die Verschlüsselung aller Kubernetes-API-Daten und nicht nur für Secrets verwendet wird?

Nein. Unsere Implementierung mit KMS v2 reduziert die Anzahl der Anrufe an AWS KMS erheblich. Dies wiederum reduziert die mit Ihrem CMK verbundenen Kosten, unabhängig davon, ob die zusätzlichen Kubernetes-Daten in Ihrem EKS-Cluster ver- oder entschlüsselt werden.

Wie oben beschrieben, wird der generierte DEK-Seed, der für die Verschlüsselung von Kubernetes-Ressourcen verwendet wird, lokal im Cache des Kubernetes-API-Servers gespeichert, nachdem er mit dem Remote-KEK verschlüsselt wurde. Wenn sich der verschlüsselte DEK-Seed nicht im Cache des API-Servers befindet, ruft der API-Server AWS KMS auf, um den DEK-Seed zu verschlüsseln. Der API-Server speichert dann den verschlüsselten DEK-Seed für die future Verwendung im Cluster zwischen, ohne KMS aufzurufen. In ähnlicher Weise ruft der API-Server bei Entschlüsselungsanforderungen AWS KMS für die erste Entschlüsselungsanforderung auf. Danach wird der entschlüsselte DEK-Seed zwischengespeichert und für future Entschlüsselungsvorgänge verwendet.

Weitere Informationen finden Sie unter [KEP-3299: KMS v2-Verbesserungen in den Kubernetes-Erweiterungen](#) unter. GitHub

Kann ich denselben CMK-Schlüssel für mehrere Amazon EKS-Cluster verwenden?

Ja. Um einen Schlüssel erneut zu verwenden, können Sie ihn mit einem Cluster in derselben Region verknüpfen, indem Sie den ARN bei der Erstellung dem Cluster zuordnen. Wenn Sie jedoch dasselbe CMK für mehrere EKS-Cluster verwenden, sollten Sie die erforderlichen Maßnahmen ergreifen, um eine willkürliche Deaktivierung des CMK zu verhindern. Andernfalls hat ein deaktiviertes CMK, das mehreren EKS-Clustern zugeordnet ist, je nach Schlüssel größere Auswirkungen auf die Cluster.

Was passiert mit meinem EKS-Cluster, wenn mein CMK nach der Aktivierung der Standard-Envelope-Verschlüsselung nicht mehr verfügbar ist?

Wenn Sie einen KMS-Schlüssel deaktivieren, kann er für keine [kryptografische](#) Operation verwendet werden. Ohne Zugriff auf ein vorhandenes CMK ist der API-Server nicht in der Lage, neu erstellte Kubernetes-Objekte zu verschlüsseln und zu speichern sowie alle zuvor verschlüsselten Kubernetes-Objekte, die in etcd gespeichert sind, zu entschlüsseln. [Wenn der CMK deaktiviert ist, wird der Cluster sofort in einen fehlerhaften/heruntergekommenen Zustand versetzt. Ab diesem Zeitpunkt](#)

können wir unsere Serviceverpflichtung erst erfüllen, wenn Sie den zugehörigen CMK wieder aktivieren.

Wenn ein CMK deaktiviert ist, erhalten Sie Benachrichtigungen über den eingeschränkten Zustand Ihres EKS-Clusters und darüber, dass Sie Ihren CMK innerhalb von 30 Tagen nach der Deaktivierung erneut aktivieren müssen, um eine erfolgreiche Wiederherstellung Ihrer Ressourcen auf der Kubernetes-Steuerebene sicherzustellen.

Wie kann ich meinen EKS-Cluster vor den Auswirkungen eines deaktivierten/gelöschten CMK schützen?

Um Ihre EKS-Cluster vor einem solchen Ereignis zu schützen, sollten Ihre Schlüsseladministratoren den Zugriff auf KMS-Schlüsseloperationen mithilfe von IAM-Richtlinien nach dem Prinzip der geringsten Rechte verwalten, um das Risiko einer willkürlichen Deaktivierung oder Löschung von Schlüsseln im Zusammenhang mit EKS-Clustern zu verringern. Darüber hinaus können Sie einen [CloudWatch Alarm](#) einrichten, um über den Status Ihres CMK informiert zu werden.

Wird mein EKS-Cluster wiederhergestellt, wenn ich den CMK erneut aktiviere?

Um eine erfolgreiche Wiederherstellung Ihres EKS-Clusters sicherzustellen, empfehlen wir dringend, Ihren CMK innerhalb der ersten 30 Tage nach seiner Deaktivierung erneut zu aktivieren. Die erfolgreiche Wiederherstellung Ihres EKS-Clusters hängt jedoch auch davon ab, ob er aufgrund eines automatischen Kubernetes-Upgrades, das möglicherweise stattfindet, während sich der Cluster in einem fehlerhaften/heruntergestuften Zustand befindet, Änderungen erfährt, die die API beeinträchtigen.

Warum wird mein EKS-Cluster nach der Deaktivierung des CMK in einen fehlerhaften/heruntergekommenen Zustand versetzt?

Der API-Server der EKS-Steuerebene verwendet einen DEK-Schlüssel, der verschlüsselt und im Speicher des API-Servers zwischengespeichert wird, um alle Objekte während der Erstellungs- und Aktualisierungsvorgänge zu verschlüsseln, bevor sie in etcd gespeichert werden. Wenn ein vorhandenes Objekt von etcd abgerufen wird, verwendet der API-Server denselben zwischengespeicherten DEK-Schlüssel und entschlüsselt das Kubernetes-Ressourcenobjekt. Wenn Sie das CMK deaktivieren, wird der API-Server aufgrund des zwischengespeicherten DEK-Schlüssels im Speicher des API-Servers keine unmittelbaren Auswirkungen haben. Wenn die API-Serverinstanz jedoch neu gestartet wird, hat sie kein zwischengespeichertes DEK und muss AWS KMS für Verschlüsselungs- und Entschlüsselungsvorgänge aufrufen. Ohne CMK schlägt dieser Prozess mit dem Fehlercode `KMS_KEY_DISABLED` fehl, sodass der API-Server nicht erfolgreich gestartet werden kann.

Was passiert mit meinem EKS-Cluster, wenn ich meinen CMK lösche?

Durch das Löschen des CMK-Schlüssels, der Ihrem EKS-Cluster zugeordnet ist, wird dessen Integrität so stark beeinträchtigt, dass er nicht wiederhergestellt werden kann. Ohne das CMK Ihres Clusters ist der API-Server nicht mehr in der Lage, neue Kubernetes-Objekte zu verschlüsseln und zu speichern sowie alle zuvor verschlüsselten Kubernetes-Objekte, die in der etcd-Datenbank gespeichert sind, zu entschlüsseln. Sie sollten erst dann mit dem Löschen eines CMK-Schlüssels für Ihren EKS-Cluster fortfahren, wenn Sie sicher sind, dass Sie den EKS-Cluster nicht mehr verwenden müssen.

Bitte beachten Sie, dass Ihr Cluster nicht wiederherstellbar ist, wenn das CMK nicht gefunden wird (KMS_KEY_NOT_FOUND) oder die Grants für das CMK, das Ihrem Cluster zugeordnet ist, widerrufen werden (KMS_GRANT_REVOKED). [Weitere Informationen zum Clusterstatus und zu Fehlercodes finden Sie unter Clusterstatus und Fehlercodes mit Lösungspfaden. FAQs](#)

Muss ich trotzdem für einen heruntergekommen/fehlerhaften EKS-Cluster bezahlen, weil ich meinen CMK deaktiviert oder gelöscht habe?

Ja. Die EKS-Kontrollebene ist zwar im Falle eines deaktivierten CMK nicht nutzbar, nutzt aber AWS weiterhin dedizierte Infrastrukturressourcen, die dem EKS-Cluster zugewiesen sind, bis sie vom Kunden gelöscht werden. Darüber hinaus gilt unsere [Serviceverpflichtung](#) in einem solchen Fall nicht, da es sich um eine freiwillige Maßnahme oder Untätigkeit des Kunden handelt, die den normalen Zustand und Betrieb Ihres EKS-Clusters verhindert.

Kann mein EKS-Cluster automatisch aktualisiert werden, wenn er sich aufgrund eines deaktivierten CMK in einem fehlerhaften/heruntergestuften Zustand befindet?

Ja. Wenn Ihr Cluster jedoch über ein deaktiviertes CMK verfügt, haben Sie 30 Tage Zeit, um es wieder zu aktivieren. In diesem Zeitraum von 30 Tagen wird Ihr Kubernetes-Cluster nicht automatisch aktualisiert. Wenn dieser Zeitraum jedoch abgelaufen ist und Sie das CMK nicht erneut aktiviert haben, wird der Cluster automatisch auf die nächste Version (n+1) aktualisiert, die standardmäßig unterstützt wird, und zwar entsprechend dem Lebenszyklus der Kubernetes-Version in EKS.

Wir empfehlen dringend, ein deaktiviertes CMK schnell wieder zu aktivieren, wenn Sie auf einen betroffenen Cluster aufmerksam werden. Es ist wichtig zu beachten, dass EKS diese betroffenen Cluster zwar automatisch aktualisiert, es jedoch keine Garantie dafür gibt, dass sie erfolgreich wiederhergestellt werden, insbesondere wenn der Cluster mehreren automatischen Upgrades unterzogen wird, da dies Änderungen an der Kubernetes-API und unerwartetes Verhalten im Bootstrap-Prozess des API-Servers beinhalten kann.

Kann ich einen KMS-Schlüsselalias verwenden?

Ja. Amazon EKS [unterstützt die Verwendung von KMS-Schlüsselaliasen](#). Ein Alias ist ein benutzerfreundlicher Name für einen [Amazon Web Service KMS-Schlüssel](#). Ein Alias ermöglicht es Ihnen beispielsweise, einen KMS-Schlüssel statt als my-key zu bezeichnen.

1234abcd-12ab-34cd-56ef-1234567890ab

Kann ich meine Cluster-Ressourcen trotzdem mit meiner eigenen Kubernetes-Backup-Lösung sichern und wiederherstellen?

Ja. Sie können eine Kubernetes-Backup-Lösung (wie [Velero](#)) für die Notfallwiederherstellung, Datenmigration und Datenschutz in Kubernetes-Clustern verwenden. Wenn Sie eine Kubernetes-Backup-Lösung ausführen, die über den API-Server auf die Clusterressourcen zugreift, werden alle Daten, die die Anwendung abrufen, entschlüsselt, bevor sie den Client erreichen. Auf diese Weise können Sie die Clusterressourcen in einem anderen Kubernetes-Cluster wiederherstellen.

Sicherheitsüberlegungen für den Amazon EKS Auto Mode

In diesem Thema werden die Sicherheitsarchitektur, Kontrollen und bewährte Methoden für Amazon EKS Auto Mode beschrieben. Da Unternehmen containerisierte Anwendungen in großem Umfang einsetzen, wird die Aufrechterhaltung eines starken Sicherheitsniveaus immer komplexer. Der automatische Modus von EKS implementiert automatisierte Sicherheitskontrollen und lässt sich in AWS Sicherheitsdienste integrieren, um Sie beim Schutz Ihrer Cluster-Infrastruktur, Workloads und Daten zu unterstützen. Durch integrierte Sicherheitsfunktionen wie das erzwungene Knotenlebenszyklusmanagement und die automatisierte Patch-Bereitstellung hilft Ihnen der EKS Auto Mode dabei, bewährte Sicherheitsmethoden aufrechtzuerhalten und gleichzeitig den betrieblichen Aufwand zu reduzieren.

Bevor Sie mit diesem Thema fortfahren, sollten Sie sicherstellen, dass Sie mit den grundlegenden Konzepten des EKS-Automatikmodus vertraut sind und die Voraussetzungen für die Aktivierung des EKS-Automatikmodus auf Ihren Clustern geprüft haben. Allgemeine Informationen zur Sicherheit von Amazon EKS finden Sie unter [Sicherheit](#).

Amazon EKS Auto Mode baut auf den bestehenden Sicherheitsgrundlagen von Amazon EKS auf und führt gleichzeitig zusätzliche automatisierte Sicherheitskontrollen für EC2 verwaltete Instances ein.

API-Sicherheit und Authentifizierung

Amazon EKS Auto Mode verwendet AWS Plattformsicherheitsmechanismen, um Aufrufe der Amazon EKS-API zu sichern und zu authentifizieren.

- Der Zugriff auf die Kubernetes-API wird durch EKS-Zugriffseinträge gesichert, die in IAM-Identitäten AWS integriert sind.
 - Weitere Informationen finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#).
- Kunden können durch die Konfiguration der EKS-Zugriffseinträge eine detaillierte Zugriffskontrolle für den Kubernetes-API-Endpunkt implementieren.

Netzwerksicherheit

Amazon EKS Auto Mode unterstützt mehrere Ebenen der Netzwerksicherheit:

- VPC-Integration
 - Arbeitet in Ihrer Amazon Virtual Private Cloud (VPC)
 - Unterstützt benutzerdefinierte VPC-Konfigurationen und Subnetz-Layouts
 - Ermöglicht private Netzwerke zwischen Clusterkomponenten
 - Weitere Informationen finden Sie unter [Verwaltung der Sicherheitsaufgaben für Amazon Virtual Private Cloud](#)
- Netzwerkrichtlinien
 - Native Unterstützung für Kubernetes-Netzwerkrichtlinien
 - Fähigkeit, detaillierte Regeln für den Netzwerkverkehr zu definieren
 - Weitere Informationen finden Sie unter [the section called “Kubernetes-Richtlinien”](#)

EC2 Sicherheit verwalteter Instanzen

Amazon EKS Auto Mode betreibt EC2 verwaltete Instances mit den folgenden Sicherheitskontrollen:

EC2 Sicherheit

- EC2 verwaltete Instances behalten die Sicherheitsfunktionen von Amazon bei EC2.
- Weitere Informationen zu EC2 verwalteten Instances finden Sie unter [Sicherheit in Amazon EC2](#).

Verwaltung des Instanzlebenszyklus

EC2 verwaltete Instanzen, die von EKS Auto Mode betrieben werden, haben eine maximale Lebensdauer von 21 Tagen. Amazon EKS Auto Mode beendet automatisch Instances,

die diese Lebensdauer überschreiten. Diese Lebenszyklusbegrenzung trägt dazu bei, Konfigurationsabweichungen zu verhindern und den Sicherheitsstatus aufrechtzuerhalten.

Datenschutz

- Amazon EC2 Instance Storage ist verschlüsselt, das ist Speicher, der direkt an die Instance angehängt ist. Weitere Informationen finden Sie unter [Datenschutz bei Amazon EC2](#).
- Der automatische Modus von EKS verwaltet die Volumes, die den EC2 Instances zum Zeitpunkt der Erstellung zugewiesen wurden, einschließlich Stamm- und Datenvolumes. Der automatische Modus von EKS verwaltet EBS-Volumes, die mithilfe der persistenten Speicherfunktionen von Kubernetes erstellt wurden, nicht vollständig.

Patch-Management

- Amazon EKS Auto Mode wendet automatisch Patches auf verwaltete Instances an.
- Zu den Patches gehören:
 - Betriebssystemupdates
 - Sicherheits-Patches
 - Komponenten für den automatischen Modus von Amazon EKS

Note

Die Kunden behalten die Verantwortung für die Sicherung und Aktualisierung der Workloads, die auf diesen Instances ausgeführt werden.

Zugriffskontrollen

- Der direkte Instanzzugriff ist eingeschränkt:
 - SSH-Zugriff ist nicht verfügbar.
 - AWS Der Zugriff auf den Systems Manager Session Manager (SSM) ist nicht verfügbar.
- Verwaltungsvorgänge werden über die Amazon EKS-API und die Kubernetes-API ausgeführt.

Automatisiertes Ressourcenmanagement

Amazon EKS Auto Mode verwaltet Amazon Elastic Block Store (Amazon EBS) -Volumes, die mit persistenten Kubernetes-Speicherfunktionen erstellt wurden, nicht vollständig. Der automatische Modus von EKS verwaltet auch keine Elastic Load Balancers (ELB). Amazon EKS Auto Mode automatisiert Routineaufgaben für diese Ressourcen.

Sicherheit des Speichers

- AWS empfiehlt, die Verschlüsselung für EBS-Volumes zu aktivieren, die über persistente Kubernetes-Speicherfunktionen bereitgestellt werden. Weitere Informationen finden Sie unter [the section called “Erstellen StorageClass”](#).
- Verschlüsselung im Ruhezustand mit KMS AWS
- Sie können Ihr AWS Konto so konfigurieren, dass die Verschlüsselung der neuen EBS-Volumes und Snapshot-Kopien, die Sie erstellen, erzwungen wird. Weitere Informationen finden Sie unter [Amazon EBS-Verschlüsselung standardmäßig aktivieren](#) im Amazon EBS-Benutzerhandbuch.
- Weitere Informationen finden Sie unter [Sicherheit in Amazon EBS](#).

Sicherheit des Load Balancers

- Automatisierte Konfiguration von Elastic Load Balancers
- SSL/TLS-Zertifikatsverwaltung durch Certificate AWS Manager-Integration
- Automatisierung von Sicherheitsgruppen für die Load Balancer-Zugriffskontrolle
- Weitere Informationen finden Sie unter [Sicherheit in Elastic Load Balancing](#).

Bewährte Methoden für die Gewährleistung der Sicherheit

Im folgenden Abschnitt werden bewährte Sicherheitsmethoden für Amazon EKS Auto Mode beschrieben.

- Überprüfen Sie regelmäßig die AWS IAM-Richtlinien und EKS-Zugriffseinträge.
- Implementieren Sie Zugriffsmuster mit den geringsten Rechten für Workloads.
- Überwachen Sie die Cluster-Aktivität über AWS CloudTrail und Amazon CloudWatch. Weitere Informationen erhalten Sie unter [the section called “ AWS CloudTrail”](#) und [the section called “Amazon CloudWatch”](#).

- Verwenden Sie AWS Security Hub für die Bewertung der Sicherheitslage.
- Implementieren Sie Pod-Sicherheitsstandards, die für Ihre Workloads geeignet sind.

Identitäts- und Zugriffsverwaltung für Amazon EKS

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert (mit Berechtigungen ausgestattet) werden kann, um Amazon-EKS-Ressourcen zu nutzen. IAM ist ein AWS Dienst, den Sie ohne zusätzliche Kosten nutzen können.

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt davon ab, welche Arbeit Sie in Amazon EKS ausführen.

Service-Benutzer – Wenn Sie den Amazon-EKS-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Je mehr Amazon-EKS-Funktionen Sie für Ihre Arbeit nutzen, desto mehr Berechtigungen benötigen Sie möglicherweise. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter [the section called “Fehlerbehebung”](#) finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in Amazon EKS haben.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon EKS-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon EKS. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon EKS Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Amazon EKS verwenden kann, finden Sie unter [the section called “Amazon EKS und IAM”](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon EKS zu verwalten. Beispiele für identitätsbasierte Amazon-EKS-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [the section called “Identitätsbasierte Richtlinien”](#).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als Root-Benutzer des AWS Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (angemeldet AWS) sein.

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über einen Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie unter [So melden Sie sich bei Ihrem AWS Konto an](#) im AWS Anmelde-Benutzerhandbuch. AWS

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Factor Authentication](#) im AWS IAM Identity Center User Guide und Using [Multi-Factor Authentication \(MFA\) AWS im](#) IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie ein AWS Konto erstellen, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto hat. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für alltägliche Aufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für

die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres AWS Kontos, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI- oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert,

so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center-Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen AWS Diensten können Sie jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS Dienste verwenden Funktionen in anderen AWS Diensten. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Service kann dies mithilfe der Berechtigungen des aufrufenden Prinzipals, einer Servicerolle oder einer serviceverknüpften Rolle tun.
- Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS Dienst aufruft, in Kombination mit dem anfordernden AWS Dienst, um Anfragen an nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS Diensten oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst](#).

- **Dienstverknüpfte Rolle** — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einem Dienst verknüpft ist. AWS Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen werden in Ihrem AWS Konto angezeigt und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon ausgeführte Anwendungen EC2** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS CLI- oder AWS API-Anfragen stellen. Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch [unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden](#).

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen

auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console, der AWS CLI oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS Konto zuordnen können. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS Dienste gehören.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten. ACLs Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen stellen die Schnittmenge zwischen den identitätsbasierten Richtlinien einer Entität und ihren Berechtigungsgrenzen dar. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Dienststeuerungsrichtlinien (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in AWS Organizations festlegen. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer AWS Konten, die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen AWS Root-Benutzer. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations User Guide.
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind die Schnittmenge der identitätsbasierten Richtlinien des Benutzers oder der Rolle und der Sitzungsrichtlinien.

Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Funktionsweise von Amazon EKS mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon EKS zu verwalten, sollten Sie verstehen, welche IAM-Funktionen für die Verwendung mit Amazon EKS verfügbar sind. Einen allgemeinen Überblick darüber, wie Amazon EKS und andere AWS Services mit IAM zusammenarbeiten, finden Sie im [IAM-Benutzerhandbuch unter AWS Services, die mit IAM funktionieren](#).

Themen

- [Identitätsbasierte Amazon-EKS-Richtlinien](#)
- [Ressourcenbasierte Amazon-EKS-Richtlinien](#)
- [Autorisierung auf der Basis von Amazon-EKS-Tags](#)
- [Amazon EKS IAM-Rollen](#)

Identitätsbasierte Amazon-EKS-Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Amazon EKS unterstützt bestimmte Aktionen, Ressourcen und Zustandsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Amazon EKS verwenden das folgende Präfix vor der Aktion: `eks:`. Um jemandem beispielsweise die Berechtigung zum Abrufen von Informationen zu einem Amazon-EKS-Cluster zu erteilen, fügen Sie die Aktion `DescribeCluster` in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": ["eks:action1", "eks:action2"]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "eks:Describe*"
```

Eine Liste der Amazon-EKS-Aktionen finden Sie unter [Von Amazon Elastic Kubernetes Service definierte Aktionen](#) in der Serviceautorisierungsreferenz.

Ressourcen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie bei Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, wie z. B. das Auflisten von Vorgängen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Die Amazon-EKS-Cluster-Ressource verfügt über den folgenden ARN:

```
arn:aws:eks:region-code:account-id:cluster/cluster-name
```

Weitere Informationen zum Format von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\) und AWS Service-Namespaces](#).

Um beispielsweise den Cluster mit dem Namen *my-cluster* in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN:

```
"Resource": "arn:aws:eks:region-code:111122223333:cluster/my-cluster"
```

Um alle Cluster anzugeben, die zu einem bestimmten Konto und einer bestimmten AWS Region gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:eks:region-code:111122223333:cluster/*"
```

Einige Amazon EKS-Aktionen, z. B. zum Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Eine Liste der Amazon EKS-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter [Von Amazon Elastic Kubernetes Service definierte Ressourcen in der Service Authorization Reference](#). Um zu erfahren, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, lesen Sie von [Amazon Elastic Kubernetes Service definierte Aktionen](#).

Bedingungsschlüssel

Amazon EKS definiert seinen eigenen Satz von Konditionsschlüsseln und unterstützt auch die Verwendung einiger globaler Konditionsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [AWS Global Condition Context Keys](#) im IAM-Benutzerhandbuch.

Sie können Bedingungsschlüssel festlegen, wenn Sie Ihrem Cluster einen OpenID Connect-Anbieter zuordnen. Weitere Informationen finden Sie unter [the section called “Beispiel für eine IAM-Richtlinie”](#).

Alle EC2 Amazon-Aktionen unterstützen die Tasten `aws:RequestedRegion` und `ec2:Region` Condition. Weitere Informationen finden Sie unter [Beispiel: Beschränkung des Zugriffs auf eine bestimmte AWS Region](#).

Eine Liste der Amazon EKS-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für Amazon Elastic Kubernetes Service](#) in der Service-Autorisierungsreferenz. Um zu erfahren, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, lesen Sie von [Amazon Elastic Kubernetes Service definierte Aktionen](#).

Beispiele

Beispiele für identitätsbasierte Amazon-EKS-Richtlinien finden Sie unter [the section called “Identitätsbasierte Richtlinien”](#).

Wenn Sie einen Amazon EKS-Cluster erstellen, erhält der [IAM-Principal](#), der den Cluster erstellt, automatisch `system:masters` Berechtigungen für die rollenbasierte Zugriffskontrolle (RBAC) des Clusters in der Amazon EKS-Kontrollebene. Dieser Prinzipal wird in keiner sichtbaren Konfiguration angezeigt. Vergewissern Sie sich daher, dass Sie stets im Auge behalten, welcher Prinzipal den Cluster ursprünglich erstellt hat. Um weiteren IAM-Prinzipalen die Möglichkeit zu geben, mit Ihrem Cluster zu interagieren, bearbeiten Sie die `aws-auth` ConfigMap in Kubernetes und erstellen Sie ein Kubernetes `rolebinding` oder `clusterrolebinding` mit dem Namen einer Gruppe, den Sie in der angeben. `aws-auth` ConfigMap

Weitere Informationen zur Arbeit mit dem finden Sie unter. ConfigMap [the section called “Kubernetes-API-Zugriff”](#)

Ressourcenbasierte Amazon-EKS-Richtlinien

Amazon EKS unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Basis von Amazon-EKS-Tags

Sie können Tags an Amazon-EKS-Ressourcen anhängen oder Tags in einer Anforderung an Amazon EKS übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name` , `aws:RequestTag/key-name` , oder `aws:TagKeys` Bedingung verwenden. Weitere Informationen über die Markierung von Amazon-EKS-Ressourcen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#). Weitere Informationen darüber, mit welchen Aktionen Sie Tags in Bedingungsschlüsseln verwenden können, finden Sie unter [Von Amazon EKS definierte Aktionen](#) in der [Service-Authorization-Referenz](#).

Amazon EKS IAM-Rollen

Eine [IAM-Rolle](#) ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit Amazon EKS

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS-API-Operationen wie [AssumeRole](#) oder [GetFederationToken](#) aufrufen.

Amazon EKS unterstützt die Verwendung temporärer Anmeldeinformationen.

Serviceverknüpfte Rollen

[Mit Diensten verknüpfte Rollen](#) ermöglichen es AWS Diensten, auf Ressourcen in anderen Diensten zuzugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein Administrator kann die Berechtigungen für dienstbezogene Rollen einsehen, aber nicht bearbeiten.

Amazon EKS unterstützt Service-verknüpfte Rollen. Details zum Erstellen oder Verwalten von serviceverknüpften Amazon-EKS-Rollen finden Sie unter [the section called “Service-verknüpfte Rollen”](#).

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer [Servicerolle](#) in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto.

Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Services beeinträchtigen.

Amazon EKS unterstützt Servicerollen. Weitere Informationen erhalten Sie unter [the section called “Cluster-IAM-Rolle”](#) und [the section called “Knoten-IAM-Rolle”](#).

Auswählen einer IAM-Rolle in Amazon EKS

Wenn Sie eine Cluster-Ressource in Amazon EKS erstellen, müssen Sie eine Rolle auswählen, damit Amazon EKS in Ihrem Namen auf mehrere andere AWS Ressourcen zugreifen kann. Wenn Sie zuvor eine Servicerolle erstellt haben, stellt Ihnen Amazon EKS eine Liste der Rollen bereit, aus denen Sie auswählen können. Es ist wichtig, eine Rolle auszuwählen, der die von Amazon EKS verwalteten Richtlinien zugeordnet sind. Weitere Informationen erhalten Sie unter [the section called “Überprüfen, ob eine Clusterrolle vorhanden ist”](#) und [the section called “Nach einer vorhandenen Knotenrolle suchen”](#).

Beispiele für identitätsbasierte Amazon-EKS-Richtlinien

Standardmäßig sind IAM-Benutzer und -Rollen nicht berechtigt, Amazon EKS-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console, AWS CLI oder der AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von Richtlinien auf der JSON-Registerkarte](#) im IAM-Benutzerhandbuch.

Wenn Sie einen Amazon EKS-Cluster erstellen, erhält der [IAM-Principal](#), der den Cluster erstellt, automatisch `system:masters` Berechtigungen für die rollenbasierte Zugriffskontrolle (RBAC) des Clusters in der Amazon EKS-Kontrollebene. Dieser Principal erscheint in keiner sichtbaren Konfiguration. Vergewissern Sie sich daher, dass Sie stets im Auge behalten, welcher Prinzipal den Cluster ursprünglich erstellt hat. Um weiteren IAM-Prinzipalen die Möglichkeit zu geben, mit Ihrem Cluster zu interagieren, bearbeiten Sie die `aws-auth ConfigMap` in Kubernetes und erstellen Sie ein Kubernetes `rolebinding` oder `clusterrolebinding` mit dem Namen `easgroup`, den Sie in der angeben. `aws-auth ConfigMap`

Weitere Informationen zur Arbeit mit dem finden Sie unter. `ConfigMap` [the section called “Kubernetes-API-Zugriff”](#)

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Amazon-EKS-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für IAM-Benutzer](#)
- [Erstellen Sie einen Kubernetes-Cluster in der Cloud AWS](#)
- [Erstellen Sie einen lokalen Kubernetes-Cluster auf einem Outpost](#)
- [Aktualisieren eines Kubernetes-Clusters](#)
- [Auflisten oder Beschreiben aller Cluster](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien können festlegen, ob jemand Amazon-EKS-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder daraus löschen kann. Diese Aktionen können zu Kosten für Ihr AWS Konto führen. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem Konto verfügbar. AWS Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch

Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten AWS Dienst verwendet werden, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem AWS Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Amazon-EKS-Konsole

Um auf die Amazon EKS-Konsole zugreifen zu können, muss ein [IAM-Prinzipal](#) über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen ermöglichen es dem Principal, Details zu den Amazon EKS-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Prinzipale, denen diese Richtlinie zugewiesen ist, nicht wie vorgesehen.

Um sicherzustellen, dass Ihre IAM-Prinzipale die Amazon EKS-Konsole weiterhin verwenden können, erstellen Sie eine Richtlinie mit Ihrem eigenen eindeutigen Namen, z. B. AmazonEKSAAdminPolicy. Hängen Sie die Richtlinie an die Prinzipale an. Informationen finden Sie im Abschnitt [Hinzufügen und Entfernen von IAM-Identitätsberechtigungen](#) im IAM-Benutzerhandbuch.

Important

Mit der folgenden Beispielrichtlinie kann ein Prinzipal Informationen auf der Registerkarte Konfiguration in der Konsole anzeigen. Um Informationen auf den Registerkarten „Übersicht“

und „Ressourcen“ im anzeigen zu können AWS Management Console, benötigt der Principal außerdem Kubernetes-Berechtigungen. Weitere Informationen finden Sie unter [the section called “Erforderliche Berechtigungen”](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Sie müssen keine Mindestkonsolenberechtigungen für Principals gewähren, die nur die AWS CLI oder die AWS API aufrufen. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API-Vorgang entsprechen, den Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für IAM-Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ViewOwnUserInfo",
    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsForUser",
      "iam:ListAttachedUserPolicies",
      "iam:ListUserPolicies",
      "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
  },
  {
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

Erstellen Sie einen Kubernetes-Cluster in der Cloud AWS

Diese Beispielrichtlinie umfasst die Mindestberechtigungen, die erforderlich sind, um einen Amazon EKS-Cluster mit *my-cluster* dem Namen *us-west-2* AWS Region zu erstellen. Sie können die AWS Region durch die AWS Region ersetzen, in der Sie einen Cluster erstellen möchten. Wenn Sie eine Warnung sehen, die besagt, dass die Aktionen in Ihrer Richtlinie keine Berechtigungen auf Ressourcenebene unterstützen und Sie sich für die entscheiden **All resources** müssen AWS Management Console, können Sie diese problemlos ignorieren. Wenn Ihr Konto bereits über die *AWSServiceRoleForAmazonEKS*-Rolle verfügt, können Sie die `iam:CreateServiceLinkedRole`-Aktion aus der Richtlinie entfernen. Wenn Sie jemals einen

Amazon EKS-Cluster in Ihrem Konto erstellt haben, ist diese Rolle bereits vorhanden, sofern Sie sie nicht gelöscht haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "eks:CreateCluster",
      "Resource": "arn:aws: eks:us-west-2:111122223333:cluster/my-cluster"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws: iam::111122223333:role/aws-service-role/
eks.amazonaws.com/AWSServiceRoleForAmazonEKS",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "iam:AWSServiceName": "eks"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws: iam::111122223333:role/cluster-role-name"
    }
  ]
}
```

Erstellen Sie einen lokalen Kubernetes-Cluster auf einem Outpost

Diese Beispielrichtlinie umfasst die Mindestberechtigungen, die erforderlich sind, um einen lokalen Amazon EKS-Cluster mit *my-cluster* dem Namen eines Außenpostens in der *us-west-2* AWS Region zu erstellen. Sie können die AWS Region durch die AWS Region ersetzen, in der Sie einen Cluster erstellen möchten. Wenn Sie eine Warnung sehen, die besagt, dass die Aktionen in Ihrer Richtlinie keine Berechtigungen auf Ressourcenebene unterstützen und Sie sich für die entscheiden **All resources** müssen AWS Management Console, können Sie diese problemlos ignorieren. Wenn Ihr Konto bereits über die `AWSServiceRoleForAmazonEKSLocalOutpost`-Rolle verfügt, können Sie die `iam:CreateServiceLinkedRole`-Aktion aus der Richtlinie entfernen. Wenn Sie

jemals einen lokalen Amazon EKS-Cluster auf einem Outpost in Ihrem Konto erstellt haben, ist diese Rolle bereits vorhanden, sofern Sie sie nicht gelöscht haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "eks:CreateCluster",
      "Resource": "arn:aws: eks:us-west-2:111122223333:cluster/my-cluster"
    },
    {
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:GetRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws: iam::111122223333:role/aws-service-role/outposts.eks-
local.amazonaws.com/AWSServiceRoleForAmazonEKSLocalOutpost"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": "arn:aws: iam::111122223333:role/cluster-role-name"
    },
    {
      "Action": [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:GetInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
    }
  ]
}
```



```
        "Resource": "arn:aws: iam::*:instance-profile/eks-local-*",
        "Effect": "Allow"
    },
]
}
```

Aktualisieren eines Kubernetes-Clusters

Diese Beispielrichtlinie umfasst die Mindestberechtigungen, die zum Aktualisieren eines Clusters mit dem Namen der *my-cluster* Region us-west-2 AWS erforderlich sind.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "eks:UpdateClusterVersion",
      "Resource": "arn:aws: eks:us-west-2:111122223333:cluster/my-cluster"
    }
  ]
}
```

Auflisten oder Beschreiben aller Cluster

Diese Beispielrichtlinie enthält die benötigten Mindestberechtigungen zum Auflisten und Beschreiben aller Cluster in Ihrem Konto. Ein [IAM-Prinzipal](#) muss in der Lage sein, Cluster aufzulisten und zu beschreiben, um den `update-kubeconfig` AWS CLI-Befehl verwenden zu können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks:DescribeCluster",
        "eks:ListClusters"
      ],
      "Resource": "*"
    }
  ]
}
```

Verwendung von serviceverknüpften Rollen für Amazon EKS

[Amazon Elastic Kubernetes Service verwendet dienstbezogene Rollen für AWS Identity and Access Management \(IAM\)](#). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Themen

- [Verwenden von Rollen für Amazon-EKS-Cluster](#)
- [Verwenden von Rollen für Amazon-EKS-Knotengruppen](#)
- [Verwenden von Rollen für Amazon-EKS-Fargate-Profile](#)
- [Verbinden eines Kubernetes-Clusters mithilfe von Rollen mit Amazon EKS](#)
- [Verwenden von Rollen für lokale Amazon-EKS-Cluster in Outpost](#)
- [Rollen für das Amazon EKS-Dashboard verwenden](#)

Verwenden von Rollen für Amazon-EKS-Cluster

[Amazon Elastic Kubernetes Service verwendet dienstbezogene Rollen für AWS Identity and Access Management \(IAM\)](#). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EKS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EKS definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur Amazon EKS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte

Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Serviceverknüpfte Rollenberechtigungen für Amazon EKS

Amazon EKS verwendet die mit dem Service verknüpfte Rolle namens `AWSServiceRoleForAmazonEKS`. Die Rolle ermöglicht Amazon EKS, Cluster in Ihrem Konto zu verwalten. Die beigefügten Richtlinien ermöglichen es der Rolle, die folgenden Ressourcen zu verwalten: Netzwerkschnittstellen, Sicherheitsgruppen, Protokolle und VPCs.

Note

Die serviceverknüpfte `AWSServiceRoleForAmazonEKS`-Rolle unterscheidet sich von der Rolle, die für die Clustererstellung erforderlich ist. Weitere Informationen finden Sie unter [the section called “Cluster-IAM-Rolle”](#).

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEKS` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `eks.amazonaws.com`

Die Richtlinie für Rollenberechtigungen erlaubt Amazon EKS, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- [AmazonEKSServiceRolePolicy](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon EKS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen Cluster in der AWS Management Console, der AWS CLI oder der AWS API erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Cluster anlegen, legt Amazon EKS die servicegebundene Rolle wieder für Sie an.

Bearbeiten einer serviceverknüpften Rolle für Amazon EKS

Amazon EKS verhindert die Bearbeitung der serviceverknüpften Rolle `AWSServiceRoleForAmazonEKS`. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer servicegebundenen Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EKS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

Note

Wenn der Amazon-EKS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus.
3. Wenn Ihr Cluster über Knotengruppen oder Fargate-Profilen verfügt, müssen Sie diese löschen, bevor Sie den Cluster löschen können. Weitere Informationen erhalten Sie unter [the section called "Löschen"](#) und [the section called "Profile löschen"](#).
4. Wählen Sie auf der Seite Cluster den Cluster aus, den Sie löschen möchten, und wählen Sie Löschen.

5. Geben Sie den Namen des Clusters im Bestätigungsfenster zum Löschen ein, und wählen Sie dann Bestätigen.
6. Wiederholen Sie diesen Vorgang für alle anderen Cluster in Ihrem Konto. Warten Sie, bis alle Löschoperationen abgeschlossen sind.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die `AWSServiceRoleForAmazonEKS` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für Amazon EKS serviceverknüpfte Rollen

Amazon EKS unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [Amazon-EKS-Endpunkte und -Kontingente](#).

Verwenden von Rollen für Amazon-EKS-Knotengruppen

Amazon EKS verwendet [dienstbezogene](#) Rollen für AWS Identity and Access Management (IAM). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EKS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EKS definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur Amazon EKS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Serviceverknüpfte Rollenberechtigungen für Amazon EKS

Amazon EKS verwendet die mit dem Service verknüpfte Rolle mit dem Namen `AWSServiceRoleForAmazonEKSNodegroup`. Die Rolle ermöglicht Amazon EKS, Knotengruppen in Ihrem Konto zu verwalten. Die beigefügte `AWSServiceRoleForAmazonEKSNodegroup` Richtlinie ermöglicht es der Rolle, die folgenden Ressourcen zu verwalten: Auto Scaling Scaling-Gruppen, Sicherheitsgruppen, Startvorlagen und IAM-Instanzprofile. Weitere Informationen finden Sie unter [the section called “AWS verwaltete Richtlinie: AWSService RoleForAmazon EKSNodegroup”](#).

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEKSNodegroup` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `eks-nodegroup.amazonaws.com`

Die Richtlinie für Rollenberechtigungen erlaubt Amazon EKS, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- [AWSServiceRoleForAmazonEKSNodegroup](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon EKS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie sich `CreateNodegroup` in der AWS Management Console, der AWS CLI oder der AWS API befinden, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Wenn Sie den Amazon EKS-Service vor dem 1. Januar 2017 genutzt haben, als er begann, serviceverknüpfte Rollen zu unterstützen, hat Amazon EKS die `AWSService RoleForAmazon EKSNodegroup` Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter [In meinem IAM-Konto wird eine neue Rolle angezeigt](#).

Eine serviceverknüpfte Rolle in Amazon EKS (AWS API) erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine verwaltete Knotengruppe in der AWS Management Console, der AWS CLI oder der AWS API erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine andere verwaltete Knotengruppe erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon EKS

Amazon EKS verhindert die Bearbeitung der serviceverknüpften Rolle `AWSServiceRoleForAmazonEKSCluster`. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer servicegebundenen Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EKS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

Note

Wenn der Amazon-EKS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus.

3. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
4. Wählen Sie im Abschnitt Node groups (Knotengruppen) die zu löschende Knotengruppe aus.
5. Geben Sie den Namen der Knotengruppe im Bestätigungsfenster zum Löschen ein und wählen Sie dann Bestätigen.
6. Wiederholen Sie diesen Vorgang für alle anderen Knotengruppen im Cluster. Warten Sie, bis alle Löschoperationen abgeschlossen sind.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die `AWSServiceRoleForAmazonEKSNodegroup` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für Amazon EKS serviceverknüpfte Rollen

Amazon EKS unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [Amazon-EKS-Endpunkte und -Kontingente](#).

Verwenden von Rollen für Amazon-EKS-Fargate-Profile

Amazon EKS verwendet [dienstbezogene](#) Rollen für AWS Identity and Access Management (IAM). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EKS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EKS definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur Amazon EKS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte

Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Serviceverknüpfte Rollenberechtigungen für Amazon EKS

Amazon EKS verwendet die mit dem Service verknüpfte Rolle mit dem Namen `AWSServiceRoleForAmazonEKSFargate`. Die Rolle ermöglicht Amazon EKS Fargate, das für Fargate Pods erforderliche VPC-Netzwerk zu konfigurieren. Die angehängten Richtlinien ermöglichen es der Rolle, Elastic Network Interfaces zu erstellen und zu löschen und Elastic Network Interfaces und Ressourcen zu beschreiben.

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEKSFargate` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `eks-fargate.amazonaws.com`

Die Richtlinie für Rollenberechtigungen erlaubt Amazon EKS, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- [AmazonEKSFargateServiceRolePolicy](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon EKS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Fargate-Profil in der AWS Management Console, der AWS CLI oder der AWS API erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Wenn Sie den Amazon EKS-Service vor dem 13. Dezember 2019 genutzt haben, als er begann, serviceverknüpfte Rollen zu unterstützen, hat Amazon EKS die `AWSServiceRoleForAmazonEKSFargate`-Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem IAM-Konto erschienen](#).

Eine serviceverknüpfte Rolle in Amazon EKS (AWS API) erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Fargate-Profil in der AWS Management Console, der AWS CLI oder der AWS API erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine andere verwaltete Knotengruppe erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon EKS

Amazon EKS verhindert die Bearbeitung der serviceverknüpften Rolle

`AWSServiceRoleForAmazonEKSForFargate`. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer servicegebundenen Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EKS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

Note

Wenn der Amazon-EKS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster aus.

3. Wählen Sie auf der Seite Cluster (Cluster) den Cluster aus.
4. Wählen Sie die Registerkarte Compute (Datenverarbeitung) aus.
5. Wenn im Abschnitt Fargate profiles (Fargate-Profil) Fargate-Profil vorhanden sind, wählen Sie jedes einzeln aus und wählen Sie dann Delete (Löschen).
6. Geben Sie den Namen des Profils im Bestätigungsfenster zum Löschen ein, und wählen Sie dann Bestätigen.
7. Wiederholen Sie diesen Vorgang für alle anderen Fargate-Profil im Cluster und für alle anderen Cluster in Ihrem Konto.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die dienstverknüpfte AWSService RoleForAmazon EKSFor Fargate-Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für Amazon EKS serviceverknüpfte Rollen

Amazon EKS unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [Amazon-EKS-Endpunkte und -Kontingente](#).

Verbinden eines Kubernetes-Clusters mithilfe von Rollen mit Amazon EKS

Amazon EKS verwendet [dienstbezogene](#) Rollen für AWS Identity and Access Management (IAM). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EKS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EKS definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur Amazon EKS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Serviceverknüpfte Rollenberechtigungen für Amazon EKS

Amazon EKS verwendet die mit dem Service verknüpfte Rolle namens `AWSServiceRoleForAmazonEKSCollector`. Die Rolle ermöglicht Amazon EKS, Kubernetes-Cluster zu verbinden. Die beigefügten Richtlinien ermöglichen es der Rolle, die für die Verbindung mit Ihrem registrierten Kubernetes-Cluster erforderlichen Ressourcen zu verwalten.

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEKSCollector` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `eks-collector.amazonaws.com`

Die Richtlinie für Rollenberechtigungen erlaubt Amazon EKS, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- [AmazonEKSCollectorServiceRolePolicy](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon EKS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen, um einen Cluster zu verbinden. Wenn Sie einen Cluster in der AWS Management Console, der AWS CLI oder der AWS API verbinden `eksctl`, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Cluster verbinden, legt Amazon EKS die servicegebundene Rolle wieder für Sie an.

Bearbeiten einer serviceverknüpften Rolle für Amazon EKS

Amazon EKS verhindert die Bearbeitung der serviceverknüpften Rolle `AWSServiceRoleForAmazonEKSCollector`. Da möglicherweise verschiedene Entitäten auf die

Rolle verweisen, kann der Rollename nach dem Erstellen einer servicegebundenen Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EKS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

Note

Wenn der Amazon-EKS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Cluster aus.
3. Wählen Sie auf der Seite Cluster (Cluster) den Cluster aus.
4. Wählen Sie die Registerkarte Abmelden und dann die Registerkarte OK.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die AWSService RoleForAmazon EKSCconnector serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Verwenden von Rollen für lokale Amazon-EKS-Cluster in Outpost

[Amazon Elastic Kubernetes Service verwendet dienstbezogene Rollen für AWS Identity and Access Management \(IAM\)](#). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt

mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EKS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EKS definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur Amazon EKS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Serviceverknüpfte Rollenberechtigungen für Amazon EKS

Amazon EKS verwendet die mit dem Service verknüpfte Rolle namens `AWSServiceRoleForAmazonEKSLocalOutpost`. Die Rolle ermöglicht Amazon EKS, lokale Cluster in Ihrem Konto zu verwalten. Die beigefügten Richtlinien ermöglichen es der Rolle, die folgenden Ressourcen zu verwalten: Netzwerkschnittstellen, Sicherheitsgruppen, Protokolle und EC2 Amazon-Instances.

Note

Die serviceverknüpfte `AWSServiceRoleForAmazonEKSLocalOutpost`-Rolle unterscheidet sich von der Rolle, die für die Clustererstellung erforderlich ist. Weitere Informationen finden Sie unter [the section called "Cluster-IAM-Rolle"](#).

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEKSLocalOutpost` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `outposts.eks-local.amazonaws.com`

Die Richtlinie für Rollenberechtigungen erlaubt Amazon EKS, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- [AmazonEKSServiceRolePolicy](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon EKS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen Cluster in der AWS Management Console, der AWS CLI oder der AWS API erstellen, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Cluster anlegen, legt Amazon EKS die servicegebundene Rolle wieder für Sie an.

Bearbeiten einer serviceverknüpften Rolle für Amazon EKS

Amazon EKS verhindert die Bearbeitung der serviceverknüpften Rolle

`AWSServiceRoleForAmazonEKSLocalOutpost`. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht ändern, da verschiedene Entitäten möglicherweise auf die Rolle verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EKS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

 Note

Wenn der Amazon-EKS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Clusters (Cluster) für Amazon EKS aus.
3. Wenn Ihr Cluster über Knotengruppen oder Fargate-Profilen verfügt, müssen Sie diese löschen, bevor Sie den Cluster löschen können. Weitere Informationen erhalten Sie unter [the section called “Löschen”](#) und [the section called “Profile löschen”](#).
4. Wählen Sie auf der Seite Cluster den Cluster aus, den Sie löschen möchten, und wählen Sie Löschen.
5. Geben Sie den Namen des Clusters im Bestätigungsfenster zum Löschen ein, und wählen Sie dann Bestätigen.
6. Wiederholen Sie diesen Vorgang für alle anderen Cluster in Ihrem Konto. Warten Sie, bis alle Löschoperationen abgeschlossen sind.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die `AWSServiceRoleForAmazonEKSLocalOutpost` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für Amazon EKS serviceverknüpfte Rollen

Amazon EKS unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [Amazon-EKS-Endpunkte und -Kontingente](#).

Rollen für das Amazon EKS-Dashboard verwenden

Das Amazon EKS-Dashboard verwendet diese serviceverknüpfte Rolle, um Informationen über Cluster-Ressourcen aus mehreren Regionen und Konten zu aggregieren. Das Dashboard ist in AWS Organizations integriert, um Informationen über mehrere Konten in Ihrer Organisation sicher zu lesen.

Weitere Informationen zum Amazon EKS-Dashboard finden Sie unter [the section called “Amazon EKS-Übersicht”](#).

Hintergrund

Amazon EKS verwendet [dienstbezogene](#) Rollen für AWS Identity and Access Management (IAM). Eine servicegebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EKS verknüpft ist. Servicebezogene Rollen sind von Amazon EKS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EKS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EKS definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur Amazon EKS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EKS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Serviceverknüpfte Rollenberechtigungen für Amazon EKS

Amazon EKS verwendet die mit dem Service verknüpfte Rolle mit dem Namen `AWSServiceRoleForAmazonEKSDashboard`. Die Rolle ermöglicht Amazon EKS, das EKS-Dashboard zu generieren und anzuzeigen, einschließlich aggregierter Informationen zu Cluster-Ressourcen. Die beigefügte `AmazonEKSDashboardServiceRolePolicy` Richtlinie ermöglicht es der Rolle, die folgenden Ressourcen zu verwalten: Auto Scaling Scaling-Gruppen, Sicherheitsgruppen, Startvorlagen und IAM-Instanzprofile. Weitere Informationen finden Sie unter [the section called “AWS verwaltete Richtlinie: Amazon EKSDashboard ServiceRolePolicy”](#).

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEKSDashboard` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `dashboard.eks.amazonaws.com`

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSDashboard ServiceRolePolicy](#) im AWS Managed Policy Reference Guide.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon EKS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie das Dashboard in der AWS Konsole aktivieren, erstellt Amazon EKS die serviceverknüpfte Rolle für Sie.

Weitere Informationen zur Aktivierung des EKS-Dashboards finden Sie unter [the section called “Organisationen konfigurieren”](#).

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet.

Bearbeiten einer serviceverknüpften Rolle für Amazon EKS

Amazon EKS verhindert die Bearbeitung der serviceverknüpften Rolle `AWSServiceRoleForAmazonEKSDashboard`. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer servicegebundenen Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EKS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

 Note

Wenn der Amazon-EKS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Weitere Informationen zur Deaktivierung des EKS-Dashboards finden Sie unter [the section called “Organisationen konfigurieren”](#).

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die `AWSServiceRoleForAmazonEKSDashboard` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für Amazon EKS serviceverknüpfte Rollen

Amazon EKS unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [Amazon-EKS-Endpunkte und -Kontingente](#).

IAM-Rolle für die Ausführung von Amazon EKS Pod

Die Amazon EKS Pod-Ausführungsrolle ist erforderlich, um Pods auf der AWS Fargate-Infrastruktur auszuführen.

Wenn Ihr Cluster Pods auf der AWS Fargate-Infrastruktur erstellt, müssen die Komponenten, die auf der Fargate-Infrastruktur ausgeführt werden, in AWS APIs Ihrem Namen Aufrufe tätigen. Auf diese Weise können sie Aktionen wie das Abrufen von Container-Images aus Amazon ECR oder das Weiterleiten von Protokollen an andere AWS Dienste ausführen. Die Amazon EKS Pod-Ausführungsrolle stellt die IAM-Berechtigungen dafür bereit.

Wenn Sie ein Fargate-Profil erstellen, müssen Sie mithilfe des Profils eine Pod-Ausführungsrolle für die Amazon EKS-Komponenten angeben, die auf der Fargate-Infrastruktur ausgeführt werden. Diese Rolle wird zur Autorisierung der [rollenbasierten Zugriffskontrolle](#) (RBAC) von Kubernetes des Clusters hinzugefügt. Dadurch kann sich `kubelet` das, was auf der Fargate-Infrastruktur läuft, bei Ihrem Amazon EKS-Cluster registrieren, sodass es in Ihrem Cluster als Knoten erscheinen kann.

 Note

Das Fargate-Profil muss eine andere IAM-Rolle haben als EC2 Amazon-Knotengruppen.

 Important

Die Container, die im Fargate-Pod ausgeführt werden, können die mit einer Pod-Ausführungsrolle verbundenen IAM-Berechtigungen nicht annehmen. Um den Containern in Ihrem Fargate-Pod Berechtigungen für den Zugriff auf andere AWS Dienste zu erteilen, müssen Sie [IAM-Rollen für Dienstkonten](#) verwenden.

Bevor Sie ein Fargate-Profil erstellen, müssen Sie eine IAM-Rolle bei Amazon erstellen. [EKSFargatePodExecutionRolePolicy](#)

Suchen Sie nach einer korrekt konfigurierten vorhandenen Pod-Ausführungsrolle

Mithilfe des folgenden Verfahrens können Sie überprüfen, ob Ihr Konto bereits über eine korrekt konfigurierte Amazon EKS-Pod-Ausführungsrolle verfügt. Um ein unübersichtliches Sicherheitsproblem zu vermeiden, ist es wichtig, dass die Rolle den Zugriff auf SourceArn folgende Kriterien einschränkt: Sie können die Ausführungsrolle nach Bedarf ändern, um Fargate-Profile auch auf anderen Clustern zu unterstützen.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Suchen Sie auf der Seite Rollen in der Liste der Rollen für Amazon EKSFargate PodExecutionRole. Wenn die Rolle nicht existiert, finden Sie weitere Informationen unter [the section called “Die Amazon EKS Pod-Ausführungsrolle erstellen”](#) So erstellen Sie die Rolle. Wenn die Rolle vorhanden ist, wählen Sie sie aus.
4. Gehen Sie auf der EKSFargatePodExecutionRoleAmazon-Seite wie folgt vor:
 - a. Wählen Sie Permissions (Berechtigungen).
 - b. Stellen Sie sicher, dass die von EKSFargatePodExecutionRolePolicyAmazon verwaltete Richtlinie mit der Rolle verknüpft ist.
 - c. Wählen Sie Trust Relationships (Vertrauensbeziehungen) aus.
 - d. Wählen Sie Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.

5. Prüfen Sie auf der Seite Edit trust policy (Vertrauensrichtlinie bearbeiten), dass die Vertrauensbeziehung die folgende Richtlinie und eine Zeile für Fargate-Profile in Ihrem Cluster enthält. Wenn ja, wählen Sie Cancel (Abbrechen) aus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws: eks:region-code:111122223333:fargateprofile/
my-cluster/*"
        }
      },
      "Principal": {
        "Service": "eks-fargate-pods.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Wenn die Richtlinie übereinstimmt, aber keine Zeile enthält, in der die Fargate-Profile in Ihrem Cluster angegeben sind, können Sie die folgende Zeile oben im ArnLike Objekt hinzufügen.

region-code Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet, *111122223333* durch Ihre Konto-ID und *my-cluster* durch den Namen Ihres Clusters.

```
"aws:SourceArn": "arn:aws: eks:region-code:111122223333:fargateprofile/my-cluster/*",
```

Wenn die Richtlinie nicht übereinstimmt, kopieren Sie die vollständige vorherige Richtlinie in das Formular und wählen Sie Richtlinie aktualisieren aus. *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. Wenn Sie dieselbe Rolle in allen AWS Regionen Ihres Kontos verwenden möchten, *region-code* ersetzen Sie es durch *. Ersetzen Sie *111122223333* durch Ihre Konto-ID und *my-cluster* durch den Namen Ihres Clusters. Wenn Sie dieselbe Rolle für alle Cluster in Ihrem Konto verwenden möchten, ersetzen Sie *my-cluster* durch *.

Die Amazon EKS Pod-Ausführungsrolle erstellen

Wenn Sie noch nicht über die Amazon EKS-Pod-Ausführungsrolle für Ihren Cluster verfügen, können Sie die AWS Management Console oder die AWS CLI verwenden, um sie zu erstellen.

AWS Management Console

- a. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
- b. Wählen Sie im linken Navigationsbereich Roles aus.
- c. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
- d. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
 - i. Wählen Sie im Abschnitt Vertrauenswürdiger Entitätstyp die Option AWS Service aus.
 - ii. Wählen Sie aus der Dropdownliste Anwendungsfälle für andere AWS Dienste die Option EKS aus.
 - iii. Wählen Sie EKS - Fargate Pod.
 - iv. Wählen Sie Weiter.
- e. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
- f. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
 - i. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. AmazonEKSFargatePodExecutionRole.
 - ii. Fügen Sie der Rolle unter Tags hinzufügen (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Markieren von IAM-Ressourcen](#) im IAM-Benutzerhandbuch.
 - iii. Wählen Sie Rolle erstellen.
- g. Suchen Sie auf der Seite Rollen in der Liste der Rollen für Amazon EKSFargate PodExecutionRole. Wählen Sie die Rolle aus.
- h. Gehen Sie auf der EKSFargatePodExecutionRoleAmazon-Seite wie folgt vor:
 - i. Wählen Sie Trust Relationships (Vertrauensbeziehungen) aus.
 - ii. Wählen Sie Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
- i. Führen Sie auf der Seite Edit trust policy (Vertrauensrichtlinie bearbeiten) die folgenden Schritte aus:

- i. Kopieren Sie die folgenden Inhalte in das Formular unter Edit trust policy (Vertrauensrichtlinie bearbeiten). *region-code* Ersetzen Sie es durch die AWS Region, in der sich Ihr Cluster befindet. Wenn Sie dieselbe Rolle in allen AWS Regionen Ihres Kontos verwenden möchten, *region-code* ersetzen Sie es durch *. Ersetzen Sie *111122223333* durch Ihre Konto-ID und *my-cluster* durch den Namen Ihres Clusters. Wenn Sie dieselbe Rolle für alle Cluster in Ihrem Konto verwenden möchten, ersetzen Sie *my-cluster* durch *.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:eks:region-code:111122223333:fargateprofile/my-cluster/*"
        }
      },
      "Principal": {
        "Service": "eks-fargate-pods.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- ii. Wählen Sie Update policy.

AWS CLI

- a. Kopieren Sie den folgenden Inhalt in eine Datei namens pod-execution-role-trust-policy.json. *region-code* Ersetzen Sie durch die AWS Region, in der sich Ihr Cluster befindet. Wenn Sie dieselbe Rolle in allen AWS Regionen Ihres Kontos verwenden möchten, *region-code* ersetzen Sie es durch *. Ersetzen Sie *111122223333* durch Ihre Konto-ID und *my-cluster* durch den Namen Ihres Clusters. Wenn Sie dieselbe Rolle für alle Cluster in Ihrem Konto verwenden möchten, ersetzen Sie *my-cluster* durch *.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
"Effect": "Allow",
"Condition": {
  "ArnLike": {
    "aws:SourceArn": "arn:aws:eks:region-
code:111122223333:fargateprofile/my-cluster/*"
  }
},
"Principal": {
  "Service": "eks-fargate-pods.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
```

b. Erstellen Sie eine IAM-Rolle für die Pod-Ausführung.

```
aws iam create-role \
  --role-name AmazonEKSFargatePodExecutionRole \
  --assume-role-policy-document file:///pod-execution-role-trust-policy.json
```

c. Hängen Sie die erforderliche von Amazon EKS verwaltete IAM-Richtlinie an die Rolle an.

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy \
  --role-name AmazonEKSFargatePodExecutionRole
```

Amazon-EKS-Konnektor-IAM-Rolle

Sie können Kubernetes-Cluster verbinden, um sie in Ihrem anzuzeigen. AWS Management Console
Um eine Verbindung zu einem Kubernetes-Cluster herzustellen, erstellen Sie eine IAM-Rolle.

Überprüfen auf eine vorhandene EKS-Connector-Rolle

Mit dem folgenden Verfahren können Sie feststellen, ob Ihr Konto bereits über die Amazon-EKS-Konnektorrolle verfügt.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.

3. Suchen Sie in der Liste der Rollen nach `AmazonEKSClusterAgentRole`. Wenn eine Rolle, die Folgendes beinhaltet, nicht `AmazonEKSClusterAgentRole` existiert, finden Sie weitere Informationen [the section called “Erstellen der Rolle des Amazon-EKS-Connector-Agenten”](#) zum Erstellen der Rolle. Wenn eine Rolle mit `AmazonEKSClusterAgentRole` vorhanden ist, wählen Sie die Rolle aus, um die angefügten Richtlinien anzuzeigen.
4. Wählen Sie Permissions (Berechtigungen).
5. Stellen Sie sicher, dass die von Amazon EKSCluster AgentPolicy verwaltete Richtlinie der Rolle zugeordnet ist. Wenn die Richtlinie angefügt ist, ist Ihre Amazon-EKS-Connector-Rolle ordnungsgemäß konfiguriert.
6. Wählen Sie Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
7. Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält. Wenn die Vertrauensstellung mit der folgenden Richtlinie übereinstimmt, wählen Sie Cancel (Abbrechen) aus. Wenn das Vertrauensverhältnis nicht übereinstimmt, kopieren Sie die Richtlinie in das Fenster Vertrauensrichtlinie bearbeiten und wählen Sie Richtlinie aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Erstellen der Rolle des Amazon-EKS-Connector-Agenten

Sie können das AWS Management Console oder verwenden AWS CloudFormation , um die Connector-Agent-Rolle zu erstellen.

AWS CLI

- a. Erstellen Sie eine Datei mit dem Namen `eks-connector-agent-trust-policy.json`, die die folgende JSON enthält, die für die IAM-Rolle verwendet werden soll.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- b. Erstellen Sie eine Datei mit dem Namen `eks-connector-agent-policy.json`, die die folgende JSON enthält, die für die IAM-Rolle verwendet werden soll.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SsmControlChannel",
      "Effect": "Allow",
      "Action": [
        "ssmmessages:CreateControlChannel"
      ],
      "Resource": "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid": "ssmDataplaneOperations",
      "Effect": "Allow",
      "Action": [
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource": "*"
    }
  ]
}
```

```
    }
  ]
}
```

- c. Erstellen Sie die Agentenrolle von Amazon EKS Connector mithilfe der Vertrauensrichtlinie und Richtlinie, die Sie in den vorherigen Listenelementen erstellt haben.

```
aws iam create-role \
  --role-name AmazonEKSCoordinatorAgentRole \
  --assume-role-policy-document file://eks-coordinator-agent-trust-policy.json
```

- d. Hängen Sie die Richtlinie an Ihre Amazon-EKS-Coordinator-Agentenrolle an.

```
aws iam put-role-policy \
  --role-name AmazonEKSCoordinatorAgentRole \
  --policy-name AmazonEKSCoordinatorAgentPolicy \
  --policy-document file://eks-coordinator-agent-policy.json
```

AWS CloudFormation

- a. Speichern Sie die folgende AWS CloudFormation Vorlage in einer Textdatei auf Ihrem lokalen System.

Note

Diese Vorlage erstellt auch die mit dem Service verknüpfte Rolle, die andernfalls beim Aufruf der `registerCluster`-API erstellt würde. Details dazu finden Sie unter [the section called “Rolle des Cluster-Connectors”](#).

```
---
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Provisions necessary resources needed to register clusters in EKS'
Parameters: {}
Resources:
  EKSCoordinatorSLR:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: eks-coordinator.amazonaws.com

  EKSCoordinatorAgentRole:
    Type: AWS::IAM::Role
```

```

Properties:
  AssumeRolePolicyDocument:
    Version: '2012-10-17'
    Statement:
      - Effect: Allow
        Action: [ 'sts:AssumeRole' ]
        Principal:
          Service: 'ssm.amazonaws.com'

EKSCoordinatorAgentPolicy:
  Type: AWS::IAM::Policy
  Properties:
    PolicyName: EKSCoordinatorAgentPolicy
    Roles:
      - {Ref: 'EKSCoordinatorAgentRole'}
    PolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: 'Allow'
          Action: [ 'ssmmessages:CreateControlChannel' ]
          Resource:
            - Fn::Sub: 'arn:${AWS::Partition}:eks:*:*:cluster/*'
        - Effect: 'Allow'
          Action: [ 'ssmmessages:CreateDataChannel',
'ssmmessages:OpenDataChannel', 'ssmmessages:OpenControlChannel' ]
          Resource: "*"
Outputs:
  EKSCoordinatorAgentRoleArn:
    Description: The agent role that EKS coordinator uses to communicate with AWS
    services.
    Value: !GetAtt EKSCoordinatorAgentRole.Arn

```

- b. Öffnen Sie die [AWS CloudFormation -Konsole](#).
- c. Wählen Sie Stapel mit neuen Ressourcen erstellen (Standard).
- d. Wählen Sie für Specify template (Vorlage festlegen) Upload a template file (Vorlagendatei hochladen) aus und wählen Sie dann Choose file (Datei wählen).
- e. Wählen Sie die zuvor erstellte Datei und klicken Sie dann auf Next (Weiter).
- f. Geben Sie für Stack name (Stack-Name) einen Namen für Ihre Rolle ein, wie z. B. `eksCoordinatorAgentRole`. Klicken Sie dann auf Next (Weiter).
- g. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.

- h. Überprüfen Sie auf der Seite Überprüfen Ihre Informationen, bestätigen Sie, dass der Stack IAM-Ressourcen erstellen kann, und wählen Sie dann Erstellen aus.

AWS verwaltete Richtlinien für Amazon Elastic Kubernetes Service

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [vom Kunden verwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn ein neuer AWS Dienst gestartet wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: Amazoneks_CNI_Policy

Sie können die AmazonEKS_CNI_Policy an Ihre IAM-Entitäten anhängen. Bevor Sie eine EC2 Amazon-Knotengruppe erstellen, muss diese Richtlinie entweder an die [Knoten-IAM-Rolle oder an eine IAM-Rolle](#) angehängt werden, die speziell vom Amazon VPC CNI-Plugin für Kubernetes verwendet wird. Dies dient dazu, Aktionen in Ihrem Namen auszuführen. Wir empfehlen, dass Sie die Richtlinie einer Rolle zuordnen, die nur vom Plugin verwendet wird. Weitere Informationen erhalten Sie unter [the section called “Amazon VPC CNI”](#) und [the section called “Für IRSA konfigurieren”](#).

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **ec2:*NetworkInterface** und **ec2:*PrivateIpAddresses** — Ermöglicht dem Amazon VPC CNI-Plugin, Aktionen wie die Bereitstellung von Elastic Network Interfaces und IP-Adressen

für Pods durchzuführen, um Netzwerke für Anwendungen bereitzustellen, die in Amazon EKS ausgeführt werden.

- **ec2**Aktionen lesen — Ermöglicht dem Amazon VPC CNI-Plugin, Aktionen wie das Beschreiben von Instances und Subnetzen durchzuführen, um die Anzahl der freien IP-Adressen in Ihren Amazon VPC-Subnetzen zu sehen. Das VPC CNI kann die freien IP-Adressen in jedem Subnetz verwenden, um die Subnetze mit den meisten freien IP-Adressen auszuwählen, die bei der Erstellung einer elastischen Netzwerkschnittstelle verwendet werden sollen.

Die neueste Version des JSON-Richtliniendokuments finden Sie unter [AmazonEKS_CNI_Policy im Managed Policy Reference Guide](#). AWS

AWS verwaltete Richtlinie: EKSCluster Amazon-Richtlinie

Sie können AmazonEKSClusterPolicy an Ihre IAM-Entitäten anhängen. Bevor Sie einen Cluster erstellen, müssen Sie über eine [Cluster-IAM-Rolle](#) mit dieser angehängten Richtlinie verfügen. Kubernetes-Cluster, die von Amazon EKS verwaltet werden, rufen in Ihrem Namen andere AWS Services auf. Sie tun dies, um die Ressourcen zu verwalten, die Sie mit dem Service verwenden.

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **autoscaling**— Lesen und aktualisieren Sie die Konfiguration einer Auto Scaling Scaling-Gruppe. Diese Berechtigungen werden von Amazon EKS nicht verwendet, bleiben aber aus Gründen der Abwärtskompatibilität in der Richtlinie enthalten.
- **ec2**— Arbeiten Sie mit Volumes und Netzwerkressourcen, die EC2 Amazon-Knoten zugeordnet sind. Dies ist erforderlich, damit die Kubernetes-Steuerebene Instances zu einem Cluster verbinden und von persistenten Kubernetes-Volumes angeforderte Amazon-EBS-Volumes dynamisch bereitstellen und verwalten kann.
- **ec2**- Löschen Sie elastische Netzwerkschnittstellen, die vom VPC-CNI erstellt wurden. Dies ist erforderlich, damit EKS elastische Netzwerkschnittstellen bereinigen kann, die zurückbleiben, wenn das VPC-CNI unerwartet beendet wird.
- **elasticloadbalancing**— Arbeiten Sie mit Elastic Load Balancern und fügen Sie ihnen Knoten als Ziele hinzu. Dies ist erforderlich, damit die Kubernetes-Steuerebene von Kubernetes-Diensten angeforderte Elastic Load Balancer dynamisch bereitstellen kann.
- **iam**— Erstellen Sie eine serviceverknüpfte Rolle. Dies ist erforderlich, damit die Kubernetes-Steuerebene von Kubernetes-Services angeforderte Elastic Load Balancer dynamisch bereitstellen kann.

- **kms**— Liest einen Schlüssel aus AWS KMS. Dies ist erforderlich, damit die Kubernetes-Steuerebene die [Secrets-Verschlüsselung](#) von Kubernetes-Secrets unterstützt, die in etcd gespeichert sind.

Die neueste Version des JSON-Richtliniendokuments finden Sie unter [Amazon EKSCluster Policy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSDashboard ConsoleReadOnly

Sie können AmazonEKSDashboardConsoleReadOnly an Ihre IAM-Entitäten anhängen.

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **eks**- Schreibgeschützter Zugriff auf EKS-Dashboard-Daten, Ressourcen und Informationen zu Cluster-Versionen. Dies ermöglicht die Anzeige von EKS-bezogenen Metriken und Cluster-Konfigurationsdetails.
- **organizations**- Schreibgeschützter Zugriff auf Unternehmensinformationen AWS , einschließlich:
 - Organisationsdetails und Servicezugriff anzeigen
 - Auflisten von Unternehmenswurzeln, Konten und Organisationseinheiten
 - Organisationsstruktur anzeigen

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSDashboard ConsoleReadOnly](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSFargate PodExecutionRolePolicy

Sie können AmazonEKSFargatePodExecutionRolePolicy an Ihre IAM-Entitäten anhängen. Bevor Sie ein Fargate-Profil erstellen können, müssen Sie eine Fargate-Pod-Ausführungsrolle erstellen und ihr diese Richtlinie anhängen. Weitere Informationen erhalten Sie unter [the section called “Schritt 2: Erstellen Sie eine Fargate Pod-Ausführungsrolle”](#) und [the section called “Definieren Sie Profile”](#).

Diese Richtlinie gewährt der Rolle die Berechtigungen, die den Zugriff auf andere AWS Serviceressourcen ermöglichen, die für die Ausführung von Amazon EKS-Pods auf Fargate erforderlich sind.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **ecr**— Ermöglicht Pods, die auf Fargate ausgeführt werden, das Abrufen von Container-Images, die in Amazon ECR gespeichert sind.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSFargate PodExecutionRolePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSFargateServiceRolePolicy

Sie können keine Verbindungen AmazonEKSFargateServiceRolePolicy zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist mit einer servicegebundenen Rolle verknüpft, die es Amazon EKS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter `AWSServiceRoleforAmazonEKSFargate`.

Diese Richtlinie erteilt Amazon EKS die erforderlichen Berechtigungen zum Ausführen von Fargate-Aufgaben. Die Richtlinie wird nur verwendet, wenn Sie über Fargate-Knoten verfügen.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen.

- **ec2**— Elastic Network Interfaces erstellen und löschen und Elastic Network Interfaces und Ressourcen beschreiben. Dies ist erforderlich, damit der Amazon EKS Fargate-Service das VPC-Netzwerk konfigurieren kann, das für Fargate Pods erforderlich ist.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSFargateServiceRolePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: EKSCoordinate Amazon-Richtlinie

Sie können AmazonEKSCoordinatePolicy an Ihre IAM-Entitäten anhängen. Sie können diese Richtlinie an Ihre [Cluster-IAM-Rolle](#) anhängen, um die Ressourcen zu erweitern, die EKS in Ihrem Konto verwalten kann.

Diese Richtlinie gewährt die Berechtigungen, die Amazon EKS benötigt, um EC2 Instances für den EKS-Cluster zu erstellen und zu verwalten, sowie die erforderlichen IAM-Berechtigungen für die Konfiguration EC2. Außerdem gewährt diese Richtlinie Amazon EKS die Erlaubnis, die mit dem EC2 Spot-Dienst verknüpfte Rolle in Ihrem Namen zu erstellen.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **ec2**Berechtigungen:
 - `ec2:CreateFleet` und `ec2:RunInstances` — Ermöglicht das Erstellen von EC2 Instanzen und die Verwendung bestimmter EC2 Ressourcen (Bilder, Sicherheitsgruppen, Subnetze) für EKS-Clusterknoten.
 - `ec2:CreateLaunchTemplate`- Ermöglicht das Erstellen von EC2 Startvorlagen für EKS-Clusterknoten.
 - Die Richtlinie enthält auch Bedingungen, um die Verwendung dieser EC2 Berechtigungen auf Ressourcen zu beschränken, die mit dem EKS-Clusternamen und anderen relevanten Tags gekennzeichnet sind.
 - `ec2:CreateTags`- Ermöglicht das Hinzufügen von Tags zu EC2 Ressourcen `CreateFleet`, die durch die `CreateLaunchTemplate` Aktionen `RunInstances`, und erstellt wurden.
- **iam**Berechtigungen:
 - `iam:AddRoleToInstanceProfile`— Ermöglicht das Hinzufügen einer IAM-Rolle zum EKS-Compute-Instance-Profil.
 - `iam:PassRole`— Ermöglicht die Übergabe der erforderlichen IAM-Rollen an den EC2 Dienst.

Die neueste Version des JSON-Richtliniendokuments finden Sie unter [Amazon EKSCoordinate Policy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: EKSNetworking Amazon-Richtlinie

Sie können `AmazonEKSCoordinatePolicy` an Ihre IAM-Entitäten anhängen. Sie können diese Richtlinie an Ihre [Cluster-IAM-Rolle](#) anhängen, um die Ressourcen zu erweitern, die EKS in Ihrem Konto verwalten kann.

Diese Richtlinie wurde entwickelt, um Amazon EKS die erforderlichen Berechtigungen zur Erstellung und Verwaltung von Netzwerkschnittstellen für den EKS-Cluster zu gewähren, sodass die Steuerungsebene und die Worker-Knoten ordnungsgemäß kommunizieren und funktionieren können.

Details zu Berechtigungen

Diese Richtlinie gewährt Amazon EKS die folgenden Berechtigungen, um es Amazon EKS zu ermöglichen, Netzwerkschnittstellen für den Cluster zu verwalten:

- **ec2**Berechtigungen für Netzwerkschnittstellen:
 - `ec2:CreateNetworkInterface`- Ermöglicht das Erstellen von EC2 Netzwerkschnittstellen.
 - Die Richtlinie enthält Bedingungen, um die Verwendung dieser Berechtigung auf Netzwerkschnittstellen zu beschränken, die mit dem EKS-Clusternamen und dem Kubernetes-CNI-Knotennamen gekennzeichnet sind.
 - `ec2:CreateTags`— Ermöglicht das Hinzufügen von Tags zu den Netzwerkschnittstellen, die durch die Aktion erstellt wurden. `CreateNetworkInterface`
- **ec2**Berechtigungen zur Verwaltung von Netzwerkschnittstellen:
 - `ec2:AttachNetworkInterface`, `ec2:DetachNetworkInterface` - Ermöglicht das Anhängen und Trennen von Netzwerkschnittstellen an EC2 Instanzen.
 - `ec2:UnassignPrivateIpAddresses`,
`ec2:UnassignIpv6Addresses``ec2:AssignPrivateIpAddresses`,
`ec2:AssignIpv6Addresses` - Ermöglicht die Verwaltung der IP-Adresszuweisungen der Netzwerkschnittstellen.
 - Diese Berechtigungen sind auf Netzwerkschnittstellen beschränkt, die mit dem EKS-Clusternamen gekennzeichnet sind.

Die neueste Version des JSON-Richtliniendokuments finden Sie unter [Amazon EKSNetworking Policy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSBLOCK StoragePolicy

Sie können `AmazonEKSBLOCKStoragePolicy` an Ihre IAM-Entitäten anhängen. Sie können diese Richtlinie an Ihre [Cluster-IAM-Rolle](#) anhängen, um die Ressourcen zu erweitern, die EKS in Ihrem Konto verwalten kann.

Diese Richtlinie gewährt Amazon EKS die erforderlichen Berechtigungen, um EC2 Volumes und Snapshots für den EKS-Cluster zu erstellen, zu verwalten und zu verwalten, sodass die

Steuerungsebene und die Worker-Knoten persistenten Speicher bereitstellen und verwenden können, wie es für Kubernetes-Workloads erforderlich ist.

Details zu Berechtigungen

Diese IAM-Richtlinie gewährt die folgenden Berechtigungen, damit Amazon EKS EC2 Volumes und Snapshots verwalten kann:

- **ec2Berechtigungen zur Volume-Verwaltung:**
 - `ec2:AttachVolume`, `ec2:DetachVolume`, `ec2:ModifyVolume`, `ec2:EnableFastSnapshotRestores` - Ermöglicht das Anhängen, Trennen, Ändern und Aktivieren schneller Snapshot-Wiederherstellungen für EC2 Volumes.
 - Diese Berechtigungen sind auf Volumes beschränkt, die mit dem EKS-Clusternamen gekennzeichnet sind.
 - `ec2:CreateTags` - Ermöglicht das Hinzufügen von Tags zu den EC2 Volumes und Snapshots, die mit den `CreateSnapshot` Aktionen `CreateVolume` und erstellt wurden.
- **ec2Berechtigungen zur Erstellung von Volumes:**
 - `ec2:CreateVolume` - Ermöglicht das Erstellen neuer EC2 Volumes.
 - Die Richtlinie enthält Bedingungen, um die Verwendung dieser Berechtigung auf Volumes zu beschränken, die mit dem EKS-Clusternamen und anderen relevanten Tags gekennzeichnet sind.
 - `ec2:CreateSnapshot` - Ermöglicht das Erstellen neuer EC2 Volume-Snapshots.
 - Die Richtlinie enthält Bedingungen, um die Verwendung dieser Berechtigung auf Snapshots zu beschränken, die mit dem EKS-Clusternamen und anderen relevanten Tags gekennzeichnet sind.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSBLOCK StoragePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSLoad BalancingPolicy

Sie können `AmazonEKSLoadBalancingPolicy` an Ihre IAM-Entitäten anhängen. Sie können diese Richtlinie an Ihre [Cluster-IAM-Rolle](#) anhängen, um die Ressourcen zu erweitern, die EKS in Ihrem Konto verwalten kann.

Diese IAM-Richtlinie gewährt Amazon EKS die erforderlichen Berechtigungen für die Zusammenarbeit mit verschiedenen AWS Diensten zur Verwaltung von Elastic Load Balancern (ELBs) und verwandten Ressourcen.

Details zu Berechtigungen

Die wichtigsten Berechtigungen, die durch diese Richtlinie gewährt werden, sind:

- **elasticloadbalancing**: Ermöglicht das Erstellen, Ändern und Verwalten von Elastic Load Balancern und Zielgruppen. Dazu gehören Berechtigungen zum Erstellen, Aktualisieren und Löschen von Load Balancern, Zielgruppen, Listenern und Regeln.
- **ec2**: Ermöglicht das Erstellen und Verwalten von Sicherheitsgruppen, die für die Kubernetes-Steuerebene erforderlich sind, um Instances zu einem Cluster zusammenzuführen und Amazon EBS-Volumes zu verwalten. Ermöglicht auch das Beschreiben und Auflisten von EC2 Ressourcen wie Instances VPCs, Subnetzen, Sicherheitsgruppen und anderen Netzwerkressourcen.
- **iam**: Ermöglicht die Erstellung einer serviceverknüpften Rolle für Elastic Load Balancing, die für die dynamische Bereitstellung durch die Kubernetes-Steuerebene erforderlich ist. ELBs
- **kms**: Ermöglicht das Lesen eines Schlüssels aus AWS KMS, der erforderlich ist, damit die Kubernetes-Steuerebene die Verschlüsselung von in etcd gespeicherten Kubernetes-Geheimnissen unterstützt.
- **wafv2** und **shield**: Ermöglicht das Zuordnen und Trennen von ACLs Webanwendungen und das Erstellen/Löschen von AWS Shield-Schutzmaßnahmen für die Elastic Load Balancer.
- **cognito-idp** und **elasticloadbalancing**: Erteilt Berechtigungen zur Beschreibung von Benutzerpool-Clients, zum Auflisten und Beschreiben von Zertifikaten und zur Beschreibung von Zielgruppen, die für die Kubernetes-Steuerebene zur Verwaltung der Elastic Load Balancer erforderlich sind.

Die Richtlinie umfasst auch mehrere Bedingungsprüfungen, um sicherzustellen, dass die Berechtigungen auf den spezifischen EKS-Cluster beschränkt sind, der mithilfe des Tags verwaltet wird. `eks:eks-cluster-name`

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSLoad BalancingPolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: EKSService Amazon-Richtlinie

Sie können `AmazonEKSServicePolicy` an Ihre IAM-Entitäten anhängen. Für Cluster, die vor dem 16. April 2020 erstellt wurden, mussten Sie eine IAM-Rolle erstellen und diese Richtlinie anhängen.

Für Cluster, die am oder nach dem 16. April 2020 erstellt wurden, müssen Sie keine Rolle erstellen und Sie müssen diese Richtlinie nicht zuweisen. Wenn Sie einen Cluster mithilfe eines IAM-Prinzips erstellen, der über die `iam:CreateServiceLinkedRole` entsprechende Berechtigung verfügt, wird die mit dem [AWSServiceRoleforAmazonEKS-Dienst](#) verknüpfte Rolle automatisch für Sie erstellt. Der serviceverknüpften Rolle ist die [verwaltete Richtlinie: Amazon EKSService RolePolicy](#) zugeordnet.

Diese Richtlinie ermöglicht Amazon EKS, die erforderlichen Ressourcen für den Betrieb von Amazon-EKS-Clustern zu erstellen und zu verwalten.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen.

- **eks**— Aktualisieren Sie die Kubernetes-Version Ihres Clusters, nachdem Sie ein Update initiiert haben. Diese Berechtigung wird von Amazon EKS nicht verwendet, bleibt aber aus Gründen der Abwärtskompatibilität in der Richtlinie enthalten.
- **ec2**— Arbeiten Sie mit Elastic Network Interfaces und anderen Netzwerkressourcen und Tags. Dies wird von Amazon EKS benötigt, um ein Netzwerk zu konfigurieren, das die Kommunikation zwischen Knoten und der Kubernetes-Steuerebene erleichtert. Lesen Sie Informationen über Sicherheitsgruppen. Aktualisieren Sie die Tags für Sicherheitsgruppen.
- **route53**— Ordnet eine VPC einer Hosting-Zone zu. Dies wird von Amazon EKS benötigt, um ein privates Endpunktnetzwerk für Ihren Kubernetes-Cluster-API-Server zu aktivieren.
- **logs**— Ereignisse protokollieren. Dies ist erforderlich, damit Amazon EKS die Protokolle der Kubernetes-Steuerebene an senden kann. CloudWatch
- **iam**— Erstellen Sie eine serviceverknüpfte Rolle. Dies ist erforderlich, damit Amazon EKS die serviceverknüpfte [the section called “Serviceverknüpfte Rollenberechtigungen für Amazon EKS”](#)-Rolle in Ihrem Namen erstellt.

Die neueste Version des JSON-Richtliniendokuments finden Sie unter [Amazon EKSService Policy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSService RolePolicy

Sie können keine Verbindungen `AmazonEKSServiceRolePolicy` zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist mit einer servicegebundenen Rolle verknüpft, die es Amazon EKS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter

[the section called “Serviceverknüpfte Rollenberechtigungen für Amazon EKS”](#). Wenn Sie einen Cluster mithilfe eines IAM-Prinzips erstellen, der über die `iam:CreateServiceLinkedRole` entsprechende Berechtigung verfügt, wird die dienstbezogene [AWSServiceRoleforAmazonEKS-Rolle](#) automatisch für Sie erstellt, und diese Richtlinie wird ihr angehängt.

Diese Richtlinie ermöglicht es der serviceverknüpften Rolle, AWS Dienste in Ihrem Namen aufzurufen.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen.

- **ec2**— Erstellen und beschreiben Sie Elastic Network Interfaces und EC2 Amazon-Instances, die Cluster-Sicherheitsgruppe und die VPC, die für die Erstellung eines Clusters erforderlich sind. Weitere Informationen finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Lesen Sie Informationen zu Sicherheitsgruppen. Aktualisieren Sie die Tags für Sicherheitsgruppen. Lesen Sie Informationen zu Kapazitätsreservierungen auf Abruf.
- **ec2:Automatischer Modus** — Beendet EC2 Instanzen, die mit dem automatischen Modus von EKS erstellt wurden. Weitere Informationen finden Sie unter [Automatischer EKS-Modus](#).
- **iam**— Listet alle verwalteten Richtlinien auf, die einer IAM-Rolle zugeordnet sind. Dies ist erforderlich, damit Amazon EKS alle verwalteten Richtlinien und Berechtigungen auflisten und validieren kann, die zum Erstellen von Clustern erforderlich sind.
- Eine VPC mit einer gehosteten Zone verknüpfen – Dies wird von Amazon EKS benötigt, um ein privates Endpunktnetzwerk für Ihren Kubernetes-Cluster-API-Server zu aktivieren.
- Ereignis protokollieren — Dies ist erforderlich, damit Amazon EKS die Protokolle der Kubernetes-Steuerebene an senden kann. CloudWatch
- Metrik angeben — Dies ist erforderlich, damit Amazon EKS die Protokolle der Kubernetes-Steuerebene an senden kann. CloudWatch
- **eks**- Verwalten Sie Cluster-Zugriffseinträge und -richtlinien und ermöglichen Sie so eine genaue Kontrolle darüber, wer auf EKS-Ressourcen zugreifen kann und welche Aktionen sie ausführen können. Dazu gehört die Zuordnung von Standardzugriffsrichtlinien für Rechen-, Netzwerk-, Lastausgleichs- und Speichervorgänge.
- **elasticloadbalancing**- Erstellen, verwalten und löschen Sie Load Balancer und ihre Komponenten (Listener, Zielgruppen, Zertifikate), die mit EKS-Clustern verknüpft sind. Zeigen Sie die Attribute und den Integritätsstatus des Load Balancers an.

- **events**- Erstellen und verwalten Sie EventBridge Regeln für Überwachungs EC2 - und AWS Integritätsereignisse im Zusammenhang mit EKS-Clustern und ermöglichen Sie so automatisierte Reaktionen auf Infrastrukturänderungen und Integritätswarnungen.
- **iam**- Verwalten Sie EC2 Instanzprofile mit dem Präfix „eks“, einschließlich Erstellung, Löschung und Rollenzuweisung, was für die EKS-Knotenverwaltung erforderlich ist.
- **pricing& shield**— Greifen Sie auf AWS Preisinformationen und den Shield-Schutzstatus zu und ermöglichen so Kostenmanagement und erweiterte Sicherheitsfunktionen für EKS-Ressourcen.
- Säuberung von Ressourcen — Löschen Sie während der Cluster-Bereinigung auf sichere Weise EKS-markierte Ressourcen wie Volumes, Snapshots, Startvorlagen und Netzwerkschnittstellen.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSService RolePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSVPCResource Controller

Sie können die AmazonEKSVPCResourceController-Richtlinie an Ihre IAM-Identitäten anfügen. Wenn Sie [Sicherheitsgruppen für Pods](#) verwenden, müssen Sie diese Richtlinie an Ihre [Amazon EKS-Cluster-IAM-Rolle](#) anhängen, um Aktionen in Ihrem Namen durchzuführen.

Diese Richtlinie gewährt der Clusterrolle Berechtigungen zum Verwalten von Elastic Network Interfaces und IP-Adressen für Knoten.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **ec2**— Verwalten Sie Elastic Network-Schnittstellen und IP-Adressen, um Pod-Sicherheitsgruppen und Windows-Knoten zu unterstützen.

Die neueste Version des JSON-Richtliniendokuments finden Sie unter [Amazon EKSVPCResource Controller](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSWorker NodePolicy

Sie können die AmazonEKSWorkerNodePolicy an Ihre IAM-Entitäten anhängen. Sie müssen diese Richtlinie einer [Node-IAM-Rolle](#) zuordnen, die Sie angeben, wenn Sie EC2 Amazon-Knoten

erstellen, die es Amazon EKS ermöglichen, Aktionen in Ihrem Namen durchzuführen. Wenn Sie eine Knotengruppe mit `eksctl` erstellen, wird die Knoten-IAM-Rolle erstellt und diese Richtlinie automatisch an die Rolle angehängt.

Diese Richtlinie gewährt Amazon EKS EC2 Amazon-Knoten die Erlaubnis, sich mit Amazon EKS-Clustern zu verbinden.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **ec2**— Lesen Sie das Instance-Volumen und die Netzwerkinformationen. Dies ist erforderlich, damit Kubernetes-Knoten Informationen über EC2 Amazon-Ressourcen beschreiben können, die erforderlich sind, damit der Knoten dem Amazon EKS-Cluster beiträgt.
- **eks**— Beschreiben Sie den Cluster optional als Teil des Node-Bootstrapping.
- **eks-auth:AssumeRoleForPodIdentity**— Erlaubt das Abrufen von Anmeldeinformationen für EKS-Workloads auf dem Knoten. Dies ist erforderlich, damit EKS Pod Identity ordnungsgemäß funktioniert.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSWorker NodePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSWorker NodeMinimalPolicy

Sie können Amazon EKSWorker NodeMinimalPolicy an Ihre IAM-Entitäten anhängen. Sie können diese Richtlinie an eine Node-IAM-Rolle anhängen, die Sie angeben, wenn Sie EC2 Amazon-Knoten erstellen, die es Amazon EKS ermöglichen, Aktionen in Ihrem Namen durchzuführen.

Diese Richtlinie gewährt Amazon EKS EC2 Amazon-Knoten die Erlaubnis, sich mit Amazon EKS-Clustern zu verbinden. Diese Richtlinie hat im Vergleich zu Amazon weniger Berechtigungen EKSWorkerNodePolicy.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **eks-auth:AssumeRoleForPodIdentity**— Erlaubt das Abrufen von Anmeldeinformationen für EKS-Workloads auf dem Knoten. Dies ist erforderlich, damit EKS Pod Identity ordnungsgemäß funktioniert.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSWorker NodePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: AWSService RoleForAmazon EKSNodegroup

Sie können keine Verbindungen `AWSServiceRoleForAmazonEKSNodegroup` zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist mit einer servicegebundenen Rolle verknüpft, die es Amazon EKS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter [the section called “Serviceverknüpfte Rollenberechtigungen für Amazon EKS”](#).

Diese Richtlinie gewährt der `AWSServiceRoleForAmazonEKSNodegroup` Rolle Berechtigungen, die es ihr ermöglichen, EC2 Amazon-Knotengruppen in Ihrem Konto zu erstellen und zu verwalten.

Details zu Berechtigungen

Diese Richtlinie enthält die folgenden Berechtigungen, die es Amazon EKS ermöglichen, die folgenden Aufgaben auszuführen:

- **ec2**— Arbeiten Sie mit Sicherheitsgruppen, Tags, Kapazitätsreservierungen und Startvorlagen. Dies ist für von Amazon EKS verwaltete Knotengruppen erforderlich, um die Konfiguration des Fernzugriffs zu ermöglichen und Kapazitätsreservierungen zu beschreiben, die in verwalteten Knotengruppen verwendet werden können. Darüber hinaus erstellen von Amazon EKS verwaltete Knotengruppen in Ihrem Namen eine Startvorlage. Dies dient dazu, die Amazon EC2 Auto Scaling Scaling-Gruppe zu konfigurieren, die jede verwaltete Knotengruppe unterstützt.
- **iam**— Erstellen Sie eine serviceverknüpfte Rolle und übergeben Sie eine Rolle. Dies ist für von Amazon EKS verwaltete Knotengruppen erforderlich, um Instance-Profile für die Rolle zu verwalten, die beim Erstellen einer verwalteten Knotengruppe übergeben wird. Dieses Instance-Profil wird von EC2 Amazon-Instances verwendet, die als Teil einer verwalteten Knotengruppe gestartet wurden. Amazon EKS muss serviceverknüpfte Rollen für andere Services wie Amazon EC2 Auto Scaling Scaling-Gruppen erstellen. Diese Berechtigungen werden bei der Erstellung einer verwalteten Knotengruppe verwendet.
- **autoscaling**— Arbeiten Sie mit Sicherheits-Auto Scaling-Gruppen. Dies ist für von Amazon EKS verwaltete Knotengruppen erforderlich, um die Amazon EC2 Auto Scaling Scaling-Gruppe zu verwalten, die jede verwaltete Knotengruppe unterstützt. Es wird auch verwendet, um Funktionen

wie das Entfernen von Pods zu unterstützen, wenn Knoten beendet oder während Knotengruppen-Updates recycelt werden.

Die neueste Version des JSON-Richtliniendokuments finden Sie [AWSServiceRoleForAmazonEKSNodegroup](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon EKSDashboard ServiceRolePolicy

Sie können keine Verbindungen `AmazonEKSDashboardServiceRolePolicy` zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist mit einer servicegebundenen Rolle verknüpft, die es Amazon EKS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter [the section called “Serviceverknüpfte Rollenberechtigungen für Amazon EKS”](#).

Diese Richtlinie gewährt der `AWSServiceRoleForAmazonEKSDashboard` Rolle Berechtigungen, die es ihr ermöglichen, EC2 Amazon-Knotengruppen in Ihrem Konto zu erstellen und zu verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die den Zugriff auf die Ausführung dieser Aufgaben ermöglichen:

- **organizations**— Informationen zur Struktur und zu den Konten Ihrer AWS Organizations anzeigen. Dazu gehören Berechtigungen zum Auflisten von Konten in Ihrer Organisation, zum Anzeigen von Organisationseinheiten und Stammverzeichnissen, zum Auflisten delegierter Administratoren, zum Anzeigen von Diensten, die Zugriff auf Ihre Organisation haben, und zum Abrufen detaillierter Informationen zu Ihrer Organisation und Ihren Konten.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSDashboard ServiceRolePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: EBSCSIDriver Amazon-Richtlinie

Die `AmazonEBSCSIDriverPolicy`-Richtlinie ermöglicht es dem Amazon-EBS-Container-Storage-Interface-Treiber (CSI), Volumes in Ihrem Namen zu erstellen, zu ändern, anzuhängen, zu trennen und zu löschen. Dazu gehören das Ändern von Tags auf vorhandenen Volumes und das Aktivieren von Fast Snapshot Restore (FSR) auf EBS-Volumes. Es gewährt dem EBS-CSI-Treiber auch Berechtigungen zum Erstellen, Wiederherstellen und Löschen von Snapshots sowie zum Auflisten Ihrer Instances, Volumes und Snapshots.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EBSCSIDriver ServiceRolePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: EFSCSIDriver Amazon-Richtlinie

Die AmazonEFSCSIDriverPolicy-Richtlinie ermöglicht es dem Amazon EFS Container Storage Interface (CSI), Zugriffspunkte in Ihrem Namen zu erstellen und zu löschen. Es gewährt dem Amazon EFS CSI-Treiber auch Berechtigungen, Ihre Access Points, Dateisysteme, Mount-Ziele und EC2 Amazon-Verfügbarkeitszonen aufzulisten.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EFSCSIDriver ServiceRolePolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSLocal OutpostClusterPolicy

Sie können diese Richtlinie mit IAM-Entitäten verknüpfen. Bevor Sie einen lokalen Cluster erstellen, müssen Sie diese Richtlinie an Ihre [Clusterrolle](#) anhängen. Kubernetes-Cluster, die von Amazon EKS verwaltet werden, rufen in Ihrem Namen andere AWS Services auf. Sie tun dies, um die Ressourcen zu verwalten, die Sie mit dem Service verwenden.

Die AmazonEKSLocalOutpostClusterPolicy umfasst folgende Berechtigungen.

- **ec2**Aktionen lesen — Ermöglicht Instances der Kontrollebene, die Eigenschaften der Availability Zone, der Routing-Tabelle, der Instanz und der Netzwerkschnittstelle zu beschreiben. Erforderliche Berechtigungen für EC2 Amazon-Instances, um dem Cluster erfolgreich als Kontrollebene-Instances beizutreten.
- **ssm**— Ermöglicht Amazon EC2 Systems Manager Manager-Verbindung zur Kontrollebene-Instance, die von Amazon EKS zur Kommunikation und Verwaltung des lokalen Clusters in Ihrem Konto verwendet wird.
- **logs**— Ermöglicht Instances, Logs an Amazon zu übertragen CloudWatch.
- **secretsmanager**— Ermöglicht Instances das sichere Abrufen und Löschen von Bootstrap-Daten für die Kontrollebeneninstanzen aus AWS Secrets Manager.
- **ecr**— Ermöglicht Pods und Containern, die auf den Instances der Kontrollebene ausgeführt werden, das Abrufen von Container-Images, die in Amazon Elastic Container Registry gespeichert sind.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSLocal OutpostClusterPolicy](#) im AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: Amazon EKSLocal OutpostServiceRolePolicy

Sie können diese Richtlinie nicht an Ihre IAM-Entitäten anhängen. Wenn Sie einen Cluster mit einem IAM-Prinzipal erstellen, der über die `iam:CreateServiceLinkedRole` entsprechende Berechtigung verfügt, erstellt Amazon EKS automatisch die serviceverknüpfte [AWSServiceRoleforAmazonEKSLocalOutpost-Rolle](#) für Sie und fügt ihr diese Richtlinie hinzu. Diese Richtlinie ermöglicht es der serviceverknüpften Rolle, in Ihrem Namen AWS Dienste für lokale Cluster aufzurufen.

Die AmazonEKSLocalOutpostServiceRolePolicy umfasst folgende Berechtigungen.

- **ec2**— Ermöglicht Amazon EKS, mit Sicherheits-, Netzwerk- und anderen Ressourcen zu arbeiten, um Kontrollebeneninstanzen in Ihrem Konto erfolgreich zu starten und zu verwalten.
- **ssm, ssmmessages** — Ermöglicht Amazon EC2 Systems Manager eine Verbindung zu den Instances der Kontrollebene, die von Amazon EKS zur Kommunikation und Verwaltung des lokalen Clusters in Ihrem Konto verwendet wird.
- **iam**— Ermöglicht Amazon EKS die Verwaltung des Instance-Profils, das den Instances der Kontrollebene zugeordnet ist.
- **secretsmanager**- Ermöglicht Amazon EKS, Bootstrap-Daten für die Instances der Kontrollebene in AWS Secrets Manager zu übertragen, sodass sie beim Instance-Bootstrapping sicher referenziert werden können.
- **outposts**— Ermöglicht Amazon EKS, Outpost-Informationen von Ihrem Konto abzurufen, um erfolgreich einen lokalen Cluster in einem Outpost zu starten.

Die neueste Version des JSON-Richtliniendokuments finden Sie [bei Amazon EKSLocal OutpostServiceRolePolicy](#) im AWS Managed Policy Reference Guide.

Amazon EKS-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon EKS an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Um Benachrichtigungen über alle Änderungen an der Quelldatei auf dieser speziellen Dokumentationsseite zu erhalten, können Sie die folgende URL mit einem RSS-Reader abonnieren:

```
https://github.com/awsdocs/amazon-eks-user-guide/commits/mainline/latest/ug/security/iam-reference/security-iam-awsmanpol.adoc.atom
```

Änderung	Beschreibung	Datum
Die Erlaubnis wurde hinzugefügt für the section called “AWS verwaltete Richtlinie: Amazon EKSLocal OutpostServiceRole Policy”	ssmmessages:OpenDataChannel Erlaubnis zu hinzugefügtAmazonEKSLocalOutpostServiceRolePolicy .	26. Juni 2025
Erlaubnis zu hinzugefügt the section called “AWS verwaltete Richtlinie: EKSCompute Amazon-Richtlinie” .	Die Ressourcenberechtigungen für die ec2:RunInstances und ec2:CreateFleet Aktionen wurden aktualisiert und umfassen nun auch Kapazitätssreservierungen arn:aws:ec2:*:*:capacity-reservation/* . Dadurch kann Amazon EKS Auto Mode Instances mithilfe der EC2 On-Demand-Kapazitätssreservierungen in Ihrem Konto starten. Hinzugefügtiam:CreateServiceLinkedRole , damit Amazon EKS Auto Mode die mit dem EC2 Spot-Dienst verknüpfte Rolle in AWSServiceRoleForEC2Spot Ihrem Namen erstellen kann.	20. Juni 2025
Die Erlaubnis wurde Amazon hinzugefügt EKSServiceRolePolicy.	Es wurde die ec2:DescribeCapacityReservations Berechtigung hinzugefügt, Amazon EKS Auto Mode das Starten von Instances mithilfe der EC2 On-Demand-Kapazitätsreservi	20. Juni 2025

Änderung	Beschreibung	Datum
	erungen in Ihrem Konto zu ermöglichen.	
Eingeführt the section called “AWS verwaltete Richtlinie: Amazon EKSDashboard ConsoleReadOnly” .	Neue AmazonEKS DashboardConsoleReadOnly Richtlinie eingeführt.	19. Juni 2025
Eingeführt the section called “AWS verwaltete Richtlinie: Amazon EKSDashboard ServiceRolePolicy” .	Neue AmazonEKS DashboardServiceRolePolicy Richtlinie eingeführt.	21. Mai 2025
Berechtigungen zur EKSClusterAmazon-Richtlinie hinzugefügt.	Es wurde die <code>ec2:DeleteNetworkInterfaces</code> Berechtigung hinzugefügt, Amazon EKS das Löschen von Elastic Network-Schnittstellen zu ermöglichen, die zurückbleiben, wenn das VPC-CNI unerwartet beendet wird.	16. April 2025
Die Erlaubnis wurde Amazon hinzugefügt EKSServiceRolePolicy.	Es wurden <code>ec2:AuthorizeSecurityGroupEgress</code> Berechtigungen hinzugefügt <code>ec2:RevokeSecurityGroupEgress</code> , die es AI/ML EKS-Kunden ermöglichen, als Teil der Version EKS 1.33 Sicherheitsgruppenausgangsregeln zur standardmäßigen EKS-Cluster-SG hinzuzufügen, die mit EFA kompatibel sind.	14. April 2025

Änderung	Beschreibung	Datum
Berechtigungen für Amazon hinzugefügt EKSServiceRolePolicy.	Die Berechtigung zum Beenden von EC2 Instances, die mit EKS Auto Mode erstellt wurden, wurde hinzugefügt.	28. Februar 2025

Änderung	Beschreibung	Datum
Berechtigungen zur EBSCSIDriverAmazon-Richtlinie hinzugefügt.	Es wurde eine neue Anweisung hinzugefügt, mit der der EBS-CSI-Treiber autorisiert wird, alle Snapshots wiederherzustellen. Dies war zuvor durch die bestehende Richtlinie erlaubt, aber aufgrund einer Änderung in der Handhabung von IAM for ist eine neue ausdrückliche Anweisung erforderlich. <code>CreateVolume</code> Dem EBS-CSI-Treiber wurde die Möglichkeit hinzugefügt, Tags auf vorhandenen Volumes zu ändern. Der EBS CSI-Treiber kann Tags vorhandener Volumes über Parameter in Kubernetes ändern. <code>VolumeAttributesClasses</code> Dem EBS-CSI-Treiber wurde die Möglichkeit hinzugefügt, Fast Snapshot Restore (FSR) auf EBS-Volumes zu aktivieren. Der EBS CSI-Treiber kann FSR auf neuen Volumes über Parameter in Kubernetes-Speicherklassen aktivieren.	13. Januar 2025

Änderung	Beschreibung	Datum
Berechtigungen wurden hinzugefügt zu the section called “AWS verwaltete Richtlinie: Amazon EKSLoadBalancingPolicy” .	Aktualisiert AmazonEKS LoadBalancingPolicy, um das Auflisten und Beschreiben von Netzwerk- und IP-Adressressourcen zu ermöglichen.	26. Dezember 2024
Berechtigungen wurden hinzugefügt zu the section called “AWS verwaltete Richtlinie: AWSServiceRoleForAmazonEKSClusterPolicy” .	Aus AWSServiceRoleForAmazonEKSClusterPolicy Gründen der Kompatibilität mit China Regionen aktualisiert.	22. November 2024
Es wurden Berechtigungen hinzugefügt zu the section called “AWS verwaltete Richtlinie: Amazon EKSLocalOutpostClusterPolicy”	Es wurde eine ec2:DescribeAvailabilityZones Berechtigung hinzugefügt, AmazonEKSLocalOutpostClusterPolicy damit der AWS Cloud Controller Manager auf der Cluster-Sauerebene die Availability Zone identifizieren kann, in der sich jeder Knoten befindet.	21. November 2024

Änderung	Beschreibung	Datum
Es wurden Berechtigungen für hinzugefügt the section called “AWS verwaltete Richtlinie: AWSService RoleForAmazon EKSNodegroup” .	Die <code>AWSServiceRoleForAmazonEKSNodegroup</code> Richtlinie wurde aktualisiert, <code>ec2:RebootInstances</code> um Instances zuzulassen, die von Amazon EKS verwaltet en Knotengruppen erstellt wurden. Die <code>ec2:CreateTags</code> Berechtigungen für EC2 Amazon-Ressourcen wurden eingeschränkt.	20. November 2024
Berechtigungen wurden hinzugefügt zu the section called “AWS verwaltete Richtlinie: Amazon EKSService RolePolicy” .	EKS hat die AWS verwaltete Richtlinie aktualisiert <code>AmazonEKSServiceRolePolicy</code> . Es wurden Berechtigungen für EKS-Zugriffsrichtlinien, Load Balancer-Management und automatische Cluster-Ressourcen bereinigung hinzugefügt.	16. November 2024
Eingeführt the section called “AWS verwaltete Richtlinie: EKSService Amazon-Richtlinie” .	EKS hat die AWS verwaltete Richtlinie aktualisiert <code>AmazonEKSServiceRolePolicy</code> . Die Ressourcenerweiterungen für die <code>iam:AddRoleToInstanceProfile</code> Aktion wurden aktualisiert.	7. November 2024
Eingeführt the section called “AWS verwaltete Richtlinie: EKSService Amazon-Richtlinie” .	AWS führte die <code>AmazonEKSServiceRolePolicy</code> .	1. November 2024

Änderung	Beschreibung	Datum
Berechtigungen wurden hinzugefügt zu AmazonEKS ClusterPolicy	Es wurde die <code>ec2:DescribeInstanceTopology</code> Berechtigung hinzugefügt, damit Amazon EKS Topologieinformationen als Labels an den Knoten anhängen kann.	1. November 2024
Eingeführt the section called “AWS verwaltete Richtlinie: Amazon EKSBLOCK StoragePolicy” .	AWS führte die <code>AmazonEKSBLOCKStoragePolicy</code> .	30. Oktober 2024
Eingeführt the section called “AWS verwaltete Richtlinie: Amazon EKSLoad BalancingPolicy” .	AWS führte die <code>AmazonEKSLoadBalancingPolicy</code> .	30. Oktober 2024
Berechtigungen für Amazon hinzugefügt <code>EKSServiceRolePolicy</code> .	Es wurden <code>cloudwatch:PutMetricData</code> Berechtigungen hinzugefügt, die es Amazon EKS ermöglichen, Metriken auf Amazon zu veröffentlichen CloudWatch.	29. Oktober 2024
Eingeführt the section called “AWS verwaltete Richtlinie: EKSNetworking Amazon-Richtlinie” .	AWS führte die <code>AmazonEKSNetworkingPolicy</code> .	28. Oktober 2024
Es wurden Berechtigungen für <code>AmazonEKSServicePolicy</code> und hinzugefügt <code>AmazonEKSServiceRolePolicy</code>	Tag-Berechtigungen wurden hinzugefügt <code>ec2:GetSecurityGroupsForVpc</code> und verknüpft, damit EKS Sicherheitsgruppeninformationen lesen und zugehörige Tags aktualisieren kann.	10. Oktober 2024

Änderung	Beschreibung	Datum
Amazon eingeführt EKSWorkerNodeMinimalPolicy.	AWS führte das einAmazonEKSWorkerNodeMinimalPolicy .	3. Oktober 2024
Berechtigungen wurden hinzugefügt zu AWSServiceRoleForAmazonEKSNodegroup .	Es wurden autoscaling:SuspendProcesses Berechtigungen hinzugefügtautoscaling:ResumeProcesses , die es Amazon EKS ermöglichen, AZRebalance in Amazon EKS-verwalteten Auto Scaling Scaling-Gruppen zu unterbrechen und wieder aufzunehmen.	21. August 2024
Berechtigungen wurden hinzugefügt zu. AWSServiceRoleForAmazonEKSNodegroup	Es wurde die ec2:DescribeCapacityReservations Erlaubnis hinzugefügt, Amazon EKS zu erlauben, die Kapazitätsreservierung im Benutzerkonto zu beschreiben. Es wurde die autoscaling:PutScheduledUpdateGroupAction Berechtigung hinzugefügt, die Einstellung der geplanten Skalierung für CAPACITY_BLOCK Knotengruppen zu aktivieren.	27. Juni 2024

Änderung	Beschreibung	Datum
AmazonEKS_CNI_Policy — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat neue <code>ec2:DescribeSubnets</code> Berechtigungen hinzugefügt, damit das Amazon VPC CNI-Plugin für Kubernetes die Anzahl der freien IP-Adressen in Ihren Amazon VPC-Subnetzen sehen kann. Das VPC CNI kann die freien IP-Adressen in jedem Subnetz verwenden, um die Subnetze mit den meisten freien IP-Adressen auszuwählen, die bei der Erstellung einer elastischen Netzwerkschnittstelle verwendet werden sollen.	4. März 2024
Amazon EKSWorkerNodePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon EKS wurden neue Berechtigungen hinzugefügt, die EKS-Pod-Identitäten zulassen. Der Amazon EKS Pod Identity-Agent verwendet die Knotenrolle.	26. November 2023
Einführung der EFSCSIDriverAmazon-Richtlinie .	AWS führte die <code>AmazonEFSCSIDriverPolicy</code> .	26. Juli 2023

Änderung	Beschreibung	Datum
Berechtigungen zur EKSClusterAmazon-Richtlinie hinzugefügt.	Die <code>ec2:DescribeAvailabilityZones</code> -Berechtigung wurde hinzugefügt, damit Amazon EKS die AZ-Details während der automatischen Subnetzerkennung beim Erstellen von Load Balancern abrufen kann.	07. Februar 2023
Die Versicherungsbedingungen in den EBSCSIDriverAmazon-Richtlinien wurden aktualisiert.	Ungültige Richtlinienbedingungen mit Platzhalterzeichen im <code>StringLike</code> -Schlüselfeld wurden entfernt. Außerdem wurde eine neue Bedingung <code>ec2:ResourceTag/kubernetes.io/created-for/pvc/name: "*"</code> zu <code>ec2:DeleteVolume</code> hinzugefügt, die es dem EBS-CSI-Treiber ermöglicht, vom In-Tree-Plugin erstellte Volumes zu löschen.	17. November 2022

Änderung	Beschreibung	Datum
Berechtigungen für Amazon hinzugefügt EKSLocalOutpostServiceRolePolicy.	<code>ec2:DescribeVPCAttributes</code> , <code>ec2:GetConsoleOutput</code> und <code>ec2:DescribeSecrets</code> wurden hinzugefügt, um eine bessere Validierung der Voraussetzungen und eine bessere Kontrolle des Lebenszyklus zu ermöglichen. Außerdem wurde <code>ec2:DescribePlacementGroups</code> und hinzugefügt <code>"arn:aws:ec2:*:*:placement-group/*"</code> , <code>ec2:RunInstances</code> um die Platzierungskontrolle der EC2 Amazon-Instances auf der Kontrollebene auf Outposts zu unterstützen.	24. Oktober 2022

Änderung	Beschreibung	Datum
Aktualisieren Sie die Amazon Elastic Container Registry-Berechtigungen in Amazon EKSLocal OutpostClusterPolicy .	Die Aktion <code>ecr:GetDownloadUrlForLayer</code> wurde von allen Ressourcenschnitten in einen Bereich mit begrenztem Umfang verschoben. Ressource <code>arn:aws:ecr:*:*:repository/eks/</code> wurde hinzugefügt. Entfernen Sie die Ressource <code>arn:aws:ecr:.</code> . Diese Ressource wird durch die hinzugefügte <code>arn:aws:ecr:*:*:repository/eks/*</code> -Ressource abgedeckt.	20. Oktober 2022
Berechtigungen für Amazon hinzugefügt <code>EKSLocalOutpostClusterPolicy</code> .	Das <code>arn:aws:ecr:*:*:repository/kubelet-config-updater</code> Repository der Amazon-Elastic-Container-Registry wurde hinzugefügt, damit die Cluster-Steuerebenen-Instanzen einige kubelet-Argumente aktualisieren können.	31. August 2022
Amazon eingeführt <code>EKSLocalOutpostClusterPolicy</code> .	AWS führte das <code>einAmazonEKSLocalOutpostClusterPolicy</code> .	24. August 2022
Amazon eingeführt <code>EKSLocalOutpostServiceRolePolicy</code> .	AWS führte das <code>einAmazonEKSLocalOutpostServiceRolePolicy</code> .	23. August 2022

Änderung	Beschreibung	Datum
Einführung der EBSCSIDriverAmazon-Richtlinie .	AWS führte die einAmazonEBSCSIDriver Policy .	4. April 2022
Berechtigungen für Amazon hinzugefügt EKSWorker NodePolicy.	Hinzugefügt ec2:DescribeInstanceTypes , um Amazon EKS-Optimized zu aktivieren AMIs , das Eigenschaften auf Instance-Ebene auto erkennen kann.	21. März 2022
Berechtigungen wurden hinzugefügt zu. AWSServiceRoleForAmazonEKSNodegroup	autoscaling:EnableMetricsCollection - Berechtigung hinzugefügt, um Amazon EKS die Aktivierung der Kennzahlenerfassung zu ermöglichen.	13. Dezember 2021
Berechtigungen zur EKSClusterAmazon-Richtlinie hinzugefügt.	ec2:DescribeAccountAttributes -, ec2:DescribeAddresses - und ec2:DescribeInternetGateways -Berechtigungen hinzugefügt, damit Amazon EKS eine serviceverknüpfte Rolle für einen Network Load Balancer erstellen kann.	17. Juni 2021
Amazon EKS hat mit der Nachverfolgung von Änderungen begonnen.	Amazon EKS hat damit begonnen, Änderungen für seine AWS verwalteten Richtlinien nachzuverfolgen.	17. Juni 2021

Fehlersuche bei IAM

In diesem Thema werden einige häufige Fehler bei der Verwendung von Amazon EKS mit IAM sowie deren Lösung behandelt.

AccessDeniedException

Wenn Sie `AccessDeniedException` beim Aufrufen eines AWS API-Vorgangs eine Meldung erhalten, verfügen die von Ihnen verwendeten [IAM-Prinzipalanmeldedaten](#) nicht über die erforderlichen Berechtigungen, um diesen Aufruf durchzuführen.

```
An error occurred (AccessDeniedException) when calling the DescribeCluster operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
eks:DescribeCluster on resource: arn:aws:eks:region:111122223333:cluster/my-cluster
```

In der vorigen Beispielmeldung hat der Benutzer keine Berechtigung zum Aufruf der API-Operation `DescribeCluster` von Amazon EKS. Um einem IAM-Prinzipal Amazon-EKS-Administratorrechte zu erteilen, lesen Sie [the section called “Identitätsbasierte Richtlinien”](#).

Weitere allgemeine Informationen zu IAM finden Sie unter [Steuern des Zugriffs mit Richtlinien](#) im IAM User Guide aus.

Sie können keine Knoten auf der Registerkarte „Compute“ oder etwas anderes auf der Registerkarte „Ressourcen“ sehen und Sie erhalten eine Fehlermeldung in AWS Management Console

Möglicherweise sehen Sie eine Konsolenfehlermeldung, die folgendermaßen lautet: `Your current user or role does not have access to Kubernetes objects on this EKS cluster`. Stellen Sie sicher, dass der [IAM-Prinzipalbenutzer](#), AWS Management Console mit dem Sie den verwenden, über die erforderlichen Berechtigungen verfügt. Weitere Informationen finden Sie unter [the section called “Erforderliche Berechtigungen”](#).

Die `aws-auth-ConfigMap` gewährt keinen Zugriff auf den Cluster

Der [AWS IAM Authenticator](#) erlaubt keinen Pfad in der Rolle ARN, die in der verwendet wird. `ConfigMap` Entfernen Sie daher den Pfad, bevor Sie `rolearn` angeben. Sie können beispielsweise `arn:aws:iam::111122223333:role/team/developers/eks-admin` in `arn:aws:iam::111122223333:role/eks-admin` ändern.

Ich bin nicht berechtigt, IAM auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon EKS übergeben können.

Bei einigen AWS Diensten können Sie eine bestehende Rolle an diesen Service übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Service.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon EKS auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: {arn-aws}iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen Marys Richtlinien aktualisiert werden, damit sie die `iam:PassRole` Aktion ausführen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon EKS-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Amazon EKS diese Features unterstützt, finden Sie unter [the section called “Amazon EKS und IAM”](#).
- Informationen dazu, wie Sie den Zugriff auf Ihre Ressourcen mit Ihren AWS Konten gewähren können, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS Konto, das Sie besitzen](#).

- Informationen dazu, wie Sie AWS Konten von Drittanbietern Zugriff auf Ihre Ressourcen gewähren, finden Sie im IAM-Benutzerhandbuch [unter Zugriff auf AWS Konten, die Dritten gehören](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Pod-Container erhalten folgenden Fehler: **An error occurred (SignatureDoesNotMatch) when calling the GetCallerIdentity operation: Credential should be scoped to a valid region**

Ihre Container erhalten diesen Fehler, wenn Ihre Anwendung explizit Anfragen an den globalen AWS STS-Endpunkt (<https://sts.amazonaws>) sendet und Ihr Kubernetes-Dienstkonto für die Verwendung eines regionalen Endpunkts konfiguriert ist. Sie können das Problem mit einer der folgenden Optionen beheben:

- Aktualisieren Sie Ihren Anwendungscode, um explizite Aufrufe an den globalen AWS STS-Endpunkt zu entfernen.
- Aktualisieren Sie Ihren Anwendungscode, um explizite Anrufe an regionale Endpunkte wie <https://sts.us-west-2.amazonaws.com> zu senden. Ihre Anwendung sollte über eine integrierte Redundanz verfügen, sodass bei einem Ausfall des Dienstes in der AWS Region eine andere AWS Region ausgewählt werden kann. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [AWS STS in einer AWS Region verwalten](#).
- Konfigurieren Sie Ihre Servicekonten so, dass sie den globalen Endpunkt verwenden. Cluster verwenden standardmäßig den regionalen Endpunkt. Weitere Informationen finden Sie unter [the section called “STS-Endpunkte”](#).

Amazon-EKS-Cluster-IAM-Rolle

Für jeden Cluster ist eine Amazon EKS-Cluster-IAM-Rolle erforderlich. Von Amazon EKS verwaltete Kubernetes-Cluster verwenden diese Rolle zur Verwaltung von Knoten, und der [ältere Cloud-Anbieter](#) verwendet diese Rolle, um Load Balancer mit Elastic Load Balancing für Services zu erstellen.

Bevor Sie Amazon-EKS-Cluster erstellen können, müssen Sie eine IAM-Rolle mit einer der folgenden IAM-Richtlinien erstellen:

- [EKSClusterAmazon-Richtlinie](#)
- Eine benutzerdefinierten IAM-Richtlinie. Die folgenden Mindestberechtigungen ermöglichen es dem Kubernetes-Cluster, Knoten zu verwalten, dem [alten Cloud-Anbieter](#) jedoch nicht, Load Balancer mit Elastic Load Balancing zu erstellen. Ihre benutzerdefinierte IAM-Richtlinie muss mindestens folgende Berechtigungen haben:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "aws:TagKeys": "kubernetes.io/cluster/*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstanceTopology",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

 Note

Vor dem 3. Oktober 2023 war eine [EKSClusterAmazon-Richtlinie](#) für die IAM-Rolle für jeden Cluster erforderlich.

Vor dem 16. April 2020 waren [EKSServiceAmazon-Richtlinien](#) und [EKSClusterAmazon-Richtlinien](#) erforderlich, und der vorgeschlagene Name für die Rolle lautet `eksServiceRole`. Mit der `AWSServiceRoleForAmazonEKS` serviceverknüpften Rolle ist die [EKSServiceAmazon-Richtlinienrichtlinie](#) für Cluster, die am oder nach dem 16. April 2020 erstellt wurden, nicht mehr erforderlich.

Überprüfen, ob eine Clusterrolle vorhanden ist

Mit dem folgenden Verfahren können Sie feststellen, ob Ihr Konto bereits über die Amazon-EKS-Clusterrolle verfügt.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Suchen Sie in der Liste der Rollen nach `eksClusterRole`. Wenn eine Rolle, die Folgendes beinhaltet, nicht `eksClusterRole` existiert, finden Sie weitere Informationen [the section called "Erstellen der Amazon-EKS-Cluster-Rolle"](#) zum Erstellen der Rolle. Wenn eine Rolle mit `eksClusterRole` vorhanden ist, wählen Sie die Rolle aus, um die angefügten Richtlinien anzuzeigen.
4. Wählen Sie Permissions (Berechtigungen).
5. Stellen Sie sicher, dass die von Amazon EKSCluster Policy verwaltete Richtlinie der Rolle zugeordnet ist. Wenn die Richtlinie angefügt ist, ist Ihre Amazon-EKS-Clusterrolle korrekt konfiguriert.
6. Wählen Sie Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
7. Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält. Wenn die Vertrauensstellung mit der folgenden Richtlinie übereinstimmt, wählen Sie Cancel (Abbrechen) aus. Wenn das Vertrauensverhältnis nicht übereinstimmt, kopieren Sie die Richtlinie in das Fenster Vertrauensrichtlinie bearbeiten und wählen Sie Richtlinie aktualisieren.

```
{  
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "eks.amazonaws.com"  
    },  
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

Erstellen der Amazon-EKS-Cluster-Rolle

Sie können die AWS Management Console oder die AWS CLI verwenden, um die Clusterrolle zu erstellen.

AWS Management Console

- Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
- Wählen Sie Roles (Rollen) und anschließend Create Role (Rolle erstellen) aus.
- Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS Dienst aus.
- Wählen Sie aus der Dropdownliste Anwendungsfälle für andere AWS Dienste die Option EKS aus.
- Wählen Sie EKS - Cluster (EKS – Cluster) für Ihren Anwendungsfall und dann Next (Weiter) aus.
- Wählen Sie auf der Registerkarte Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
- Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. `eksClusterRole`.
- Geben Sie unter Description (Beschreibung) einen beschreibenden Text wie `Amazon EKS - Cluster role` ein.
- Wählen Sie Create role (Rolle erstellen) aus.

AWS CLI

- Kopieren Sie den folgenden Inhalt in eine Datei namens *cluster-trust-policy.json*.

```
{  
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "eks.amazonaws.com"  
    },  
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

- b. Erstellen Sie die -Rolle. Sie können *eksClusterRole* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
aws iam create-role \  
  --role-name eksClusterRole \  
  --assume-role-policy-document file://"cluster-trust-policy.json"
```

- c. Fügen Sie der Rolle die erforderliche IAM-Richtlinie an.

```
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy \  
  --role-name eksClusterRole
```

Amazon-EKS-Knoten-IAM-Rolle

Der Amazon EKS Node kubelet Daemon ruft in Ihrem Namen AWS APIs an. Knoten erhalten über ein IAM-Instance-Profil und zugehörige Richtlinien Berechtigungen für diese API-Aufrufe. Bevor Sie Knoten starten und in einem Cluster registrieren können, müssen Sie eine IAM-Rolle erstellen, die diese Knoten beim Start verwenden können. Diese Anforderung gilt für Knoten, die mit dem von Amazon bereitgestellten Amazon EKS-optimierten AMI oder mit einem anderen Knoten AMIs, den Sie verwenden möchten, gestartet wurden. Darüber hinaus gilt diese Anforderung sowohl für verwaltete Knotengruppen als auch für selbstverwaltete Knoten.

Note

Sie können nicht dieselbe Rolle verwenden, die zum Erstellen von Clustern verwendet wird.

Bevor Sie Knoten erstellen, müssen Sie eine IAM-Rolle mit folgenden Berechtigungen erstellen:

- Berechtigungen für kubelet die Beschreibung von EC2 Amazon-Ressourcen in der VPC, wie sie in der [EKSWorkerNodePolicyAmazon-Richtlinie](#) vorgesehen sind. Diese Richtlinie stellt auch die Berechtigungen für den Amazon EKS Pod Identity Agent bereit.
- Berechtigungen für die kubelet Verwendung von Container-Images aus Amazon Elastic Container Registry (Amazon ECR), wie sie beispielsweise in der [EC2ContainerRegistryPullOnlyAmazon-Richtlinie](#) vorgesehen sind. Die Berechtigungen zur Verwendung von Container-Images aus Amazon Elastic Container Registry (Amazon ECR) sind erforderlich, da die integrierten Add-Ons für Netzwerke Pods ausführen, die Container-Images von Amazon ECR verwenden.
- (Optional) Berechtigungen für den Amazon EKS Pod Identity Agent zum Verwenden der Aktion `eks-auth:AssumeRoleForPodIdentity`, um Anmeldeinformationen für Pods abzurufen. Wenn Sie [Amazon](#) nicht verwenden EKSWorkerNodePolicy, müssen Sie diese Genehmigung zusätzlich zu den EC2 Berechtigungen zur Verwendung von EKS Pod Identity erteilen.
- (Optional) Wenn Sie IRSA oder EKS Pod Identity nicht verwenden, um den VPC-CNI-Pods Berechtigungen zu erteilen, müssen Sie Berechtigungen für das VPC-CNI in der Instance-Rolle bereitstellen. Sie können entweder die [AmazonEKS_CNI_Policy](#) verwaltete Richtlinie (wenn Sie Ihren Cluster mit der IPv4 Familie erstellt haben) oder eine von Ihnen erstellte [IPv6 Richtlinie](#) ([wenn Sie](#) Ihren Cluster mit der Familie erstellt haben) verwenden. IPv6 Anstatt die Richtlinie jedoch an diese Rolle anzuhängen, empfehlen wir Ihnen, die Richtlinie an eine separate Rolle anzuhängen, die speziell für das Amazon VPC CNI-Add-on verwendet wird. Weitere Informationen zum Erstellen einer separaten Rolle für das Amazon VPC CNI-Add-on finden Sie unter [the section called "Für IRSA konfigurieren"](#).

Note

Die EC2 Amazon-Knotengruppen müssen eine andere IAM-Rolle als das Fargate-Profil haben. Weitere Informationen finden Sie unter [the section called "IAM-Rolle zur Pod-Ausführung"](#).

Nach einer vorhandenen Knotenrolle suchen

Mit dem folgenden Verfahren können Sie feststellen, ob Ihr Konto bereits über die Amazon-EKS-Knotenrolle verfügt.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.

2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Suchen Sie in der Liste der Rollen nach eksNodeRole, AmazonEKSNodeRole oder NodeInstanceRole. Wenn eine Rolle mit einem dieser Namen nicht existiert, finden Sie weitere Informationen [the section called “Erstellen der Amazon-EKS-Knoten-IAM-Rolle”](#) zum Erstellen der Rolle. Wenn eine Rolle mit eksNodeRole, AmazonEKSNodeRole oder NodeInstanceRole vorhanden ist, wählen Sie die Rolle aus, um die angehängten Richtlinien anzuzeigen.
4. Wählen Sie Permissions (Berechtigungen).
5. Stellen Sie sicher, dass die von Amazon EKSWorker NodePolicy und Amazon EC2 ContainerRegistryPullOnly verwalteten Richtlinien an die Rolle angehängt sind oder dass eine benutzerdefinierte Richtlinie mit den Mindestberechtigungen angehängt ist.

 Note

Wenn die AmazonEKS_CNI_Policy-Richtlinie an die Rolle angehängt ist, empfehlen wir, sie zu entfernen und einer IAM-Rolle anzuhängen, die stattdessen dem aws-node-Kubernetes-Servicekonto zugeordnet ist. Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#).

6. Wählen Sie Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
7. Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält. Wenn die Vertrauensstellung mit der folgenden Richtlinie übereinstimmt, wählen Sie Cancel (Abbrechen) aus. Wenn das Vertrauensverhältnis nicht übereinstimmt, kopieren Sie die Richtlinie in das Fenster Vertrauensrichtlinie bearbeiten und wählen Sie Richtlinie aktualisieren aus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Principal": {
        "Service": [
          "ec2.amazonaws.com"
        ]
      }
    }
  ]
}
```

```
}  
  ]  
}
```

Erstellen der Amazon-EKS-Knoten-IAM-Rolle

Sie können die Node-IAM-Rolle mit der AWS Management Console oder der AWS CLI erstellen.

AWS Management Console

- a. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
- b. Wählen Sie im linken Navigationsbereich Roles aus.
- c. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
- d. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
 - i. Wählen Sie im Abschnitt Vertrauenswürdiger Entitätstyp die Option AWS Service aus.
 - ii. Wählen Sie unter Use case (Anwendungsfall) EC2 aus.
 - iii. Wählen Sie Weiter.
- e. Führen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die folgenden Schritte aus:
 - i. Geben Sie im Feld Filter policies (Filterrichtlinien) AmazonEKSTaskRolePolicy ein.
 - ii. Aktivieren Sie EKSTaskRolePolicy in den Suchergebnissen das Kontrollkästchen links neben Amazon.
 - iii. Wählen Sie Clear filters (Filter löschen) aus.
 - iv. Geben Sie im Feld Filter policies (Filterrichtlinien) AmazonEC2ContainerRegistryPullOnly ein.
 - v. Aktivieren Sie EC2 ContainerRegistryPullOnly in den Suchergebnissen das Kontrollkästchen links neben Amazon.

Entweder die von AmazonEKS_CNI_Policy verwaltete Richtlinie oder eine von Ihnen erstellte [IPv6 Richtlinie](#) muss ebenfalls entweder dieser Rolle oder einer anderen Rolle zugewiesen werden, die dem Kubernetes-Dienstkonto zugeordnet ist. Wir empfehlen, die Richtlinie der Rolle zuzuweisen, die dem Kubernetes-Dienstkonto zugeordnet ist, anstatt sie dieser Rolle zuzuweisen. Weitere Informationen finden Sie unter [the section called "Für IRSA konfigurieren"](#).

vi. Wählen Sie Weiter.

- f. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
 - i. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. AmazonEKSTNodeRole.
 - ii. Ersetzen Sie unter Description (Beschreibung) den aktuellen Text durch beschreibenden Text wie beispielsweise Amazon EKS - Node role.
 - iii. Fügen Sie der Rolle unter Tags hinzufügen (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Markieren von IAM-Ressourcen](#) im IAM-Benutzerhandbuch.
- iv. Wählen Sie Rolle erstellen.

AWS CLI

- a. Führen Sie den folgenden Befehl aus, um die Datei node-role-trust-relationship.json zu erstellen.

```
cat >node-role-trust-relationship.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Principal": {
        "Service": [
          "ec2.amazonaws.com"
        ]
      }
    }
  ]
}
EOF
```

- b. Erstellen Sie die IAM-Rolle.

```
aws iam create-role \
  --role-name AmazonEKSTNodeRole \
```

```
--assume-role-policy-document file://"node-role-trust-relationship.json"
```

- c. Hängen Sie die beiden erforderlichen verwalteten IAM-Richtlinien an die IAM-Rolle an.

```
aws iam attach-role-policy \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSWorkerNodePolicy \  
  --role-name AmazonEKSNodeRole  
aws iam attach-role-policy \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEC2ContainerRegistryPullOnly \  
  --role-name AmazonEKSNodeRole
```

- d. Hängen Sie eine der folgenden IAM-Richtlinien an die IAM-Rolle an, je nachdem, mit welcher IP-Familie Sie Ihren Cluster erstellt haben. Die Richtlinie muss dieser Rolle oder einer Rolle zugeordnet sein, die dem aws-node Kubernetes-Servicekonto zugeordnet ist, das für das Amazon VPC CNI-Plugin für Kubernetes verwendet wird. Wir empfehlen, die Richtlinie der Rolle zuzuweisen, die dem Kubernetes-Servicekonto zugeordnet ist. Um die Richtlinie der Rolle zuzuweisen, die dem Kubernetes-Servicekonto zugeordnet ist, siehe [the section called “Für IRSA konfigurieren”](#).

- IPv4

```
aws iam attach-role-policy \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKS_CNI_Policy \  
  --role-name AmazonEKSNodeRole
```

- IPv6

- A. Kopieren Sie den folgenden Text und speichern Sie ihn in einer Datei mit dem Namen `vpc-cni-ipv6-policy.json`.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2:AssignIpv6Addresses",  
        "ec2:DescribeInstances",  
        "ec2:DescribeTags",  
        "ec2:DescribeNetworkInterfaces",  
        "ec2:DescribeInstanceTypes"  
      ],  
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

B. Erstellen Sie die IAM-Richtlinie.

```
aws iam create-policy --policy-name AmazonEKS_CNI_IPv6_Policy --policy-document file://vpc-cni-ipv6-policy.json
```

C. Fügen Sie die IAM-Richtlinie an die IAM-Rolle an. Ersetzen Sie **111122223333** durch Ihre Konto-ID.

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::111122223333:policy/AmazonEKS_CNI_IPv6_Policy \
  --role-name AmazonEKSNodeRole
```

Cluster-IAM-Rolle für Amazon EKS Auto Mode

Für jeden Cluster ist eine Amazon EKS-Cluster-IAM-Rolle erforderlich. Von Amazon EKS verwaltete Kubernetes-Cluster verwenden diese Rolle, um Routineaufgaben für Speicher, Netzwerke und automatische Rechenskalierung zu automatisieren.

Bevor Sie Amazon EKS-Cluster erstellen können, müssen Sie eine IAM-Rolle mit den für den automatischen Modus von EKS erforderlichen Richtlinien erstellen. Sie können entweder die vorgeschlagenen AWS IAM-verwalteten Richtlinien anhängen oder benutzerdefinierte Richtlinien mit entsprechenden Berechtigungen erstellen.

- [EKSCoordinateAmazon-Richtlinie](#)
- [AmazonEKSBLOCKStoragePolicy](#)
- [AmazonEKSLoadBalancingPolicy](#)

- [EKSNetworkingAmazon-Richtlinie](#)
- [EKSClusterAmazon-Richtlinie](#)

Überprüfen, ob eine Clusterrolle vorhanden ist

Mit dem folgenden Verfahren können Sie feststellen, ob Ihr Konto bereits über die Amazon-EKS-Clusterrolle verfügt.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Suchen Sie in der Liste der Rollen nach AmazonEKSAutoClusterRole. Wenn eine Rolle, die Folgendes beinhaltet, nicht AmazonEKSAutoClusterRole existiert, lesen Sie die Anweisungen im nächsten Abschnitt, um die Rolle zu erstellen. Wenn eine Rolle mit AmazonEKSAutoClusterRole vorhanden ist, wählen Sie die Rolle aus, um die angefügten Richtlinien anzuzeigen.
4. Wählen Sie Permissions (Berechtigungen).
5. Stellen Sie sicher, dass die von Amazon EKSCluster Policy verwaltete Richtlinie der Rolle zugeordnet ist. Wenn die Richtlinie angefügt ist, ist Ihre Amazon-EKS-Clusterrolle korrekt konfiguriert.
6. Wählen Sie Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
7. Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält. Wenn die Vertrauensstellung mit der folgenden Richtlinie übereinstimmt, wählen Sie Cancel (Abbrechen) aus. Wenn das Vertrauensverhältnis nicht übereinstimmt, kopieren Sie die Richtlinie in das Fenster Vertrauensrichtlinie bearbeiten und wählen Sie Richtlinie aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

```
    ]  
  }  
]  
}
```

 Note

AWS benötigt den Namen `AmazonEKSAutoClusterRole` für diese Rolle nicht.

Erstellen der Amazon-EKS-Cluster-Rolle

Sie können die AWS Management Console oder die AWS CLI verwenden, um die Clusterrolle zu erstellen.

AWS Management Console

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie Roles (Rollen) und anschließend Create Role (Rolle erstellen) aus.
3. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS Dienst aus.
4. Wählen Sie aus der Dropdownliste Anwendungsfälle für andere AWS Dienste die Option EKS aus.
5. Wählen Sie EKS - Cluster (EKS – Cluster) für Ihren Anwendungsfall und dann Next (Weiter) aus.
6. Wählen Sie auf der Registerkarte Berechtigungen hinzufügen die Richtlinien aus und klicken Sie dann auf Weiter.
 - [EKSCComputeAmazon-Richtlinie](#)
 - [AmazonEKSBLOCKStoragePolicy](#)
 - [AmazonEKSLoadBalancingPolicy](#)
 - [EKSNetworkingAmazon-Richtlinie](#)
 - [EKSClusterAmazon-Richtlinie](#)
7. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. `AmazonEKSAutoClusterRole`.
8. Geben Sie unter Description (Beschreibung) einen beschreibenden Text wie Amazon EKS - Cluster role ein.
9. Wählen Sie Rolle erstellen aus.

AWS CLI

1. Kopieren Sie den folgenden Inhalt in eine Datei namens *cluster-trust-policy.json*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

2. Erstellen Sie die -Rolle. Sie können *AmazonEKSAutoClusterRole* mit einem beliebigen Namen ersetzen, den Sie wählen.

```
aws iam create-role \
  --role-name AmazonEKSAutoClusterRole \
  --assume-role-policy-document file://cluster-trust-policy.json
```

3. Hängen Sie die erforderlichen IAM-Richtlinien an die Rolle an:

EKSClusterAmazon-Richtlinie:

```
aws iam attach-role-policy \
  --role-name AmazonEKSAutoClusterRole \
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
```

EKSComputeAmazon-Richtlinie:

```
aws iam attach-role-policy \
  --role-name AmazonEKSAutoClusterRole \
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSComputePolicy
```

Amazon EKSBLOCK StoragePolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSBLOCKStoragePolicy
```

Amazon EKSLoad BalancingPolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSLoadBalancingPolicy
```

EKSNetworkingAmazon-Richtlinie:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoClusterRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSNetworkingPolicy
```

IAM-Rolle für Knoten im automatischen Modus von Amazon EKS

Note

Sie können nicht dieselbe Rolle verwenden, die zum Erstellen von Clustern verwendet wird.

Bevor Sie Knoten erstellen, müssen Sie eine IAM-Rolle mit den folgenden Richtlinien oder gleichwertigen Berechtigungen erstellen:

- [AmazonEKSWorkerNodeMinimalPolicy](#)
- [AmazonEC2ContainerRegistryPullOnly](#)

Nach einer vorhandenen Knotenrolle suchen

Mit dem folgenden Verfahren können Sie feststellen, ob Ihr Konto bereits über die Amazon-EKS-Knotenrolle verfügt.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.

3. Suchen Sie in der Liste der Rollen nach `AmazonEKSAutoNodeRole`. Wenn eine Rolle mit einem dieser Namen nicht existiert, lesen Sie die Anweisungen im nächsten Abschnitt, um die Rolle zu erstellen. Wenn eine Rolle mit `AmazonEKSAutoNodeRole` vorhanden ist, wählen Sie die Rolle aus, um die angehängten Richtlinien anzuzeigen.
4. Wählen Sie Permissions (Berechtigungen).
5. Stellen Sie sicher, dass die oben genannten erforderlichen Richtlinien oder entsprechende benutzerdefinierte Richtlinien angehängt sind.
6. Wählen Sie Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
7. Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält. Wenn die Vertrauensstellung mit der folgenden Richtlinie übereinstimmt, wählen Sie Cancel (Abbrechen) aus. Wenn die Vertrauensstellung nicht übereinstimmt, kopieren Sie die Richtlinie in das Fenster Vertrauensrichtlinie bearbeiten und wählen Sie Richtlinie aktualisieren aus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Erstellen der Amazon-EKS-Knoten-IAM-Rolle

Sie können die Node-IAM-Rolle mit der AWS Management Console oder der AWS CLI erstellen.

AWS Management Console

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Klicken Sie auf der Seite Roles (Rollen) auf Create role (Rolle erstellen).
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:

- a. Wählen Sie im Abschnitt Vertrauenswürdiger Entitätstyp die Option AWS Service aus.
 - b. Wählen Sie unter Use case (Anwendungsfall) EC2 aus.
 - c. Wählen Sie Weiter aus.
5. Fügen Sie auf der Seite „Berechtigungen hinzufügen“ die folgenden Richtlinien hinzu:
- [AmazonEKSWorkerNodeMinimalPolicy](#)
 - [AmazonEC2ContainerRegistryPullOnly](#)
6. Gehen Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) wie folgt vor:
- a. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. AmazonEKSAutoNodeRole.
 - b. Ersetzen Sie unter Description (Beschreibung) den aktuellen Text durch beschreibenden Text wie beispielsweise Amazon EKS - Node role.
 - c. Fügen Sie der Rolle unter Tags hinzufügen (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Markieren von IAM-Ressourcen](#) im IAM-Benutzerhandbuch.
 - d. Wählen Sie Rolle erstellen aus.

AWS CLI

Erstellen Sie die Node-IAM-Rolle

Verwenden Sie die node-trust-policyJSON-Datei aus dem vorherigen Schritt, um zu definieren, welche Entitäten die Rolle übernehmen können. Führen Sie den folgenden Befehl aus, um die Node-IAM-Rolle zu erstellen:

```
aws iam create-role \
  --role-name AmazonEKSAutoNodeRole \
  --assume-role-policy-document file://node-trust-policy.json
```

Notieren Sie sich die Rolle ARN

Rufen Sie nach dem Erstellen der Rolle den ARN der Node-IAM-Rolle ab und speichern Sie ihn. Sie benötigen diesen ARN in den nachfolgenden Schritten. Verwenden Sie den folgenden Befehl, um den ARN abzurufen:

```
aws iam get-role --role-name AmazonEKSAutoNodeRole --query "Role.Arn" --output text
```

Erforderliche Richtlinien anhängen

Fügen Sie der Node-IAM-Rolle die folgenden AWS verwalteten Richtlinien hinzu, um die erforderlichen Berechtigungen bereitzustellen:

So hängen Sie Amazon an EKSWorkerNodeMinimalPolicy:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoNodeRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy
```

So hängen Sie Amazon an EC2ContainerRegistryPullOnly:

```
aws iam attach-role-policy \  
  --role-name AmazonEKSAutoNodeRole \  
  --policy-arn arn:aws: iam::aws:policy/AmazonEC2ContainerRegistryPullOnly
```

Überwachen Sie die Leistung Ihres Clusters und sehen Sie sich Logs an

Sie können Ihre Daten in Amazon EKS mit vielen verfügbaren Überwachungs- oder Protokollierungstools beobachten. Ihre Amazon EKS-Protokolldaten können an AWS Services oder Partner-Tools zur Datenanalyse gestreamt werden. In der sind viele Dienste verfügbar AWS Management Console , die Daten zur Behebung Ihrer Amazon EKS-Probleme bereitstellen. Sie können auch eine AWS-unterstützte Open-Source-Lösung für die [Überwachung der Amazon EKS-Infrastruktur](#) verwenden.

Nachdem Sie im linken Navigationsbereich der Amazon EKS-Konsole Cluster ausgewählt haben, können Sie den Zustand und die Details des Clusters anzeigen, indem Sie den Namen Ihres Clusters und dann die Registerkarte Observability auswählen. Informationen zu vorhandenen Kubernetes-Ressourcen, die in Ihrem Cluster bereitgestellt werden, finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#).

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon EKS und Ihren AWS Lösungen. Wir empfehlen Ihnen, Überwachungsdaten aus allen Teilen Ihrer AWS Lösung zu sammeln. Auf diese Weise können Sie Ausfälle, die sich über mehrere Punkte erstrecken, leichter debuggen. Bevor Sie mit der Überwachung von Amazon EKS beginnen, sollten Sie sicherstellen, dass für Ihren Überwachungsplan folgende Fragen beantwortet sind.

- Was sind Ihre Ziele? Benötigen Sie Echtzeit-Benachrichtigungen, wenn Ihre Cluster drastisch skaliert werden?
- Welche Ressourcen müssen beachtet werden?
- Wie oft müssen Sie diese Ressourcen beobachten? Muss Ihr Unternehmen schnell auf Risiken reagieren?
- Welche Tools möchten Sie verwenden? Wenn Sie AWS Fargate bereits als Teil Ihres Starts ausführen, können Sie den integrierten [Log-Router](#) verwenden.
- Wen beabsichtigen Sie, die Überwachungsaufgaben auszuführen?
- An wen sollen Benachrichtigungen gesendet werden, wenn etwas schief geht?

Überwachung und Protokollierung auf Amazon EKS

Amazon EKS bietet integrierte Tools für die Überwachung und Protokollierung. Bei unterstützten Versionen bietet das Observability-Dashboard Einblick in die Leistung Ihres Clusters. Es hilft Ihnen, Probleme schnell zu erkennen, zu beheben und zu beheben. Zusätzlich zu den Überwachungsfunktionen enthält es Listen, die auf den Auditprotokollen der Kontrollebene basieren. Die Kubernetes-Steuerebene stellt eine Reihe von Metriken zur Verfügung, die auch außerhalb der Konsole abgerufen werden können.

Die Protokollierung der Steuerebene zeichnet alle API-Aufrufe zu Ihren Clustern. Diese enthält Überwachungsinformationen darüber, welche Benutzer welche Aktionen an Ihren Clustern durchgeführt haben, sowie rollenbasierte Informationen. Weitere Informationen finden Sie unter [Protokollierung und Überwachung auf Amazon EKS](#) in den AWS präskriptiven Leitlinien.

Die Protokollierung auf der Amazon EKS-Kontrollebene stellt Prüf- und Diagnoseprotokolle direkt von der Amazon EKS-Steuerebene zu den CloudWatch Protokollen in Ihrem Konto bereit. Diese Protokolle erleichtern Ihnen die Absicherung und Ausführung Ihrer Cluster. Sie können genau die Protokolltypen auswählen, die Sie benötigen, und die Protokolle werden als Protokollstreams an eine Gruppe für jeden Amazon EKS-Cluster gesendet CloudWatch. Weitere Informationen finden Sie unter [the section called "Protokolle der Kontrollebene"](#).

Note

Wenn Sie die Amazon EKS-Authentifikatorprotokolle in Amazon überprüfen CloudWatch, werden die Einträge angezeigt, die Text enthalten, der dem folgenden Beispieltext ähnelt.

```
level=info msg="mapping IAM role" groups="[]" role="arn:aws:iam::111122223333:role/XXXXXXXXXXXXXXXXXXXX-NodeManagerRole-XXXXXXXX"
username="eks:node-manager"
```

Einträge, die diesen Text enthalten, werden erwartet. Das username ist eine interne Amazon EKS-Servicerolle, die bestimmte Vorgänge für verwaltete Knotengruppen und Fargate ausführt.

Für eine detaillierte, anpassbare Protokollierung ist [Kubernetes-Protokollierung](#) verfügbar.

Amazon EKS ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon EKS ausgeführt

wurden. CloudTrail erfasst alle API-Aufrufe für Amazon EKS als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon-EKS-Konsole und Code-Aufrufe der Amazon-EKS-API-Operationen. Weitere Informationen finden Sie unter [the section called “AWS CloudTrail”](#).

Der Kubernetes-API-Server stellt eine Reihe von Metriken zur Verfügung, die für die Überwachung und Analyse hilfreich sind. Weitere Informationen finden Sie unter [the section called “Prometheus-Metriken”](#).

Informationen zur Konfiguration von Fluent Bit für benutzerdefinierte CloudWatch Amazon-Protokolle finden Sie unter [Fluent Bit einrichten](#) im CloudWatch Amazon-Benutzerhandbuch.

Überwachungs- und Protokollierungstools von Amazon EKS

Amazon Web Services bietet verschiedene Tools, mit deren Hilfe Sie Amazon EKS überwachen können. Sie können einige Tools konfigurieren, um eine automatische Überwachung einzurichten, einige erfordern jedoch manuelle Anrufe. Wir empfehlen, dass Sie Überwachungsaufgaben so weit automatisieren, wie es Ihre Umgebung und Ihr vorhandenes Toolset zulassen.

In der folgenden Tabelle werden verschiedene Optionen für Überwachungstools beschrieben.

Bereiche	Tool	Beschreibung	Aufstellen
Steuerebene	Dashboard zur Beobachtbarkeit	Bei unterstützten Versionen bietet das Observability-Dashboard Einblick in die Leistung Ihres Clusters. Es hilft Ihnen, Probleme schnell zu erkennen, zu beheben und zu beheben.	Einrichtungsverfahren
Anwendungen/Steuerungsebene	Prometheus	Prometheus kann zur Überwachung von Metriken und Warnmeldungen für Anwendungen und	Einrichtungsverfahren

Bereiche	Tool	Beschreibung	Aufstellen
		die Steuerungsebene verwendet werden.	
Anwendungen	CloudWatch Container Insights	CloudWatch Container Insights sammelt, aggregiert und fasst Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices zusammen.	Einrichtungsverfahren
Anwendungen	AWS Distribution für (ADOT) OpenTelemetry	ADOT kann korrelierte Metriken, Rückverfolgungsdaten und Metadaten sammeln und an AWS Überwachungsdienste oder Partner senden. Es kann über CloudWatch Container Insights eingerichtet werden.	Einrichtungsverfahren
Anwendungen	DevOpsAmazon-Guru	Amazon DevOps Guru erkennt die Betriebsleistung und Verfügbarkeit auf Knotenebene.	Einrichtungsverfahren

Bereiche	Tool	Beschreibung	Aufstellen
Anwendungen	AWS X-Ray	AWS X-Ray empfängt Trace-Daten über Ihre Anwendung. Diese Trace-Daten enthalten ein- und ausgehende Anfragen und Metadaten zu diesen. Für Amazon EKS ist für die Implementierung das OpenTelemetry Add-on erforderlich.	Einrichtungsverfahren
Anwendungen	Amazon CloudWatch	CloudWatch stellt einige grundlegende Amazon EKS-Metriken in unterstützten Versionen kostenlos zur Verfügung. Sie können diese Funktionalität mit dem CloudWatch Observability Operator erweitern, um das Sammeln von Metriken, Protokollen und Trace-Daten zu verwalten.	Einrichtungsverfahren

In der folgenden Tabelle werden verschiedene Optionen des Logging-Tools beschrieben.

Bereiche	Tool	Beschreibung	Aufstellen
Steuerebene	Dashboard zur Beobachtbarkeit	Für unterstützte Versionen zeigt das Observability-Dashboard Listen an, die auf den Auditprotokollen der Kontrollebene basieren. Es enthält auch Links zu Protokollen von Kontrollflugzeugen bei Amazon CloudWatch.	Einrichtungsverfahren
Anwendungen	Einblicke in Amazon CloudWatch Container	Amazon CloudWatch Container Insights sammelt, aggregiert und fasst Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices zusammen.	Einrichtungsverfahren
Steuerebene	CloudWatch Amazon-Protokolle	Sie können Prüf- und Diagnoseprotokolle direkt von der Amazon EKS-Steuerebene an die CloudWatch Protokolle in Ihrem Konto senden.	Einrichtungsverfahren
Steuerebene	AWS CloudTrail	Protokolliert API-Aufrufe eines Benutzers, einer Rolle oder eines Service.	Einrichtungsverfahren

Bereiche	Tool	Beschreibung	Aufstellen
Mehrere Bereiche für AWS Fargate-Instanzen	AWS Fargate-Protokollrouter	Bei AWS Fargate-Instances streamt der Log-Router Logs an AWS Dienste oder Partner-Tools. Es wird AWS für Fluent Bit verwendet. Protokolle können an andere AWS Dienste oder Partner-Tools gestreamt werden.	Einrichtungsverfahren

Überwachen Sie Ihren Cluster mit dem Observability-Dashboard

Die Amazon EKS-Konsole umfasst ein Observability-Dashboard, das einen Überblick über die Leistung Ihres Clusters bietet. Die bereitgestellten Informationen helfen Ihnen dabei, Probleme schnell zu erkennen, zu beheben und zu beheben. Sie können den entsprechenden Abschnitt des Observability-Dashboards öffnen, indem Sie ein Element in der Health and Performance Summary auswählen. Diese Zusammenfassung ist an mehreren Stellen enthalten, unter anderem auf der Registerkarte Beobachtbarkeit.

Das Observability-Dashboard ist in mehrere Tabs aufgeteilt.

Übersicht

In der Health- und Leistungsübersicht ist die Anzahl der Artikel in verschiedenen Kategorien aufgeführt. Jede Zahl fungiert als Hyperlink zu einer Stelle im Observability-Dashboard mit einer Liste für diese Kategorie.

Zustand des Clusters

Der Clusterstatus enthält wichtige Benachrichtigungen, auf die Sie achten sollten. Bei einigen dieser Benachrichtigungen müssen Sie möglicherweise so schnell wie möglich Maßnahmen ergreifen. In dieser Liste finden Sie Beschreibungen und die betroffenen Ressourcen. Der Clusterstatus umfasst zwei Tabellen: Integritätsprobleme und Einblicke in die Konfiguration. Um den Status

von Gesundheitsproblemen zu aktualisieren, wählen Sie die Schaltfläche „Aktualisieren“ (↻). Configuration Insights werden automatisch alle 24 Stunden aktualisiert und können nicht manuell aktualisiert werden.

Weitere Informationen zu Gesundheitsproblemen finden Sie unter [the section called “FAQs Cluster-Integritäts- und Fehlercodes mit Lösungspfaden”](#). Weitere Informationen zu Configuration Insights finden Sie unter [the section called “Cluster-Erkenntnisse”](#).

Überwachung der Steuerungsebene

Die Registerkarte „Überwachung der Kontrollebene“ ist in drei Abschnitte unterteilt, von denen jeder Ihnen hilft, die Steuerungsebene Ihres Clusters zu überwachen und Fehler zu beheben.

Metriken

Für Cluster mit Kubernetes-Version 1.28 und höher zeigt der Abschnitt Metriken Diagramme verschiedener Metriken, die für verschiedene Komponenten der Kontrollebene gesammelt wurden.

Sie können den Zeitraum festlegen, der von der X-Achse jedes Diagramms verwendet wird, indem Sie oben im Abschnitt eine Auswahl treffen. Sie können Daten mit der Aktualisierungstaste (↻) aktualisieren. Für jedes einzelne Diagramm öffnet die Schaltfläche mit den vertikalen Ellipsen (⋮) ein Menü mit Optionen von CloudWatch.

Diese und weitere Metriken sind automatisch als grundlegende Überwachungsmetriken CloudWatch unter dem AWS/EKS Namespace verfügbar. Weitere Informationen finden Sie unter [Grundlegende Überwachung und detaillierte Überwachung](#) im CloudWatch Amazon-Benutzerhandbuch. Ausführlichere Metriken, Visualisierungen und Einblicke finden Sie unter [Container Insights](#) im CloudWatch Amazon-Benutzerhandbuch. Oder wenn Sie eine Überwachung auf Prometheus-Basis bevorzugen, finden Sie weitere Informationen unter [the section called “Prometheus-Metriken”](#).

In der folgenden Tabelle werden die verfügbaren Metriken beschrieben.

Metrik	Beschreibung
APIServer Anfragen	Die Anfragen pro Minute an den API-Server.
APIServer Gesamtzahl der Anfragen 4XX	Die Anzahl der API-Serveranfragen pro Minute mit HTTP 4XX-Antwortcodes (clientseitige Fehler).

Metrik	Beschreibung
APIServer Gesamtzahl der Anfragen: 5XX	Die Anzahl der API-Serveranfragen pro Minute mit HTTP 5XX-Antwortcodes (serverseitige Fehler).
APIServer Anfragen insgesamt 429	Die Anzahl der API-Serveranfragen pro Minute mit HTTP-429-Antwortcodes (zu viele Anfragen).
Speichergröße	Die Größe der Speicherdatenbank (etcd).
Der Scheduler versucht	Die Anzahl der Versuche, Pods nach den Ergebnissen „nicht planbar“, „Fehler“ und „geplant“ zu planen.
Ausstehende Pods	Die Anzahl der ausstehenden Pods nach Warteschlangenart „aktiv“, „geblockt“, „nicht planbar“ und „gesperrt“.
Latenz bei API-Serveranfragen	Die Latenz für API-Serveranfragen.
Aktuelle eingehende Anfragen des API-Servers	Die aktuellen laufenden Anfragen für den API-Server.
Webhook-Anfragen	Die Webhook-Anfragen pro Minute.
Ablehnungen von Webhook-Anfragen	Die Anzahl der Webhook-Anfragen, die abgelehnt wurden.
Latenz bei Webhook-Anfragen: P99.	Das 99. Perzentil der Latenz externer Webhook-Anfragen von Drittanbietern.

CloudWatch Einblicke protokollieren

Im Abschnitt CloudWatch Log Insights werden verschiedene Listen angezeigt, die auf den Auditprotokollen der Kontrollebene basieren. Die Amazon EKS-Steuerebenenprotokolle müssen aktiviert sein, um diese Funktion nutzen zu können. Dies können Sie im CloudWatch Abschnitt Kontrollebenenprotokolle anzeigen im tun.

Wenn genügend Zeit verstrichen ist, um Daten zu sammeln, können Sie alle Abfragen ausführen oder die Option Abfrage für jeweils eine einzelne Liste ausführen auswählen. Jedes Mal, CloudWatch wenn Sie Abfragen ausführen, fallen zusätzliche Kosten an. Wählen Sie oben im Abschnitt den Zeitraum aus, für den die Ergebnisse angezeigt werden sollen. Wenn Sie eine erweiterte Steuerung für eine Abfrage wünschen, können Sie „Ansicht in“ wählen CloudWatch. Auf diese Weise können Sie eine Abfrage CloudWatch an Ihre Bedürfnisse anpassen.

Weitere Informationen finden Sie unter [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

Logs auf der Kontrollebene anzeigen CloudWatch

Wählen Sie Protokollierung verwalten, um die verfügbaren Protokolltypen zu aktualisieren. Es dauert mehrere Minuten, bis die Protokolle nach der Aktivierung der CloudWatch Protokollierung in den Protokollen angezeigt werden. Wenn genügend Zeit verstrichen ist, klicken Sie auf einen der Links „Anzeigen“ in diesem Abschnitt, um zum entsprechenden Protokoll zu gelangen.

Weitere Informationen finden Sie unter [the section called “Protokolle der Kontrollebene”](#).

Cluster-Erkenntnisse

In der Tabelle mit den Upgrade-Erkenntnissen werden sowohl Probleme aufgedeckt als auch Korrekturmaßnahmen empfohlen, wodurch der Validierungsprozess für Upgrades auf neue Kubernetes-Versionen beschleunigt wird. Amazon EKS scannt Cluster automatisch anhand einer Liste potenzieller Probleme beim Upgrade der Kubernetes-Version. In der Tabelle mit den Upgrade-Erkenntnissen werden die von Amazon EKS anhand dieses Clusters durchgeführten Insight-Checks zusammen mit den zugehörigen Status aufgeführt.

Amazon EKS verwaltet und aktualisiert regelmäßig die Liste der durchzuführenden Insight-Checks auf der Grundlage von Bewertungen von Änderungen im Kubernetes-Projekt sowie Amazon EKS-Serviceänderungen im Zusammenhang mit neuen Versionen. Die Amazon EKS-Konsole aktualisiert automatisch den Status jedes Insights, der in der Spalte „Zeit der letzten Aktualisierung“ angezeigt wird.

Weitere Informationen finden Sie unter [the section called “Cluster-Erkenntnisse”](#).

Probleme mit dem Zustand des Knotens

Der Amazon EKS Node Monitoring Agent liest automatisch Knotenprotokolle, um Gesundheitsprobleme zu erkennen. Unabhängig von der Einstellung für die auto Reparatur werden

alle Probleme mit dem Zustand des Knotens gemeldet, sodass Sie sie bei Bedarf untersuchen können. Wenn ein Problemtyp ohne Beschreibung aufgeführt ist, können Sie die Beschreibung in seinem Popover-Element nachlesen.

Wenn Sie die Seite aktualisieren, verschwinden alle gelösten Probleme aus der Liste. Wenn die auto Reparatur aktiviert ist, können vorübergehend einige Gesundheitsprobleme auftreten, die ohne Ihr Zutun behoben werden. Probleme, die von der auto Reparatur nicht unterstützt werden, erfordern je nach Typ möglicherweise manuelle Maßnahmen von Ihnen.

Damit Probleme mit dem Knotenstatus gemeldet werden können, muss Ihr Cluster den Amazon EKS Auto Mode verwenden oder über das Node Monitoring Agent Add-on verfügen. Weitere Informationen finden Sie unter [the section called “Zustand des Knotens”](#).

Überwachen Sie Ihre Cluster-Metriken mit Prometheus

[Prometheus](#) ist eine Überwachungs- und Zeitreihendatenbank, die Endpunkte scrapiert. Sie bietet die Möglichkeit, gesammelte Daten abzufragen, zu aggregieren und zu speichern. Sie können sie auch für Warnungen und für die Aggregation von Warnungen verwenden. In diesem Thema wird erklärt, wie Sie Prometheus entweder als verwaltete oder als Open-Source-Option einrichten. Die Überwachung der Metriken der Amazon-EKS-Steuerebene ist ein häufiger Anwendungsfall.

Amazon Managed Service for Prometheus ist ein Prometheus-kompatibler Überwachungs- und Warndienst, der es einfach macht, containerisierte Anwendungen und Infrastruktur im großen Maßstab zu überwachen. Es ist ein vollständig verwalteter Service, der die Aufnahme, Speicherung, Abfrage und Warnung Ihrer Metriken automatisch skaliert. Es lässt sich auch in AWS Sicherheitsdienste integrieren, um einen schnellen und sicheren Zugriff auf Ihre Daten zu ermöglichen. Sie können die Open-Source-PromQL-Abfragesprache verwenden, um Ihre Metriken abzufragen und darauf zu warnen. Außerdem können Sie den Alert Manager in Amazon Managed Service for Prometheus verwenden, um Warnregeln für kritische Alerts einzurichten. Sie können diese kritischen Benachrichtigungen dann als Benachrichtigungen an ein Amazon SNS SNS-Thema senden.

Es gibt verschiedene Optionen für die Verwendung von Prometheus mit Amazon EKS:

- Sie können Prometheus-Metriken aktivieren, wenn Sie zum ersten Mal einen Amazon EKS-Cluster erstellen, oder Sie können Ihren eigenen Prometheus-Scraper für bestehende Cluster erstellen. Beide Optionen werden in diesem Thema behandelt.
- Sie können Prometheus mit Helm einsetzen. Weitere Informationen finden Sie unter [the section called “Mit Helm bereitstellen”](#).

- Sie können Rohmetriken der Kontrollebene im Prometheus-Format anzeigen. Weitere Informationen finden Sie unter [the section called “Steuerebene”](#).

Schritt 1: Prometheus-Metriken aktivieren

Important

Die Ressourcen von Amazon Managed Service for Prometheus befinden sich außerhalb des Cluster-Lebenszyklus und müssen unabhängig vom Cluster verwaltet werden. Wenn Sie Ihren Cluster löschen, stellen Sie sicher, dass Sie auch alle entsprechenden Scraper löschen, um die anfallenden Kosten zu stoppen. Weitere Informationen [finden Sie unter Suchen und Löschen von Scrapern](#) im Amazon Managed Service for Prometheus Benutzerhandbuch.

Prometheus erkennt und sammelt Metriken aus Ihrem Cluster mithilfe eines Pull-basierten Modells namens Scraping. Scraper sind dafür eingerichtet, Daten aus Ihrer Cluster-Infrastruktur und containerisierten Anwendungen zu sammeln. Wenn Sie die Option zum Senden von Prometheus-Metriken aktivieren, bietet Amazon Managed Service for Prometheus einen vollständig verwalteten Scraper ohne Agenten.

Wenn Sie den Cluster noch nicht erstellt haben, können Sie bei der ersten Erstellung des Clusters die Option zum Senden von Metriken an Prometheus aktivieren. In der Amazon EKS-Konsole befindet sich diese Option im Schritt Observability konfigurieren beim Erstellen eines neuen Clusters. Weitere Informationen finden Sie unter [the section called “Erstellen eines -Clusters”](#).

Wenn Sie bereits über einen vorhandenen Cluster verfügen, können Sie Ihren eigenen Prometheus-Scraper erstellen. Navigieren Sie dazu in der Amazon EKS-Konsole zur Registerkarte Observability Ihres Clusters und wählen Sie die Schaltfläche Scraper hinzufügen. Wenn Sie dies lieber mit der AWS API oder AWS CLI tun möchten, finden Sie weitere Informationen unter [Create a Scraper](#) im Amazon Managed Service for Prometheus User Guide.

Die folgenden Optionen sind verfügbar, wenn Sie den Scraper mit der Amazon EKS-Konsole erstellen.

Scraper-Alias

(Optional) Geben Sie einen eindeutigen Alias für den Scraper ein.

Zieladresse

Wählen Sie einen Workspace für Amazon Managed Service für Prometheus aus. Ein Workspace ist ein logischer Bereich, der der Speicherung und Abfrage von Prometheus-Metriken gewidmet ist. In diesem Arbeitsbereich können Sie die Prometheus-Metriken aller Konten einsehen, die Zugriff darauf haben. Die Option **Neuen Workspace erstellen** weist Amazon EKS an, unter Verwendung des von Ihnen angegebenen Workspace-Alias einen Workspace in Ihrem Namen zu erstellen. Mit der Option **Bestehenden Workspace auswählen** können Sie einen vorhandenen Workspace aus einer Dropdown-Liste auswählen. Weitere Informationen zu Workspaces finden Sie unter [Workspaces verwalten](#) im Benutzerhandbuch von Amazon Managed Service für Prometheus.

Zugriff auf den Service

In diesem Abschnitt werden die Berechtigungen zusammengefasst, die Sie beim Senden von Prometheus-Metriken gewähren:

- Zulassen, dass Amazon Managed Service für Prometheus den gescrapten Amazon-EKS-Cluster beschreibt
- Fernschreiben in den Amazon Managed Prometheus-Workspace zulassen

Wenn `AmazonManagedScraperRole` bereits vorhanden ist, verwendet der Scraper diese Rolle. Wählen Sie den `AmazonManagedScraperRole`-Link aus, um die Berechtigungsdetails anzuzeigen. Falls die `AmazonManagedScraperRole` noch nicht existiert, wählen Sie den Link `Berechtigungsdetails anzeigen`, um die spezifischen Berechtigungen zu sehen, die Sie durch Senden von Prometheus-Metriken gewähren.

Subnets

Ändern Sie die Subnetze, die der Scraper erben soll, nach Bedarf. Wenn Sie eine ausgegraute Subnetzoption hinzufügen müssen, kehren Sie zum Schritt **Cluster erstellen Netzwerk angeben** zurück.

Scraper-Konfiguration

Ändern Sie die Scraper-Konfiguration nach Bedarf im YAML-Format. Verwenden Sie dazu das Formular oder laden Sie eine YAML-Ersatzdatei hoch. Weitere Informationen finden Sie unter [Scraper-Konfiguration](#) im Benutzerhandbuch von Amazon Managed Service für Prometheus.

Amazon Managed Service for Prometheus bezieht sich auf den agentenlosen Scraper, der zusammen mit dem Cluster als verwalteter Collector erstellt wird. AWS Weitere Informationen zu

AWS Managed Collectors finden Sie unter [Ingest Metrics with AWS Managed Collectors](#) im Amazon Managed Service for Prometheus User Guide.

Important

- Wenn Sie einen Prometheus-Scraper mithilfe der AWS CLI oder AWS API erstellen, müssen Sie seine Konfiguration anpassen, um dem Scraper Cluster-interne Berechtigungen zu erteilen. Weitere Informationen finden Sie unter [Konfigurieren Ihres Amazon-EKS-Clusters](#) im Benutzerhandbuch von Amazon Managed Service für Prometheus.
- Wenn Sie einen Prometheus-Scraper haben, der vor dem 11. November 2024 erstellt wurde und `aws-auth ConfigMap` anstelle von Access-Einträgen verwendet, müssen Sie ihn aktualisieren, um auf zusätzliche Metriken aus der Amazon EKS-Cluster-Steuerebene zuzugreifen. Die aktualisierte Konfiguration finden Sie unter [Manuelles Konfigurieren von Amazon EKS für den Scraper-Zugriff](#) im Amazon Managed Service for Prometheus Benutzerhandbuch.

Schritt 2: Verwenden Sie die Prometheus-Metriken

Weitere Informationen zur Verwendung der Prometheus-Metriken, nachdem Sie sie für Ihren Cluster aktiviert haben, finden Sie im [Amazon Managed Service for Prometheus](#) User Guide.

Schritt 3: Prometheus-Scraper verwalten

Um Scraper zu verwalten, wählen Sie in der Amazon EKS-Konsole die Registerkarte Observability. Eine Tabelle zeigt eine Liste der Scraper für den Cluster, einschließlich Informationen wie Scraper-ID, Alias, Status und Erstellungsdatum. Sie können weitere Scraper hinzufügen, Scraper bearbeiten, Scraper löschen oder weitere Informationen zu den aktuellen Scrapern anzeigen.

Um weitere Informationen zu einem Scraper zu erhalten, wählen Sie den Link zur Scraper-ID. Sie können beispielsweise den ARN, die Umgebung, die Workspace-ID, die IAM-Rolle, die Konfiguration und die Netzwerkinformationen anzeigen. Sie können die Scraper-ID als Eingabe für Amazon Managed Service für Prometheus-API-Operationen wie [DescribeScraper](#), [UpdateScraper](#) und [DeleteScraper](#) verwenden. Weitere Informationen zur Verwendung der Prometheus-API finden Sie in der [Amazon Managed Service for Prometheus](#) API-Referenz.

Stellen Sie Prometheus mit Helm bereit

Als Alternative zur Verwendung von Amazon Managed Service for Prometheus können Sie Prometheus mit Helm in Ihrem Cluster bereitstellen. Wenn Sie Helm bereits installiert haben, können Sie Ihre Version mit dem `helm version`-Befehl überprüfen. Helm ist ein Paket-Manager für Kubernetes-Cluster. Weitere Informationen zu Helm und zur Installation finden Sie unter [the section called "Stellen Sie Apps mit Helm bereit"](#).

Nachdem Sie Helm für Ihren Amazon-EKS-Cluster konfiguriert haben, können Sie damit die folgenden Schritte ausführen, um Prometheus bereitzustellen.

1. Erstellen Sie einen Prometheus-Namespace.

```
kubectl create namespace prometheus
```

2. Fügen Sie das prometheus-community-Diagramm-Repository hinzu.

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
```

3. Stellen Sie Prometheus bereit.

```
helm upgrade -i prometheus prometheus-community/prometheus \
  --namespace prometheus \
  --set alertmanager.persistence.storageClass="gp2" \
  --set server.persistentVolume.storageClass="gp2"
```

Note

Wenn Sie bei der Ausführung dieses Befehls die Fehlermeldung `Error: failed to download "stable/prometheus"` (hint: running `helm repo update` may help) erhalten, führen Sie `helm repo update prometheus-community` aus, und versuchen Sie dann erneut, den Befehl aus Schritt 2 auszuführen.

Wenn Sie die Fehlermeldung `Error: rendered manifests contain a resource that already exists` erhalten, führen Sie `helm uninstall your-release-name -n namespace` aus, und versuchen Sie dann, den Befehl aus Schritt 3 erneut auszuführen.

4. Stellen Sie sicher, dass sich alle Pods im prometheus Namespace im Status befinden. READY

```
kubectl get pods -n prometheus
```

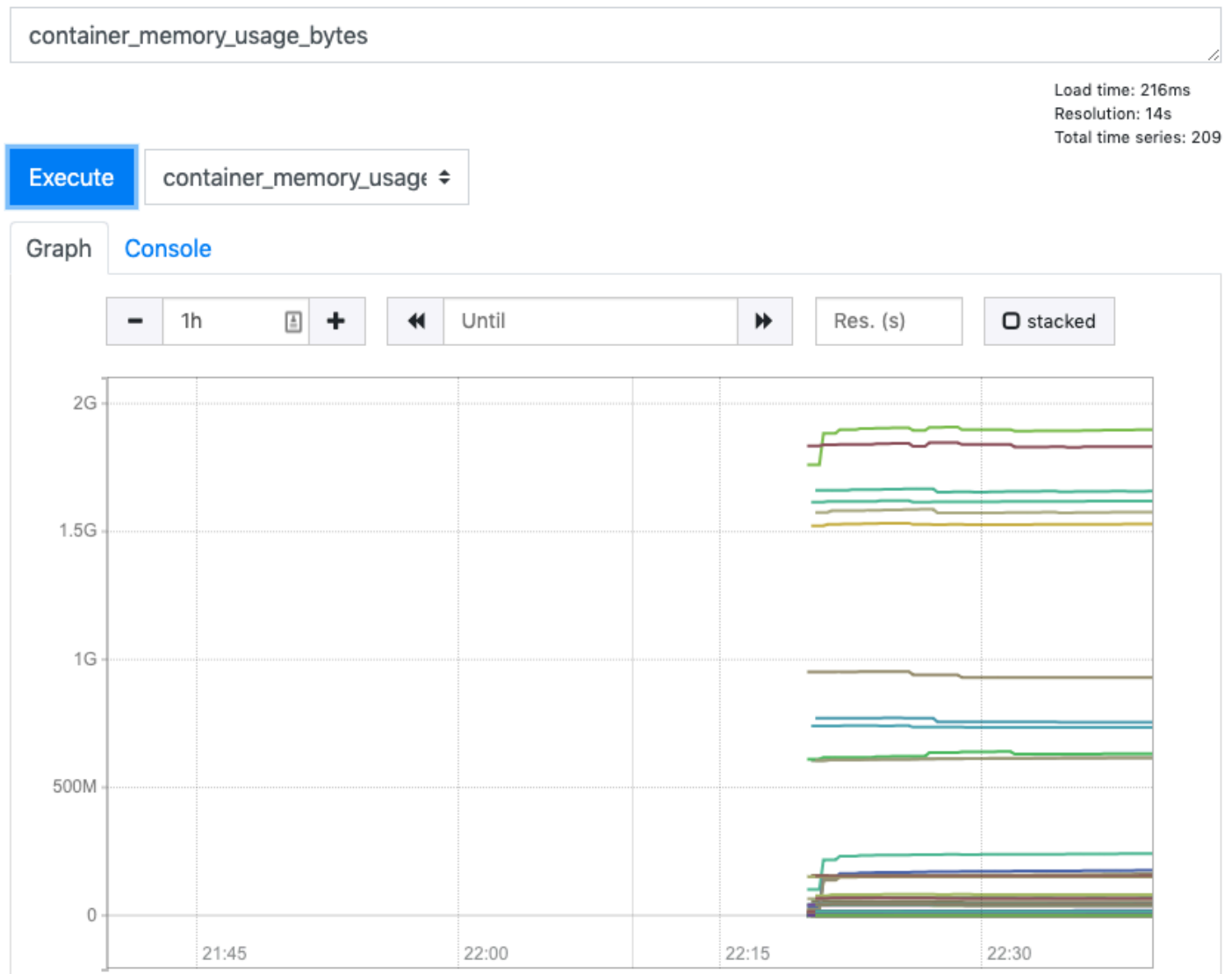
Eine Beispielausgabe sieht wie folgt aus.

NAME	READY	STATUS	RESTARTS	AGE
prometheus-alertmanager-59b4c8c744-r7bgp	1/2	Running	0	48s
prometheus-kube-state-metrics-7cfd87cf99-jkz2f	1/1	Running	0	48s
prometheus-node-exporter-jcjzqz	1/1	Running	0	48s
prometheus-node-exporter-jxv2h	1/1	Running	0	48s
prometheus-node-exporter-vbdk5	1/1	Running	0	48s
prometheus-pushgateway-76c444b68c-82tnw	1/1	Running	0	48s
prometheus-server-775957f748-mmht9	1/2	Running	0	48s

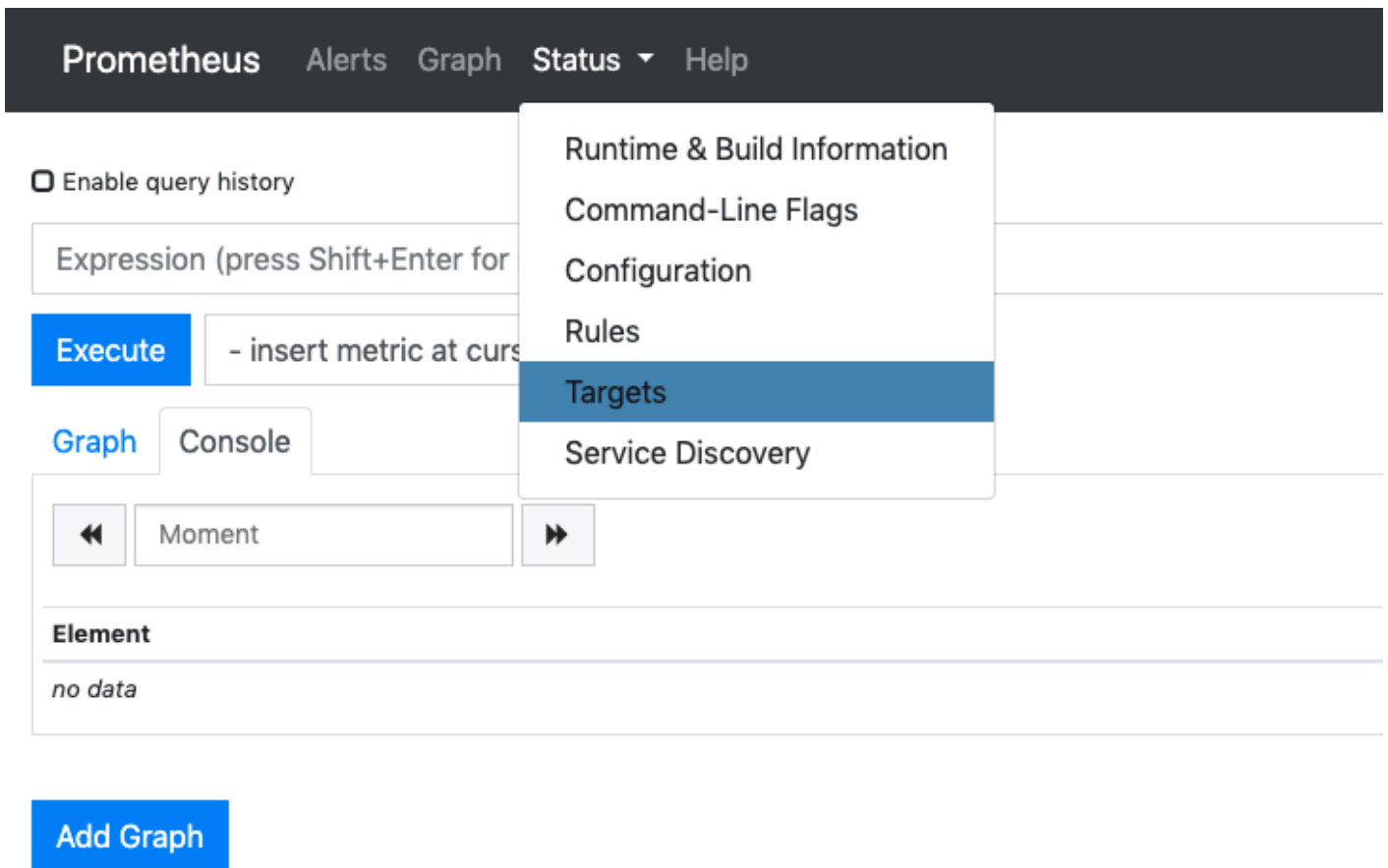
5. Verwenden Sie `kubectl`, um die Prometheus-Konsole auf Ihren lokalen Computer weiterzuleiten.

```
kubectl --namespace=prometheus port-forward deploy/prometheus-server 9090
```

6. Zeigen Sie mit einem Webbrowser auf, <http://localhost:9090> um die Prometheus-Konsole aufzurufen.
7. Wählen Sie eine Metrik aus dem Menü - insert metric at cursor (Metrik bei Cursor eingeben) und danach Execute (Ausführen). Wählen Sie die Registerkarte Graph (Diagramm) aus, um die Metrik im Zeitverlauf anzuzeigen. Das folgende Image zeigt `container_memory_usage_bytes` im Zeitverlauf.



8. Wählen Sie in der oberen Navigationsleiste Status, dann Targets (Ziele).



Es werden alle Kubernetes-Endpunkte angezeigt, die über die Service-Erkennung mit Prometheus verbunden sind.

Ruft Rohmetriken der Kontrollebene im Prometheus-Format ab

[Die Kubernetes-Steuerebene stellt eine Reihe von Metriken zur Verfügung, die in einem Prometheus-Format dargestellt werden.](#) Diese Metriken sind für die Überwachung und Analyse hilfreich. Sie werden intern über Metrik-Endpunkte verfügbar gemacht und können abgerufen werden, ohne Prometheus vollständig einsetzen zu müssen. Die einfachere Bereitstellung von Prometheus ermöglicht jedoch die Analyse von Metriken im Laufe der Zeit.

Um die Ausgabe der Rohmetriken anzuzeigen, ersetzen Sie den folgenden endpoint Befehl und führen Sie ihn aus.

```
kubectl get --raw endpoint
```

Mit diesem Befehl können Sie einen beliebigen Endpunktpfad übergeben und die Rohantwort zurückgeben. In der Ausgabe werden verschiedene Metriken aufgeführt line-by-line, wobei jede Zeile einen Metrikenamen, Tags und einen Wert enthält.

```
metric_name{tag="value"[,...]} value
```

Metriken vom API-Server abrufen

Der allgemeine API-Serverendpunkt ist auf der Amazon EKS-Steuerebene verfügbar. Dieser Endpunkt ist in erster Linie nützlich, wenn Sie sich eine bestimmte Metrik ansehen.

```
kubectl get --raw /metrics
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
# HELP rest_client_requests_total Number of HTTP requests, partitioned by status code,
# method, and host.
# TYPE rest_client_requests_total counter
rest_client_requests_total{code="200",host="127.0.0.1:21362",method="POST"} 4994
rest_client_requests_total{code="200",host="127.0.0.1:443",method="DELETE"} 1
rest_client_requests_total{code="200",host="127.0.0.1:443",method="GET"} 1.326086e+06
rest_client_requests_total{code="200",host="127.0.0.1:443",method="PUT"} 862173
rest_client_requests_total{code="404",host="127.0.0.1:443",method="GET"} 2
rest_client_requests_total{code="409",host="127.0.0.1:443",method="POST"} 3
rest_client_requests_total{code="409",host="127.0.0.1:443",method="PUT"} 8
# HELP ssh_tunnel_open_count Counter of ssh tunnel total open attempts
# TYPE ssh_tunnel_open_count counter
ssh_tunnel_open_count 0
# HELP ssh_tunnel_open_fail_count Counter of ssh tunnel failed open attempts
# TYPE ssh_tunnel_open_fail_count counter
ssh_tunnel_open_fail_count 0
```

Diese Rohausgabe zeigt exakt das, was der API-Server bereitstellt.

Rufen Sie Metriken der Kontrollebene ab mit **metrics.eks.amazonaws.com**

Für Cluster mit Kubernetes-Version 1.28 und höher stellt Amazon EKS auch Metriken unter der API-Gruppe zur Verfügung. **metrics.eks.amazonaws.com** Zu diesen Metriken gehören Komponenten der Steuerungsebene wie **und kube-scheduler kube-controller-manager**

 Note

Wenn Sie über eine Webhook-Konfiguration verfügen, die die Erstellung der neuen APIService Ressource in `v1.metrics.eks.amazonaws.com` Ihrem Cluster blockieren könnte, ist die Metrik-Endpunktfunktion möglicherweise nicht verfügbar. Sie können dies im kube-apiserver Audit-Protokoll überprüfen, indem Sie nach dem `v1.metrics.eks.amazonaws.com` Schlüsselwort suchen.

Metriken abrufen **kube-scheduler**

Verwenden Sie den folgenden Befehl, um kube-scheduler Metriken abzurufen.

```
kubectl get --raw "/apis/metrics.eks.amazonaws.com/v1/ksh/container/metrics"
```

Eine Beispielausgabe sieht wie folgt aus.

```
# TYPE scheduler_pending_pods gauge
scheduler_pending_pods{queue="active"} 0
scheduler_pending_pods{queue="backoff"} 0
scheduler_pending_pods{queue="gated"} 0
scheduler_pending_pods{queue="unschedulable"} 18
# HELP scheduler_pod_scheduling_attempts [STABLE] Number of attempts to successfully
  schedule a pod.
# TYPE scheduler_pod_scheduling_attempts histogram
scheduler_pod_scheduling_attempts_bucket{le="1"} 79
scheduler_pod_scheduling_attempts_bucket{le="2"} 79
scheduler_pod_scheduling_attempts_bucket{le="4"} 79
scheduler_pod_scheduling_attempts_bucket{le="8"} 79
scheduler_pod_scheduling_attempts_bucket{le="16"} 79
scheduler_pod_scheduling_attempts_bucket{le="+Inf"} 81
[...]
```

Metriken abrufen **kube-controller-manager**

Verwenden Sie den folgenden Befehl, um kube-controller-manager Metriken abzurufen.

```
kubectl get --raw "/apis/metrics.eks.amazonaws.com/v1/kcm/container/metrics"
```

Eine Beispielausgabe sieht wie folgt aus.

```
[...]
workqueue_work_duration_seconds_sum{name="pvprotection"} 0
workqueue_work_duration_seconds_count{name="pvprotection"} 0
workqueue_work_duration_seconds_bucket{name="replicaset",le="1e-08"} 0
workqueue_work_duration_seconds_bucket{name="replicaset",le="1e-07"} 0
workqueue_work_duration_seconds_bucket{name="replicaset",le="1e-06"} 0
workqueue_work_duration_seconds_bucket{name="replicaset",le="9.999999999999999e-06"} 0
workqueue_work_duration_seconds_bucket{name="replicaset",le="9.999999999999999e-05"} 19
workqueue_work_duration_seconds_bucket{name="replicaset",le="0.001"} 109
workqueue_work_duration_seconds_bucket{name="replicaset",le="0.01"} 139
workqueue_work_duration_seconds_bucket{name="replicaset",le="0.1"} 181
workqueue_work_duration_seconds_bucket{name="replicaset",le="1"} 191
workqueue_work_duration_seconds_bucket{name="replicaset",le="10"} 191
workqueue_work_duration_seconds_bucket{name="replicaset",le="+Inf"} 191
workqueue_work_duration_seconds_sum{name="replicaset"} 4.265655885000002
[...]
```

Machen Sie sich mit den Metriken für Scheduler und Controller Manager vertraut

In der folgenden Tabelle werden die Scheduler- und Controller-Manager-Metriken beschrieben, die für Scraping im Prometheus-Stil zur Verfügung gestellt werden. Weitere Informationen zu diesen Metriken finden Sie unter [Kubernetes Metrics Reference in der Kubernetes-Dokumentation](#).

Metrik	Komponente der Steuerungsebene	Beschreibung
<code>scheduler_pending_pods</code>	Scheduler	Die Anzahl der Pods, die darauf warten, zur Ausführung auf einem Knoten geplant zu werden.
<code>scheduler_schedule_attempts_total</code>	Scheduler	Die Anzahl der Versuche, Pods zu planen.
<code>scheduler_preemption_attempts_total</code>	Scheduler	Die Anzahl der Versuche des Schedulers, Pods mit höherer Priorität einzuplanen, indem er Pods mit niedrigerer Priorität entfernt.

Metrik	Komponente der Steuerungsebene	Beschreibung
<code>scheduler_preemption_victims</code>	Scheduler	Die Anzahl der Pods, die für die Räumung ausgewählt wurden, um Platz für Pods mit höherer Priorität zu schaffen.
<code>scheduler_pod_scheduling_attempts</code>	Scheduler	Die Anzahl der Versuche, einen Pod erfolgreich zu planen.
<code>scheduler_scheduling_attempt_duration_seconds</code>	Scheduler	Gibt an, wie schnell oder langsam der Scheduler auf der Grundlage verschiedener Faktoren wie Ressourcerverfügbarkeit und Planungsregeln in der Lage ist, einen geeigneten Ort für die Ausführung eines Pods zu finden.
<code>scheduler_pod_scheduling_latency_duration_seconds</code>	Scheduler	Die end-to-end Latenz für einen geplanten Pod ab dem Zeitpunkt, zu dem der Pod in die Warteschlange für die Terminplanung aufgenommen wird. Dies kann mehrere Planungsversuche beinhalten.
<code>cronjob_controller_job_creation_skew_duration_seconds</code>	Controller-Manager	Die Zeit zwischen der geplanten Ausführung eines Cronjobs und der Erstellung des entsprechenden Jobs.
<code>workqueue_depth</code>	Controller-Manager	Die aktuelle Tiefe der Warteschlange.

Metrik	Komponente der Steuerungsebene	Beschreibung
workqueue_adds_total	Controller-Manager	Die Gesamtzahl der von der Workqueue verarbeiteten Hinzufügungen.
workqueue_queue_duration_seconds	Controller-Manager	Die Zeit in Sekunden, in der ein Element in der Arbeitswarteschlange verbleibt, bevor es angefordert wird.
workqueue_work_duration_seconds	Controller-Manager	Die Zeit in Sekunden, die die Verarbeitung eines Elements aus der Arbeitswarteschlange dauert.

Setzen Sie einen Prometheus-Scraper ein, um Kennzahlen konsistent zu erfassen

Verwenden Sie die folgende Konfiguration, um einen Prometheus-Scraper zur konsistenten Erfassung der Metriken einzusetzen:

```
---
apiVersion: v1
kind: ConfigMap
metadata:
  name: prometheus-conf
data:
  prometheus.yml: |-
    global:
      scrape_interval: 30s
    scrape_configs:
      # apiserver metrics
      - job_name: apiserver-metrics
        kubernetes_sd_configs:
          - role: endpoints
        scheme: https
        tls_config:
          ca_file: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
          insecure_skip_verify: true
```

```

bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
relabel_configs:
- source_labels:
  [
    __meta_kubernetes_namespace,
    __meta_kubernetes_service_name,
    __meta_kubernetes_endpoint_port_name,
  ]
  action: keep
  regex: default;kubernetes;https
# Scheduler metrics
- job_name: 'ksh-metrics'
  kubernetes_sd_configs:
  - role: endpoints
  metrics_path: /apis/metrics.eks.amazonaws.com/v1/ksh/container/metrics
  scheme: https
  tls_config:
    ca_file: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
    insecure_skip_verify: true
  bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
  relabel_configs:
  - source_labels:
    [
      __meta_kubernetes_namespace,
      __meta_kubernetes_service_name,
      __meta_kubernetes_endpoint_port_name,
    ]
    action: keep
    regex: default;kubernetes;https
# Controller Manager metrics
- job_name: 'kcm-metrics'
  kubernetes_sd_configs:
  - role: endpoints
  metrics_path: /apis/metrics.eks.amazonaws.com/v1/kcm/container/metrics
  scheme: https
  tls_config:
    ca_file: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
    insecure_skip_verify: true
  bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
  relabel_configs:
  - source_labels:
    [
      __meta_kubernetes_namespace,
      __meta_kubernetes_service_name,

```

```

        __meta_kubernetes_endpoint_port_name,
    ]
    action: keep
    regex: default;kubernetes;https
---
apiVersion: v1
kind: Pod
metadata:
  name: prom-pod
spec:
  containers:
  - name: prom-container
    image: prom/prometheus
    ports:
    - containerPort: 9090
    volumeMounts:
    - name: config-volume
      mountPath: /etc/prometheus/
  volumes:
  - name: config-volume
    configMap:
      name: prometheus-conf

```

Die folgende Berechtigung ist erforderlich, damit der Pod auf den neuen Metriken-Endpunkt zugreifen kann.

```

{
  "effect": "allow",
  "apiGroups": [
    "metrics.eks.amazonaws.com"
  ],
  "resources": [
    "kcm/metrics",
    "ksh/metrics"
  ],
  "verbs": [
    "get"
  ] },

```

Um die verwendete Rolle zu patchen, können Sie den folgenden Befehl verwenden.

```

kubectl patch clusterrole <role-name> --type=json -p='[
{

```

```
"op": "add",
"path": "/rules/-",
"value": {
  "verbs": ["get"],
  "apiGroups": ["metrics.eks.amazonaws.com"],
  "resources": ["kcm/metrics", "ksh/metrics"]
}
}]'
```

Anschließend können Sie das Prometheus-Dashboard anzeigen, indem Sie den Port des Prometheus-Scrapers an Ihren lokalen Port weiterleiten.

```
kubectl port-forward pods/prom-pod 9090:9090
```

Für Ihren Amazon EKS-Cluster werden die Kernmetriken der Kubernetes-Steuerebene auch in Amazon CloudWatch Metrics unter dem Namespace aufgenommen. AWS/EKS Um sie anzuzeigen, öffnen Sie die [CloudWatch Konsole](#) und wählen Sie im linken Navigationsbereich Alle Metriken aus. Wählen Sie auf der Seite zur Auswahl der Metriken den AWS/EKS Namespace und eine Metrikdimension für Ihren Cluster aus.

Überwachen Sie Clusterdaten mit Amazon CloudWatch

Amazon CloudWatch ist ein Überwachungsdienst, der Metriken und Protokolle aus Ihren Cloud-Ressourcen sammelt. CloudWatch stellt einige grundlegende Amazon EKS-Metriken kostenlos zur Verfügung, wenn Sie einen neuen Cluster der Version 1.28 und höher verwenden. Wenn Sie den CloudWatch Observability Operator jedoch als Amazon EKS-Add-on verwenden, können Sie erweiterte Observability-Funktionen nutzen.

Grundlegende Kennzahlen in Amazon CloudWatch

Für Cluster der Kubernetes-Version 1.28 und höher erhalten Sie CloudWatch Metriken kostenlos im Namespace. AWS/EKS Die folgende Tabelle enthält eine Liste der grundlegenden Metriken, die für die unterstützten Versionen verfügbar sind. Jede aufgelistete Metrik hat eine Frequenz von einer Minute.

Metrikname	Beschreibung
<code>scheduler_schedule_attempts_total</code>	Die Gesamtzahl der Versuche des Schedulers, Pods im Cluster für einen bestimmten Zeitraum einzuplanen. Diese Metrik hilft bei der Überwachung der Arbeitslast des Schedulers und kann auf Termindruck oder potenzielle Probleme bei der Pod-Platzierung hinweisen. Einheiten: Anzahl Gültige Statistiken: Summe
<code>scheduler_schedule_attempts_SCHEDULED</code>	Die Anzahl der erfolgreichen Versuche des Schedulers, Pods für Knoten im Cluster für einen bestimmten Zeitraum einzuplanen. Einheiten: Anzahl Gültige Statistiken: Summe
<code>scheduler_schedule_attempts_UNSCHEDULABLE</code>	Die Anzahl der Versuche, Pods zu planen, die für einen bestimmten Zeitraum aufgrund gültiger Einschränkungen, wie z. B. unzureichender CPU oder Arbeitsspeicher auf einem Knoten, nicht planbar waren. Einheiten: Anzahl Gültige Statistiken: Summe
<code>scheduler_schedule_attempts_ERROR</code>	Die Anzahl der Versuche, Pods zu planen, die für einen bestimmten Zeitraum aufgrund eines internen Problems mit dem Scheduler selbst, wie z. B. Verbindungsproblemen mit dem API-Server, fehlgeschlagen sind. Einheiten: Anzahl

Metrikname	Beschreibung
	Gültige Statistiken: Summe
scheduler_pending_pods	Die Gesamtzahl der ausstehenden Pods, die vom Scheduler im Cluster für einen bestimmten Zeitraum geplant werden sollen. Einheiten: Anzahl Gültige Statistiken: Summe
scheduler_pending_pods_ACTIVEQ	Die Anzahl der ausstehenden Pods in ActiveQ, die darauf warten, im Cluster für einen bestimmten Zeitraum geplant zu werden. Einheiten: Anzahl Gültige Statistiken: Summe
scheduler_pending_pods_UNSCHEULABLE	Die Anzahl der ausstehenden Pods, die der Scheduler versucht hat, einen Zeitplan zu erstellen, was aber fehlschlug und die für einen erneuten Versuch in einem Zustand gehalten werden, in dem sie nicht planbar sind. Einheiten: Anzahl Gültige Statistiken: Summe
scheduler_pending_pods_BACKOFF	Die Anzahl der ausstehenden Pods, die sich backoffQ im Backoff-Status befinden und auf den Ablauf ihrer Backoff-Periode warten. Einheiten: Anzahl Gültige Statistiken: Summe

Metrikname	Beschreibung
scheduler_pending_pods_GATED	Die Anzahl der ausstehenden Pods, die derzeit in einem geschlossenen Zustand warten, da sie erst geplant werden können, wenn sie die erforderlichen Bedingungen erfüllen. Einheiten: Anzahl Gültige Statistiken: Summe
apiserver_request_total	Die Anzahl der HTTP-Anfragen, die über alle API-Server im Cluster gestellt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
apiserver_request_total_4XX	Die Anzahl der HTTP-Anfragen an alle API-Server im Cluster, die zu Statuscodes 4XX (Client-Fehler) führten. Einheiten: Anzahl Gültige Statistiken: Summe
apiserver_request_total_429	Die Anzahl der HTTP-Anfragen an alle API-Server im Cluster, die zu einem 429 Statuscode geführt haben, der auftritt, wenn Clients die Schwellenwerte für die Ratenbegrenzung überschreiten. Einheiten: Anzahl Gültige Statistiken: Summe

Metrikname	Beschreibung
apiserver_request_total_5XX	Die Anzahl der HTTP-Anfragen an alle API-Server im Cluster, die zu Statuscodes 5XX (Serverfehler) führten. Einheiten: Anzahl Gültige Statistiken: Summe
apiserver_request_total_LIST_PODS	Die Anzahl der LIST Pods-Anfragen, die an alle API-Server im Cluster gestellt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
apiserver_request_duration_seconds_PUT_P99	Das 99. Perzentil der Latenz für PUT Anfragen, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, unter der 99% aller PUT Anfragen abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt
apiserver_request_duration_seconds_PATCH_P99	Das 99. Perzentil der Latenz für PATCH Anfragen, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, unter der 99% aller PATCH Anfragen abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt

Metrikname	Beschreibung
apiserver_request_duration_seconds_POST_P99	Das 99. Perzentil der Latenz für POST Anfragen, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, unter der 99% aller POST Anfragen abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt
apiserver_request_duration_seconds_GET_P99	Das 99. Perzentil der Latenz für GET Anfragen, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, unter der 99% aller GET Anfragen abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt
apiserver_request_duration_seconds_LIST_P99	Das 99. Perzentil der Latenz für LIST Anfragen, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, unter der 99% aller LIST Anfragen abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt

Metrikname	Beschreibung
<code>apiserver_request_duration_seconds_DELETE_P99</code>	Das 99. Perzentil der Latenz für DELETE Anfragen, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, unter der 99% aller DELETE Anfragen abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt
<code>apiserver_current_inflight_requests_MUTATING</code>	Die Anzahl der mutierenden Anfragen (POST,,PUT,PATCH)DELETE, die derzeit auf allen API-Servern im Cluster verarbeitet werden. Diese Metrik steht für Anfragen, die gerade bearbeitet werden und deren Verarbeitung noch nicht abgeschlossen ist. Einheiten: Anzahl Gültige Statistiken: Summe
<code>apiserver_current_inflight_requests_READONLY</code>	Die Anzahl der schreibgeschützten Anfragen (GET,LIST), die derzeit auf allen API-Servern im Cluster verarbeitet werden. Diese Metrik stellt Anfragen dar, die gerade bearbeitet werden und deren Verarbeitung noch nicht abgeschlossen ist. Einheiten: Anzahl Gültige Statistiken: Summe

Metrikname	Beschreibung
<code>apiserver_admission_webhook_request_total</code>	Die Anzahl der Webhook-Zulassungsanfragen, die auf allen API-Servern im Cluster gestellt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
<code>apiserver_admission_webhook_request_total_ADMIT</code>	Die Anzahl der Webhook-Anfragen mit mutierender Zulassung, die auf allen API-Servern im Cluster gestellt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
<code>apiserver_admission_webhook_request_total_VALIDATING</code>	Die Anzahl der Webhook-Anfragen zur Validierung der Zulassung, die auf allen API-Servern im Cluster gestellt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
<code>apiserver_admission_webhook_rejection_count</code>	Die Anzahl der Webhook-Zulassungsanfragen, die auf allen API-Servern im Cluster gestellt und abgelehnt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
<code>apiserver_admission_webhook_rejection_count_ADMIT</code>	Die Anzahl der Webhook-Anfragen mit mutierender Zulassung, die auf allen API-Servern im Cluster gestellt und abgelehnt wurden. Einheiten: Anzahl Gültige Statistiken: Summe

Metrikname	Beschreibung
<code>apiserver_admission_webhook_rejection_count_VALIDATING</code>	Die Anzahl der Webhook-Anfragen zur Validierung der Zulassung, die auf allen API-Servern im Cluster gestellt und abgelehnt wurden. Einheiten: Anzahl Gültige Statistiken: Summe
<code>apiserver_admission_webhook_admission_duration_seconds</code>	Das 99. Perzentil der Latenz für Webhook-Anfragen mit Zulassung durch Dritte, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, bis zu der 99% aller Webhook-Anfragen mit Zulassung durch Dritte abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt
<code>apiserver_admission_webhook_admission_duration_seconds_ADMIT_P99</code>	Das 99. Perzentil der Latenz für Webhook-Anfragen von Drittanbietern mit mutierender Zulassung, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, bei deren Unterschreitung 99% aller Webhook-Anfragen von Drittanbietern mit mutierender Zulassung abgeschlossen werden. Einheiten: Sekunden Gültige Statistiken: Durchschnitt

Metrikname	Beschreibung
apiserver_admission_webhook_admission_duration_seconds_VALIDATING_P99	Das 99. Perzentil der Latenz für Webhook-Anfragen von Drittanbietern, die die Zulassung validieren, berechnet anhand aller Anfragen auf allen API-Servern im Cluster. Stellt die Antwortzeit dar, bei deren Unterschreitung 99% aller Webhook-Anfragen von Drittanbietern, die die Zulassung validieren, abgeschlossen sind. Einheiten: Sekunden Gültige Statistiken: Durchschnitt
apiserver_storage_size_bytes	Die physische Größe der etcd-Speicherdatenbankdatei in Byte, die von den API-Servern im Cluster verwendet wird. Diese Metrik stellt den tatsächlichen Festplattenspeicher dar, der dem Speicher zugewiesen wurde. Einheiten: Byte Gültige Statistiken: Maximum

Amazon CloudWatch Observability-Betreiber

Amazon CloudWatch Observability sammelt Protokolle, Metriken und Trace-Daten in Echtzeit. Es sendet sie an [Amazon CloudWatch](#) und [AWS X-Ray](#). Sie können dieses Add-on installieren, um sowohl CloudWatch Application Signals als auch CloudWatch Container Insights mit verbesserter Observability für Amazon EKS zu aktivieren. Dies hilft Ihnen, den Zustand und die Leistung Ihrer Infrastruktur und containerisierten Anwendungen zu überwachen. Der Amazon CloudWatch Observability Operator ist für die Installation und Konfiguration der erforderlichen Komponenten konzipiert.

Amazon EKS unterstützt den CloudWatch Observability Operator als [Amazon EKS-Add-on](#). Das Add-on ermöglicht Container Insights sowohl auf Linux- als auch auf Windows-Worker-Knoten im Cluster. Um Container Insights unter Windows zu aktivieren, muss die Amazon EKS-Add-On-Version

1.5.0 oder höher sein. Derzeit wird CloudWatch Application Signals auf Amazon EKS Windows nicht unterstützt.

In den folgenden Themen werden die ersten Schritte mit der Verwendung von CloudWatch Observability Operator für Ihren Amazon EKS-Cluster beschrieben.

- Anweisungen zur Installation dieses Add-ons finden Sie unter [Installieren des CloudWatch Agenten mit dem Amazon CloudWatch Observability EKS-Add-on oder dem Helm-Diagramm](#) im CloudWatch Amazon-Benutzerhandbuch.
- Weitere Informationen zu CloudWatch Application Signals finden Sie unter [Application Signals](#) im CloudWatch Amazon-Benutzerhandbuch.
- Weitere Informationen zu Container Insights finden Sie unter [Using Container Insights](#) im CloudWatch Amazon-Benutzerhandbuch.

Protokolle der Kontrollebene an CloudWatch Logs senden

Die Protokollierung auf der Amazon EKS-Kontrollebene stellt Prüf- und Diagnoseprotokolle direkt von der Amazon EKS-Steuerebene zu den CloudWatch Protokollen in Ihrem Konto bereit. Diese Protokolle erleichtern Ihnen die Absicherung und Ausführung Ihrer Cluster. Sie können genau die Protokolltypen auswählen, die Sie benötigen, und die Protokolle werden als Protokollstreams an eine Gruppe für jeden Amazon EKS-Cluster gesendet CloudWatch. Sie können CloudWatch Abonnementfilter verwenden, um die Protokolle in Echtzeit zu analysieren oder sie an andere Dienste weiterzuleiten (die Protokolle werden Base64-codiert und im GZIP-Format komprimiert). Weitere Informationen finden Sie unter [CloudWatch Amazon-Protokollierung](#).

Sie können mit der Protokollierung der Amazon-EKS-Steuerebene beginnen, indem Sie die für jeden neuen oder bestehenden Amazon-EKS-Cluster zu aktivierenden Protokolltypen auswählen. Sie können jeden Protokolltyp auf Clusterbasis mit der AWS Management Console AWS CLI (Version 1.16.139 oder höher) oder über die Amazon EKS-API aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, werden Protokolle automatisch vom Amazon EKS-Cluster an CloudWatch Logs im selben Konto gesendet.

Wenn Sie die Protokollierung auf der Amazon EKS-Kontrollebene verwenden, werden Ihnen die Amazon EKS-Standardpreise für jeden Cluster, den Sie ausführen, berechnet. Für alle CloudWatch Protokolle, die von Ihren Clustern an Logs gesendet werden, werden Ihnen die standardmäßigen Kosten für die Aufnahme und Speicherung von CloudWatch Logs in Rechnung gestellt. Ihnen werden

auch alle AWS Ressourcen, wie EC2 Amazon-Instances oder Amazon EBS-Volumes, in Rechnung gestellt, die Sie als Teil Ihres Clusters bereitstellen.

Die folgenden Cluster-Steuerebenen-Protokolltypen sind verfügbar. Jeder Protokolltyp entspricht einer Komponente der Kubernetes-Steuerebene. Um mehr über diese Komponenten zu erfahren, lesen Sie [Kubernetes-Komponenten](#) in der Kubernetes-Dokumentation.

API-Server**api** ()

Der API-Server Ihres Clusters ist die Komponente der Steuerungsebene, die die Kubernetes-API verfügbar macht. Wenn Sie API-Serverprotokolle beim Starten des Clusters oder kurz danach aktivieren, enthalten die Protokolle API-Server-Markierungen, die zum Starten des API-Servers verwendet wurden. Weitere Informationen finden Sie unter [kube-apiserver](#) und in der [Prüfungsrichtlinie](#) in der Kubernetes-Dokumentation.

Prüfung**audit** ()

Kubernetes-Audit-Logs enthalten eine Aufzeichnung der einzelnen Benutzer, Administratoren oder Systemkomponenten, die sich auf Ihren Cluster ausgewirkt haben. Weitere Informationen finden Sie unter [Prüfung](#) in der Kubernetes-Dokumentation.

Authenticator**authenticator** ()

Authenticator-Protokolle sind eindeutig für Amazon EKS. Diese Protokolle stellen die Steuerebenenkomponente dar, die Amazon EKS für die Kubernetes-Authentifizierung per [rollenbasierter Zugriffssteuerung](#) (RBAC) mit IAM-Anmeldeinformationen verwendet. Weitere Informationen finden Sie unter [Clusterverwaltung](#).

Controller-Manager**controllerManager** ()

Der Controller-Manager verwaltet die zentralen Regelkreise, die im Lieferumfang von Kubernetes enthalten sind. Weitere Informationen finden Sie unter [kube-controller-manager](#) in der Kubernetes-Dokumentation.

Scheduler**scheduler** ()

Die Scheduler-Komponente verwaltet, wann und wo Pods in Ihrem Cluster ausgeführt werden sollen. Weitere Informationen finden Sie unter [kube-scheduler](#) in der Kubernetes-Dokumentation.

Aktivieren oder deaktivieren Sie die Protokolle der Kontrollebene

Standardmäßig werden Protokolle der Cluster-Steuerungsebene nicht an CloudWatch Logs gesendet. Sie müssen jeden Protokolltyp einzeln aktivieren, um Protokolle für Ihren Cluster zu

senden. CloudWatch Die Raten für die Aufnahme von Protokollen, die Archivierung und das Scannen von Daten gelten für aktivierte Protokolle auf der Kontrollebene. Weitere Informationen finden Sie unter [CloudWatch Preise](#).

Um die Protokollierungskonfiguration der Steuerebene zu aktualisieren, benötigt Amazon EKS bis zu fünf verfügbare IP-Adressen in jedem Subnetz. Wenn Sie einen Protokolltyp aktivieren, werden die Protokolle mit der Protokollausführungsstufe 2 gesendet.

Sie können die Protokolle der Steuerungsebene entweder mit der [AWS Management Console](#) oder der [AWS CLI](#) aktivieren oder deaktivieren.

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie den Namen des Clusters aus, um Ihre Cluster-Informationen anzuzeigen.
3. Wählen Sie den Registerkarte Beobachtbarkeit.
4. Wählen Sie im Abschnitt Steuerebenen-Protokollierung die Option Protokollierung verwalten aus.
5. Wählen Sie für jeden Protokolltyp aus, ob er aktiviert oder deaktiviert sein soll. Standardmäßig sind alle Protokollierungstypen deaktiviert.
6. Wählen Sie Änderungen speichern, um den Vorgang abzuschließen.

AWS CLI

1. Überprüfen Sie Ihre AWS CLI-Version mit dem folgenden Befehl.

```
aws --version
```

Wenn Ihre AWS CLI-Version älter als ist 1.16.139, müssen Sie zuerst auf die neueste Version aktualisieren. Informationen zur Installation oder zum Upgrade der AWS CLI finden Sie unter [Installation der AWS Befehlszeilenschnittstelle](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

2. Aktualisieren Sie die Protokoll-Exportkonfiguration der Steuerungsebene Ihres Clusters mit dem folgenden AWS CLI-Befehl. Ersetzen Sie *my-cluster* durch den Namen Ihres Clusters und geben Sie die gewünschten Endpunkt-Zugriffswerte ein.

 Note

Der folgende Befehl sendet alle verfügbaren Protokolltypen an CloudWatch Logs.

```
aws eks update-cluster-config \
  --region region-code \
  --name my-cluster \
  --logging '{"clusterLogging":[{"types":
["api","audit","authenticator","controllerManager","scheduler"],"enabled":true}]}'
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "update": {
    "id": "883405c8-65c6-4758-8cee-2a7c1340a6d9",
    "status": "InProgress",
    "type": "LoggingUpdate",
    "params": [
      {
        "type": "ClusterLogging",
        "value": "{\"clusterLogging\":{\"types\":[\"api\", \"audit\",
\"authenticator\", \"controllerManager\", \"scheduler\"], \"enabled\":true}}}"
      }
    ],
    "createdAt": 1553271814.684,
    "errors": []
  }
}
```

3. Überwachen Sie den Status Ihres Protokoll-Konfigurationsupdates mit dem folgenden Befehl unter Verwendung des Cluster-Namens und der Update-ID, die vom vorherigen Befehl zurückgegeben wurden. Ihre Aktualisierung ist abgeschlossen, wenn als Status **Successful** angezeigt wird.

```
aws eks describe-update \
  --region region-code \
  --name my-cluster \
  --update-id 883405c8-65c6-4758-8cee-2a7c1340a6d9
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "update": {
    "id": "883405c8-65c6-4758-8cee-2a7c1340a6d9",
    "status": "Successful",
    "type": "LoggingUpdate",
    "params": [
      {
        "type": "ClusterLogging",
        "value": "{\"clusterLogging\":{\"types\":[\"api\",\"audit\",
\\\"authenticator\\\",\\\"controllerManager\\\",\\\"scheduler\\\"],\\\"enabled\\\":true}}}"
      }
    ],
    "createdAt": 1553271814.684,
    "errors": []
  }
}
```

Protokolle der Cluster-Steuerungsebene anzeigen

Nachdem Sie einen der Protokolltypen der Kontrollebene für Ihren Amazon EKS-Cluster aktiviert haben, können Sie ihn auf der CloudWatch Konsole anzeigen.

Weitere Informationen zum Anzeigen, Analysieren und Verwalten von Logs in CloudWatch Amazon Logs finden Sie im [Amazon CloudWatch Logs-Benutzerhandbuch](#).

1. Öffnen Sie die [CloudWatch -Konsole](#). Der Link öffnet die Konsole und zeigt Ihre aktuell verfügbaren Protokollgruppen an und filtert sie mit dem /aws/eks-Präfix.
2. Wählen Sie den Cluster aus, für den Sie die Protokolle anzeigen möchten. Das Format für den Namen der Protokollgruppen lautet /aws/eks/*my-cluster*/cluster.
3. Wählen Sie den anzuzeigenden Protokollstream aus. Die folgende Liste beschreibt das Namensformat des Protokollstreams der einzelnen Protokolltypen.

Note

Wenn die Daten des Protokollstreams ansteigen, werden die Namen des Protokollstreams rotiert. Wenn mehrere Protokollstreams für einen bestimmten Protokolltyp vorhanden sind, können Sie den neuesten Protokollstream anzeigen, indem Sie nach dem Namen des Protokollstreams mit der letzten Last event time (Uhrzeit des letzten Ereignisses) suchen.

- Kubernetes-API-Server-Komponentenprotokolle (**api**) – kube-apiserver-*1234567890abcdef01234567890abcde*
- Prüfung (**audit**) – kube-apiserver-audit-*1234567890abcdef01234567890abcde*
- Authentifikator (**authenticator**) – authenticator-*1234567890abcdef01234567890abcde*
- Controller-Manager (**controllerManager**) – kube-controller-manager-*1234567890abcdef01234567890abcde*
- Scheduler (**scheduler**) – kube-scheduler-*1234567890abcdef01234567890abcde*

4. Sehen Sie sich die Ereignisse des Protokollstreams an.

Sie sollten beispielsweise die anfänglichen API-Server-Flags für den Cluster sehen, wenn Sie den oberen Teil von kube-apiserver-*1234567890abcdef01234567890abcde* anzeigen.

Note

Wenn Sie die API-Serverprotokolle nicht am Anfang des Log-Streams sehen, ist es wahrscheinlich, dass die API-Server-Protokolldatei auf dem Server rotiert wurde, bevor Sie die API-Serverprotokollierung auf dem Server aktiviert haben. Protokolldateien, die rotiert wurden, bevor die API-Serverprotokollierung aktiviert wurde, können nicht exportiert werden CloudWatch.

Sie können jedoch einen neuen Cluster mit derselben Kubernetes-Version erstellen und beim Erstellen des Clusters die API-Serverprotokollierung aktivieren. Bei Clustern mit derselben Plattformversion sind dieselben Flags aktiviert, sodass Ihre Flags mit den Flags des neuen Clusters übereinstimmen sollten. Wenn Sie die Anzeige der Flags für den neuen Cluster in abgeschlossen haben CloudWatch, können Sie den neuen Cluster löschen.

API-Aufrufe als AWS CloudTrail Ereignisse protokollieren

Amazon EKS ist integriert in AWS CloudTrail. CloudTrail ist ein Service, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Amazon EKS bereitstellt. CloudTrail erfasst alle API-Aufrufe für Amazon EKS als Ereignisse. Dazu gehören Aufrufe von der Amazon-EKS-Konsole und von Code-Aufrufen der Amazon-EKS-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren. Dies umfasst Ereignisse von Amazon EKS. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der CloudTrail gesammelten Informationen können Sie verschiedene Details zu einer Anfrage ermitteln. Sie können zum Beispiel ermitteln, wann eine Anfrage an Amazon EKS gestellt wurde, von welcher IP-Adresse aus die Anfrage gestellt wurde und wer die Anfrage gestellt hat.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Themen

- [Hilfreiche Referenzen anzeigen für AWS CloudTrail](#)
- [AWS CloudTrail Logdateieinträge analysieren](#)
- [Metriken für Amazon EC2 Auto Scaling Scaling-Gruppen anzeigen](#)

Hilfreiche Referenzen anzeigen für AWS CloudTrail

Wenn Sie Ihr AWS Konto erstellen, CloudTrail ist es auch für Ihr AWS Konto aktiviert. Wenn eine Aktivität in Amazon EKS auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für Amazon EKS, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen AWS Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in den folgenden Ressourcen.

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle Amazon EKS-Aktionen werden von der Amazon [EKS-API-Referenz](#) protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der [DeleteCluster](#)Abschnitte [CreateCluster](#), [ListClusters](#)und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen über die Art der für die Abfrage genutzten IAM-Identität und dazu, welche Anmeldeinformationen verwendet wurden. Wenn temporäre Anmeldeinformationen verwendet wurden, zeigt der Eintrag, wie die Anmeldeinformationen bezogen wurden.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

AWS CloudTrail Logdateieinträge analysieren

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion. Dazu gehören Informationen wie Datum und Uhrzeit der Aktion sowie die verwendeten Anforderungsparameter. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die [CreateCluster](#)Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/username",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "username"
  },
  "eventTime": "2018-05-28T19:16:43Z",
  "eventSource": "eks.amazonaws.com",
  "eventName": "CreateCluster",
  "awsRegion": "region-code",
  "sourceIPAddress": "205.251.233.178",
  "userAgent": "PostmanRuntime/6.4.0",
  "requestParameters": {
    "resourcesVpcConfig": {
```



```

    "subnetIds": [
      "subnet-a670c2df",
      "subnet-4f8c5004"
    ],
    },
    "roleArn": "arn:aws:iam::111122223333:role/AWSServiceRoleForAmazonEKS-
CAC1G1VH3ZKZ",
    "clusterName": "test"
  },
  "responseElements": {
    "cluster": {
      "clusterName": "test",
      "status": "CREATING",
      "createdAt": 1527535003.208,
      "certificateAuthority": {},
      "arn": "arn:aws:eks:region-code:111122223333:cluster/test",
      "roleArn": "arn:aws:iam::111122223333:role/AWSServiceRoleForAmazonEKS-
CAC1G1VH3ZKZ",
      "version": "1.10",
      "resourcesVpcConfig": {
        "securityGroupIds": [],
        "vpcId": "vpc-21277358",
        "subnetIds": [
          "subnet-a670c2df",
          "subnet-4f8c5004"
        ]
      }
    }
  },
  "requestID": "a7a0735d-62ab-11e8-9f79-81ce5b2b7d37",
  "eventID": "eab22523-174a-499c-9dd6-91e7be3ff8e3",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

Protokolleinträge für serviceverknüpfte Amazon-EKS-Rollen

Die mit dem Amazon EKS-Service verknüpften Rollen führen API-Aufrufe an AWS Ressourcen durch. CloudTrail Protokolleinträge mit `username: AWSServiceRoleForAmazonEKS` und `username: AWSServiceRoleForAmazonEKSNodegroup` erscheinen für Aufrufe, die von den mit dem Amazon EKS-Service verknüpften Rollen getätigt wurden. Weitere Informationen zu Amazon EKS und serviceverknüpften Rollen finden Sie unter [the section called “Service-verknüpfte Rollen”](#).

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der eine [DeleteInstanceProfile](#)Aktion demonstriert, die von der `AWSServiceRoleForAmazonEKSNodegroup` serviceverknüpften Rolle ausgeführt wird, wie im `vermerktsessionContext`.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO3WHGPEZ7SJ2CW55C5:EKS",
    "arn": "arn:aws: sts::111122223333:assumed-role/
AWSServiceRoleForAmazonEKSNodegroup/EKS",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO3WHGPEZ7SJ2CW55C5",
        "arn": "arn:aws: iam::111122223333:role/aws-service-role/eks-
nodegroup.amazonaws.com/AWSServiceRoleForAmazonEKSNodegroup",
        "accountId": "111122223333",
        "userName": "AWSServiceRoleForAmazonEKSNodegroup"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-02-26T00:56:33Z"
      }
    },
    "invokedBy": "eks-nodegroup.amazonaws.com"
  },
  "eventTime": "2020-02-26T00:56:34Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "DeleteInstanceProfile",
  "awsRegion": "region-code",
  "sourceIPAddress": "eks-nodegroup.amazonaws.com",
  "userAgent": "eks-nodegroup.amazonaws.com",
  "requestParameters": {
    "instanceProfileName": "eks-11111111-2222-3333-4444-abcdef123456"
  },
  "responseElements": null,
  "requestID": "11111111-2222-3333-4444-abcdef123456",
  "eventID": "11111111-2222-3333-4444-abcdef123456",
}
```

```
"eventType": "AwsApiCall",  
"recipientAccountId": "111122223333"  
}
```

Metriken für Amazon EC2 Auto Scaling Scaling-Gruppen anzeigen

Für von Amazon EKS verwaltete Knotengruppen sind Amazon EC2 Auto Scaling Scaling-Gruppenmetriken standardmäßig ohne zusätzliche Kosten aktiviert. Die Auto Scaling Scaling-Gruppe sendet CloudWatch jede Minute Stichprobendaten an Amazon. Diese Metriken können durch den Namen der Auto Scaling Scaling-Gruppen verfeinert werden. Sie bieten Ihnen einen kontinuierlichen Einblick in den Verlauf der Auto Scaling Scaling-Gruppe, die Ihre verwalteten Knotengruppen unterstützt, z. B. über Veränderungen der Gruppengröße im Laufe der Zeit. Auto Scaling Scaling-Gruppenmetriken sind in der [Amazon CloudWatch](#) - oder Auto Scaling Scaling-Konsole verfügbar. Weitere Informationen finden Sie unter [Überwachen von CloudWatch Metriken für Ihre Auto Scaling Scaling-Gruppen und -Instances](#).

Mit der Erfassung von Auto Scaling Scaling-Gruppenmetriken können Sie die Skalierung verwalteter Knotengruppen überwachen. Die Auto-Scaling-Gruppenmetriken zeigen die minimale, maximale und gewünschte Größe einer Auto-Scaling-Gruppe an. Sie können eine Warnung auslösen, wenn die Anzahl der Knoten in einer Knotengruppe unter die Mindestgröße fällt, was auf eine fehlerhafte Knotengruppe hindeuten würde. Die Überwachung der Knotengruppengröße ist auch nützlich, um die maximale Anzahl so anzupassen, dass Ihrer Datenebene nicht die Kapazität ausgeht.

Wenn Sie es vorziehen, dass diese Metriken nicht erfasst werden, können Sie wählen, ob Sie alle oder nur einige davon deaktivieren möchten. Sie können dies beispielsweise tun, um Rauschen in Ihren CloudWatch Dashboards zu vermeiden. Weitere Informationen finden Sie unter [CloudWatch Amazon-Metriken für Amazon EC2 Auto Scaling](#).

Senden Sie Metrik- und Trace-Daten mit ADOT Operator

Amazon EKS unterstützt die Verwendung der AWS Management Console AWS CLI und der Amazon EKS-API zur Installation und Verwaltung des [AWS Distro for OpenTelemetry \(ADOT\)](#) Operators. [Auf diese Weise können Sie Ihre auf Amazon EKS ausgeführten Anwendungen einfacher in die Lage versetzen, Metrik- und Trace-Daten an mehrere Überwachungsservice-Optionen wie Amazon CloudWatch, Prometheus und X-Ray zu senden.](#)

Weitere Informationen finden Sie in der Dokumentation unter [Erste Schritte mit AWS Distro für die OpenTelemetry Verwendung von EKS-Add-Ons](#) in der AWS Distro. OpenTelemetry

Zeigen Sie aggregierte Daten zu Cluster-Ressourcen mit dem EKS-Dashboard an

image::images/eks-dashboard.png[screenshot of account level cluster metrics]

Was ist das Amazon EKS Dashboard?

Das Amazon EKS-Dashboard bietet konsolidierten Einblick in Ihre Kubernetes-Cluster in mehreren AWS Regionen und AWS Konten. Mit diesem Dashboard können Sie:

- Verfolgen Sie Cluster, für die innerhalb der nächsten 90 Tage end-of-support automatische Upgrades geplant sind.
- Das Projekt EKS kontrolliert die Kosten für Cluster im Rahmen des erweiterten Supports.
- Überprüfen Sie die Cluster anhand von Erkenntnissen, die vor dem Upgrade berücksichtigt werden müssen.
- Identifizieren Sie verwaltete Knotengruppen, auf denen bestimmte AMI-Versionen ausgeführt werden.
- Überwachen Sie die Verteilung der Clusterunterstützung (Standard im Vergleich zu erweitertem Support).

Das EKS-Dashboard ist in EKS Cluster Insights integriert, um Probleme mit Ihren Clustern aufzudecken, wie z. B. die Verwendung von veraltetem Kubernetes. APIs Weitere Informationen finden Sie unter [the section called "Cluster-Erkenntnisse"](#).

Note

Das EKS-Dashboard ist nicht in Echtzeit und wird alle 12 Stunden aktualisiert. Informationen zur Cluster-Überwachung in Echtzeit finden Sie unter [Überwachen Sie Cluster](#)

Wie verwendet das Dashboard AWS Organizations?

Für die Funktionalität des Amazon EKS-Dashboards ist die Integration von AWS Organizations erforderlich. Es nutzt AWS Organizations, um Clusterinformationen sicher kontenübergreifend zu sammeln. Diese Integration ermöglicht eine zentrale Verwaltung und Steuerung, wenn Ihre AWS Infrastruktur skaliert.

Wenn AWS Organizations für Ihre Infrastruktur nicht aktiviert ist, finden Sie Anweisungen zur Einrichtung im AWS [Organizations-Benutzerhandbuch](#).

Regions- und kontoübergreifender Zugriff

Das EKS-Dashboard kann Clusterressourcen in jedem Konto anzeigen, das Mitglied der AWS Organisation ist. Informationen zum Generieren einer Liste der AWS Konten in Ihrer Organisation finden Sie unter [Exportieren von Details für alle Konten in einer Organisation](#).

Die AWS Region us-east-1 generiert das Dashboard. Sie müssen sich in dieser Region anmelden, um das Dashboard zu sehen. Das Dashboard aggregiert Daten über AWS Regionen hinweg, beinhaltet jedoch keine Regionen in China. GovCloud

Wichtige Begriffe

- **AWS Organisation:** Eine einheitliche Verwaltungsstruktur für mehrere AWS Konten.
- **Verwaltungskonto:** Das Hauptkonto, das die AWS Organisation kontrolliert.
- **Mitgliedskonto:** Jedes Konto innerhalb der Organisation mit Ausnahme des Verwaltungskontos.
- **Delegierter Administrator:** Ein Mitgliedskonto, dem bestimmte kontoübergreifende Administratorrechte gewährt wurden. Innerhalb des Verwaltungskontos können Sie pro Dienst ein delegiertes Administratorkonto auswählen. AWS
- **Vertrauenswürdiger Zugriff:** Autorisierung für das EKS-Dashboard für den Zugriff auf Clusterinformationen über Unternehmenskonten hinweg.
- **Serviceverknüpfte Rolle (SLRs):** Eine einzigartige Art von IAM-Rolle, die direkt mit einem AWS Service verknüpft ist. Das EKS-Dashboard verwendet eine Spiegelreflexkamera, um Informationen über Ihre Konten und Organisationen zu lesen.
- Weitere Informationen finden Sie unter [Terminologie und Konzepte](#) im AWS Organizations User Guide.

Allgemeiner Überblick

1. Greifen Sie auf das Verwaltungskonto Ihrer AWS Organisation zu.
 - Die Schritte für den Zugriff auf das Verwaltungskonto hängen davon ab, wie Sie Ihre AWS Organisation konfiguriert haben. Sie können beispielsweise über AWS [Identity Center](#) oder [Okta](#) auf das Verwaltungskonto zugreifen.
2. Aktivieren Sie den vertrauenswürdigen Zugriff über die EKS-Konsole.

3. Weisen Sie anhand seiner AWS Konto-ID einen delegierten Administrator zu.
4. Wechseln Sie zum delegierten Administratorkonto.
5. Greifen Sie auf die erweiterte EKS-Konsole mit unternehmensweiter Transparenz zu.

Aktivieren Sie das EKS-Dashboard über die Konsole AWS

Important

Sie müssen mit dem Verwaltungskonto Ihrer AWS Organisation angemeldet sein, um das EKS-Dashboard zu aktivieren.

Rufen Sie die EKS-Dashboard-Einstellungen auf

1. Überprüfen Sie Folgendes:
 - a. Sie haben AWS Organizations aktiviert und konfiguriert.
 - b. Sie sind beim Verwaltungskonto der Organisation angemeldet.
 - c. Sie sehen die AWS Management Console in der Region US-East-1.
2. Navigieren Sie zur EKS-Konsole.
3. Öffnen Sie in der linken Seitenleiste die Dashboard-Einstellungen.

Zugriff auf das Amazon EKS-Dashboard einrichten

1. Suchen Sie die AWS Konto-ID des AWS Kontos, dem Sie die Anzeige des EKS-Dashboards ermöglichen möchten.
 - a. Dieser Schritt ist optional, wird aber empfohlen. Wenn Sie dies nicht tun, können Sie nur über das Verwaltungskonto auf das Dashboard zugreifen. Als bewährte Methode sollten Sie den Zugriff auf das Verwaltungskonto einschränken.
2. Klicken Sie auf Vertrauenswürdigen Zugriff aktivieren.
 - a. Sie können das Dashboard jetzt vom Verwaltungskonto aus aufrufen.
3. Klicken Sie auf Delegierten Administrator registrieren und geben Sie die Konto-ID des AWS Kontos ein, mit dem Sie das Dashboard aufrufen möchten.
 - a. Sie können das Dashboard jetzt vom delegierten Administratorkonto oder vom Verwaltungskonto aus aufrufen.

Informationen zu den für die Aktivierung des Dashboards erforderlichen Berechtigungen finden Sie unter [Mindestanzahl an erforderlichen IAM-Richtlinien](#).

Sehen Sie sich das EKS-Dashboard an

1. Melden Sie sich mit dem delegierten Administratorkonto (vorgeschlagen) oder dem Verwaltungskonto an.
2. Melden Sie sich in der Region us-east-1 an.
3. Gehen Sie zum EKS-Dienst und wählen Sie in der linken Seitenleiste Dashboard aus.

Note

[Überprüfen Sie die IAM-Berechtigungen, die für die Anzeige des EKS-Dashboards erforderlich sind.](#)

Konfigurieren Sie das Dashboard

Sie können die Ansicht des Dashboards konfigurieren und Ressourcen filtern.

Verfügbare Ressourcen

- Cluster: Zeigen Sie aggregierte Informationen über den Status und den Standort von EKS-Clustern an.
 - Cluster mit Gesundheitsproblemen.
 - Cluster auf EKS Extended Support.
 - Aufschlüsselung der Cluster nach Kubernetes-Version.
- Verwaltete Knotengruppen: Sehen Sie sich die verwalteten Knotengruppen und EC2 Instanzen an.
 - Knotengruppen nach AMI-Typ, z. B. Amazon Linux oder Bottlerocket.
 - Probleme mit dem Zustand von Knotengruppen.
 - Verteilung des Instanztyps.
- Add-Ons: Erfahren Sie, welche Amazon EKS Add-ons Sie installiert haben und welchen Status sie haben.
 - Anzahl der Installationen pro Add-on.
 - Add-ons mit Gesundheitsproblemen.

- Versionsverteilung pro Add-on.

Verfügbare Ansichten

- Diagrammansicht
 - Eine anpassbare Widget-Ansicht, in der Grafiken und Visualisierungen der ausgewählten Ressource angezeigt werden.
 - Änderungen an der Diagrammansicht, z. B. das Entfernen eines Widgets, sind für alle Benutzer des EKS-Dashboards sichtbar.
- Ansicht „Ressourcen“
 - Eine Listenansicht der ausgewählten Ressource mit Unterstützung von Filtern.
- Kartenansicht
 - Zeigt die geografische Verteilung der ausgewählten Ressource an.

Filtern Sie das EKS-Dashboard

Sie können das EKS-Dashboard nach folgenden Kriterien filtern:

- AWS Konto
- Organisationseinheit, definiert durch AWS Organizations
- AWS Region

Deaktivieren Sie das EKS-Dashboard über die AWS Konsole

1. Überprüfen Sie Folgendes:
 - a. Sie haben AWS Organizations aktiviert und konfiguriert.
 - b. Sie sind beim Verwaltungskonto der Organisation angemeldet.
 - c. Sie sehen die AWS Management Console in der Region US-East-1.
2. Navigieren Sie zur EKS-Konsole.
3. Öffnen Sie in der linken Seitenleiste die Dashboard-Einstellungen.
4. Klicken Sie auf Vertrauenswürdigen Zugriff deaktivieren.

Beheben Sie Fehler im EKS-Dashboard

Problem beim Aktivieren des EKS-Dashboards

- Sie müssen mit dem Verwaltungskonto einer AWS Organisation angemeldet sein.
 - Wenn Sie noch keine AWS Organisation haben, erstellen Sie eine. Erfahren Sie, wie Sie [eine Organisation erstellen und konfigurieren](#).
 - Wenn Ihr AWS Konto bereits Mitglied einer AWS Organisation ist, identifizieren Sie den Administrator der Organisation.
- Sie müssen mit dem AWS Konto angemeldet sein und über ausreichende IAM-Berechtigungen verfügen, um AWS Organisationsressourcen erstellen und aktualisieren zu können.

Problem beim Anzeigen des EKS-Dashboards

- Sie müssen mit einem der folgenden AWS Konten angemeldet sein:
 - Das Verwaltungskonto der AWS Organisation
 - Ein delegiertes Administratorkonto, das in den EKS-Dashboard-Einstellungen des Verwaltungskontos angegeben ist.
- Wenn Sie das EKS-Dashboard kürzlich aktiviert haben, beachten Sie bitte, dass das erstmalige Einpflegen der Daten bis zu 12 Stunden dauern kann.
- [Versuchen Sie, das Dashboard mithilfe der CLI erneut zu aktivieren](#), einschließlich der Erstellung der serviceverknüpften Rolle.

Dashboard-Widgets werden unerwartet verschoben

- Das EKS-Dashboard speichert die konfigurierbare Widget-Ansicht auf AWS Kontoebene. Wenn Sie die Widget-Ansicht ändern, können andere Personen, die dasselbe AWS Konto verwenden, die Änderungen sehen.

Konfiguration der EKS-Dashboard-Integration mit AWS Organizations

Dieser Abschnitt enthält step-by-step Anweisungen zur Konfiguration der Integration des EKS-Dashboards mit AWS Organizations. Sie erfahren, wie Sie den vertrauenswürdigen Zugriff zwischen Diensten aktivieren und deaktivieren und wie Sie delegierte Administratorkonten registrieren und

abmelden. Jede Konfigurationsaufgabe kann entweder über die AWS Konsole oder die AWS CLI ausgeführt werden.

Den vertrauenswürdigen Zugriff aktivieren

Vertrauenswürdiger Zugriff autorisiert das EKS-Dashboard, sicher auf Clusterinformationen aller Konten in Ihrer Organisation zuzugreifen.

Verwenden der Konsole AWS

1. Loggen Sie sich in das Verwaltungskonto Ihrer AWS Organisation ein.
2. Navigieren Sie zur EKS-Konsole in der Region us-east-1.
3. Wählen Sie in der linken Seitenleiste Dashboard-Einstellungen aus.
4. Klicken Sie auf Vertrauenswürdigen Zugriff aktivieren.

Note

Wenn Sie den vertrauenswürdigen Zugriff über die EKS-Konsole aktivieren, erstellt das System automatisch die `AWSServiceRoleForAmazonEKSDashboard` serviceverknüpfte Rolle. Diese automatische Erstellung erfolgt nicht, wenn Sie den vertrauenswürdigen Zugriff über die AWS CLI oder die AWS Organisationskonsole aktivieren.

Verwenden der AWS CLI

1. Melden Sie sich beim Verwaltungskonto Ihrer AWS Organisation an.
2. Führen Sie die folgenden Befehle aus:

```
aws iam create-service-linked-role --aws-service-name dashboard.eks.amazonaws.com
aws organizations enable-aws-service-access --service-principal eks.amazonaws.com
```

So deaktivieren Sie den vertrauenswürdigen Zugriff

Durch die Deaktivierung des vertrauenswürdigen Zugriffs wird dem EKS-Dashboard die Berechtigung entzogen, auf Clusterinformationen aller Konten Ihrer Organisation zuzugreifen.

Verwenden der Konsole AWS

1. Loggen Sie sich in das Verwaltungskonto Ihrer AWS Organisation ein.
2. Navigieren Sie zur EKS-Konsole in der Region us-east-1.
3. Wählen Sie in der linken Seitenleiste Dashboard-Einstellungen aus.
4. Klicken Sie auf Vertrauenswürdigen Zugriff deaktivieren.

Verwenden der AWS CLI

1. Melden Sie sich beim Verwaltungskonto Ihrer AWS Organisation an.
2. Führen Sie den folgenden Befehl aus:

```
aws organizations disable-aws-service-access --service-principal eks.amazonaws.com
```

Aktivieren eines delegierten Administrators

Ein delegierter Administrator ist ein Mitgliedskonto, dem die Berechtigung zum Zugriff auf das EKS-Dashboard erteilt wurde.

Verwenden der Konsole AWS

1. Loggen Sie sich in das Verwaltungskonto Ihrer AWS Organisation ein.
2. Navigieren Sie zur EKS-Konsole in der Region us-east-1.
3. Wählen Sie in der linken Seitenleiste Dashboard-Einstellungen aus.
4. Klicken Sie auf Delegierten Administrator registrieren.
5. Geben Sie die Konto-ID des AWS Kontos ein, das Sie als delegierten Administrator auswählen möchten.
6. Bestätigen Sie die Registrierung.

Verwenden der AWS CLI

1. Melden Sie sich beim Verwaltungskonto Ihrer AWS Organisation an.
2. Führen Sie den folgenden Befehl aus und 123456789012 ersetzen Sie ihn durch Ihre Konto-ID:

```
aws organizations register-delegated-administrator --account-id 123456789012 --  
service-principal eks.amazonaws.com
```

Deaktivieren Sie ein delegiertes Administratorkonto

Durch die Deaktivierung eines delegierten Administrators wird dem Konto die Zugriffsberechtigung für das EKS-Dashboard entzogen.

Verwenden der Konsole AWS

1. Loggen Sie sich in das Verwaltungskonto Ihrer AWS Organisation ein.
2. Navigieren Sie zur EKS-Konsole in der Region us-east-1.
3. Wählen Sie in der linken Seitenleiste Dashboard-Einstellungen aus.
4. Suchen Sie den delegierten Administrator in der Liste.
5. Klicken Sie neben dem Konto, das Sie als delegierter Administrator entfernen möchten, auf Abmelden.

Verwenden der AWS CLI

1. Melden Sie sich beim Verwaltungskonto Ihrer AWS Organisation an.
2. Führen Sie den folgenden Befehl aus und 123456789012 ersetzen Sie ihn durch die Konto-ID des delegierten Administrators:

```
aws organizations deregister-delegated-administrator --account-id 123456789012 --  
service-principal eks.amazonaws.com
```

Minimale IAM-Richtlinien erforderlich

In diesem Abschnitt werden die IAM-Mindestrichtlinien beschrieben, die erforderlich sind, um vertrauenswürdigen Zugriff zu ermöglichen und einen Administrator für die EKS-Dashboard-Integration mit AWS Organizations zu delegieren.

Richtlinie zur Aktivierung des vertrauenswürdigen Zugriffs

Um den vertrauenswürdigen Zugriff zwischen EKS Dashboard und AWS Organizations zu aktivieren, benötigen Sie die folgenden Berechtigungen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/
dashboard.eks.amazonaws.com/AWSServiceRoleForAmazonEKSDashboard"
    }
  ]
}
```

Richtlinie für die Delegierung eines Administrators

Um einen delegierten Administrator für das EKS-Dashboard zu registrieren oder abzumelden, benötigen Sie die folgenden Berechtigungen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*"
    }
  ]
}
```

Richtlinie zum Anzeigen des EKS-Dashboards

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonEKSDashboardReadOnly",
      "Effect": "Allow",
      "Action": [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AmazonOrganizationsReadOnly",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AmazonOrganizationsDelegatedAdmin",
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}
```

 Note

Diese Richtlinien müssen dem IAM-Prinzipal (Benutzer oder Rolle) im Verwaltungskonto Ihrer AWS Organisation zugeordnet sein. Mitgliedskonten können keinen vertrauenswürdigen Zugriff ermöglichen oder Administratoren delegieren.

Erweitern Sie EKS mit integrierten AWS Services

Zusätzlich zu den in anderen Abschnitten behandelten Services arbeitet Amazon EKS mit weiteren AWS Services zusammen, um zusätzliche Lösungen bereitzustellen. In diesem Thema werden einiger der weiteren Services aufgeführt, die mithilfe von Amazon EKS ihre Funktionalität erweitern, sowie Services, die Amazon EKS zur Ausführung von Aufgaben nutzt.

Themen

- [Erstellen Sie Amazon EKS-Ressourcen mit AWS CloudFormation](#)
- [Analysieren Sie Sicherheitsereignisse auf EKS mit Amazon Detective](#)
- [Erkennen Sie Bedrohungen mit Amazon GuardDuty](#)
- [Beurteilen Sie die Widerstandsfähigkeit von EKS-Clustern mit AWS Resilience Hub](#)
- [Zentralisieren und analysieren Sie EKS-Sicherheitsdaten mit Security Lake](#)
- [Ermöglichen Sie sichere clusterübergreifende Konnektivität mit Amazon VPC Lattice](#)
- [Starten Sie EKS-Cluster mit niedriger Latenz und AWS Local Zones](#)

Erstellen Sie Amazon EKS-Ressourcen mit AWS CloudFormation

Amazon EKS ist integriert mit AWS CloudFormation, ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt, z. B. einen Amazon EKS-Cluster, und AWS CloudFormation kümmert sich um die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie sie verwenden AWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Amazon EKS-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einfach einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren AWS Konten und Regionen bereit.

Amazon EKS und AWS CloudFormation Vorlagen

Um Ressourcen für Amazon EKS und verwandte Dienstleistungen bereitzustellen und zu konfigurieren, müssen Sie [AWS CloudFormation -Vorlagen](#) kennen und verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie

in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen bei den ersten Schritten mit Vorlagen zu helfen. AWS CloudFormation Weitere Informationen finden Sie unter [Was ist AWS CloudFormation Designer?](#) im AWS CloudFormation Benutzerhandbuch.

Amazon EKS unterstützt das Erstellen von Clustern und Knotengruppen in AWS CloudFormation. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Ihre Amazon EKS-Ressourcen, finden Sie in der [Amazon EKS-Ressourcentyp-Referenz](#) im AWS CloudFormation Benutzerhandbuch.

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

- [AWS CloudFormation](#)
- [AWS CloudFormation Benutzerhandbuch](#)
- [AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle](#)

Analysieren Sie Sicherheitereignisse auf EKS mit Amazon Detective

[Amazon Detective](#) hilft Ihnen, die Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren. Detective sammelt automatisch Protokolldaten von Ihren AWS Ressourcen. Es verwendet dann Machine Learning, statistische Analysen und die Diagrammtheorie, um Visualisierungen zu erstellen, mit denen Sie effektive Sicherheitsuntersuchungen schneller und effizienter durchführen können. Detective bietet vordefinierte Datenaggregationen, Übersichten und Kontexte, mit denen Sie Art und Ausmaß möglicher Sicherheitsprobleme schnell analysieren und feststellen können. Weitere Informationen finden Sie im [Benutzerhandbuch von Amazon Detective](#).

Detective organisiert Kubernetes und AWS Daten zu Ergebnissen wie:

- Amazon EKS-Clusterdetails, einschließlich der IAM-Identität, mit der der Cluster erstellt wurde, und der Servicerolle des Clusters. Sie können die Aktivität AWS und die Kubernetes-API-Aktivität dieser IAM-Identitäten mit Detective untersuchen.
- Container-Details, wie das Image und der Sicherheitskontext. Sie können auch die Details zu beendeten Pods überprüfen.

- Kubernetes-API-Aktivität, einschließlich allgemeiner Trends bei der API-Aktivität und Details zu bestimmten API-Aufrufen. Sie können beispielsweise die Anzahl der erfolgreichen und fehlgeschlagenen Kubernetes-API-Aufrufe anzeigen, die in einem ausgewählten Zeitraum ausgegeben wurden. Darüber hinaus kann der Abschnitt über neu beobachtete API-Aufrufe hilfreich sein, um verdächtige Aktivitäten zu identifizieren.

Amazon EKS Audit Logs sind ein optionales Datenquellenpaket, das Ihrem Detective-Verhaltensdiagramm hinzugefügt werden kann. Sie können die verfügbaren optionalen Quellpakete und deren Status in Ihrem Konto einsehen. Weitere Informationen finden Sie unter [Amazon-EKS-Auditprotokolle für Detective](#) im Benutzerhandbuch von Amazon Detective.

Verwenden Sie Amazon Detective mit Amazon EKS

Bevor Sie die Ergebnisse überprüfen können, muss Detective für mindestens 48 Stunden in derselben AWS Region aktiviert sein, in der sich Ihr Cluster befindet. Weitere Informationen finden Sie unter [Einrichten von Amazon Detective](#) im Benutzerhandbuch von Amazon Detective.

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie Search (Suche) im linken Navigationsbereich.
3. Wählen Sie Choose type (Typ auswählen) und anschließend EKS cluster (EKS-Cluster) aus.
4. Geben Sie den Clusternamen oder ARN ein und wählen Sie dann Search (Suchen) aus.
5. Wählen Sie in den Suchergebnissen den Namen des Clusters aus, für den Sie Aktivitäten anzeigen möchten. Weitere Informationen darüber, was Sie sich ansehen können, finden Sie unter [Allgemeine Kubernetes-API-Aktivität mit einem Amazon EKS-Cluster](#) im Amazon Detective User Guide.

Erkennen Sie Bedrohungen mit Amazon GuardDuty

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der Ihnen hilft, Ihre Konten, Container, Workloads und die Daten in Ihrer AWS Umgebung zu schützen. Mithilfe von Modellen für maschinelles Lernen (ML) und Funktionen zur Erkennung von Anomalien und Bedrohungen werden GuardDuty kontinuierlich verschiedene Protokollquellen und Laufzeitaktivitäten überwacht, um potenzielle Sicherheitsrisiken und böswillige Aktivitäten in Ihrer Umgebung zu identifizieren und zu priorisieren.

GuardDuty Bietet unter anderem die folgenden beiden Funktionen zur Erkennung potenzieller Bedrohungen für Ihre EKS-Cluster: EKS-Schutz und Runtime Monitoring.

 Note

Neu: Amazon EKS Auto Mode lässt sich integrieren GuardDuty.

EKS-Schutz

Diese Funktion deckt die Bedrohungserkennung ab und hilft Ihnen, Amazon EKS-Cluster zu schützen, indem die zugehörigen Kubernetes-Audit-Logs überwacht werden. Kubernetes-Audit-Logs erfassen sequentielle Aktionen innerhalb Ihres Clusters, einschließlich Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden, und der Kontrollebene. So GuardDuty können Sie beispielsweise feststellen, dass Aufrufe zur potenziellen Manipulation von Ressourcen in einem Kubernetes-Cluster von einem nicht authentifizierten Benutzer APIs aufgerufen wurden.

Wenn Sie EKS Protection aktivieren, können GuardDuty Sie nur zur kontinuierlichen Erkennung von Bedrohungen auf Ihre Amazon EKS-Auditprotokolle zugreifen. Wenn eine potenzielle Bedrohung für Ihren Cluster GuardDuty identifiziert wird, generiert es ein zugehöriges Kubernetes-Audit-Log-Ergebnis eines bestimmten Typs. Weitere Informationen zu den Arten von Ergebnissen, die in Kubernetes-Audit-Logs verfügbar sind, finden Sie unter [Kubernetes-Audit-Logs — Finding Types im Amazon-Benutzerhandbuch](#). GuardDuty

Weitere Informationen finden Sie unter [EKS-Schutz](#) im GuardDuty Amazon-Benutzerhandbuch.

Überwachung der Laufzeit

Diese Funktion überwacht und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen.

Wenn Sie Runtime Monitoring aktivieren und den GuardDuty Agenten in Ihren Amazon EKS-Clustern installieren, GuardDuty beginnt die Überwachung der Runtime-Ereignisse, die mit diesem Cluster verknüpft sind. Beachten Sie, dass der GuardDuty Agent und Runtime Monitoring nicht für Amazon EKS-Hybridknoten verfügbar sind, sodass Runtime Monitoring nicht für Runtime-Ereignisse verfügbar ist, die auf Ihren Hybridknoten auftreten. Wenn eine potenzielle Bedrohung für Ihren Cluster GuardDuty identifiziert wird, wird ein zugehöriges Runtime Monitoring-Ergebnis

generiert. Beispielsweise kann eine Bedrohung möglicherweise damit beginnen, dass ein einzelner Container kompromittiert wird, auf dem eine anfällige Webanwendung ausgeführt wird. Diese Webanwendung verfügt möglicherweise über Zugriffsberechtigungen für die zugrunde liegenden Container und Workloads. In diesem Szenario könnten falsch konfigurierte Anmeldeinformationen möglicherweise zu einem umfassenderen Zugriff auf das Konto und die darin gespeicherten Daten führen.

Um Runtime Monitoring zu konfigurieren, installieren Sie den GuardDuty Agenten als Amazon EKS-Add-on in Ihrem Cluster. Weitere Informationen zum Add-on finden Sie unter [the section called “ AWS Add-Ons”](#).

Weitere Informationen finden Sie unter [Runtime Monitoring](#) im GuardDuty Amazon-Benutzerhandbuch.

Beurteilen Sie die Widerstandsfähigkeit von EKS-Clustern mit AWS Resilience Hub

AWS Resilience Hub bewertet die Resilienz eines Amazon EKS-Clusters anhand der Analyse seiner Infrastruktur. AWS Resilience Hub verwendet die Konfiguration für die rollenbasierte Zugriffskontrolle (RBAC) von Kubernetes, um die in Ihrem Cluster bereitgestellten Kubernetes-Workloads zu bewerten. Weitere Informationen finden Sie unter [Aktivieren des AWS Resilience Hub-Zugriffs auf Ihren Amazon EKS-Cluster](#) im AWS Resilience Hub-Benutzerhandbuch.

Zentralisieren und analysieren Sie EKS-Sicherheitsdaten mit Security Lake

Amazon Security Lake ist ein vollständig verwalteter Security Data Lake-Service, mit dem Sie Sicherheitsdaten aus verschiedenen Quellen, einschließlich Amazon EKS, zentralisieren können. Durch die Integration von Amazon EKS mit Security Lake können Sie tiefere Einblicke in die Aktivitäten gewinnen, die auf Ihren Kubernetes-Ressourcen ausgeführt werden, und die Sicherheitslage Ihrer Amazon EKS-Cluster verbessern.

Note

Weitere Informationen zur Verwendung von Security Lake mit Amazon EKS und zur Einrichtung von Datenquellen finden Sie in der [Amazon Security Lake-Dokumentation](#).

Vorteile der Verwendung von Security Lake mit Amazon Amazon EKS

Zentralisierte Sicherheitsdaten — Security Lake sammelt und zentralisiert automatisch Sicherheitsdaten aus Ihren Amazon EKS-Clustern zusammen mit Daten von anderen AWS Diensten, SaaS-Anbietern, lokalen Quellen und Quellen von Drittanbietern. Dies bietet einen umfassenden Überblick über Ihre Sicherheitslage in Ihrem gesamten Unternehmen.

Standardisiertes Datenformat — Security Lake konvertiert die gesammelten Daten in das [Open Cybersecurity Schema Framework \(OCSF\) -Format](#), bei dem es sich um ein Standard-Open-Source-Schema handelt. Diese Normalisierung ermöglicht eine einfachere Analyse und Integration mit anderen Sicherheitstools und -diensten.

Verbesserte Bedrohungserkennung — Durch die Analyse der zentralen Sicherheitsdaten, einschließlich der Protokolle der Amazon EKS-Kontrollebene, können Sie potenziell verdächtige Aktivitäten in Ihren Amazon EKS-Clustern effektiver erkennen. Dies hilft dabei, Sicherheitsvorfälle zu identifizieren und umgehend darauf zu reagieren.

Vereinfachtes Datenmanagement — Security Lake verwaltet den Lebenszyklus Ihrer Sicherheitsdaten mit anpassbaren Aufbewahrungs- und Replikationseinstellungen. Dies vereinfacht die Datenverwaltungsaufgaben und stellt sicher, dass Sie die für Compliance- und Auditzwecke erforderlichen Daten aufbewahren.

Security Lake für Amazon EKS aktivieren

1. Aktivieren Sie die Protokollierung der Amazon EKS-Kontrollebene für Ihre EKS-Cluster. Ausführliche Anweisungen finden Sie unter [Aktivieren und Deaktivieren von Protokollen auf Kontrollebene](#).
2. [Fügen Sie Amazon EKS Audit Logs als Quelle in Security Lake hinzu](#). Security Lake beginnt dann mit der Erfassung detaillierter Informationen über die Aktivitäten, die auf den Kubernetes-Ressourcen ausgeführt werden, die in Ihren EKS-Clustern ausgeführt werden.
3. [Konfigurieren Sie die Aufbewahrungs- und Replikationseinstellungen](#) für Ihre Sicherheitsdaten in Security Lake auf der Grundlage Ihrer Anforderungen.
4. Verwenden Sie die in Security Lake gespeicherten normalisierten OCSF-Daten für die Reaktion auf Vorfälle, Sicherheitsanalysen und die Integration mit anderen AWS Diensten oder Tools von Drittanbietern. Beispielsweise können Sie [mithilfe von Amazon Ingestion Sicherheitsinformationen aus Amazon Security Lake-Daten generieren](#). OpenSearch

Analysieren von EKS-Protokollen in Security Lake

Security Lake normalisiert EKS-Protokollereignisse auf das OCSF-Format, wodurch es einfacher wird, die Daten zu analysieren und mit anderen Sicherheitsereignissen zu korrelieren. Sie können verschiedene Tools und Dienste wie Amazon Athena, Amazon oder Sicherheitsanalysetools von Drittanbietern verwenden QuickSight, um die normalisierten Daten abzufragen und zu visualisieren.

Weitere Informationen zur OCSF-Zuordnung für EKS-Protokollereignisse finden Sie in den <https://github.com/ocsf/examples/tree/main/mappings/markdown/> AWS/v1.1.0/EKS Audit Logs [Zuordnungsreferenz] im OCSF-Repository. GitHub

Ermöglichen Sie sichere clusterübergreifende Konnektivität mit Amazon VPC Lattice

Amazon VPC Lattice ist ein vollständig verwalteter Anwendungsnetzwerk-Service, der direkt in die AWS Netzwerkinfrastruktur integriert ist und mit dem Sie Ihre Services über mehrere Konten und Virtual Private Clouds (VPCs) verbinden, sichern und überwachen können. [Mit Amazon EKS können Sie Amazon VPC Lattice mithilfe des AWS Gateway API Controllers, einer Implementierung der Kubernetes Gateway API, nutzen.](#) Mit Amazon VPC Lattice können Sie auf einfache und konsistente Weise clusterübergreifende Konnektivität mit standardmäßiger Kubernetes-Semantik einrichten. Informationen zum Einstieg in die Verwendung von Amazon VPC Lattice mit Amazon EKS finden Sie im [AWS -Gateway-API-Controller-Benutzerhandbuch](#).

Starten Sie EKS-Cluster mit niedriger Latenz und AWS Local Zones

Eine [AWS lokale Zone](#) ist eine Erweiterung einer AWS Region in geografischer Nähe zu Ihren Benutzern. Local Zones haben ihre eigenen Verbindungen zum Internet und unterstützen [AWS Direct Connect](#). Ressourcen, die in einer Local Zone erstellt wurden, können von lokalen Benutzern mit sehr latenzarmen Verbindungen genutzt werden. Weitere Informationen finden Sie im [AWS Local Zones User Guide](#) und [Local Zones](#) im EC2 Amazon-Benutzerhandbuch.

Amazon EKS unterstützt bestimmte Ressourcen in Local Zones. Dazu gehören [verwaltete Knotengruppen](#), [selbstverwaltete EC2 Amazon-Knoten](#), Amazon EBS-Volumes und Application Load Balancers (ALBs). Es wird empfohlen, Folgendes zu berücksichtigen, wenn Sie Local Zones als Teil Ihres Amazon-EKS-Clusters verwenden.

- Mit Amazon EKS können Sie keine Fargate-Knoten in Local Zones erstellen.

- Die von Amazon EKS verwaltete Kubernetes-Steuerebene wird immer in der AWS Region ausgeführt. Die von Amazon EKS verwaltete Kubernetes-Steuerebene kann nicht in der lokalen Zone ausgeführt werden. Da Local Zones in Ihrer VPC als Subnetz angezeigt werden, sieht Kubernetes Ihre lokalen Zonenressourcen als Teil dieses Subnetzes.
- Der Amazon EKS Kubernetes-Cluster kommuniziert über von Amazon EKS verwaltete [elastische](#) Netzwerkschnittstellen mit den EC2 Amazon-Instances, die Sie in der AWS Region oder Lokalen Zone ausführen. Weitere Informationen zur Amazon EKS Network-Architektur finden Sie unter [Netzwerk konfigurieren](#) aus.
- Im Gegensatz zu regionalen Subnetzen kann Amazon EKS keine Netzwerkschnittstellen in Ihren lokalen Zonen-Subnetzen platzieren. Das bedeutet, dass Sie beim Erstellen des Clusters keine Subnetze der lokalen Zone angeben dürfen. Sie können jedoch Worker-Knoten in verschiedenen Local Zones haben, die mit demselben Cluster verbunden sind.

Probleme mit Amazon EKS-Clustern und -Knoten beheben

In diesem Kapitel werden einige häufige Fehler bei der Verwendung von Amazon EKS sowie deren Lösung behandelt. Wenn Sie Probleme in bestimmten Amazon-EKS-Bereichen beheben müssen, lesen Sie die separaten Themen [the section called “Fehlerbehebung”](#), [the section called “Problembehandlung beim EKS-Connector”](#) und [Fehlerbehebung für ADOT mithilfe von EKS-Add-ons](#).

Weitere Informationen zur Fehlerbehebung finden Sie in den [Knowledge Center-Inhalten zu Amazon Elastic Kubernetes Service](#) auf AWS re:POST.

Unzureichende Kapazität

Wenn Sie beim Versuch, einen Amazon EKS-Cluster zu erstellen, die folgende Fehlermeldung erhalten, verfügt eine der von Ihnen angegebenen Availability Zones nicht über ausreichend Kapazität, um einen Cluster zu unterstützen.

```
Cannot create cluster 'example-cluster' because region-1d, the targeted Availability Zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these Availability Zones: region-1a, region-1b, region-1c
```

Versuchen Sie erneut, den Cluster mit Subnetzen in Ihrer Cluster-VPC zu erstellen, die in den Availability Zones gehostet werden, die diesen Fehler verursacht haben.

Es gibt Availability Zones, in denen sich ein Cluster nicht befinden kann. Vergleichen Sie die Availability Zones, in denen sich Ihre Subnetze befinden, mit der Liste der Availability Zones in den [Subnetzanforderungen](#) und Überlegungen.

Knoten können nicht mit dem Cluster verknüpft werden

Es gibt zwei häufige Gründe, aus denen Knoten nicht mit dem Cluster verknüpft werden können:

- Wenn es sich bei den Knoten um verwaltete Knoten handelt, fügt Amazon EKS Einträge zu `aws-auth ConfigMap` hinzu, wenn Sie die Knotengruppe erstellen. Wenn der Eintrag entfernt oder geändert wurde, müssen Sie ihn erneut hinzufügen. Weitere Informationen erhalten Sie durch

Eingabe von `eksctl create iamidentitymapping --help` im Terminal. Sie können Ihre aktuellen `aws-auth ConfigMap` Einträge anzeigen, indem Sie *my-cluster* den folgenden Befehl durch den Namen Ihres Clusters ersetzen und dann den geänderten Befehl ausführen:

```
eksctl get iamidentitymapping --cluster my-cluster
```

Der ARN der Rolle, die Sie angeben, darf keinen anderen [Pfad](#) als enthalten/. Wenn der Name Ihrer Rolle beispielsweise lautet `development/apps/my-role`, müssen Sie ihn `my-role` bei der Angabe des ARN für die Rolle in ändern. Achten Sie darauf, den ARN der IAM-Rolle des Knotens (nicht den ARN des Instances-Profiles) anzugeben.

Wenn die Knoten selbst verwaltet werden und Sie keine [Zugriffseinträge](#) für den ARN der IAM-Rolle des Knotens erstellt haben, führen Sie dieselben Befehle aus, die für verwaltete Knoten aufgeführt sind. Wenn Sie einen Zugriffseintrag für den ARN für die IAM-Rolle Ihres Knotens erstellt haben, ist er im Zugriffseintrag möglicherweise nicht richtig konfiguriert. Achten Sie darauf, dass in Ihrem `aws-auth ConfigMap`-Eintrag oder Zugriffseintrag der ARN der IAM-Rolle des Knotens (nicht der ARN des Instances-Profiles) als Haupt-ARN angegeben ist. Weitere Informationen zu Zugriffseinträgen finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#).

- Die AWS CloudFormation Vorlage `ClusterName` in Ihrem Knoten entspricht nicht genau dem Namen des Clusters, dem Ihre Knoten beitreten sollen. Die Übergabe eines falschen Werts an dieses Feld führt zu einer falschen Konfiguration der `/var/lib/kubelet/kubeconfig` Knotendatei und die Knoten werden dem Cluster nicht beitreten.
- Der Knoten ist nicht als Eigentum des Clusters gekennzeichnet. Auf Ihre Worker-Knoten muss die folgende Markierung angewendet werden, wobei *my-cluster* durch den Namen des Clusters ersetzt wird.

Schlüssel	Wert
<code>kubernetes.io/cluster/</code> <i>my-cluste</i> <i>r</i>	<code>owned</code>

- Die Knoten können möglicherweise nicht über eine öffentliche IP-Adresse auf den Cluster zugreifen. Stellen Sie sicher, dass den Knoten, die in öffentlichen Subnetzen bereitgestellt werden, eine öffentliche IP-Adresse zugewiesen wird. Wenn nicht, können Sie einem Knoten nach dem Start eine Elastic IP-Adresse zuordnen. Weitere Informationen dazu finden Sie unter [Zuordnen einer Elastic-IP-Adresse zu einer laufenden Instance oder einer Netzwerkschnittstelle](#). Wenn das öffentliche Subnetz nicht so eingestellt ist, dass es Instances, die es nutzen, automatisch öffentliche IP-Adressen zuweist, empfehlen wir, diese Einstellung zu aktivieren. Weitere

Informationen finden Sie unter [Ändern des Public IPv4 Addressing-Attributs für Ihr Subnetz](#). Wenn der Arbeitsknoten in einem privaten Subnetz bereitgestellt wird, muss das Subnetz über eine Route zu einem NAT-Gateway verfügen, dem eine öffentliche IP-Adresse zugewiesen ist.

- Der AWS STS-Endpunkt für die AWS Region, in der Sie die Knoten bereitstellen, ist für Ihr Konto nicht aktiviert. Informationen zur [Aktivierung der Region finden Sie unter AWS STS in einer AWS Region aktivieren und deaktivieren](#).
- Der Knoten hat keinen privaten DNS-Eintrag, was dazu führt, dass das kubelet Protokoll einen `node "" not found` Fehler enthält. Stellen Sie sicher, dass für die VPC, in der der Knoten erstellt wird, Werte für `domain-name` und `domain-name-servers` als Options in einem DHCP options set festgelegt sind. Die Standard-Werte sind `domain-name:<region>.compute.internal` und `domain-name-servers:AmazonProvidedDNS`. Weitere Informationen finden Sie unter [DHCP-Optionssätze](#) im Amazon-VPC-Benutzerhandbuch.
- Wenn die Knoten in der verwalteten Knotengruppe innerhalb von 15 Minuten keine Verbindung zum Cluster herstellen, wird ein Systemfehler von `NodeCreationFailure ""` ausgegeben und der Konsolenstatus wird auf `gesetztCreate failed`. Bei Windows AMIs mit langsamen Startzeiten kann dieses Problem mithilfe des [Schnellstarts](#) behoben werden.

Zur Ermittlung und Behebung häufiger Ursachen, die den Beitritt von Worker-Knoten zu einem Cluster verhindern, können Sie das Runbook [AWSsupport-TroubleshootEKSWorkerNode](#) verwenden. Weitere Informationen finden Sie [AWSsupport-TroubleshootEKSWorkerNode](#) in der Runbook-Referenz für AWS Systems Manager Automation.

Nicht autorisiert oder Zugriff verweigert (**kubectl**)

Wenn Sie beim Ausführen von `kubectl` Befehlen einen der folgenden Fehler erhalten, haben Sie entweder nicht richtig für Amazon EKS `kubectl` konfiguriert oder die Anmeldeinformationen für den IAM-Prinzipal (Rolle oder Benutzer), den Sie verwenden, sind keinem Kubernetes-Benutzernamen zugeordnet, der über ausreichende Berechtigungen für Kubernetes-Objekte in Ihrem Amazon EKS-Cluster verfügt.

- `could not get token: AccessDenied: Access denied`
- `error: You must be logged in to the server (Unauthorized)`
- `error: the server doesn't have a resource type "svc"`

Das kann auf eine der folgenden Ursachen zurückzuführen sein:

- Der Cluster wurde mit Anmeldeinformationen für einen bestimmten IAM-Prinzipal erstellt und `kubectl` ist für die Verwendung von Anmeldeinformationen für einen anderen IAM-Prinzipal konfiguriert. Aktualisieren Sie in diesem Fall die Datei `kube config` mit den Anmeldeinformationen, mit denen der Cluster erstellt wurde, um das Problem zu beheben. Weitere Informationen finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).
- Wenn Ihr Cluster die minimalen Plattformanforderungen im Abschnitt Voraussetzungen von [Gewähren Sie IAM-Benutzern Zugriff auf Kubernetes mit EKS-Zugriffseinträgen](#) gewährt, erfüllt, ist mit Ihrem IAM-Prinzipal kein Zugriffseintrag vorhanden. Falls er existiert, sind für ihn nicht die erforderlichen Kubernetes-Gruppennamen definiert oder ihm ist nicht die richtige Zugriffsrichtlinie zugeordnet. Weitere Informationen finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#).
- Wenn Ihr Cluster die minimalen Plattformanforderungen unter [Gewähren Sie IAM-Benutzern Zugriff auf Kubernetes mit EKS-Zugriffseinträgen](#) gewährt, nicht erfüllt, ist kein Eintrag mit Ihrem IAM-Prinzipal in der vorhanden. `aws-auth ConfigMap` Falls er existiert, ist er nicht den Kubernetes-Gruppennamen zugeordnet, die an ein Kubernetes gebunden sind oder über die erforderlichen Berechtigungen verfügen. `Role ClusterRole` [Weitere Informationen zu Objekten der Rollenbasierten Autorisierung \(RBAC\) von Kubernetes finden Sie in der Kubernetes-Dokumentation unter Verwenden der RBAC-Autorisierung](#). Sie können Ihre aktuellen `aws-auth ConfigMap` Einträge anzeigen, indem Sie den folgenden Befehl durch den Namen Ihres Clusters ersetzen `my-cluster` und dann den geänderten Befehl ausführen: `eksctl get iamidentitymapping --cluster my-cluster` Wenn ein Eintrag für mit dem ARN Ihres IAM-Prinzipals nicht in der enthalten ist `ConfigMap`, geben Sie ihn `eksctl create iamidentitymapping --help` in Ihr Terminal ein, um zu erfahren, wie Sie einen erstellen.

Wenn Sie die AWS CLI installieren und konfigurieren, können Sie die von Ihnen verwendeten IAM-Anmeldeinformationen konfigurieren. Weitere Informationen finden Sie unter [Configuring the AWS CLI](#) im AWS Command Line Interface User Guide. Sie können auch die Verwendung einer IAM-Rolle konfigurieren `kubectl`, wenn Sie eine IAM-Rolle für den Zugriff auf Kubernetes-Objekte in Ihrem Cluster annehmen. Weitere Informationen finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).

hostname doesn't match

Die Python-Version Ihres Systems muss 2.7.9 oder höher sein. Andernfalls erhalten Sie `hostname doesn't match` Fehler bei AWS CLI-Aufrufen an Amazon EKS. Weitere Informationen finden Sie

unter [Was sind „Hostname stimmt nicht überein“-Fehler?](#) in den Python-Anfragen häufig gestellte Fragen.

getsockopt: no route to host

Docker wird im 172.17.0.0/16-CIDR-Bereich in Amazon-EKS-Clustern ausgeführt. Wir empfehlen, dass sich die VPC-Subnetze Ihres Clusters nicht mit diesem Bereich überschneiden. Andernfalls erhalten Sie den folgenden Fehler:

```
Error: : error upgrading connection: error dialing backend: dial tcp
172.17.<nn>.<nn>:10250: getsockopt: no route to host
```

Instances failed to join the Kubernetes cluster

Wenn Sie den Fehler `Instances failed to join the Kubernetes cluster` erhalten, stellen Sie sicher AWS Management Console, dass entweder der private Endpunktzugriff des Clusters aktiviert ist oder dass Sie die CIDR-Blöcke für den Zugriff auf öffentliche Endpunkte korrekt konfiguriert haben. Weitere Informationen finden Sie unter [the section called “Cluster-Endpointzugriff”](#).

Fehlercodes bei verwalteten Knotengruppen

Wenn bei Ihrer verwaltete Knotengruppe ein Hardwarezustandsproblem auftritt, gibt Amazon EKS einen Fehlercode zurück, der Ihnen bei der Diagnose des Problems hilft. Diese Gesundheitschecks erkennen keine Softwareprobleme, da sie auf [EC2 Amazon-Gesundheitschecks](#) basieren. Die Fehlercodes sind in der folgenden Liste beschrieben.

AccessDenied

Amazon EKS oder einer oder mehrere Ihrer verwalteten Knoten können sich nicht bei Ihrem Kubernetes-Cluster-API-Server authentifizieren oder autorisieren. Weitere Informationen zum Beheben einer häufigen Ursache finden Sie unter [the section called “Behebung einer häufigen Ursache für AccessDenied-Fehler bei verwalteten Knotengruppen”](#). Private Windows AMIs kann diesen Fehlercode auch zusammen mit der Fehlermeldung verursachen. `Not authorized for images` Weitere Informationen finden Sie unter [the section called “Not authorized for images”](#).

AmildNotFound

Wir konnten die mit Ihrer Startvorlage verknüpfte AMI-ID nicht finden. Stellen Sie sicher, dass das AMI vorhanden ist und für Ihr Konto freigegeben ist.

AutoScalingGroupNotFound

Wir konnten die Auto Scaling Scaling-Gruppe, die der verwalteten Knotengruppe zugeordnet ist, nicht finden. Möglicherweise können Sie eine Auto-Scaling-Gruppe mit den gleichen Einstellungen zur Wiederherstellung erstellen.

ClusterUnreachable

Amazon EKS oder einer oder mehrere Ihrer verwalteten Knoten können nicht mit Ihrem Kubernetes-Cluster-API-Server kommunizieren. Dies kann passieren, wenn Netzwerkunterbrechungen auftreten oder wenn API-Server eine Zeitüberschreitung für die Verarbeitung von Anforderungen vornehmen.

Ec2 SecurityGroupNotFound

Wir konnten die Cluster-Sicherheitsgruppe für den Cluster nicht finden. Sie müssen Ihren Cluster neu erstellen.

Ec2 SecurityGroupDeletionFailure

Die RAS-Sicherheitsgruppe für Ihre verwaltete Knotengruppe konnte nicht gelöscht werden. Entfernen Sie alle Abhängigkeiten aus der Sicherheitsgruppe.

Ec2 LaunchTemplateNotFound

Wir konnten die EC2 Amazon-Startvorlage für Ihre verwaltete Knotengruppe nicht finden. Sie müssen Ihre Knotengruppe neu erstellen, um sie wiederherzustellen.

Ec2 LaunchTemplateVersionMismatch

Die Version der EC2 Amazon-Startvorlage für Ihre verwaltete Knotengruppe entspricht nicht der Version, die Amazon EKS erstellt hat. Möglicherweise können Sie zu der Version zurückkehren, die Amazon EKS für die Wiederherstellung erstellt hat.

IamInstanceProfileNotFound

Wir konnten das IAM-Instance-Profil für Ihre verwaltete Knotengruppe nicht finden. Möglicherweise können Sie erneut ein Instance-Profil mit den gleichen Einstellungen zur Wiederherstellung erstellen.

IamNodeRoleNotFound

Wir konnten die IAM-Rolle für Ihre verwaltete Knotengruppe nicht finden. Möglicherweise können Sie erneut eine IAM-Rolle mit den gleichen Einstellungen zur Wiederherstellung erstellen.

AsgInstanceLaunchFailures

Beim Versuch, Instances zu starten, treten in Ihrer Auto-Scaling-Gruppe Fehlfunktionen auf.

NodeCreationFailure

Ihre gestarteten Instances können sich nicht bei Ihrem Amazon-EKS-Cluster registrieren. Häufige Ursachen für diesen Fehler sind unzureichende [Knoten-IAM-Rollen](#)-Berechtigungen oder fehlender ausgehender Internetzugriff für die Knoten. Ihre Knoten müssen eine der folgenden Anforderungen erfüllen:

- Kann über eine öffentliche IP-Adresse auf das Internet zugreifen. Die Sicherheitsgruppe, die mit dem Subnetz verknüpft ist, in dem sich der Knoten befindet, muss die Kommunikation zulassen. Weitere Informationen erhalten Sie unter [the section called “Subnetz-Anforderungen und -Überlegungen”](#) und [the section called “Anforderungen an Sicherheitsgruppen”](#).
- Ihre Knoten und VPC müssen die Anforderungen unter [Bereitstellen von privaten Clustern mit eingeschränktem Internetzugang](#) erfüllen.

InstanceLimitExceeded

Ihr AWS Konto kann keine weiteren Instances des angegebenen Instanztyps starten. Möglicherweise können Sie eine Erhöhung des EC2 Amazon-Instance-Limits für die Wiederherstellung beantragen.

InsufficientFreeAddresses

In einem oder mehreren der Subnetze, die Ihrer verwalteten Knotengruppe zugeordnet sind, sind nicht genügend IP-Adressen für neue Knoten verfügbar.

InternalFailure

Diese Fehler werden normalerweise durch ein serverseitiges Amazon-EKS-Problem verursacht.

Behebung einer häufigen Ursache für **AccessDenied**-Fehler bei verwalteten Knotengruppen

Die häufigste Ursache für AccessDenied-Fehler beim Ausführen von Vorgängen auf verwalteten Knotengruppen ist das Fehlen von `eks:node-manager`, `ClusterRole` oder

ClusterRoleBinding. Amazon EKS richtet diese Ressourcen in Ihrem Cluster als Teil des Onboarding mit verwalteten Knotengruppen ein, die für die Verwaltung der Knotengruppen erforderlich sind.

Die ClusterRole kann sich im Laufe der Zeit ändern, sollte aber dem folgenden Beispiel ähneln:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: eks:node-manager
rules:
- apiGroups:
  - ''
  resources:
  - pods
  verbs:
  - get
  - list
  - watch
  - delete
- apiGroups:
  - ''
  resources:
  - nodes
  verbs:
  - get
  - list
  - watch
  - patch
- apiGroups:
  - ''
  resources:
  - pods/eviction
  verbs:
  - create
```

Die ClusterRoleBinding kann sich im Laufe der Zeit ändern, sollte aber dem folgenden Beispiel ähneln:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
```

```
name: eks:node-manager
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: eks:node-manager
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: eks:node-manager
```

Stellen Sie sicher, dass die Ressource `eks:node-manager ClusterRole` besteht.

```
kubectl describe clusterrole eks:node-manager
```

Wenn bestehend, vergleichen Sie die Ausgabe mit dem vorherigen `ClusterRole`-Beispiel.

Stellen Sie sicher, dass die Ressource `eks:node-manager ClusterRoleBinding` besteht.

```
kubectl describe clusterrolebinding eks:node-manager
```

Wenn bestehend, vergleichen Sie die Ausgabe mit dem vorherigen `ClusterRoleBinding`-Beispiel.

Wenn Sie bei der Anforderung verwalteter Knotengruppenoperationen ein fehlendes `ClusterRole` oder `ClusterRoleBinding` defektes Objekt oder die Ursache für einen `AcessDenied` Fehler festgestellt haben, können Sie es wiederherstellen. Speichern Sie den folgenden Inhalt in einer Datei mit dem Namen *eks-node-manager-role.yaml*.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: eks:node-manager
rules:
- apiGroups:
  - ''
  resources:
  - pods
  verbs:
  - get
  - list
  - watch
  - delete
```



```
- apiGroups:
  - ''
  resources:
  - nodes
  verbs:
  - get
  - list
  - watch
  - patch
- apiGroups:
  - ''
  resources:
  - pods/eviction
  verbs:
  - create
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: eks:node-manager
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: eks:node-manager
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: eks:node-manager
```

Wenden Sie die Datei an.

```
kubectl apply -f eks-node-manager-role.yaml
```

Wiederholen Sie den Vorgang der Knotengruppe, um festzustellen, ob das Problem dadurch behoben wurde.

Not authorized for images

Eine mögliche Ursache für eine `Not authorized for images` Fehlermeldung ist die Verwendung eines privaten Amazon EKS-Windows-AMI zum Starten von verwalteten Windows-Knotengruppen. Nach der Veröffentlichung neuer Windows-Versionen AMIs, AWS AMIs die älter als 4 Monate sind,

sind privat, sodass nicht mehr darauf zugegriffen werden kann. Wenn Ihre verwaltete Knotengruppe ein privates Windows-AMI verwendet, sollten Sie erwägen, [Ihre verwaltete Windows-Knotengruppe zu aktualisieren](#). Wir können zwar nicht garantieren, dass wir Zugriff auf privat gemachte AMIs Inhalte gewähren können, aber du kannst den Zugriff beantragen, indem du ein Ticket beim AWS Support einreichst. Weitere Informationen finden Sie unter [Patches](#) im EC2 Amazon-Benutzerhandbuch.

Der Knoten befindet sich im **NotReady** Status

Wenn Ihr Knoten in einen NotReady Status wechselt, deutet dies wahrscheinlich darauf hin, dass der Knoten fehlerhaft ist und für die Planung neuer Pods nicht verfügbar ist. Dies kann verschiedene Ursachen haben, z. B. wenn dem Knoten nicht genügend Ressourcen für CPU, Arbeitsspeicher oder verfügbaren Festplattenspeicher zur Verfügung stehen.

Für Amazon EKS-optimiertes Windows gibt es keine Reservierung für Rechenressourcen AMIs, die standardmäßig in der kubelet Konfiguration angegeben sind. [Um Ressourcenprobleme zu vermeiden, können Sie Rechenressourcen für Systemprozesse reservieren, indem Sie ihnen Konfigurationswerte für kube-reserved und/oder system-reserved zur Verfügung stellen.](#) kubelet Dazu verwenden Sie den `-KubeletExtraArgs` Befehlszeilenparameter im Bootstrap-Skript. Weitere Informationen finden Sie unter [Reserve Compute Resources for System Daemons](#) in der Kubernetes-Dokumentation und in diesem Benutzerhandbuch. [the section called “Bootstrap-Skript-Konfigurationsparameter”](#)

EKS Log Collector

Um Probleme mit Amazon EKS-Knoten zu beheben, steht für Knoten unter `/etc/eks/log-collector-script/eks-log-collector.sh` ein vorgefertigtes Skript zur Verfügung. Sie können das Skript verwenden, um Diagnoseprotokolle für Support-Fälle und allgemeine Fehlerbehebung zu sammeln.

Mit dem folgenden Befehl können Sie das Skript auf dem Knoten ausführen:

```
sudo bash /etc/eks/log-collector-script/eks-log-collector.sh
```

Note

Wenn das Skript an diesem Ort nicht vorhanden ist. Sie können das Skript mit dem folgenden Befehl manuell herunterladen und ausführen:

```
curl -O https://amazon-eks.s3.amazonaws.com/support/log-collector-script/linux/eks-log-collector.sh
sudo bash eks-log-collector.sh
```

Das Skript sammelt die folgenden Diagnoseinformationen:

```
$ sudo bash /etc/eks/log-collector-script/eks-log-collector.sh

This is version 0.7.8. New versions can be found at https://github.com/awslabs/
amazon-eks-ami/blob/main/log-collector-script/

Trying to collect common operating system logs...
Trying to collect kernel logs...
Trying to collect mount points and volume information...
...
...

Done... your bundled logs are located in /var/log/eks_i-EXAMPLE_2025-03-25_0000-
UTC_0.7.8.tar.gz
```

Die Diagnoseinformationen werden gesammelt und gespeichert unter:

```
/var/log/eks_i-EXAMPLE_2025-03-25_0000-UTC_0.7.8.tar.gz
```

Weitere Informationen zum Abrufen des Protokollpakets für Bottlerocket-Knoten finden Sie unter [Bottlerocket Log](#).

Container-Laufzeitnetzwerk nicht bereit

Möglicherweise erhalten Sie einen Container runtime network not ready-Fehler und einen Autorisierungsfehler, die den folgenden ähneln:

```
4191 kubelet.go:2130] Container runtime network not ready: NetworkReady=false
reason:NetworkPluginNotReady message:docker: network plugin is not ready: cni config
uninitialized
4191 reflector.go:205] k8s.io/kubernetes/pkg/kubelet/kubelet.go:452: Failed to list
*v1.Service: Unauthorized
4191 kubelet_node_status.go:106] Unable to register node
"ip-10-40-175-122.ec2.internal" with API server: Unauthorized
```

```
4191 reflector.go:205] k8s.io/kubernetes/pkg/kubelet/kubelet.go:452: Failed to list
*v1.Service: Unauthorized
```

Dieses Problem kann folgende Ursachen haben:

1. Sie haben entweder kein in `aws-auth ConfigMap` Ihrem Cluster oder es enthält keine Einträge für die IAM-Rolle, mit der Sie Ihre Knoten konfiguriert haben.

Um das Problem zu beheben, sehen Sie sich die vorhandenen Einträge in Ihrem an, indem Sie den folgenden Befehl `ConfigMap` durch den Namen Ihres Clusters ersetzen `my-cluster` und dann den geänderten Befehl ausführen: `eksctl get iamidentitymapping --cluster my-cluster`. Wenn Sie im Zusammenhang mit dem Befehl eine Fehlermeldung erhalten, liegt das möglicherweise daran, dass Ihr Cluster keine `aws-auth ConfigMap` hat. Der folgende Befehl fügt `ConfigMap` einen Eintrag hinzu. Wenn der nicht `ConfigMap` existiert, wird er vom Befehl ebenfalls erstellt. `111122223333` Ersetzen Sie es durch die AWS Konto-ID für die IAM-Rolle und `myAmazonEKSTNodeRole` durch den Namen der Rolle Ihres Knotens.

```
eksctl create iamidentitymapping --cluster my-cluster \
    --arn arn:aws:iam::111122223333:role/myAmazonEKSTNodeRole --group
system:bootstrappers,system:nodes \
    --username system:node:{{EC2PrivateDNSName}}
```

Der ARN der Rolle, die Sie angeben, darf keinen anderen [Pfad](#) als enthalten/. Wenn der Name Ihrer Rolle beispielsweise lautet `development/apps/my-role`, müssen Sie ihn `my-role` bei der Angabe des ARN der Rolle in ändern. Achten Sie darauf, den ARN der IAM-Rolle des Knotens (nicht den ARN des Instances-Profils) anzugeben.

2. Ihre selbstverwalteten Knoten befinden sich in einem Cluster mit einer Plattformversion in der Mindestversion, die in den Voraussetzungen im Thema [Gewähren Sie IAM-Benutzern Zugriff auf Kubernetes mit EKS-Zugriff gewähren](#) aufgeführt ist, aber im Abschnitt `aws-auth ConfigMap` (siehe vorheriges Element) ist kein Eintrag für die IAM-Rolle des Knotens aufgeführt, oder es ist kein Zugriffseintrag für die Rolle vorhanden. Um das Problem zu beheben, zeigen Sie Ihre vorhandenen Zugriffseinträge `my-cluster` an, indem Sie den folgenden Befehl durch den Namen Ihres Clusters ersetzen und dann den geänderten Befehl ausführen: `aws eks list-access-entries --cluster-name my-cluster`. Der folgende Befehl fügt einen Zugriffseintrag für die IAM-Rolle des Knotens hinzu. `111122223333` Ersetzen Sie ihn durch die AWS Konto-ID für die IAM-Rolle und `myAmazonEKSTNodeRole` durch den Namen der Rolle Ihres Knotens. Wenn Sie einen Windows-Knoten haben, ersetzen Sie ihn `EC2_LINUX` durch `EC2_Windows`. Achten Sie darauf, den ARN der IAM-Rolle des Knotens (nicht den ARN des Instances-Profils) anzugeben.

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn arn:aws:iam::111122223333:role/myAmazonEKSNodeRole --type EC2_LINUX
```

TLS-Handshake-Zeitüberschreitung

Wenn ein Knoten nicht in der Lage ist, eine Verbindung zum öffentlichen API-Server-Endpunkt herzustellen, erhalten Sie möglicherweise einen Fehler ähnlich dem folgenden.

```
server.go:233] failed to run Kubelet: could not init cloud provider "aws": error finding instance i-1111f2222f333e44c: "error listing AWS instances: \"RequestError: send request failed\\ncaused by: Post net/http: TLS handshake timeout\\n\""
```

Der `kubelet`-Prozess wird weiter fortgesetzt und testet den API-Server-Endpunkt. Der Fehler kann auch vorübergehend während jeder Prozedur auftreten, die eine laufende Aktualisierung des Clusters auf der Steuerungsebene durchführt, z. B. eine Konfigurationsänderung oder eine Versionsaktualisierung.

Um das Problem zu beheben, überprüfen Sie die Routing-Tabelle und die Sicherheitsgruppen, um sicherzustellen, dass der Datenverkehr von den Knoten den öffentlichen Endpunkt erreichen kann.

InvalidClientTokenId

Wenn Sie IAM-Rollen für Dienstkonten für einen Pod verwenden oder in einem Cluster in einer AWS Region China DaemonSet bereitgestellt sind und die `AWS_DEFAULT_REGION` Umgebungsvariable nicht in der Spezifikation festgelegt haben, wird für den Pod oder die DaemonSet folgende Fehlermeldung angezeigt:

```
An error occurred (InvalidClientTokenId) when calling the GetCallerIdentity operation: The security token included in the request is invalid
```

Um das Problem zu beheben, müssen Sie die `AWS_DEFAULT_REGION` Umgebungsvariable zu Ihrem Pod oder Ihrer DaemonSet Spezifikation hinzufügen, wie in der folgenden Beispiel-Pod-Spezifikation gezeigt.

```
apiVersion: v1
kind: Pod
```

```
metadata:
  name: envar-demo
  labels:
    purpose: demonstrate-envvars
spec:
  containers:
  - name: envar-demo-container
    image: gcr.io/google-samples/node-hello:1.0
    env:
    - name: AWS_DEFAULT_REGION
      value: "region-code"
```

Die Knotengruppen müssen mit der Kubernetes-Version übereinstimmen, bevor die Kontrollebene aktualisiert wird

Bevor Sie eine Kontrollebene auf eine neue Kubernetes-Version aktualisieren, muss die Nebenversion der verwalteten Knoten und der Fargate-Knoten in Ihrem Cluster mit der Version der aktuellen Version Ihrer Kontrollebene identisch sein. Die Amazon EKS-update-cluster-version-API akzeptiert keine Anforderungen, bis für alle von Amazon EKS verwalteten Knoten ein Upgrade auf die aktuelle Cluster-Version durchgeführt wurde. Amazon EKS bietet APIs die Möglichkeit, verwaltete Knoten zu aktualisieren. Informationen zum Upgrade der Kubernetes-Version einer verwalteten Knotengruppe finden Sie unter [the section called “Aktualisierung”](#). Um die Version eines Fargate-Knotens zu aktualisieren, löschen Sie den Pod, der durch den Knoten repräsentiert wird, und stellen Sie den Pod erneut bereit, nachdem Sie Ihre Steuerungsebene aktualisiert haben. Weitere Informationen finden Sie unter [the section called “Kubernetes-Version aktualisieren”](#).

Beim Starten vieler Knoten gibt es Too Many Requests-Fehler

Wenn Sie viele Knoten gleichzeitig starten, wird in den Ausführungsprotokollen der [EC2 Amazon-Benutzerdaten](#) möglicherweise eine Fehlermeldung angezeigt, die besagt Too Many Requests. Dies kann auftreten, weil die Steuerebene mit describeCluster-Aufrufen überlastet wird. Die Überladung führt zu einer Drosselung, Knoten, die das Bootstrap-Skript nicht ausführen können, und Knoten, die dem Cluster insgesamt nicht beitreten können.

Stellen Sie sicher --apiserver-endpoint, dass die --dns-cluster-ip Argumente --b64-cluster-ca, und an das Bootstrap-Skript des Knotens übergeben werden. Wenn Sie diese Argumente einbeziehen, muss das Bootstrap-Skript keinen describeCluster Aufruf tätigen, wodurch verhindert wird, dass die Steuerungsebene überlastet wird. Weitere Informationen finden Sie

unter [the section called “Geben Sie Benutzerdaten an, um Argumente an die `bootstrap.sh` Datei zu übergeben, die in einem Amazon EKS-optimierten Linux/Bottlerocket-AMI enthalten ist”](#).

Unautorisierte Fehlerantwort (HTTP 401) bei Kubernetes-API-Serveranfragen

Diese Fehler werden angezeigt, wenn das Dienstkonto-Token eines Pods in einem Cluster abgelaufen ist.

Der Kubernetes-API-Server Ihres Amazon EKS-Clusters lehnt Anfragen ab, deren Token älter als 90 Tage sind. In früheren Kubernetes-Versionen hatten Token kein Ablaufdatum. Clients, die diese Tokens verwenden, müssen die Tokens nun innerhalb einer Stunde aktualisieren. Um zu verhindern, dass der Kubernetes-API-Server Ihre Anfrage aufgrund eines ungültigen Tokens ablehnt, muss die von Ihrem Workload verwendete [Kubernetes-Client-SDK-Version](#) dieselbe oder eine neuere als die folgenden Versionen sein:

- Go-Version 0.15.7 und höher
- Python-Version 12.0.0 und höher
- Java-Version 9.0.0 und höher
- JavaScript Version und später 0.10.3
- Ruby master-Branch
- Haskell-Version 0.3.0.0
- C#-Version 7.0.5 und höher

Sie können alle vorhandenen Pods in Ihrem Cluster identifizieren, die veraltete Token verwenden. Weitere Informationen finden Sie unter [the section called “Servicekonto-Tokens”](#).

Die Amazon-EKS-Plattformversion liegt mehr als zwei Versionen hinter der aktuellen Plattformversion

Dies kann passieren, wenn Amazon EKS die [Plattformversion](#) Ihres Clusters nicht automatisch aktualisieren kann. Obwohl es dafür viele Ursachen gibt, folgen einige der häufigsten Ursachen. Wenn eines dieser Probleme auf Ihren Cluster zutrifft, funktioniert er möglicherweise immer noch, seine Plattformversion wird nur nicht von Amazon EKS aktualisiert.

Problem

Die [Cluster-IAM-Rolle](#) wurde gelöscht – Diese Rolle wurde beim Erstellen des Clusters angegeben. Sie können mit dem folgenden Befehl überprüfen, welche Rolle angegeben wurde. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-cluster --name my-cluster --query cluster.roleArn --output text | cut -d / -f 2
```

Eine Beispielausgabe sieht wie folgt aus.

```
eksClusterRole
```

Lösung

Erstellen einer neuen [Cluster-IAM-Rolle](#) mit demselben Namen.

Problem

Ein bei der Clustererstellung festgelegtes Subnetz wurde gelöscht – Die mit dem Cluster zu verwendenden Subnetze wurden bei der Clustererstellung angegeben. Sie können mit dem folgenden Befehl überprüfen, welche Subnetze angegeben wurden. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-cluster --name my-cluster --query cluster.resourcesVpcConfig.subnetIds
```

Eine Beispielausgabe sieht wie folgt aus.

```
[  
  "subnet-EXAMPLE1",  
  "subnet-EXAMPLE2"  
]
```

Lösung

Bestätigen Sie, ob das Subnetz in Ihrem Konto IDs existiert.

```
vpc_id=$(aws eks describe-cluster --name my-cluster --query  
  cluster.resourcesVpcConfig.vpcId --output text)  
aws ec2 describe-subnets --filters "Name=vpc-id,Values=$vpc_id" --query  
  "Subnets[*].SubnetId"
```


Eine Beispielausgabe sieht wie folgt aus.

```
[  
  "subnet-EXAMPLE3",  
  "subnet-EXAMPLE4"  
]
```

Wenn das in der Ausgabe IDs zurückgegebene Subnetz nicht mit dem Subnetz übereinstimmt, das bei der Erstellung des Clusters angegeben wurde, müssen Sie, wenn Amazon EKS den Cluster aktualisieren soll, die vom Cluster verwendeten Subnetze ändern. Dies liegt daran, dass Amazon EKS, wenn Sie bei der Erstellung Ihres Clusters mehr als zwei Subnetze angegeben haben, nach dem Zufallsprinzip Subnetze auswählt, die Sie für die Erstellung neuer Elastic-Netzwerk-Schnittstellen angegeben haben. Diese Netzwerkschnittstellen ermöglichen es der Steuerebene, mit Ihren Knoten zu kommunizieren. Amazon EKS aktualisiert den Cluster nicht, wenn das ausgewählte Subnetz nicht existiert. Sie haben keine Kontrolle darüber, in welchem der Subnetze, die Sie bei der Clustererstellung angegeben haben, Amazon EKS wählt, um eine neue Netzwerkschnittstelle zu erstellen.

Wenn Sie ein Kubernetes-Versionsupdate für Ihren Cluster initiieren, kann das Update aus demselben Grund fehlschlagen.

Problem

Eine bei der Clustererstellung angegebene Sicherheitsgruppe wurde gelöscht — Wenn Sie bei der Clustererstellung Sicherheitsgruppen angegeben haben, können Sie diese IDs mit dem folgenden Befehl einsehen. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters.

```
aws eks describe-cluster --name my-cluster --query  
cluster.resourcesVpcConfig.securityGroupIds
```

Eine Beispielausgabe sieht wie folgt aus.

```
[  
  "sg-EXAMPLE1"  
]
```

Wenn zurückgegeben [] wird, wurden bei der Erstellung des Clusters keine Sicherheitsgruppen angegeben und eine fehlende Sicherheitsgruppe ist nicht das Problem. Wenn Sicherheitsgruppen zurückgegeben werden, vergewissern Sie sich, dass die Sicherheitsgruppen in Ihrem Konto vorhanden sind.

Lösung

Bestätigen Sie, ob diese Sicherheitsgruppen in Ihrem Konto vorhanden sind.

```
vpc_id=$(aws eks describe-cluster --name my-cluster --query
  cluster.resourcesVpcConfig.vpcId --output text)
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=$vpc_id" --query
  "SecurityGroups[*].GroupId"
```

Eine Beispielausgabe sieht wie folgt aus.

```
[
  "sg-EXAMPLE2"
]
```

Wenn die in der Ausgabe IDs zurückgegebene Sicherheitsgruppe nicht mit der Sicherheitsgruppe übereinstimmt IDs, die bei der Erstellung des Clusters angegeben wurde, müssen Sie, wenn Amazon EKS den Cluster aktualisieren soll, die vom Cluster verwendeten Sicherheitsgruppen ändern. Amazon EKS aktualisiert einen Cluster nicht, wenn die bei der Clustererstellung IDs angegebene Sicherheitsgruppe nicht existiert.

Wenn Sie ein Kubernetes-Versionsupdate für Ihren Cluster initiieren, kann das Update aus demselben Grund fehlschlagen.

- Sie haben nicht mindestens sechs (obwohl wir 16 empfehlen) verfügbare IP-Adressen in jedem der Subnetze, die Sie bei der Erstellung Ihres Clusters angegeben haben. Wenn Sie nicht über genügend verfügbare IP-Adressen im Subnetz verfügen, müssen Sie entweder IP-Adressen im Subnetz freigeben oder Sie müssen die vom Cluster verwendeten Subnetze so ändern, dass Subnetze mit ausreichend verfügbaren IP-Adressen verwendet werden.
- Sie haben die [Verschlüsselung von Geheimnissen](#) aktiviert, als Sie Ihren Cluster erstellt haben, und der von Ihnen angegebene AWS KMS-Schlüssel wurde gelöscht. Wenn Sie möchten, dass Amazon EKS den Cluster aktualisiert, müssen Sie einen neuen Cluster erstellen

FAQs Cluster-Integritäts- und Fehlercodes mit Lösungspfaden

Amazon EKS erkennt Probleme mit Ihren EKS-Clustern und der Cluster-Infrastruktur und speichert sie im Integritätsobjekt Ihrer EKS-Cluster-Ressource. Mithilfe von Cluster-Integritätsinformationen können Sie Cluster-Probleme schneller erkennen, behandeln und beheben. Auf diese Weise können

Sie Anwendungsumgebungen erstellen, die sicherer sind und up-to-date. Darüber hinaus kann es für Sie aufgrund von Problemen mit der erforderlichen Infrastruktur oder Clusterkonfiguration möglicherweise unmöglich sein, auf neuere Versionen von Kubernetes zu aktualisieren oder Amazon EKS Sicherheitsupdates auf einem heruntergestuften Cluster zu installieren. Es kann drei Stunden dauern, bis Amazon EKS Probleme erkennt oder feststellt, dass ein Problem behoben wurde.

Amazon EKS und die Benutzer sind gemeinsam für die Integrität eines Amazon EKS-Clusters verantwortlich. Sie selbst sind für die erforderliche Infrastruktur von IAM-Rollen und Amazon VPC-Subnetzen sowie für andere notwendige Infrastrukturkomponenten verantwortlich, die im Voraus bereitgestellt werden müssen. Amazon EKS erkennt Änderungen an der Konfiguration dieser Infrastruktur und des Clusters.

Um in der Amazon EKS-Konsole auf den Zustand Ihres Clusters zuzugreifen, suchen Sie auf der Registerkarte Cluster-Integritätsprobleme des Observability-Dashboards, auf das Sie über die Amazon EKS-Cluster-Detailseite zugreifen können, nach einer Tabelle mit dem Namen Health Issues. Diese Daten sind auch verfügbar, wenn Sie die `DescribeCluster` Aktion in der EKS-API aufrufen, beispielsweise von der AWS Befehlszeilenschnittstelle aus.

Warum sollte ich diese Funktion verwenden?

Sie erhalten einen besseren Einblick in den Zustand Ihres Amazon EKS-Clusters und können Probleme schnell diagnostizieren und beheben, ohne Zeit mit dem Debuggen oder dem Öffnen von AWS Supportanfragen verbringen zu müssen. Beispiel: Sie haben versehentlich ein Subnetz für den Amazon EKS-Cluster gelöscht. Amazon EKS kann keine kontoübergreifenden Netzwerkschnittstellen und AWS Kubernetes-CLI-Befehle wie `kubectl exec` oder `logs` erstellen. `kubectl` Bei diesen tritt folgender Fehler auf: `Error from server: error dialing backend: remote error: tls: internal error`. Nun wird ein Amazon EKS-Integritätsproblem mit folgendem Hinweis angezeigt: `subnet-da60e280 was deleted: could not create network interface`.

In welcher Beziehung steht diese Funktion zu anderen Diensten oder funktioniert mit ihnen? AWS

IAM-Rollen und Amazon VPC-Subnetze sind zwei Beispiele für erforderliche Infrastrukturkomponenten, für die die Cluster-Integritätsfunktion Probleme erkennt. Diese Funktion gibt detaillierte Informationen zurück, wenn diese Ressourcen nicht ordnungsgemäß konfiguriert sind.

Fallen für einen Cluster mit Gesundheitsproblemen Gebühren an?

Ja. Jeder Amazon EKS-Cluster wird zu den Amazon EKS-Standardpreisen abgerechnet. Die Funktion Cluster-Integrität steht ohne Aufpreis zur Verfügung.

Funktioniert diese Funktion mit Amazon EKS-Clustern auf AWS Outposts?

Ja, Clusterprobleme wurden für EKS-Cluster in der AWS Cloud erkannt, einschließlich erweiterter Cluster auf AWS Outposts und lokaler Cluster auf AWS Outposts. Der Clusterstatus erkennt keine Probleme mit Amazon EKS Anywhere oder Amazon EKS Distro (EKS-D).

Kann ich benachrichtigt werden, wenn neue Probleme erkannt werden?

Ja. AWS sendet eine E-Mail und eine Benachrichtigung über das Personal Health Dashboard, wenn neue Probleme mit dem Clusterstatus erkannt werden.

Erhalte ich von der Konsole Warnungen vor Gesundheitsproblemen?

Ja. Cluster mit Problemen verfügen über ein Banner im oberen Bereich der Konsole.

Die ersten beiden Spalten werden für API-Antwortwerte benötigt. Das dritte Feld des [ClusterIssueHealth-Objekts](#) ist ResourceIds, dessen Rückgabe vom Problemtyp abhängt.

Code	Fehlermeldung	ResourceIds	Cluster wiederherstellbar?
SUBNET_NOT_FOUND	Wir konnten ein oder mehrere Subnetze nicht finden, die derzeit mit Ihrem Cluster verknüpft sind. Call Amazon EKS update-cluster-config API to update subnets.	Subnetz-IDs	Ja
SECURITY_GROUP_NOT_FOUND	Wir konnten keine oder mehrere Sicherheitsgruppen finden, die derzeit mit Ihrem Cluster verknüpft sind. Rufen Sie die Amazon update-cluster-config EKS-API auf, um	Sicherheitsgruppen-IDs	Ja

Code	Fehlermeldung	Ressourcen	Cluster wiederherstellbar?
	Sicherheitsgruppen zu aktualisieren		
IP_NOT_AVAILABLE	One or more of the subnets associated with your cluster does not have enough available IP addresses for Amazon EKS to perform cluster management operations. Geben Sie Adressen in den Subnetzen frei oder ordnen Sie Ihrem Cluster mithilfe der Amazon update-cluster-config EKS-API verschiedene Subnetze zu.	Subnetz-IDs	Ja
VPC_NOT_FOUND	Wir konnten die mit Ihrem Cluster verknüpfte VPC nicht finden. You must delete and recreate your cluster.	VPC-ID	Nein

Code	Fehlermeldung	Ressourcelds	Cluster wiederherstellbar?
ASSUME_ROLE_ACCESS_DENIED	Ihr Cluster verwendet Amazon EKS nicht service-linked-role. Wir konnten die Ihrem Cluster zugeordnete Rolle nicht übernehmen, um die erforderlichen Amazon EKS-Verwaltungsvorgänge durchzuführen. Check the role exists and has the required trust policy.	Die IAM-Rolle des Clusters	Ja
PERMISSION_ACCESS_DENIED	Ihr Cluster verwendet Amazon EKS nicht service-linked-role. The role associated with your cluster does not grant sufficient permissions for Amazon EKS to perform required management operations. Check the policies attached to the cluster role and if any separate deny policies are applied.	Die IAM-Rolle des Clusters	Ja

Code	Fehlermeldung	Ressourcen	Cluster wiederherstellbar?
ASSUME_ROLE_ACCESS_DENIED_USING_SLR	Wir konnten nicht von der Amazon EKS-Clusterverwaltung ausgehen service-linked-role. Check the role exists and has the required trust policy.	Das Amazon EKS service-linked-role	Ja
ZUGRIFF VERWEIGERT BEI VERWENDUNG VON SLR	Die Amazon EKS-Clusterverwaltung gewährt Amazon EKS service-linked-role nicht genügend Berechtigungen, um die erforderlichen Verwaltungsvorgänge durchzuführen. Check the policies attached to the cluster role and if any separate deny policies are applied.	Das Amazon EKS service-linked-role	Ja
OPT_IN_REQUIRED	Ihr Konto hat kein EC2 Amazon-Serviceabonnement. Update your account subscriptions in your account settings page.	N/A	Ja

Code	Fehlermeldung	ResourceIds	Cluster wiederherstellbar?
STS_REGIONAL_ENDPOINT_DISABLED	Der regionale STS-Endpunkt ist deaktiviert. Enable the endpoint for Amazon EKS to perform required cluster management operations.	N/A	Ja
KMS_KEY_DISABLED	Der Ihrem Cluster zugeordnete AWS KMS-Schlüssel ist deaktiviert. Re-enable the key to recover your cluster.	Der KMS-Schlüssel Arn	Ja
KMS_KEY_NOT_FOUND	Wir konnten den mit Ihrem Cluster verknüpften KMS-Schlüssel nicht finden. AWS You must delete and recreate the cluster.	Der KMS-Schlüssel ARN	Nein
KMS_GRANT_REVOKED	Zuschüsse für den mit Ihrem Cluster verknüpften AWS KMS-Schlüssel wurden widerrufen. You must delete and recreate the cluster.	Der KMS-Schlüssel Arn	Nein

Mit Amazon EKS Connector einen Kubernetes-Cluster mit einer Amazon EKS Management Console verbinden

Sie können Amazon EKS Connector verwenden, um jeden konformen Kubernetes-Cluster zu registrieren und zu verbinden AWS und ihn in der Amazon EKS-Konsole zu visualisieren. Nachdem ein Cluster verbunden wurde, können Sie den Status, die Konfiguration und die Workloads für diesen Cluster in der Amazon-EKS-Konsole anzeigen. Sie können diese Funktion verwenden, um verbundene Cluster in der Amazon EKS-Konsole anzuzeigen, aber Sie können sie nicht verwalten. Der Amazon EKS Connector erfordert einen Agent, der ein [Open-Source-Projekt auf Github](#) ist. Zusätzliche technische Inhalte, einschließlich häufig gestellter Fragen und Problemlösungen, finden Sie unter [the section called “Problembehandlung beim EKS-Connector”](#).

Der Amazon EKS Connector kann die folgenden Typen von Kubernetes-Clustern mit Amazon EKS verbinden.

- On-Premises-Kubernetes-Cluster
- Selbstverwaltete Cluster, die auf Amazon laufen EC2
- Verwaltete Cluster von anderen Cloud-Anbietern

Überlegungen zum Amazon EKS Connector

Bevor Sie Amazon EKS Connector verwenden, sollten Sie Folgendes verstehen:

- Sie müssen über Administratorrechte für den Kubernetes-Cluster verfügen, um den Cluster mit Amazon EKS zu verbinden.
- Im Kubernetes-Cluster müssen Linux-64-Bit-Worker-Knoten (x86) vorhanden sein, bevor eine Verbindung hergestellt werden kann. ARM-Worker-Knoten werden nicht unterstützt.
- In Ihrem Kubernetes-Cluster müssen Worker-Knoten vorhanden sein, die ausgehenden Zugriff auf die `ssm.`- und `ssmmessages.`-Systems Manager-Endpunkte haben. Weitere Informationen finden Sie unter [Systems Manager Manager-Endpoints](#) in der AWS Allgemeinen Referenz.
- Standardmäßig können Sie bis zu zehn Cluster in einer Region verbinden. Sie können eine Erhöhung über die [Servicekontingentkonsole](#) anfordern. Weitere Informationen finden Sie unter [Beantragen einer Kontingenterhöhung](#).
- Nur Amazon EKSRegisterCluster, ListClustersDescribeCluster, und DeregisterCluster APIs werden für externe Kubernetes-Cluster unterstützt.

- Sie müssen über die folgenden Berechtigungen verfügen, um einen Cluster zu registrieren:
 - eks: RegisterCluster
 - ssm: CreateActivation
 - ssm: DeleteActivation
 - bin: PassRole
- Sie müssen über die folgenden Berechtigungen verfügen, um die Registrierung eines Clusters aufzuheben:
 - ex: DeregisterCluster
 - ssm: DeleteActivation
 - ssm: DeregisterManagedInstance

Erforderliche IAM-Rollen für Amazon EKS Connector

Die Verwendung des Amazon EKS Connectors erfordert die folgenden zwei IAM-Rollen:

- Die serviceverknüpfte Rolle [Amazon EKS Connector](#) wird bei der ersten Registrierung eines Clusters erstellt.
- Sie müssen die IAM-Rolle des Amazon-EKS-Connector-Agents erstellen. Details dazu finden Sie unter [the section called “Konnektor-IAM-Rolle”](#).

Um die Cluster- und Workload-Ansichtsberechtigung für [IAM-Prinzipale](#) zu aktivieren, müssen Sie die Clusterrollen eks-connector und Amazon EKS Connector auf Ihren Cluster anwenden. Folgen Sie den Schritten unter [Zugriff gewähren, um Kubernetes-Cluster-Ressourcen auf einer Amazon EKS-Konsole anzuzeigen](#).

Einen externen Kubernetes-Cluster mit der Amazon EKS Management Console verbinden

Sie können einen externen Kubernetes-Cluster mit Amazon EKS verbinden, indem Sie im folgenden Prozess mehrere Methoden verwenden. Dieser Prozess umfasst zwei Schritte: die Registrierung des Clusters bei Amazon EKS und die Installation des eks-connector-Agents im Cluster.

 Important

Der zweite Schritt muss innerhalb von 3 Tagen nach Abschluss des ersten Schritts erfolgen, bevor die Registrierung abläuft.

Überlegungen

Sie können bei der Installation des Agenten YAML-Manifeste verwenden. Alternativ können Sie Helm verwenden, wenn Sie den Cluster mit der Befehlszeilenschnittstelle AWS Management Console oder der AWS Befehlszeilenschnittstelle registrieren. Sie können Helm jedoch nicht verwenden, um den Agenten zu installieren, wenn Sie den Cluster bei `registriereneksctl`.

Voraussetzungen

- Stellen Sie sicher, dass die Agent-Rolle von Amazon EKS Connector erstellt wurde. Folgen Sie den Schritten unter [Erstellen der Amazon EKS-Connector-Agent-Rolle](#).
- Sie müssen über die folgenden Berechtigungen verfügen, um einen Cluster zu registrieren:
 - `eks:RegisterCluster`
 - `ssm:CreateActivation`
 - `ssm>DeleteActivation`
 - `iam:PassRole`

Schritt 1: Registrieren des Clusters

Um einen Cluster für den Amazon EKS-Connector zu registrieren, können Sie eines der folgenden Tools verwenden:

- [the section called “AWS CLI”](#)
- [the section called “AWS Management Console”](#)
- [the section called “eksctl”](#)

AWS CLI

1. AWS CLI muss installiert sein. Informationen zur Installation oder zum Upgrade finden Sie unter [AWS CLI installieren](#).

2. Geben Sie für die Connector-Konfiguration Ihre Amazon-EKS-Connector-Agent-IAM-Rolle an. Weitere Informationen finden Sie unter [the section called “Erforderliche IAM-Rollen für Amazon EKS Connector”](#).

```
aws eks register-cluster \  
  --name my-first-registered-cluster \  
  --connector-config roleArn=arn:aws: iam::111122223333:role/  
AmazonEKSCheckpointAgentRole,provider="OTHER" \  
  --region aws-region
```

Eine Beispielausgabe sieht wie folgt aus.

```
{  
  "cluster": {  
    "name": "my-first-registered-cluster",  
    "arn": "arn:aws: eks:region:111122223333:cluster/my-first-registered-  
cluster",  
    "createdAt": 1627669203.531,  
    "ConnectorConfig": {  
      "activationId": "xxxxxxxxACTIVATION_IDxxxxxxxx",  
      "activationCode": "xxxxxxxxACTIVATION_CODExxxxxxxx",  
      "activationExpiry": 1627672543.0,  
      "provider": "OTHER",  
      "roleArn": "arn:aws: iam::111122223333:role/AmazonEKSCheckpointAgentRole"  
    },  
    "status": "CREATING"  
  }  
}
```

Sie verwenden die Werte `aws-region`, `activationId` und `activationCode` im nächsten Schritt.

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie Add cluster (Cluster hinzufügen) und Register (Registrieren) aus, um die Konfigurationsseite aufzurufen.
3. Füllen Sie im Abschnitt Cluster konfigurieren die folgenden Felder aus:
 - Name – Ein eindeutiger Name für Ihren Cluster.

- **Provider (Provider)** – Hiermit zeigen Sie die Dropdown-Liste der Kubernetes-Clusteranbieter an. Wenn Sie den spezifischen Anbieter nicht kennen, wählen Sie **Andere** aus.
 - **Rolle EKS-Connector** – Wählen Sie die Rolle aus, die für die Verbindung mit dem Cluster verwendet werden soll.
4. Wählen Sie **Cluster registrieren** aus.
 5. Die Seite **Cluster-Übersicht** wird angezeigt. Wenn Sie das Helm-Chart verwenden möchten, kopieren Sie den Befehl `helm install` und fahren Sie mit dem nächsten Schritt fort. Wenn Sie das YAML-Manifest verwenden möchten, wählen Sie **YAML-Datei herunterladen** aus, um die Manifestdatei auf Ihr lokales Laufwerk herunterzuladen.

Important

Dies ist Ihre einzige Möglichkeit, den Befehl `helm install` zu kopieren oder diese Datei herunterzuladen. Gehen Sie nicht von dieser Seite weg, da auf den Link nicht zugegriffen werden kann und Sie den Cluster abmelden und die Schritte von vorne beginnen müssen.

Der Befehl bzw. die Manifestdatei kann nur einmal für den registrierten Cluster verwendet werden. Wenn Sie Ressourcen aus dem Kubernetes-Cluster löschen, müssen Sie den Cluster erneut registrieren und eine neue Manifestdatei abrufen.

Fahren Sie mit dem nächsten Schritt fort, um die Manifestdatei auf Ihren Kubernetes-Cluster anzuwenden.

eksctl

1. `eksctl`-Version 0.68 oder höher muss installiert sein. Informationen zur Installation oder Aktualisierung finden Sie unter [the section called “Cluster erstellen \(eksctl\)”](#).
2. Registrieren Sie den Cluster unter Angabe eines Namens, eines Anbieters und einer Region.

```
eksctl register cluster --name my-cluster --provider my-provider --region region-code
```

Beispielausgabe:

```
2021-08-19 13:47:26 [#] creating IAM role "eksctl-20210819194112186040"
2021-08-19 13:47:26 [#] registered cluster "<name>" successfully
2021-08-19 13:47:26 [#] wrote file eks-connector.yaml to <current directory>
```

```
2021-08-19 13:47:26 [#] wrote file eks-connector-clusterrole.yaml to <current
directory>
2021-08-19 13:47:26 [#] wrote file eks-connector-console-dashboard-full-access-
group.yaml to <current directory>
2021-08-19 13:47:26 [!] note: "eks-connector-clusterrole.yaml" and "eks-connector-
console-dashboard-full-access-group.yaml" give full EKS Console access to IAM
identity "<aws-arn>", edit if required; read https://eksctl.io/usage/eks-connector
for more info
2021-08-19 13:47:26 [#] run `kubectl apply -f eks-connector.yaml,eks-connector-
clusterrole.yaml,eks-connector-console-dashboard-full-access-group.yaml` before
expiry> to connect the cluster
```

Dadurch werden Dateien auf Ihrem lokalen Computer erstellt. Diese Dateien müssen innerhalb von 3 Tagen auf den externen Cluster angewendet werden, sonst läuft die Registrierung ab.

3. Wenden Sie in einem Terminal, das Zugriff auf den Cluster hat, die Datei `eks-connector-binding.yaml` an:

```
kubectl apply -f eks-connector-binding.yaml
```

Schritt 2: Installieren des **eks-connector**-Agents

Verwenden Sie eines der folgenden Tools, um den `eks-connector` Agenten zu installieren:

- [the section called “Helm”](#)
- [the section called “yaml”](#)

Helm

Note

Wenn Sie den Cluster bei registriert haben `eksctl`, verwenden Sie die YAML-Manifestmethode anstelle der Helm-Diagrammmethode.

1. Wenn Sie im vorherigen Schritt die AWS CLI verwendet haben, ersetzen Sie die Werte `ACTIVATION_CODE` und `ACTIVATION_ID` im folgenden Befehl jeweils durch die `activationId` `activationCode` Werte und. Ersetzen Sie das `aws-region` durch die AWS

Region, die Sie im vorherigen Schritt verwendet haben. Führen Sie dann den Befehl aus, um den eks-connector-Agent auf dem registrierenden Cluster zu installieren:

```
$ helm install eks-connector \
  --namespace eks-connector \
  oci://public.ecr.aws/eks-connector/eks-connector-chart \
  --set eks.activationCode=ACTIVATION_CODE \
  --set eks.activationId=ACTIVATION_ID \
  --set eks.agentRegion=aws-region
```

Wenn Sie die AWS Management Console im vorherigen Schritt verwendet haben, verwenden Sie den Befehl, den Sie aus dem vorherigen Schritt kopiert haben und bei dem diese Werte eingegeben wurden.

2. Überprüfen Sie den Zustand der installierten eks-connector-Bereitstellung und warten Sie, bis der Status des registrierten Clusters in Amazon EKS ACTIVE lautet.

yaml

Schließen Sie die Verbindung ab, indem Sie die Amazon-EKS-Connector-Manifestdatei auf Ihren Kubernetes-Cluster anwenden. Dazu müssen Sie die zuvor beschriebenen Methoden verwenden. Wenn das Manifest nicht innerhalb von drei Tagen angewendet wird, läuft die Amazon EKS Connector-Registrierung ab. Wenn die Clusterverbindung abläuft, muss die Registrierung des Clusters aufgehoben werden, bevor der Cluster erneut verbunden wird.

1. Laden Sie die Amazon EKS Connector YAML-Datei herunter.

```
curl -O https://amazon-eks.s3.us-west-2.amazonaws.com/eks-connector/manifests/eks-connector/latest/eks-connector.yaml
```

2. Bearbeiten Sie die YAML-Datei von Amazon EKS Connector und ersetzen Sie alle Verweise auf %AWS_REGION%, %EKS_ACTIVATION_ID%, %EKS_ACTIVATION_CODE% durch die aws-region, activationId und activationCode aus der Ausgabe des vorherigen Schritts.

Der folgende Beispielbefehl kann diese Werte ersetzen.

```
sed -i "s~%AWS_REGION%~$aws-region~g; s~%EKS_ACTIVATION_ID%~$EKS_ACTIVATION_ID~g; s~%EKS_ACTIVATION_CODE%~$(echo -n $EKS_ACTIVATION_CODE | base64)~g" eks-connector.yaml
```

 Important

Stellen Sie sicher, dass Ihr Aktivierungscode das base64-Format hat.

3. In einem Terminal, das auf den Cluster zugreifen kann, können Sie jetzt die aktualisierte Manifestdatei mit dem folgenden Befehl anwenden:

```
kubectl apply -f eks-connector.yaml
```

4. Nachdem die YAML-Dateien des Amazon-EKS-Connector-Manifests und der Rollenbindung auf Ihren Kubernetes-Cluster angewendet wurden, bestätigen Sie, dass der Cluster jetzt verbunden ist.

```
aws eks describe-cluster \
  --name "my-first-registered-cluster" \
  --region AWS_REGION
```

Die Ausgabe sollte `status=ACTIVE` enthalten.

5. (Optional) Fügen Sie Ihrem Cluster Tags hinzu. Weitere Informationen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#).

Nächste Schritte

Falls Sie Probleme mit diesen Schritten haben, finden Sie weitere Informationen unter [the section called “Problembehandlung beim EKS-Connector”](#).

Informationen darüber, wie Sie zusätzlichen [IAM-Prinzipalen](#) Zugriff auf die Amazon EKS-Konsole gewähren, um Kubernetes-Ressourcen in einem verbundenen Cluster anzuzeigen, finden Sie unter [the section called “Gewähren Sie Zugriff auf Cluster”](#)

Gewähren Sie Zugriff auf die Anzeige von Kubernetes-Cluster-Ressourcen auf einer Amazon EKS-Konsole

Gewähren Sie [IAM-Prinzipalen](#) Zugriff auf die Amazon EKS-Konsole, um Informationen über Kubernetes-Ressourcen anzuzeigen, die auf Ihrem verbundenen Cluster ausgeführt werden.

Voraussetzungen

Der [IAM-Principal](#), den Sie für den Zugriff verwenden, AWS Management Console muss die folgenden Anforderungen erfüllen:

- Er muss über die `eks:AccessKubernetesApi`-IAM-Berechtigung verfügen.
- Das Amazon-EKS-Connector-Service-Konto kann den IAM-Prinzipal im Cluster imitieren. Dadurch kann der Amazon EKS-Connector den IAM-Prinzipal einem Kubernetes-Benutzer zuordnen.

Um die Amazon EKS Connector-Clusterrolle zu erstellen und anzuwenden

1. Laden Sie die `eks-connector-Clusterrollenvorlage` herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/eks-connector/manifests/eks-connector-console-roles/eks-connector-clusterrole.yaml
```

2. Bearbeiten Sie die YAML-Datei der Clusterrollen-Vorlage. Ersetzen Sie die Referenzen von `%IAM_ARN%` durch den Amazon-Ressourcennamen (ARN) Ihres IAM-Prinzipals.
3. Wenden Sie die Amazon-EKS-Connector-Clusterrolle YAML auf Ihren Kubernetes-Cluster an.

```
kubectl apply -f eks-connector-clusterrole.yaml
```

Damit ein IAM-Principal Kubernetes-Ressourcen in der Amazon EKS-Konsole anzeigen kann, muss der Principal einem Kubernetes zugeordnet sein `role` oder über die erforderlichen Berechtigungen zum Lesen der Ressourcen `clusterrole` verfügen. Weitere Informationen finden Sie unter [Using RBAC Authorization](#) in der Kubernetes-Dokumentation.

Um einen IAM-Principal für den Zugriff auf den verbundenen Cluster zu konfigurieren

1. Sie können einer dieser Beispielmanifestdateien herunterladen, um eine `clusterrole` und `clusterrolebinding` oder eine `role` und `rolebinding` zu erstellen:

Kubernetes-Ressourcen in allen Namespaces anzeigen

- Die `eks-connector-console-dashboard-full-access-clusterrole`-Clusterrolle ermöglicht den Zugriff auf alle Namespaces und Ressourcen, die in der Konsole visualisiert werden können. Sie können den Namen des `role`, `clusterrole` und der entsprechenden Bindung ändern, bevor Sie ihn auf Ihren Cluster anwenden. Verwenden Sie den folgenden Befehl, um eine Beispieldatei herunterzuladen.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/eks-connector/manifests/eks-connector-console-roles/eks-connector-console-dashboard-full-access-group.yaml
```

Kubernetes-Ressourcen in einem bestimmten Namespace anzeigen

- Der Namespace in dieser Datei ist default. Wenn Sie also einen anderen Namespace angeben möchten, bearbeiten Sie die Datei, bevor Sie sie auf Ihren Cluster anwenden. Verwenden Sie den folgenden Befehl, um eine Beispieldatei herunterzuladen.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/eks-connector/manifests/eks-connector-console-roles/eks-connector-console-dashboard-restricted-access-group.yaml
```

2. Bearbeiten Sie die YAML-Datei mit vollem oder eingeschränktem Zugriff, um die Referenzen von %IAM_ARN% durch den Amazon-Ressourcennamen (ARN) Ihres IAM-Prinzips zu ersetzen.
3. Wenden Sie die YAML-Dateien mit vollem oder eingeschränktem Zugriff auf Ihren Kubernetes-Cluster an. Ersetzen Sie den Wert der YAML-Datei durch Ihren eigenen.

```
kubectl apply -f eks-connector-console-dashboard-full-access-group.yaml
```

Informationen zum Anzeigen von Kubernetes-Ressourcen in Ihrem verbundenen Cluster finden Sie unter [the section called “Auf Cluster-Ressourcen zugreifen”](#). Daten für einige Ressourcentypen auf der Registerkarte Ressourcen sind für verbundene Cluster nicht verfügbar.

Einen Kubernetes-Cluster von der Amazon EKS-Konsole abmelden

Wenn Sie mit der Verwendung eines verbundenen Clusters fertig sind, können Sie die Registrierung aufheben. Nach der Deregistrierung ist der Cluster in der Amazon EKS-Konsole nicht mehr sichtbar.

Sie müssen über die folgenden Berechtigungen verfügen, um die DeregisterCluster-API aufzurufen:

- eks:DeregisterCluster
- ssm:DeleteActivation
- ssm:DeregisterManagedInstance

Dieser Vorgang umfasst zwei Schritte: Abmeldung des Clusters von Amazon EKS und Deinstallation des Agents „eks-connector“ im Cluster.

Den Kubernetes-Cluster deregistrieren

Um einen Cluster vom Amazon EKS-Connector abzumelden, können Sie eines der folgenden Tools verwenden:

- [the section called “AWS CLI”](#)
- [the section called “AWS Management Console”](#)
- [the section called “eksctl”](#)

AWS CLI

1. AWS CLI muss installiert sein. Informationen zur Installation oder zum Upgrade finden Sie unter [AWS CLI installieren](#).
2. Stellen Sie sicher, dass die Agent-Rolle von Amazon EKS Connector erstellt wurde.
3. Den verbundenen Cluster deregistrieren.

```
aws eks deregister-cluster \
  --name my-cluster \
  --region region-code
```

AWS Management Console

1. Öffnen Sie die [Amazon-EKS-Konsole](#).
2. Wählen Sie Clusters (Cluster) aus.
3. Wählen Sie auf der Seite Cluster den verbundenen Cluster aus und wählen Sie Deregistrieren.
4. Bestätigen Sie, dass Sie den Cluster deregistrieren möchten.

eksctl

1. eksctlVersion 0.68 oder höher installieren. Informationen zur Installation oder Aktualisierung finden Sie unter [the section called “Cluster erstellen \(eksctl\)”](#).
2. Stellen Sie sicher, dass die Agent-Rolle von Amazon EKS Connector erstellt wurde.

3. Den verbundenen Cluster deregistrieren:

```
eksctl deregister cluster --name my-cluster
```

Bereinigen Sie die Ressourcen in Ihrem Kubernetes-Cluster

Verwenden Sie eines der folgenden Tools, um den eks-connector Agenten zu deinstallieren:

- [the section called “Helm”](#)
- [the section called “Yaml”](#)

Helm

Führen Sie zur Deinstallation des Agents den folgenden Befehl aus.

```
helm -n eks-connector uninstall eks-connector
```

Yaml

1. Löschen Sie die Amazon-EKS-Connector-YAML-Datei aus Ihrem Kubernetes-Cluster.

```
kubectl delete -f eks-connector.yaml
```

2. Wenn Sie zusätzliche [IAM-Prinzipale clusterrolebindings](#) für den Zugriff auf den Cluster erstellt haben `clusterrole` oder möchten, löschen Sie sie aus Ihrem Kubernetes-Cluster.

Probleme mit dem Amazon EKS Connector beheben

Dieses Thema behandelt einige der häufigsten Fehler, die bei der Verwendung des Amazon EKS Connectors auftreten können, einschließlich Anleitungen zu deren Behebung und Umgehungen.

Grundlegende Fehlersuche

In diesem Abschnitt werden Schritte zur Diagnose von Problemen mit dem Amazon EKS Connector beschrieben.

Prüfen Sie den Status von Amazon EKS Connector

Um den Status des Amazon EKS-Connectors zu überprüfen, geben Sie Folgendes ein:

```
kubectl get pods -n eks-connector
```

Überprüfen Sie die Protokolle des Amazon-EKS-Connectors

Der Amazon EKS Connector Pod besteht aus drei Containern. Führen Sie die folgenden Befehle aus, um vollständige Protokolle für alle diese Container abzurufen, damit Sie sie überprüfen können:

- **connector-init**

```
kubectl logs eks-connector-0 --container connector-init -n eks-connector  
kubectl logs eks-connector-1 --container connector-init -n eks-connector
```

- **connector-proxy**

```
kubectl logs eks-connector-0 --container connector-proxy -n eks-connector  
kubectl logs eks-connector-1 --container connector-proxy -n eks-connector
```

- **connector-agent**

```
kubectl exec eks-connector-0 --container connector-agent -n eks-connector -- cat /  
var/log/amazon/ssm/amazon-ssm-agent.log  
kubectl exec eks-connector-1 --container connector-agent -n eks-connector -- cat /  
var/log/amazon/ssm/amazon-ssm-agent.log
```

Bringen Sie den effektiven Clusternamen in Erfahrung

Amazon EKS-Cluster werden `clusterName` innerhalb eines einzigen AWS Kontos und einer AWS Region eindeutig identifiziert. Wenn Sie mehrere verbundene Cluster in Amazon EKS haben, können Sie überprüfen, für welchen Amazon EKS-Cluster der aktuelle Kubernetes-Cluster registriert ist. Geben Sie dafür Folgendes ein, um den `clusterName` des aktuellen Clusters herauszufinden.

```
kubectl exec eks-connector-0 --container connector-agent -n eks-connector \  
-- cat /var/log/amazon/ssm/amazon-ssm-agent.log | grep -m1 -oE "eks_c:[a-zA-Z0-9_-]+"  
| sed -E "s/^.*eks_c:([a-zA-Z0-9_-]+)_[a-zA-Z0-9]+.*$/\1/"  
kubectl exec eks-connector-1 --container connector-agent -n eks-connector \  
-- cat /var/log/amazon/ssm/amazon-ssm-agent.log | grep -m1 -oE "eks_c:[a-zA-Z0-9_-]+"  
| sed -E "s/^.*eks_c:([a-zA-Z0-9_-]+)_[a-zA-Z0-9]+.*$/\1/"
```

```
-- cat /var/log/amazon/ssm/amazon-ssm-agent.log | grep -m1 -oE "eks_c:[a-zA-Z0-9_-]+"  
| sed -E "s/^.*eks_c:([a-zA-Z0-9_-]+)_[a-zA-Z0-9_]+.*$/\1/"
```

Verschiedene Befehle

Die folgenden Befehle sind nützlich, um Informationen abzurufen, die Sie zur Behebung von Problemen benötigen.

- Verwenden Sie den folgenden Befehl, um Bilder zu sammeln, die von Pods in Amazon EKS Connector verwendet werden.

```
kubectl get pods -n eks-connector -o jsonpath="{.items[*].spec.containers[*].image}"  
| tr -s '[:space:]' '\n'
```

- Verwenden Sie den folgenden Befehl, um die Knotennamen zu ermitteln, auf denen Amazon-EKS-Connector ausgeführt wird.

```
kubectl get pods -n eks-connector -o jsonpath="{.items[*].spec.nodeName}" | tr -s  
'[:space:]' '\n'
```

- Führen Sie den folgenden Befehl aus, um Ihre Kubernetes-Client- und Server-Versionen abzurufen.

```
kubectl version
```

- Führen Sie den folgenden Befehl aus, um Informationen zu Ihren Knoten abzurufen.

```
kubectl get nodes -o wide --show-labels
```

Helm-Ausgabe: 403 Forbidden

Wenn Sie beim Ausführen von Helm-Installationsbefehlen die folgende Fehlermeldung erhalten haben:

```
Error: INSTALLATION FAILED: unexpected status from HEAD request to https://  
public.ecr.aws/v2/eks-connector/eks-connector-chart/manifests/0.0.6: 403 Forbidden
```

Sie können die folgende Zeile ausführen, um das Problem zu beheben:

```
docker logout public.ecr.aws
```

Konsolenfehler: Der Cluster steckt im Status „Ausstehend“ fest

Wenn der Cluster in dem Pending Status auf der Amazon EKS-Konsole hängen bleibt, nachdem Sie ihn registriert haben, kann das daran liegen, dass der Amazon EKS-Connector den Cluster AWS noch nicht erfolgreich verbunden hat. Bei einem registrierten Cluster bedeutet der Pending Status, dass die Verbindung nicht erfolgreich hergestellt wurde. Um dieses Problem zu lösen, stellen Sie sicher, dass Sie das Manifest auf den Kubernetes-Ziel-Cluster angewendet haben. Wenn Sie es auf den Cluster angewendet haben, der Cluster sich aber immer noch im Pending-Zustand befindet, ist `eks-connector-StatefulSet` möglicherweise fehlerhaft. Informationen zum Beheben dieses Problems finden Sie in diesem Thema unter [the section called “Die Pods des Amazon EKS-Connectors stürzen in einer Schleife ab”](#).

Konsolenfehler: Der Benutzer `system:serviceaccount:eks-connector:eks-connector` kann sich nicht als Ressourcenbenutzer in der API-Gruppe im Clusterbereich ausgeben

Der Amazon EKS Connector verwendet [Kubernetes-Benutzerimpersonation](#), um im Namen von [IAM-Prinzipalen](#) aus dem zu handeln. AWS Management Console Jedem Principal, der über das AWS `eks-connector` Dienstkonto auf die Kubernetes-API zugreift, muss die Erlaubnis erteilt werden, sich als der entsprechende Kubernetes-Benutzer mit einem IAM-ARN als Kubernetes-Benutzernamen auszugeben. In den folgenden Beispielen wird der IAM-ARN einem Kubernetes-Benutzer zugeordnet.

- Der IAM-Benutzer aus dem Konto ist einem Kubernetes-Benutzer zugeordnet. *john* AWS **111122223333** [Bewährte Methoden für IAM](#) empfehlen, dass Sie Rollen statt Benutzern Berechtigungen gewähren.

```
arn:aws:iam::111122223333:user/john
```

- Die IAM-Rolle *admin* aus dem AWS Konto **111122223333** ist einem Kubernetes-Benutzer zugeordnet:

```
arn:aws:iam::111122223333:role/admin
```

Das Ergebnis ist ein IAM-Rollen-ARN anstelle des ARN der AWS STS-Sitzung.

Anweisungen zum Konfigurieren der `ClusterRole` und `ClusterRoleBinding`, um dem `eks-connector`-Servicekonto die Berechtigung zu erteilen, sich als zugeordneter Benutzer auszugeben, finden Sie unter [the section called “Gewähren Sie Zugriff auf Cluster”](#). Stellen Sie sicher, dass in der Vorlage durch den IAM-ARN des IAM-Prinzips ersetzt `%IAM_ARN%` wird. AWS Management Console

Konsolenfehler: [...] ist verboten: Der Benutzer [...] kann die Ressource [...] in der API-Gruppe im Clusterbereich nicht auflisten

Betrachten Sie das folgende Problem. Der Amazon EKS-Connector hat erfolgreich die Identität des anfordernden AWS Management Console IAM-Prinzips im Kubernetes-Zielcluster angenommen. Der Principal, dessen Identität angenommen wurde, hat jedoch keine RBAC-Berechtigung für Kubernetes-API-Operationen.

Um dieses Problem zu beheben, gibt es zwei Methoden, um zusätzlichen Benutzern Berechtigungen zu erteilen. Wenn Sie „eks-connector“ zuvor über Helm-Chart installiert haben, können Sie Benutzern ganz einfach Zugriff gewähren, indem Sie den folgenden Befehl ausführen. Ersetzen Sie das `userARN1` und `userARN2` durch eine Liste der IAM-Rollen, um ARNs Zugriff auf die Kubernetes-Ressourcen zu gewähren:

```
helm upgrade eks-connector oci://public.ecr.aws/eks-connector/eks-connector-chart \
  --reuse-values \
  --set 'authentication.allowedUserARNs={userARN1,userARN2}'
```

Oder gewähren Sie als Clusteradministrator einzelnen Kubernetes-Benutzern die entsprechende Stufe an RBAC-Rechten. Weitere Informationen und Beispiele finden Sie unter [the section called “Gewähren Sie Zugriff auf Cluster”](#).

Konsolenfehler: Amazon EKS kann nicht mit Ihrem Kubernetes-Cluster-API-Server kommunizieren. Der Cluster muss sich im ACTIVE-Status befinden, um eine erfolgreiche Verbindung zu erreichen. Try again in few minutes. (Versuchen Sie es in ein paar Minuten erneut.)

Wenn der Amazon EKS-Service nicht mit dem Amazon EKS-Connector im Zielcluster kommunizieren kann, kann das an einem der folgenden Gründe liegen:

- Der Amazon-EKS-Connector im Ziel-Cluster ist fehlerhaft.

- Schlechte Konnektivität oder unterbrochene Verbindung zwischen dem Zielcluster und der AWS Region.

Um dieses Problem zu beheben, überprüfen Sie die [Amazon-EKS-Connector-Protokolle](#). Wenn Sie keinen Fehler für den Amazon EKS Connector sehen, versuchen Sie nach einigen Minuten erneut, die Verbindung herzustellen. Wenn Sie regelmäßig hohe Latenz oder intermittierende Konnektivität für den Zielcluster feststellen, sollten Sie erwägen, den Cluster erneut in einer AWS Region zu registrieren, die sich in Ihrer Nähe befindet.

Die Pods des Amazon EKS-Connectors stürzen in einer Schleife ab

Es gibt viele Gründe, die dazu führen können, dass ein Amazon EKS-Connector-Pod in den CrashLoopBackOff Status wechselt. Dieses Problem betrifft wahrscheinlich den connector-init-Container. Überprüfen Sie den Status des Amazon EKS-Connector-Pods.

```
kubectl get pods -n eks-connector
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	READY	STATUS	RESTARTS	AGE
eks-connector-0	0/2	Init:CrashLoopBackOff	1	7s

Wenn Ihre Ausgabe der vorherigen Ausgabe ähnlich ist, lesen Sie [the section called “Überprüfen Sie die Protokolle des Amazon-EKS-Connectors”](#), um das Problem zu beheben.

EKS-Connector konnte nicht initiiert werden: InvalidActivation

Wenn Sie den Amazon-EKS-Connector zum ersten Mal starten, registriert er ein activationId und activationCode bei Amazon Web Services. Die Registrierung schlägt möglicherweise fehl, was dazu führen kann, dass der connector-init-Container mit einem Fehler ähnlich dem folgenden abstürzt.

```
F1116 20:30:47.261469      1 init.go:43] failed to initiate eks-connector:
InvalidActivation:
```

Berücksichtigen Sie die folgenden Ursachen und empfohlenen Korrekturen, um dieses Problem zu beheben:

- Die Registrierung ist möglicherweise fehlgeschlagen, weil die `activationId` und `activationCode` nicht in Ihrer Manifestdatei enthalten sind. Stellen Sie in diesem Fall sicher, dass es sich um die richtigen Werte handelt, die von der `RegisterCluster`-API-Operation zurückgegeben wurden, und dass sich `activationCode` in der Manifest-Datei befindet. Das `activationCode` wird zu den Kubernetes-Geheimnissen hinzugefügt und muss daher codiert werdenbase64. Weitere Informationen finden Sie unter [the section called “Schritt 1: Registrieren des Clusters”](#).
- Die Registrierung ist möglicherweise fehlgeschlagen, da Ihre Aktivierung abgelaufen ist. Dies liegt daran, dass Sie den Amazon-EKS-Connector aus Sicherheitsgründen innerhalb von drei Tagen nach der Registrierung des Clusters aktivieren müssen. Um dieses Problem zu beheben, stellen Sie sicher, dass das Amazon EKS Connector-Manifest vor dem Ablaufdatum und der Ablaufzeit auf den Ziel-Kubernetes-Cluster angewendet wird. Um das Ablaufdatum der Aktivierung zu bestätigen, rufen Sie die `DescribeCluster`-API-Operation auf.

```
aws eks describe-cluster --name my-cluster
```

In der folgenden Beispielantwort wird das Ablaufdatum und die Uhrzeit als `2021-11-12T22:28:51.101000-08:00` aufgezeichnet.

```
{
  "cluster": {
    "name": "my-cluster",
    "arn": "arn:aws: eks:region:111122223333:cluster/my-cluster",
    "createdAt": "2021-11-09T22:28:51.449000-08:00",
    "status": "FAILED",
    "tags": {
    },
    "connectorConfig": {
      "activationId": "000000000-0000-0000-0000-000000000000",
      "activationExpiry": "2021-11-12T22:28:51.101000-08:00",
      "provider": "OTHER",
      "roleArn": "arn:aws: iam::111122223333:role/my-connector-role"
    }
  }
}
```

Wenn das `activationExpiry` erreicht wurde, melden Sie den Cluster ab und registrieren Sie ihn erneut. Dadurch wird eine neue Aktivierung generiert.

Im Cluster-Knoten fehlt die ausgehende Konnektivität

Um ordnungsgemäß zu funktionieren, benötigt der Amazon EKS Connector ausgehende Konnektivität zu mehreren AWS Endpunkten. Sie können einen privaten Cluster ohne ausgehende Konnektivität nicht mit einer Zielregion verbinden. AWS Um dieses Problem zu lösen, müssen Sie die erforderliche ausgehende Konnektivität hinzufügen. Weitere Informationen zu den Anforderungen für Konnektoren finden Sie unter [the section called “Überlegungen zum Amazon EKS Connector”](#).

Die Amazon EKS-Connector-Pods befinden sich im **ImagePullBackOff** Status

Wenn Sie den `get pods` Befehl ausführen und sich die Pods im `ImagePullBackOff` Status befinden, können sie nicht ordnungsgemäß funktionieren. Wenn sich die Amazon EKS Connector Pods im `ImagePullBackOff` Status befinden, können sie nicht ordnungsgemäß funktionieren. Überprüfen Sie den Status Ihrer Amazon EKS Connector Pods.

```
kubectl get pods -n eks-connector
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	READY	STATUS	RESTARTS	AGE
eks-connector-0	0/2	Init:ImagePullBackOff	0	4s

Die standardmäßige Amazon-EKS-Connector-Manifest-Datei verweist auf Images aus der [öffentlichen Amazon-ECR-Galerie](#). Es ist möglich, dass der Ziel-Kubernetes-Cluster keine Bilder aus der Amazon ECR Public Gallery abrufen kann. Beheben Sie entweder das Image-Abrufproblem der öffentlichen Amazon-ECR-Galerie oder erwägen Sie eine Spiegelung der Images in der privaten Container-Registry Ihrer Wahl.

AWS Häufig gestellte Fragen zum Connector

F: Wie funktioniert die zugrunde liegende Technologie hinter dem Amazon-EKS-Connector?

A: Der Amazon EKS Connector basiert auf dem AWS Systems Manager (Systems Manager) - Agenten. Der Amazon EKS Connector läuft als `StatefulSet` auf Ihrem Kubernetes-Cluster. Er stellt eine Verbindung her und ermöglicht die Kommunikation zwischen dem API-Server Ihres Clusters und Amazon Web Services. Auf diese Weise werden Cluster-Daten in der Amazon EKS-Konsole angezeigt, bis Sie die Verbindung zum Cluster trennen AWS. Der Systems-Manager-Agent

ist ein Open-Source-Projekt. Weitere Informationen zu diesem Projekt finden Sie auf der [GitHub - Projektseite](#).

F: Ich habe einen On-Premises-Kubernetes-Cluster, den ich verbinden möchte. Muss ich Firewall-Ports öffnen, um ihn zu verbinden?

A: Nein, Sie müssen keine Firewall-Ports öffnen. Der Kubernetes-Cluster benötigt nur eine ausgehende Verbindung zu Regionen. AWS AWS Dienste greifen niemals auf Ressourcen in Ihrem lokalen Netzwerk zu. Der Amazon EKS Connector läuft auf Ihrem Cluster und initiiert die Verbindung zu AWS. Wenn die Clusterregistrierung abgeschlossen ist, werden Befehle AWS erst dann an den Amazon EKS-Connector ausgegeben, wenn Sie eine Aktion von der Amazon EKS-Konsole aus starten, für die Informationen vom Kubernetes-API-Server in Ihrem Cluster erforderlich sind.

F: An welche Daten werden vom Amazon EKS Connector AWS von meinem Cluster gesendet?

A: Der Amazon EKS Connector sendet technische Informationen, die für die Registrierung Ihres Clusters erforderlich sind AWS. Er sendet auch Cluster- und Workload-Metadaten für die Funktionen der Amazon EKS-Konsole, die Kunden anfordern. Der Amazon-EKS-Connector erfasst oder sendet diese Daten nur, wenn Sie eine Aktion von der Amazon-EKS-Konsole oder der Amazon-EKS-API aus starten, die das Senden der Daten an AWS erfordert. Abgesehen von der Kubernetes-Versionsnummer speichert er standardmäßig AWS keine Daten. Er speichert Daten nur, wenn Sie dies autorisieren.

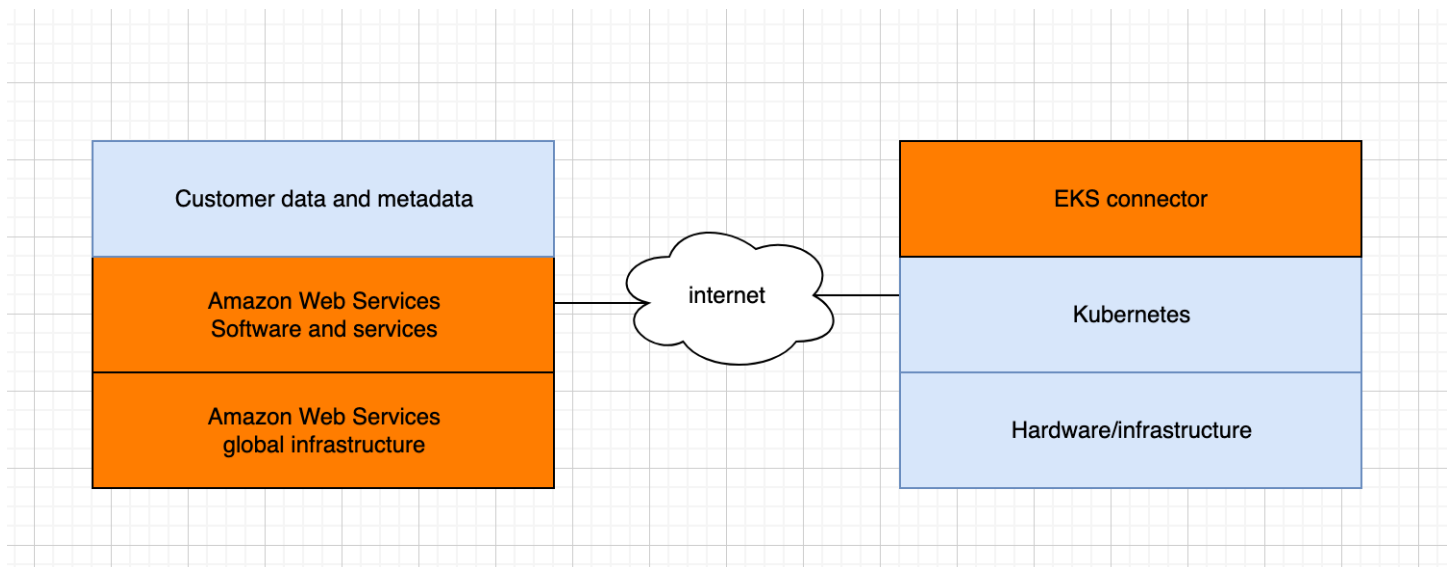
F: Kann ich einen Cluster außerhalb einer AWS Region verbinden?

A: Ja, Sie können einen Cluster von jedem Standort aus mit Amazon EKS verbinden. Darüber hinaus kann sich Ihr Amazon EKS-Service in jeder AWS öffentlichen AWS Handelsregion befinden. Dies funktioniert mit einer gültigen Netzwerkverbindung von Ihrem Cluster zur AWS Zielregion. Wir empfehlen Ihnen, eine AWS Region auszuwählen, die Ihrem Clusterstandort am nächsten liegt, um die Leistung der Benutzeroberfläche zu optimieren. Wenn Sie beispielsweise einen Cluster in Tokio haben, verbinden Sie Ihren Cluster mit der AWS Region in Tokio (d. h. der `ap-northeast-1` AWS Region), um eine geringe Latenz zu erzielen. Sie können einen Cluster von jedem Standort aus mit Amazon EKS in allen öffentlichen AWS Handelsregionen verbinden, mit Ausnahme von China oder GovCloud AWS Regionen.

Verstehen Sie die Sicherheit in Amazon EKS Connector

Der Amazon EKS Connector ist eine Open-Source-Komponente, die auf Ihrem Kubernetes-Cluster ausgeführt wird. Dieser Cluster kann sich außerhalb der AWS Umgebung befinden. Dies erfordert

zusätzliche Überlegungen zur Sicherheitsverantwortung. Das folgende Diagramm verdeutlicht diese Konfiguration. Orange steht für AWS Verantwortlichkeiten und Blau für Kundenverantwortlichkeiten:



In diesem Thema werden die Unterschiede im Verantwortungsmodell beschrieben, wenn sich der verbundene Cluster außerhalb von AWS befindet.

AWS Verantwortlichkeiten

- Wartung, Aufbau und Bereitstellung von Amazon EKS Connector, einer [Open-Source-Komponente](#), die auf dem Kubernetes-Cluster eines Kunden ausgeführt wird und mit dem kommuniziert. AWS
- Aufrechterhaltung der Kommunikationssicherheit auf Transport- und Anwendungsebene zwischen dem verbundenen Kubernetes-Cluster und den Diensten. AWS

Pflichten des Kunden

- Kubernetes-Cluster-spezifische Sicherheit, insbesondere in folgenden Bereichen:
 - Kubernetes-Geheimnisse müssen ordnungsgemäß verschlüsselt und geschützt werden.
 - Sperren des Zugriffs auf den `eks-connector`-Namespace.
- Konfigurieren der RBAC-Berechtigungen (rollenbasierte Zugriffskontrolle) zur Verwaltung des Benutzerzugriffs von [IAM-Prinzipal](#) aus AWS. Detaillierte Anweisungen finden Sie unter [the section called "Gewähren Sie Zugriff auf Cluster"](#).
- Amazon EKS Connector installieren und aktualisieren.

- Wartung der Hardware, Software und Infrastruktur, die den verbundenen Kubernetes-Cluster unterstützt.
- Sicherung ihrer AWS Konten (z. B. durch den Schutz Ihrer [Root-Benutzeranmeldedaten](#)).

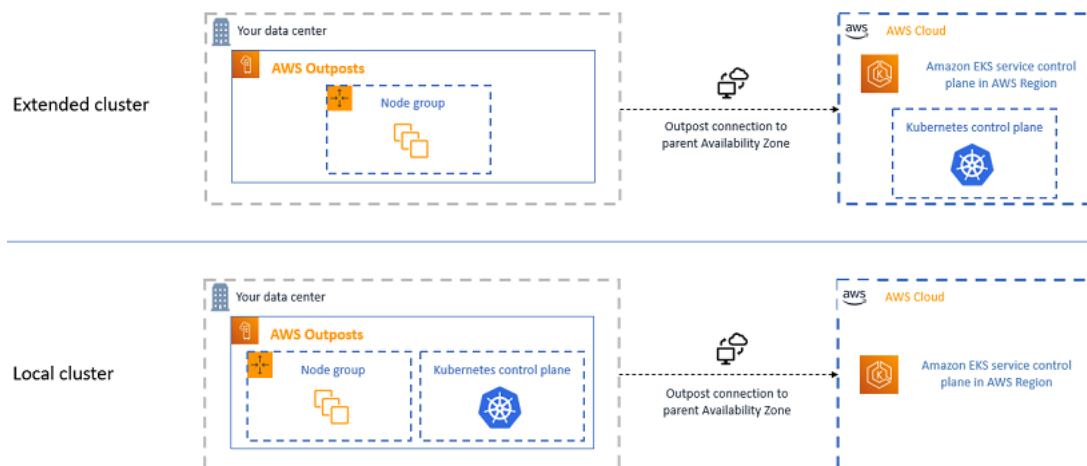
Stellen Sie Amazon EKS vor Ort mit AWS Outposts bereit

Sie können Amazon EKS verwenden, um lokale Kubernetes-Anwendungen auf Outposts auszuführen. AWS Sie können Amazon EKS auf Outposts folgendermaßen bereitstellen:

- **Erweiterte Cluster** — Führen Sie die Kubernetes-Steuerebene in einer AWS Region und Knoten in Ihrem Outpost aus.
- **Lokale Cluster** — Führen Sie die Kubernetes-Steuerebene und die Knoten auf Ihrem Outpost aus.

Bei beiden Bereitstellungsoptionen wird die Kubernetes-Steuerebene vollständig von verwaltet. AWS Sie können dieselben Amazon EKS APIs, Tools und Konsolen verwenden, die Sie in der Cloud verwenden, um Amazon EKS auf Outposts zu erstellen und auszuführen.

Das folgende Diagramm zeigt diese Optionen für die Bereitstellung.



Wann die einzelnen Bereitstellungsoptionen verwendet werden sollten

Sowohl lokale als auch erweiterte Cluster sind allgemeine Bereitstellungsoptionen und können für eine Reihe von Anwendungen verwendet werden.

Mit lokalen Clustern können Sie den gesamten Amazon-EKS-Cluster lokal auf Outposts ausführen. Mit dieser Option können Sie das Risiko von Ausfallzeiten bei Anwendungen verringern, die durch vorübergehende Netzwerkunterbrechungen in der Cloud entstehen können. Diese Netzwerkunterbrechungen können durch Glasfaserausfälle oder Wetterereignisse verursacht werden. Da der gesamte Amazon-EKS-Cluster lokal auf Outposts ausgeführt wird, bleiben Anwendungen

verfügbar. Sie können Cluster-Vorgänge während Netzwerkunterbrechungen mit der Cloud durchführen. Weitere Informationen finden Sie unter [the section called “Bereiten Sie sich auf Verbindungsabbrüche vor”](#). Wenn Sie Bedenken hinsichtlich der Qualität der Netzwerkverbindung von Ihren Outposts zur übergeordneten AWS Region haben und hohe Verfügbarkeit bei Netzwerkunterbrechungen benötigen, verwenden Sie die lokale Cluster-Bereitstellungsoption.

Mit erweiterten Clustern können Sie Kapazität in Ihrem Outpost sparen, da die Kubernetes-Steuerebene in der übergeordneten Region läuft. AWS Diese Option ist geeignet, wenn Sie in eine zuverlässige, redundante Netzwerkkonnektivität von Ihrem Outpost zur Region investieren können. AWS Die Qualität der Netzwerkverbindung ist für diese Option entscheidend. Die Art und Weise, wie Kubernetes mit Netzwerkunterbrechungen zwischen der Kubernetes-Steuerebene und den Knoten umgeht, kann zu Anwendungsausfällen führen. Weitere Informationen zum Verhalten von Kubernetes finden Sie unter [Scheduling, Preemption](#) and Eviction in der Kubernetes-Dokumentation.

Vergleich der Optionen für die Bereitstellung

Die folgende Tabelle vergleicht die Unterschiede zwischen den beiden Optionen.

Funktion	Erweiterter Cluster	Lokaler Cluster
Ort der Kubernetes-Steuerebene	AWS Region	Outpost
Konto für die Kubernetes-Steuerebene	AWS Konto	Ihr Konto
Regionale Verfügbarkeit	siehe Service-Endpunkte	USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Nordkalifornien), USA West (Oregon), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio), Kanada (Zentral), Europa (Frankfurt), Europa (Irland), Europa (London), Naher Osten (Bahrain),

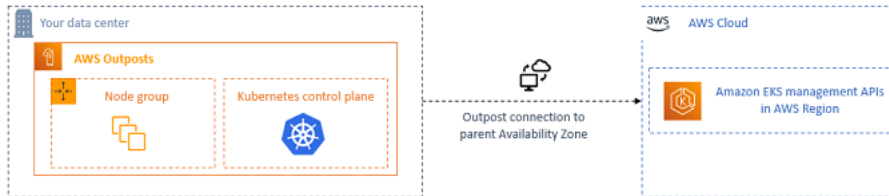
Funktion	Erweiterter Cluster	Lokaler Cluster
		Naher Osten (Bahrain) und Südamerika (São Paulo)
Kubernetes-Nebenversionen	Unterstützte Amazon-EKS-Versionen.	Unterstützte Amazon-EKS-Versionen.
Plattformversionen	Siehe the section called “Plattformversionen”	Siehe the section called “Versionen der EKS-Plattform”
Outpost-Formfaktoren	Outpost-Racks	Outpost-Racks
Benutzeroberflächen	AWS Management Console, AWS CLI, Amazon EKS-API, AWS CloudFormation, und Terraform	AWS Management Console, AWS CLI, Amazon EKS-API, AWS CloudFormation, und Terraform
Verwaltete Richtlinien	EKSClusterAmazon-Richtlinie und the section called “AWS verwaltete Richtlinie: Amazon EKSService RolePolicy”	Amazon EKSLocal OutpostClusterPolicy und the section called “AWS verwaltete Richtlinie: Amazon EKSLocal OutpostServiceRolePolicy”
Cluster-VPC und Subnetze	Siehe the section called “VPC- und Subnetz-Anforderungen”	Siehe the section called “Erstellen von VPC und Subnetzen”
Cluster-Endpunktzugriff	Öffentlich oder privat oder beides	Nur privat
Kubernetes-API-Serverauthentifizierung	AWS Identity and Access Management (IAM) und OIDC	IAM und x.509-Zertifikate
Knotentypen	Nur selbstverwaltet	Nur selbstverwaltet
Knoten-Berechnungstypen	Amazon auf EC2 Abruf	Amazon auf EC2 Abruf
Knoten-Speichertypen	Amazon EBS gp2 und lokale SSD NVMe	Amazon EBS gp2 und lokale SSD NVMe

Funktion	Erweiterter Cluster	Lokaler Cluster
Amazon EKS optimiert AMIs	Amazon Linux, Windows und Bottlerocket	Nur Amazon Linux
IP-Versionen	Nur IPv4	Nur IPv4
Add-Ons	Amazon-EKS-Add-Ons oder selbstverwaltete Add-Ons	Nur Selbstverwaltete Add-Ons
Standard-Container-Netzwerk schnittstelle	Amazon-VPC-CNI-Plug-In für Kubernetes	Amazon-VPC-CNI-Plug-In für Kubernetes
Kubernetes-Steuerebene-Protokolle	CloudWatch Amazon-Protokolle	CloudWatch Amazon-Protokolle
Load Balancing	Verwenden Sie den Load AWS Balancer Controller , um nur Application Load Balancer bereitzustellen (keine Network Load Balancer)	Verwenden Sie den Load AWS Balancer Controller , um nur Application Load Balancer bereitzustellen (keine Network Load Balancer)
Secrets-Umschlagverschlüsselung	Siehe the section called "Aktivieren Sie die geheime Verschlüsselung"	Nicht unterstützt
IAM-Rollen für Servicekonten	Siehe the section called "Referenzen bei IRSA"	Nicht unterstützt
Fehlerbehebung	Siehe Fehlerbehebung	Siehe the section called "Fehlersuche bei Clustern"

Erstellen Sie lokale Amazon EKS-Cluster auf AWS Outposts für hohe Verfügbarkeit

Sie können lokale Cluster verwenden, um Ihren gesamten Amazon EKS-Cluster lokal auf AWS Outposts auszuführen. Auf diese Weise wird das Risiko von Anwendungsausfällen, die sich aus vorübergehenden Unterbrechungen der Netzwerkverbindung zur Cloud ergeben können,

minimiert. Diese Verbindungsunterbrechungen können durch Glasfaserunterbrechungen oder Wetterereignisse verursacht werden. Da der gesamte Kubernetes-Cluster lokal auf Outposts läuft, bleiben Anwendungen verfügbar. Sie können Cluster-Vorgänge während Netzwerkunterbrechungen mit der Cloud durchführen. Weitere Informationen finden Sie unter [the section called “Bereiten Sie sich auf Verbindungsabbrüche vor”](#). Das folgende Diagramm zeigt eine lokale Cluster-Bereitstellung.



Lokale Cluster sind allgemein für die Verwendung mit Outpost-Racks verfügbar.

Unterstützte Regionen AWS

Sie können lokale Cluster in den folgenden AWS Regionen erstellen: USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Nordkalifornien), USA West (Oregon), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio), Kanada (Zentral), Europa (Frankfurt), Europa (Irland), Europa (London), Naher Osten (Bahrain) und Südamerika (São Paulo). Weitere Informationen zu unterstützten Funktionen finden Sie unter [the section called “Vergleich der Optionen für die Bereitstellung”](#).

Stellen Sie einen Amazon EKS-Cluster auf AWS Outposts bereit

Dieses Thema bietet einen Überblick darüber, was beim Ausführen eines lokalen Clusters auf einem Outpost zu beachten ist. Das Thema enthält auch Anweisungen zum Bereitstellen eines lokalen Clusters auf einem Outpost.

Important

- Diese Überlegungen werden in der zugehörigen Amazon EKS-Dokumentation nicht wiedergegeben. Wenn andere Themen der Amazon-EKS-Dokumentation mit den hier aufgeführten Überlegungen in Konflikt stehen, befolgen Sie die Überlegungen hier.
- Diese Überlegungen sind freibleibend und können sich häufig ändern. Wir empfehlen Ihnen daher, dieses Thema regelmäßig zu überprüfen.
- Viele der Überlegungen unterscheiden sich von den Überlegungen zur Erstellung eines Clusters in der AWS Cloud.

- Lokale Cluster unterstützen nur Outpost-Racks. Ein einzelner lokaler Cluster kann über mehrere physische Outpost-Racks laufen, die aus einem einzigen logischen Outpost bestehen. Ein einzelner lokaler Cluster kann nicht über mehrere logische Outposts laufen. Jeder logische Outpost hat einen einzigen Outpost-ARN.
- Lokale Cluster laufen und verwalten die Kubernetes-Steuerebene in Ihrem Konto auf dem Outpost. Sie können keine Workloads auf den Kubernetes-Steuerebeneninstanzen ausführen oder die Komponenten der Kubernetes-Steuerungsebene ändern. Diese Knoten werden vom Amazon-EKS-Service verwaltet. Änderungen an der Kubernetes-Steuerungsebene bleiben nicht durch automatische Amazon EKS-Verwaltungsaktionen, wie z. B. Patches, bestehen.
- Lokale Cluster unterstützen selbstverwaltete Add-Ons und selbstverwaltete Amazon Linux-Knotengruppen. Das [Amazon VPC CNI-Plug-In für Kubernetes, Kube-Proxy](#) und [CoreDNS wird automatisch auf lokalen Clustern installiert](#).
- Lokale Cluster erfordern die Verwendung von Amazon EBS auf Outposts. In Ihrem Outpost muss Amazon EBS für den Speicher der Kubernetes-Steuerebene verfügbar sein.
- Lokale Cluster verwenden Amazon EBS auf Outposts. In Ihrem Outpost muss Amazon EBS für den Speicher der Kubernetes-Steuerebene verfügbar sein. Outposts unterstützen nur Amazon EBS gp2-Volumes.
- Von Amazon EBS unterstützte Kubernetes PersistentVolumes werden mithilfe des Amazon EBS CSI-Treibers unterstützt.
- Die Instanzen der Steuerungsebene lokaler Cluster werden in einer [gestapelten](#) Topologie mit hoher Verfügbarkeit eingerichtet. Zwei der drei Kontrollebeneninstanzen müssen jederzeit fehlerfrei sein, um das Quorum aufrechtzuerhalten. Wenn das Quorum verloren geht, wenden Sie sich an den AWS Support, da einige Aktionen auf der Serviceseite erforderlich sind, um die neuen verwalteten Instanzen zu aktivieren.

Voraussetzungen

- Vertrautheit mit den [Outposts-Bereitstellungsoptionen](#), [Auswahl von Instance-Typen und Platzierungsgruppen für Amazon EKS-Cluster auf AWS Outposts auf der Grundlage von Kapazitätsüberlegungen sowie VPC-Anforderungen und -Überlegungen](#)
- Ein vorhandener Outpost. Weitere Informationen finden Sie unter [Was sind AWS Outposts](#).
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Computer oder AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen

zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).

- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit `aws configure`](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Ein IAM-Prinzipal (Benutzer oder Rolle) mit Berechtigungen zum Erstellen (`create`) und Beschreiben (`describe`) eines Amazon-EKS-Clusters. Weitere Informationen erhalten Sie unter [the section called “Erstellen Sie einen lokalen Kubernetes-Cluster auf einem Outpost”](#) und [the section called “Auflisten oder Beschreiben aller Cluster”](#).

Wenn ein lokaler Amazon-EKS-Cluster erstellt wird, wird der [IAM-Prinzipal](#), der den Cluster erstellt, dauerhaft hinzugefügt. Der Principal wird ausdrücklich als Administrator zur Kubernetes-RBAC-Autorisierungstabelle hinzugefügt. Diese Entität hat `system:masters`-Berechtigungen. Die Identität dieser Entität ist in Ihrer Clusterkonfiguration nicht sichtbar. Daher ist es wichtig, die Entität zu notieren, die den Cluster erstellt hat, und sicherzustellen, dass Sie ihn niemals löschen. Anfänglich kann nur der Principal, der den Server erstellt hat, über ihn Aufrufe an den Kubernetes-API-Server tätigen. `kubectl` Wenn Sie die Konsole zum Erstellen des Clusters verwenden, stellen Sie sicher, dass sich dieselben IAM-Anmeldeinformationen in der AWS SDK-Anmeldeinformationskette befinden, wenn Sie `kubectl` Befehle auf Ihrem Cluster ausführen. Nachdem Ihr Cluster erstellt wurde, können Sie anderen IAM-Prinzipalen Zugriff auf Ihren Cluster gewähren.

Einen lokalen Amazon EKS-Cluster erstellen

Sie können einen lokalen Cluster mit den folgenden auf dieser Seite beschriebenen Tools erstellen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

Sie können auch die [AWS CLI](#), die [Amazon EKS-API](#), die [AWS CloudFormation](#) oder [Terraform](#) verwenden [AWS SDKs](#), um Cluster auf Outposts zu erstellen.

eksctl

Um einen lokalen Cluster zu erstellen mit **eksctl**

1. Installieren Sie Version 0.210.0 oder höher des eksctl Befehlszeilentools auf Ihrem Gerät oder AWS CloudShell. Informationen zum Installieren und Aktualisieren von eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).
2. Kopieren Sie den folgenden Inhalt auf Ihr Gerät. Ersetzen Sie die folgenden Werte und führen Sie dann den geänderten Befehl aus, um die `outpost-control-plane.yaml`-Datei zu erstellen:
 - **region-code** Ersetzen Sie es durch die [unterstützte AWS Region](#), in der Sie Ihren Cluster erstellen möchten.
 - Ersetzen Sie **my-cluster** durch Ihren Cluster-Namen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
 - Ersetzen Sie **vpc-ExampleID1** und **subnet-ExampleID1** durch die IDs Ihrer vorhandenen VPC und Ihres Subnetzes. Die VPC und das Subnetz müssen die Anforderungen unter [Erstellen einer VPC und Subnetze für Amazon EKS-Cluster](#) auf Outposts erfüllen. AWS
 - Ersetzen Sie es durch die **uniqueid** ID Ihres Outposts.
 - Ersetzen Sie **m5.large** durch einen Instance-Typ, der auf Ihrem Outpost verfügbar ist. Bevor Sie einen Instance-Typ auswählen, lesen Sie [the section called "Überlegungen zur Kapazität"](#). Drei Steuerebenen-Instances werden bereitgestellt. Du kannst diese Nummer nicht ändern.

```
cat >outpost-control-plane.yaml <<EOF
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: region-code
  version: "1.33"

vpc:
```

```
clusterEndpoints:
  privateAccess: true
id: "vpc-vpc-ExampleID1"
subnets:
  private:
    outpost-subnet-1:
      id: "subnet-subnet-ExampleID1"

outpost:
  controlPlaneOutpostARN: arn:aws:outposts:region-code:111122223333:outpost/op-uniqueid
  controlPlaneInstanceType: m5.large
EOF
```

Eine vollständige Liste aller verfügbaren Optionen und Standardeinstellungen finden Sie in der Dokumentation unter [AWS Outposts Support](#) and [Config file schema](#). `eksctl`

3. Erstellen Sie den Cluster mit der Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben. `eksctl` erstellt eine VPC und ein Subnetz auf Ihrem Outpost, in dem Sie den Cluster bereitstellen können.

```
eksctl create cluster -f outpost-control-plane.yaml
```

Die Clusterbereitstellung dauert mehrere Minuten. Während der Cluster erstellt wird, werden mehrere Ausgabezeilen angezeigt. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

Tip

Sie können die meisten Optionen, die beim Erstellen eines Clusters mit `eksctl` angegeben werden können, über den Befehl `eksctl create cluster --help` anzeigen. Verwenden Sie eine config-Datei, um alle verfügbaren Optionen anzuzeigen. Weitere Informationen finden Sie unter [Verwenden von Config-Dateien](#) und im [Config-Datei-Schema](#) in der `eksctl`-Dokumentation. Auf GitHub finden Sie [Beispiele für Config-Dateien](#).

Der `eksctl` Befehl erstellt automatisch einen [Zugriffseintrag](#) für den IAM-Prinzipal (Benutzer oder Rolle), der den Cluster erstellt hat, und erteilt dem IAM-Prinzipaladministrator Berechtigungen für Kubernetes-Objekte auf dem Cluster. Wenn Sie nicht möchten, dass der Clusterersteller Administratorzugriff auf Kubernetes-Objekte im Cluster hat, fügen Sie der vorherigen Konfigurationsdatei den folgenden Text hinzu: `bootstrapClusterCreatorAdminPermissions: false` (auf derselben Ebene wie, und). `metadata vpc outpost` Wenn Sie die Option hinzugefügt haben, müssen Sie nach der Clustererstellung einen Zugriffseintrag für mindestens einen IAM-Prinzipal erstellen, da sonst keine IAM-Prinzipale Zugriff auf Kubernetes-Objekte im Cluster haben.

AWS Management Console

Um Ihren Cluster mit dem zu erstellen AWS Management Console

1. Sie benötigen eine bestehende VPC und ein Subnetz, die die Amazon EKS-Anforderungen erfüllen. Weitere Informationen finden Sie unter [the section called "Erstellen von VPC und Subnetzen"](#).
2. Wenn Sie bereits über eine lokale Cluster-IAM-Rolle verfügen oder mit der Sie Ihren Cluster erstellen möchten `eksctl`, können Sie diesen Schritt überspringen. Standardmäßig erstellt `eksctl` eine Rolle für Sie.
 - a. Führen Sie den folgenden Befehl aus, um eine JSON-Datei für eine IAM-Vertrauensrichtlinie zu erstellen.

```
cat >eks-local-cluster-role-trust-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
```


- b. Erstellen Sie die Amazon-EKS-Cluster-IAM-Rolle. Um eine IAM-Rolle zu erstellen, muss dem [IAM-Prinzipal](#), der die Rolle erstellt, die folgende `iam:CreateRole`-Aktion (Berechtigung) zugewiesen werden.

```
aws iam create-role --role-name myAmazonEKSLocalClusterRole --assume-role-policy-document file://"eks-local-cluster-role-trust-policy.json"
```

- c. Hängen Sie die von Amazon EKS verwaltete Richtlinie mit dem Namen [Amazon EKSLocal OutpostClusterPolicy](#) an die Rolle an. Um eine IAM-Richtlinie an einen [IAM-Prinzipal](#) anzuhängen, muss der Prinzipal, der die Richtlinie anhängt, eine der folgenden IAM-Aktionen (Berechtigungen) zugewiesen werden: `iam:AttachUserPolicy` oder `iam:AttachRolePolicy`.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy --role-name myAmazonEKSLocalClusterRole
```

3. Öffnen Sie die [Amazon-EKS-Konsole](#).
4. Vergewissern Sie sich, dass Sie oben auf dem Konsolenbildschirm eine [unterstützte AWS Region](#) ausgewählt haben.
5. Wählen Sie Cluster hinzufügen und dann Erstellen aus.
6. Füllen Sie auf der Seite Configure cluster (Cluster konfigurieren) die folgenden Felder aus oder wählen Sie sie aus:
- Standort der Kubernetes-Steuerebene — Wählen Sie AWS Outposts.
 - Outpost-ID – Wählen Sie die ID des Outposts, auf dem Sie Ihre Steuerebene erstellen möchten.
 - Instance Type (Instance-Typ) – Wählen Sie einen Instance-Typ aus. Es werden nur die in Ihrem Outpost verfügbaren Instance-Typen angezeigt. In der Dropdown-Liste beschreibt jeder Instance-Typ, für wie viele Knoten der Instance-Typ empfohlen wird. Bevor Sie einen Instance-Typ auswählen, lesen Sie [the section called “Überlegungen zur Kapazität”](#). Alle Replikate werden mit demselben Instance-Typ bereitgestellt. Sie können den Instanztyp nicht ändern, nachdem Ihr Cluster erstellt wurde. Drei Steuerebenen-Instances werden bereitgestellt. Sie können diese Nummer nicht ändern.
 - Name – Ein Name für Ihren Cluster. Sie muss in Ihrem AWS Konto eindeutig sein. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Es muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des

AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.

- **Kubernetes-Version** — Wählen Sie die Kubernetes-Version aus, die Sie für Ihren Cluster verwenden möchten. Wir empfehlen, die frühere Version auszuwählen, es sei denn, Sie müssen eine ältere Version verwenden.
- **Cluster-Servicerolle** — Wählen Sie die Amazon EKS-Cluster-IAM-Rolle aus, die Sie in einem vorherigen Schritt erstellt haben, damit die Kubernetes-Steuerebene Ressourcen verwalten kann. AWS
- **Kubernetes-Cluster-Administratorzugriff** — Wenn Sie möchten, dass der IAM-Prinzipal (Rolle oder Benutzer), der den Cluster erstellt, Administratorzugriff auf die Kubernetes-Objekte im Cluster hat, akzeptieren Sie die Standardeinstellung (allow). Amazon EKS erstellt einen Zugriffseintrag für den IAM-Prinzipal und erteilt Cluster-Administratorberechtigungen für den Zugriffseintrag. Weitere Informationen zu Zugriffseinträgen finden Sie unter [the section called “Erteilen Sie Berechtigungen”](#).

Wenn Sie möchten, dass ein anderer IAM-Prinzipal als der Prinzipal, der den Cluster erstellt, Administratorzugriff auf Kubernetes-Clusterobjekte hat, wählen Sie die Option „Nicht zulassen“. Nach der Clustererstellung kann jeder IAM-Prinzipal, der über IAM-Berechtigungen zum Erstellen von Zugriffseinträgen verfügt, Zugriffseinträge für alle IAM-Prinzipale hinzufügen, die Zugriff auf Kubernetes-Clusterobjekte benötigen. Weitere Informationen zu den erforderlichen IAM-Berechtigungen finden Sie in der Service-Authorization-Referenz unter [Von Amazon Elastic Kubernetes Service definierte Aktionen](#). Wenn Sie die Option „Nicht zulassen“ wählen und keine Zugriffseinträge erstellen, haben keine IAM-Prinzipale Zugriff auf die Kubernetes-Objekte im Cluster.

- **Tags** – (Optional) Fügen Sie Ihrem Cluster beliebige Tags hinzu. Weitere Informationen finden Sie unter [the section called “Markieren Ihrer -Ressourcen”](#). Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.

7. Wählen Sie auf der Seite Specify networking (Netzwerk angeben) die Werte für die folgenden Felder aus:

- **VPC** – Wählen Sie eine vorhandene VPC aus. Die VPC muss über eine ausreichende Anzahl von IP-Adressen für den Cluster, alle Knoten und andere Kubernetes-Ressourcen, die Sie erstellen möchten, verfügen. Ihre VPC muss die Anforderungen unter [VPC-Anforderungen und Überlegungen](#) erfüllen.

- Subnetze – Standardmäßig sind alle im vorherigen Feld angegebenen Subnetze in der VPC vorausgewählt. Die von Ihnen ausgewählten Subnetze müssen die Anforderungen unter Anforderungen und Überlegungen zu [Subnetzen](#) erfüllen.
 - Security groups (Sicherheitsgruppen) – (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die Amazon EKS den erstellten Netzwerkschnittstellen zuordnen soll. Amazon EKS erstellt automatisch eine Sicherheitsgruppe, die die Kommunikation zwischen Ihrem Cluster und Ihrer VPC ermöglicht. Amazon EKS verknüpft diese Sicherheitsgruppe und alle, die Sie wählen, mit den erstellten Netzwerkschnittstellen. Weitere Informationen zu der Cluster-Sicherheitsgruppe, die Amazon EKS erstellt, finden Sie unter [the section called “Anforderungen an Sicherheitsgruppen”](#). Sie können die Regeln in der von Amazon EKS erstellten Cluster-Sicherheitsgruppe ändern. Wenn Sie Ihre eigenen Sicherheitsgruppen hinzufügen möchten, können Sie die Gruppen, die Sie nach der Clustererstellung auswählen, nicht ändern. Damit On-Premises-Hosts mit dem Cluster-Endpoint kommunizieren können, müssen Sie eingehenden Datenverkehr von der Cluster-Sicherheitsgruppe zulassen. Für Cluster, die keine eingehende und ausgehende Internetverbindung haben (auch als private Cluster bezeichnet), müssen Sie einen der folgenden Schritte ausführen:
 - Fügen Sie die Sicherheitsgruppe hinzu, die mit den erforderlichen VPC-Endpunkten verbunden ist. Weitere Informationen zu den erforderlichen Endpunkten finden Sie unter [the section called “Verwendung von -Schnittstellen-VPC-Endpunkten”](#) [Subnetzzugriff auf Dienste](#). AWS
 - Ändern Sie die Sicherheitsgruppe, die Amazon EKS erstellt hat, um Datenverkehr von der Sicherheitsgruppe zuzulassen, die den VPC-Endpunkten zugeordnet ist. Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.
8. Auf der Seite Beobachtbarkeit konfigurieren können Sie optional auswählen, welche Metriken und Optionen zur Steuerebenen-Protokollierung Sie aktivieren möchten. Standardmäßig sind alle Protokollierungstypen deaktiviert.
- Weitere Informationen zur Option Prometheus-Metriken finden Sie unter. [the section called “Schritt 1: Prometheus-Metriken aktivieren”](#)
 - Weitere Informationen zu den Optionen für die Steuerebenen-Protokollierung finden Sie unter [the section called “Protokolle der Kontrollebene”](#). Wenn Sie mit dieser Seite fertig sind, wählen Sie Weiter aus.
9. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die Informationen, die Sie auf den vorherigen Seiten eingegeben oder ausgewählt haben. Wenn Sie Änderungen vornehmen müssen, wählen Sie Edit (Bearbeiten). Wenn Sie zufrieden sind, wählen Sie Erstellen. Das Feld Status zeigt CREATING (WIRD ERSTELLT) an, während der Cluster bereitgestellt wird.

Die Clusterbereitstellung dauert mehrere Minuten.

Ihren lokalen Amazon EKS-Cluster anzeigen

1. Nachdem Ihr Cluster erstellt wurde, können Sie die erstellten Amazon EC2 Control Plane-Instances anzeigen.

```
aws ec2 describe-instances --query 'Reservations[*].Instances[*].{Name:Tags[?Key==`Name`][0].Value}' | grep my-cluster-control-plane
```

Eine Beispielausgabe sieht wie folgt aus.

```
"Name": "my-cluster-control-plane-id1"  
"Name": "my-cluster-control-plane-id2"  
"Name": "my-cluster-control-plane-id3"
```

Jede Instance ist mit `node-role.eks-local.amazonaws.com/control-plane` gekennzeichnet, sodass auf den Instances der Steuerebene keine Workloads geplant werden. Weitere Informationen zu Taints finden Sie unter [Taints and Tolerations](#) in der Kubernetes-Dokumentation. Amazon EKS überwacht kontinuierlich den Status lokaler Cluster. Wir führen automatische Verwaltungsaktionen durch, z. B. Sicherheits-Patches und das Reparieren fehlerhafter Instances. Wenn lokale Cluster von der Cloud getrennt werden, führen wir Aktionen durch, um sicherzustellen, dass der Cluster bei der erneuten Verbindung wieder in einen fehlerfreien Zustand versetzt wird.

2. Wenn Sie Ihren Cluster mit `eksctl` erstellt haben, können Sie diesen Schritt überspringen. `eksctl` schließt diesen Schritt für Sie ab. Aktivieren Sie `kubectl`, um mit Ihrem Cluster zu kommunizieren, indem Sie einen neuen Kontext zur Datei `kubectl config` hinzufügen. Anweisungen zum Erstellen und Aktualisieren der Datei finden Sie unter [the section called “Greifen Sie mit kubectl auf den Cluster zu”](#).

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

Eine Beispielausgabe sieht wie folgt aus.

```
Added new context arn:aws:eks:region-code:111122223333:cluster/my-cluster to /home/  
username/.kube/config
```

3. Um eine Verbindung zum Kubernetes-API-Server Ihres lokalen Clusters herzustellen, haben Sie Zugriff auf das lokale Gateway für das Subnetz oder stellen Sie von der VPC aus eine Verbindung her. Weitere Informationen zum Verbinden eines Outpost-Racks mit Ihrem lokalen Netzwerk finden Sie unter [So funktionieren lokale Gateways für Racks](#) im AWS Outposts-Benutzerhandbuch. Wenn Sie Direct VPC Routing verwenden und das Outpost-Subnetz über eine Route zu Ihrem lokalen Gateway verfügt, werden die privaten IP-Adressen der Kubernetes-Steuerebeneninstanzen automatisch über Ihr lokales Netzwerk übertragen. Der Kubernetes-API-Serverendpunkt des lokalen Clusters wird in Amazon Route 53 (Route 53) gehostet. Der API-Service-Endpunkt kann von öffentlichen DNS-Servern in die privaten IP-Adressen der Kubernetes API-Server aufgelöst werden.

Die Kubernetes-Steuerungsinstanzen der lokalen Cluster sind mit statischen elastischen Netzwerkschnittstellen mit festen privaten IP-Adressen konfiguriert, die sich während des Cluster-Lebenszyklus nicht ändern. Maschinen, die mit dem Kubernetes-API-Server interagieren, haben während Netzwerkunterbrechungen möglicherweise keine Konnektivität zu Route 53. In diesem Fall empfehlen wir, `/etc/hosts` mit den statischen privaten IP-Adressen für den weiteren Betrieb zu konfigurieren. Wir empfehlen außerdem, lokale DNS-Server einzurichten und diese mit Ihrem Outpost zu verbinden. Weitere Informationen finden Sie in der [AWS Outposts-Dokumentation](#). Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Kommunikation mit Ihrem Cluster hergestellt wurde.

```
kubectl get svc
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	28h

4. (Optional) Testen Sie die Authentifizierung für Ihren lokalen Cluster, wenn dieser nicht mit der AWS Cloud verbunden ist. Detaillierte Anweisungen finden Sie unter [the section called “Bereiten Sie sich auf Verbindungsabbrüche vor”](#).

Interne Ressourcen

Amazon EKS erstellt die folgenden Ressourcen in Ihrem Cluster. Die Ressourcen sind für den internen Gebrauch von Amazon EKS bestimmt. Damit Ihr Cluster ordnungsgemäß funktioniert, sollten Sie diese Ressourcen nicht bearbeiten oder modifizieren.

- Die folgenden [Mirror-Pods](#):
 - aws-iam-authenticator-*node-hostname*
 - eks-certificates-controller-*node-hostname*
 - etcd-*node-hostname*
 - kube-apiserver-*node-hostname*
 - kube-controller-manager-*node-hostname*
 - kube-scheduler-*node-hostname*
- Die folgenden selbstverwalteten Add-Ons:
 - kube-system/coredns
 - kube-system/kube-proxy (wird erst erstellt, wenn Sie Ihren ersten Knoten hinzugefügt haben)
 - kube-system/aws-node (wird erst erstellt, wenn Sie Ihren ersten Knoten hinzugefügt haben). Lokale Cluster verwenden das Amazon VPC CNI-Plug-In für Kubernetes für Cluster-Netzwerke. Ändern Sie nicht die Konfiguration für Steuerebene-Instances (Pods mit dem Namen aws-node-controlplane-*). Es gibt Konfigurationsvariablen, die Sie verwenden können, um den Standardwert zu ändern, wenn das Plugin neue Netzwerkschnittstellen erstellt. [Weitere Informationen finden Sie in der Dokumentation zu.](#) [GitHub](#)
- Die folgenden Services:
 - default/kubernetes
 - kube-system/kube-dns
- Eine PodSecurityPolicy namens eks.system
- Eine ClusterRole namens eks:system:podsecuritypolicy
- Eine ClusterRoleBinding namens eks:system
- Zusätzlich zur [Cluster-Sicherheitsgruppe](#) erstellt Amazon EKS in Ihrem AWS Konto eine Sicherheitsgruppe mit dem Namen eks-local-internal-do-not-use-or-edit-*cluster-name-uniqueid*. Diese Sicherheitsgruppe ermöglicht den ungehinderten Datenfluss zwischen Kubernetes-Komponenten, die auf den Instances der Kontrollebene ausgeführt werden.

Empfohlene nächste Schritte:

- [Erteilen Sie dem IAM-Prinzipal, der den Cluster erstellt hat, die erforderlichen Berechtigungen zum Anzeigen von Kubernetes-Ressourcen in AWS Management Console](#)

- [Gewähren Sie IAM-Entitäten Zugriff auf Ihren Cluster](#). Wenn Sie möchten, dass die Entitäten Kubernetes-Ressourcen in der Amazon EKS-Konsole anzeigen, gewähren Sie den Entitäten die [erforderlichen Berechtigungen](#).
- [Konfigurieren Sie die Protokollierung für Ihren Cluster](#)
- Machen Sie sich mit dem vertraut, was während [Netzwerktrennungen](#) passiert.
- [Fügen Sie Knoten zu Ihrem Cluster hinzu](#)
- Erwägen Sie, einen Backup-Plan für Ihr etcd zu erstellen. Amazon EKS unterstützt keine automatische Sicherung und Wiederherstellung etcd für lokale Cluster. Weitere Informationen finden Sie unter [Sichern eines etcd-Clusters](#) in der Kubernetes-Dokumentation. Die beiden Hauptoptionen sind die Verwendung von etcdctl zur Automatisierung der Erstellung von Snapshots oder die Verwendung der Amazon-EBS-Speicher-Volume-Sicherung.

Erfahren Sie mehr über die Plattformversionen von Kubernetes und Amazon EKS für Outposts AWS

Lokale Clusterplattformversionen stellen die Funktionen des Amazon EKS-Clusters auf AWS Outposts dar. Die Versionen enthalten die Komponenten, die auf der Kubernetes-Steuerebene ausgeführt werden, wobei die Kubernetes-API-Serverflugs aktiviert sind. Sie enthalten auch die aktuelle Kubernetes-Patch-Version. Jede Kubernetes-Minor-Version hat eine oder mehrere zugehörige -Plattformversionen. Die Plattformversionen für verschiedene Kubernetes-Minor-Versionen sind voneinander unabhängig. Die Plattformversionen für lokale Cluster und Amazon-EKS-Cluster in der Cloud sind unabhängig.

Wenn eine neue Kubernetes-Nebenversion für lokale Cluster verfügbar ist, z. B. 1.31 beginnt die erste Plattformversion für diese Kubernetes-Nebenversion bei `eks-local-outposts.1`. Allerdings veröffentlicht Amazon EKS regelmäßig neue Plattformversionen, um neue Einstellungen für die Kubernetes-Steuerebene und Sicherheitsfixes bereitzustellen.

Wenn neue lokale Cluster-Plattformversionen für eine Minor-Version verfügbar werden:

- Die Versionsnummer der -Plattform wird erhöht (`eks-local-outposts.n+1`).
- Amazon EKS aktualisiert automatisch alle vorhandenen lokalen Cluster auf die neueste Plattformversion für die entsprechende Kubernetes-Nebenversion. Automatische Aktualisierungen bestehender Plattformversionen werden schrittweise durchgeführt. Der Rollout-Prozess besteht darin, die verwalteten Kubernetes-Steuerungsinstanzen, die auf dem Outpost ausgeführt werden, nacheinander zu ersetzen, bis alle 3 Instances durch neue ersetzt wurden.

- Der Austausch der Instanz auf der Kubernetes-Steuerebene wird eingestellt, wenn das Risiko einer Serviceunterbrechung besteht. Amazon EKS versucht nur dann, eine Instance zu ersetzen, wenn die anderen 2 Kubernetes-Steuerplane-Instances fehlerfrei sind und alle Bereitschaftsbedingungen als Clusterknoten erfüllen.
- Der Rollout einer Plattformversion dauert in der Regel weniger als 30 Minuten. Wenn ein Cluster über einen längeren Zeitraum im UPDATING Status verbleibt, wenden Sie sich an den Support [the section called “Fehlersuche bei Clustern”](#) und wenden Sie sich an den AWS Support. Beenden Sie Kubernetes-Steuerungsinstanzen niemals manuell, es sei denn, Sie werden vom Support dazu aufgefordert. AWS
- Amazon EKS veröffentlicht möglicherweise ein neues Knoten-AMI mit einer entsprechenden Patch-Version. Alle Patch-Versionen sind zwischen der Kubernetes-Steuerebene und dem Knoten AMIs für eine einzelne Kubernetes-Nebenversion kompatibel.

Neue Plattformversionen führen nicht zu grundlegenden Änderungen oder Betriebsunterbrechungen.

Lokale Cluster werden immer mit der neuesten verfügbaren Plattformversion (`eks-local-outposts.n`) für die angegebene Kubernetes-Version erstellt.

Die aktuellen und kürzlichen -Plattformversionen sind in den folgenden Tabellen beschrieben.

Um Benachrichtigungen über alle Änderungen an der Quelldatei auf dieser speziellen Dokumentationsseite zu erhalten, können Sie die folgende URL mit einem RSS-Reader abonnieren:

<https://github.com/awsdocs/amazon-eks-user-guide/commits/mainline/latest/ug/outposts/eks-outposts-platform-versions.adoc.atom>

Kubernetes-Version 1.31

Die folgenden Zugangscontroller sind für alle 1.31 Plattformversionen

aktiviert: `CertificateApproval`, `CertificateSigning`, `CertificateSubjectRestriction`, `ClusterDefaultIngressClass`, `DefaultStorageClass`, `DefaultTolerationSeconds`, `ExtendedResourceT` und `ValidatingAdmissionWebhook`.

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.31.6	<code>eks-local-outposts.1</code>	Erste Veröffentlichung der Kubernetes-	9. April 2025

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
		Version v1.31 für lokale Amazon EKS-Cluster auf Outposts.	

Kubernetes-Version **1.30**

Die folgenden Zugangscontroller sind für alle 1.30 Plattformversionen aktiviert:CertificateApproval,,CertificateSigning,CertificateSubjectRestriction,ClusterAccessReview,ValidatingAdmissionWebhook.

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.30.10	eks-local-outposts.3	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.30.10 AWS IAM Authenticator wurde aktualisiert auf. v0.6.29 Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.2. CoreDNS wurde aktualisiert auf. v1.11.4 AWS Cloud Controller Manager wurde aktualisiert auf. v1.30.8 Die Bottlerocket-Version	27. März 2025

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
		wurde aktualisiert auf. v1.34.0	
1.30.7	eks-local-outposts.2	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.30.7 AWS IAM Authenticator wurde aktualisiert auf. v0.6.28 Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.0. Die Bottlerocket-Version wurde aktualisiert auf. v1.29.0	10. Januar 2025
1.30.5	eks-local-outposts.1	Erste Veröffentlichung der Kubernetes-Version v1.30 für lokale Amazon EKS-Cluster auf Outposts.	13. November 2024

Kubernetes-Version 1.29

Die folgenden Zugangscontroller sind für alle 1.29 Plattformversionen aktiviert:CertificateApproval,CertificateSigning,CertificateSubjectRestriction,ClusterServiceAccount StorageObjectInUseProtectionTaintNodesByCondition, ValidatingAdmissionPolicy und. ValidatingAdmissionWebhook

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
v1.29.14	eks-local-outposts.6	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.29.14 Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.2. CoreDNS wurde aktualisiert auf. v1.11.4 AWS Cloud Controller Manager wurde aktualisiert auf. v1.29.8 Die Bottlerocket-Version wurde aktualisiert auf. v1.34.0	27. März 2025
v1.29.11	eks-local-outposts.5	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.29.11 Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.0. Das CoreDNS-Image wurde aktualisiert auf. v1.11.3 Die Bottlerocket-Version	10. Januar 2025

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.29.9	eks-local-outposts.4	wurde aktualisiert auf. v1.29.0 Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.29.9 AWS IAM Authenticator wurde aktualisiert auf. v0.6.26 Die Bottlerocket-Version wurde aktualisiert auf. v1.26.0	8. November 2024
1.29.6	eks-local-outposts.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Bottlerocket-Version wurde aktualisiert auf. v1.22.0	22. Oktober 2024
1.29.6	eks-local-outposts.2	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Bottlerocket-Version wurde aktualisiert auf. v1.21.0	27. August 2024
1.29.6	eks-local-outposts.1	Erste Veröffentlichung der Kubernetes-Version v1.29 für lokale Amazon EKS-Cluster auf Outposts.	20. August 2024

Kubernetes-Version 1.28

Die folgenden Zugangscontroller sind für alle 1.28 Plattformversionen aktiviert:CertificateApproval,CertificateSigning,CertificateSubjectRestriction,ClusterServiceAccount StorageObjectInUseProtectionTaintNodesByCondition, ValidatingAdmissionPolicy und. ValidatingAdmissionWebhook

Kubernetes Version	Amazon-EKS-Platfformversion	Versionshinweise	Datum der Veröffentlichung
1.28.15	eks-local-outposts.13	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Der v1.28.15 Kube-Proxy-Build wurde aktualisiert. Das Amazon VPC CNI-Plugin für Kubernetes wurde aktualisiert auf. v1.19.0 AWS Cloud Controller Manager wurde aktualisiert auf. v1.28.11	27. März 2025
1.28.15	eks-local-outposts.12	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.28.15 Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.0. Die Bottlerocket-Version wurde aktualisiert auf. v1.29.0	10. Januar 2025

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.28.14	eks-local-outposts.11	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.28.14 AWS IAM Authenticator wurde aktualisiert auf. v0.6.26 Das CoreDNS-Image wurde aktualisiert auf. v1.11.1 Die Bottlerocket-Version wurde aktualisiert auf. v1.26.0	8. November 2024
1.28.10	eks-local-outposts.10	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Bottlerocket-Version wurde aktualisiert auf. v1.22.0	22. Oktober 2024
1.28.10	eks-local-outposts.9	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Bottlerocket-Version wurde aktualisiert auf. v1.21.0	27. August 2024
1.28.10	eks-local-outposts.8	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Juli 2024

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.28.10	eks-local-outposts.6	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.28.10 AWS IAM Authenticator wurde aktualisiert auf. v0.6.20 Die Bottlerocket-Version wurde aktualisiert auf. v1.20.2	19. Juni 2024
1.28.6	eks-local-outposts.5	Die Bottlerocket-Version wurde auf v1.19.3 aktualisiert und enthält die neuesten Bugfixes zur Unterstützung des lokalen Boots in Outposts.	18. April 2024
1.28.6	eks-local-outposts.4	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Unterstützung oder der lokale Start in Outposts wurde wiederhergestellt. Die Bottlerocket-Version wurde aus Kompatibilitätsgründen auf heruntergestuft. v1.15.1	2. April 2024

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.28.6	eks-local-outposts.3	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	22. März 2024
1.28.6	eks-local-outposts.2	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.28.6 AWS IAM Authenticator wurde aktualisiert auf. v0.6.17 Das Amazon VPC CNI-Plugin für Kubernetes wurde aus Kompatibilitätsgründen auf herabgestuft. v1.13.2 Die v1.19.2 Bottlerocket-Version wurde aktualisiert auf.	8. März 2024
1.28.1	eks-local-outposts.1	Erste Veröffentlichung der Kubernetes-Version v1.28 für lokale Amazon EKS-Cluster auf Outposts.	04. Oktober 2023

Kubernetes-Version **1.27**

Die folgenden Zugangscontroller sind für alle 1.27 Plattformversionen aktiviert:CertificateApproval,CertificateSigning,CertificateSubjectRestriction,Cluster

ServiceAccount StorageObjectInUseProtectionTaintNodesByCondition, ValidatingAdmissionPolicy und. ValidatingAdmissionWebhook

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.27.16	eks-local-outposts.13	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.2. Bottlerocket-Version aktualisiert auf. v1.34.0	27. März 2025
1.27.16	eks-local-outposts.12	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.19.0. Die Bottlerocket-Version wurde aktualisiert auf. v1.29.0	10. Januar 2025
1.27.16	eks-local-outposts.11	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.27.16 AWS IAM Authenticator wurde aktualisiert auf. v0.6.26 Das	8. November 2024

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
		CoreDNS-Image wurde aktualisiert auf. v1.11.1 Die Bottlerocket-Version wurde aktualisiert auf. v1.26.0	
1.27.14	eks-local-outposts.10	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Bottlerocket-Version wurde aktualisiert auf. v1.22.0	22. Oktober 2024
1.27.14	eks-local-outposts.9	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Die Bottlerocket-Version wurde aktualisiert auf. v1.21.0	27. August 2024
1.27.14	eks-local-outposts.8	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	30. Juli 2024

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.27.14	eks-local-outposts.6	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.27.14 AWS IAM Authenticator wurde aktualisiert auf. v0.6.20 Die Bottlerocket-Version wurde aktualisiert auf. v1.20.2	19. Juni 2024
1.27.10	eks-local-outposts.5	Neue Plattformversion mit Sicherheitsfixes und -verbesserungen.	2. April 2024
1.27.10	eks-local-outposts.4	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy wurde aktualisiert auf. v1.27.10 AWS IAM Authenticator wurde aktualisiert auf. v0.6.17 Die Bottlerocket-Version wurde aktualisiert auf. v1.19.2	22. März 2024

Kubernetes Version	Amazon-EKS-Plattformversion	Versionshinweise	Datum der Veröffentlichung
1.27.3	eks-local-outposts.3	Neue Plattformversion mit Sicherheitskorrekturen und Verbesserungen. Kube-Proxy aktualisiert auf. v1.27.3 Amazon-VPC-CNI-Plugin für Kubernetes aktualisiert zu v1.13.2.	14. Juli 2023
1.27.1	eks-local-outposts.2	Das CoreDNS-Image wurde aktualisiert auf. v1.10.1	22. Juni 2023
1.27.1	eks-local-outposts.1	Erste Veröffentlichung der Kubernetes-Version 1.27 für lokale Amazon EKS-Cluster auf Outposts.	30. Mai 2023

Erstellen Sie eine VPC und Subnetze für Amazon EKS-Cluster auf Outposts AWS

Wenn Sie einen lokalen Cluster erstellen, geben Sie eine VPC und mindestens ein privates Subnetz an, das auf Outposts ausgeführt wird. Dieses Thema bietet einen Überblick über die VPC- und Subnetzanforderungen und -überlegungen für Ihren lokalen Cluster.

VPC-Anforderungen und -Überlegungen

Wenn Sie einen lokalen Cluster erstellen, muss die von Ihnen angegebene VPC die folgenden Anforderungen und Überlegungen erfüllen:

- Stellen Sie sicher, dass die VPC über genügend IP-Adressen für den lokalen Cluster, alle Knoten und andere Kubernetes-Ressourcen verfügt, die Sie erstellen möchten. Wenn die VPC, die Sie

verwenden möchten, nicht über genügend IP-Adressen verfügt, erhöhen Sie die Anzahl der verfügbaren IP-Adressen. Das ist möglich, indem Sie [zusätzliche CIDR-Blöcke \(Classless Inter-Domain Routing\) mit Ihrer VPC verbinden](#). Sie können entweder vor oder nach der Erstellung Ihres Clusters private (RFC 1918) und öffentliche (nicht RFC 1918) CIDR-Blöcke mit Ihrer VPC verbinden. Es kann bis zu 5 Stunden dauern, bis ein CIDR-Block, den Sie einem VPC zugeordnet haben, von einem Cluster erkannt wird.

- Der VPC kann keine IP-Präfixe oder IPv6 CIDR-Blöcke zugewiesen haben. Aufgrund dieser Einschränkungen gelten die Informationen, die unter [Zuweisen von mehr IP-Adressen zu Amazon EKS-Knoten mit Präfixen](#) behandelt werden, [the section called “IPv6”](#) nicht für Ihre VPC.
- Die VPC verfügt über einen DNS-Hostnamen und die DNS-Auflösung ist aktiviert. Ohne diese Funktionen kann der lokale Cluster nicht erstellt werden, und Sie müssen die Funktionen aktivieren und Ihren Cluster neu erstellen. Weitere Informationen finden Sie unter [DNS-Attribute für Ihre VPC](#) im Amazon-VPC-Benutzerhandbuch.
- Um über Ihr lokales Netzwerk auf Ihren lokalen Cluster zuzugreifen, muss die VPC mit der lokalen Gateway-Routing-Tabelle Ihres Outpost verknüpft sein. Weitere Informationen finden Sie unter [VPC-Verknüpfungen](#) im AWS Outposts-Benutzerhandbuch.

Subnetz-Anforderungen und -Überlegungen

Geben Sie beim Erstellen des Clusters mindestens ein privates Subnetz an. Wenn Sie mehr als ein Subnetz angeben, werden die Instanzen der Kubernetes-Steuerebene gleichmäßig auf die Subnetze verteilt. Wenn mehr als ein Subnetz angegeben wird, müssen die Subnetze auf demselben Outpost vorhanden sein. Darüber hinaus müssen die Subnetze auch über die richtigen Routen und Sicherheitsgruppen-Berechtigungen verfügen, um miteinander kommunizieren zu können. Wenn Sie einen lokalen Cluster erstellen, müssen die von Ihnen angegebenen Subnetze die folgenden Anforderungen erfüllen:

- Die Subnetze befinden sich alle auf demselben logischen Outpost.
- Die Subnetze zusammen haben mindestens drei verfügbare IP-Adressen für die Kubernetes-Steuerebeneninstanzen. Wenn drei Subnetze angegeben werden, muss jedes Subnetz über mindestens eine verfügbare IP-Adresse verfügen. Wenn zwei Subnetze angegeben werden, muss jedes Subnetz über mindestens zwei verfügbare IP-Adressen verfügen. Wenn ein Subnetz angegeben wird, muss das Subnetz über mindestens drei verfügbare IP-Adressen verfügen.
- Die Subnetze haben eine Route zum [lokalen Gateway des Outpost-Racks, um über Ihr lokales Netzwerk](#) auf den Kubernetes-API-Server zuzugreifen. Wenn die Subnetze keine Route zum

lokalen Gateway des Outpost-Racks haben, müssen Sie von der VPC aus mit Ihrem Kubernetes-API-Server kommunizieren.

- Die Subnetze müssen eine IP-Adressen-basierte Benennung aufweisen. Die EC2 [ressourcenbasierte Benennung](#) von Amazon wird von Amazon EKS nicht unterstützt.

Subnetzzugriff auf Dienste AWS

Die privaten Subnetze des lokalen Clusters auf Outposts müssen in der Lage sein, mit regionalen AWS Diensten zu kommunizieren. Dazu können Sie ein [NAT-Gateway](#) für den ausgehenden Internetzugang verwenden oder, wenn Sie den gesamten Datenverkehr innerhalb Ihrer VPC privat halten möchten, [Schnittstellen-VPC-Endpunkte](#) verwenden.

Verwenden eines NAT-Gateways

Den privaten Subnetzen des lokalen Clusters auf Outposts muss eine Routing-Tabelle zugeordnet sein, die eine Route zu einem NAT-Gateway in einem öffentlichen Subnetz enthält, das sich in der übergeordneten Availability Zone des Outposts befindet. Das öffentliche Subnetz muss über eine Route zu einem [Internet-Gateway](#) verfügen. Das NAT-Gateway ermöglicht einen ausgehenden Zugriff auf das Internet und verhindert unerwünschte eingehende Verbindungen aus dem Internet zu Instances im Outpost.

Verwendung von -Schnittstellen-VPC-Endpunkten

Wenn die privaten Subnetze des lokalen Clusters auf Outposts keine ausgehende Internetverbindung haben oder wenn Sie den gesamten Datenverkehr innerhalb Ihrer VPC privat halten möchten, müssen Sie die folgenden Schnittstellen-VPC-Endpunkte und den [Gateway-Endpunkt](#) in einem regionalen Subnetz erstellen, bevor Sie Ihren Cluster erstellen.

Endpunkt	Endpunkttyp
<code>com.amazonaws. <i>region-code</i> .ssm</code>	Schnittstelle
<code>com.amazonaws. <i>region-code</i> .ssmmessages</code>	Schnittstelle
<code>com.amazonaws. <i>region-code</i> .ec2messages</code>	Schnittstelle
<code>com.amazonaws. <i>region-code</i> .ec2</code>	Schnittstelle

Endpunkt	Endpunkttyp
<code>com.amazonaws.<i>region-code</i>.secretsmanager</code>	Schnittstelle
<code>com.amazonaws.<i>region-code</i>.logs</code>	Schnittstelle
<code>com.amazonaws.<i>region-code</i>.sts</code>	Schnittstelle
<code>com.amazonaws.<i>region-code</i>.ecr.api</code>	Schnittstelle
<code>com.amazonaws.<i>region-code</i>.ecr.dkr</code>	Schnittstelle
<code>com.amazonaws.<i>region-code</i>.s3</code>	Gateway

Die Endpunkte müssen die folgenden Anforderungen erfüllen:

- Wird in einem privaten Subnetz erstellt, das sich in der übergeordneten Availability Zone Ihres Outposts befindet
- Private DNS-Namen müssen aktiviert sein.
- Sie müssen über eine angefügte Sicherheitsgruppe verfügen, die eingehenden HTTPS-Datenverkehr aus dem CIDR-Bereich des privaten Outpost-Subnetzes zulässt.

Für die Erstellung von Endpunkten fallen Gebühren an. Weitere Informationen finden Sie unter [AWS PrivateLink Preise](#). Wenn Ihre Pods Zugriff auf andere AWS Dienste benötigen, müssen Sie zusätzliche Endpunkte einrichten. Eine umfassende Liste der Endpunkte finden Sie unter [AWS Dienste, die sich in integrieren lassen](#). AWS PrivateLink

Erstellen einer VPC

Mit einer der folgenden AWS CloudFormation Vorlagen können Sie eine VPC erstellen, die die vorherigen Anforderungen erfüllt:

- [Vorlage 1](#) — Diese Vorlage erstellt eine VPC mit einem privaten Subnetz im Outpost und einem öffentlichen Subnetz in der Region. AWS Das private Subnetz hat eine Route zu einem Internet über ein NAT-Gateway, das sich im öffentlichen Subnetz der Region befindet. AWS Diese Vorlage kann verwendet werden, um einen lokalen Cluster in einem Subnetz mit ausgehendem Internetzugriff zu erstellen.

- [Vorlage 2](#) — Diese Vorlage erstellt eine VPC mit einem privaten Subnetz auf dem Outpost und der Mindestanzahl an VPC-Endpunkten, die erforderlich sind, um einen lokalen Cluster in einem Subnetz zu erstellen, das keinen Eingangs- oder Ausgangs-Internetzugang hat (auch als privates Subnetz bezeichnet).

Bereiten Sie lokale Amazon EKS-Cluster auf AWS Outposts für Netzwerkunterbrechungen vor

Wenn Ihr lokales Netzwerk die Konnektivität mit der AWS Cloud verloren hat, können Sie Ihren lokalen Amazon EKS-Cluster weiterhin auf einem Outpost verwenden. In diesem Thema wird beschrieben, wie Sie Ihren lokalen Cluster auf Netzwerkunterbrechungen vorbereiten können, und verwandte Überlegungen.

- Lokale Cluster sorgen für Stabilität und unterbrechungsfreien Betrieb bei vorübergehenden, ungeplanten Netzwerkunterbrechungen. AWS Outposts bleibt ein vollständig vernetztes Angebot, das als Erweiterung der AWS Cloud in Ihrem Rechenzentrum fungiert. Im Falle von Netzwerkunterbrechungen zwischen Ihrem Outpost und der AWS Cloud empfehlen wir, zu versuchen, Ihre Verbindung wiederherzustellen. Eine Anleitung finden Sie in der [Checkliste zur Fehlerbehebung im AWS Outposts-Rack-Netzwerk](#) im AWS Outposts-Benutzerhandbuch. Weitere Informationen zum Beheben von Problemen mit lokalen Clustern finden Sie unter [the section called “Fehlersuche bei Clustern”](#).
- Outposts geben eine ConnectedStatus-Metrik aus, mit der Sie den Konnektivitätsstatus Ihres Outposts überwachen können. Weitere Informationen finden Sie unter [Outposts-Metriken](#) im AWS Outposts-Benutzerhandbuch.
- Lokale Cluster verwenden IAM als Standardauthentifizierungsmechanismus mithilfe des [AWS Identity and Access Management-Authentifikators für](#) Kubernetes. IAM ist bei Netzwerkunterbrechungen nicht verfügbar. Daher unterstützen lokale Cluster einen alternativen Authentifizierungsmechanismus mithilfe von x.509-Zertifikaten, die Sie verwenden können, um eine Verbindung zu Ihrem Cluster herzustellen, wenn die Netzwerkverbindung unterbrochen ist. Informationen zum Abrufen und Verwenden eines x.509-Zertifikats für Ihren Cluster finden Sie unter [the section called “Authentifizierung bei Ihrem lokalen Cluster während einer Netzwerkunterbrechung”](#).
- Wenn Sie bei Netzwerkunterbrechungen nicht auf Route 53 zugreifen können, sollten Sie die Verwendung lokaler DNS-Server in Ihrer lokalen Umgebung in Betracht ziehen. Die Instanzen der Kubernetes-Steuerebene verwenden statische IP-Adressen. Sie können die Hosts, die Sie für die Verbindung mit Ihrem Cluster verwenden, mit dem Hostnamen und den IP-Adressen

des Endpunkts als Alternative zur Verwendung lokaler DNS-Server konfigurieren. Weitere Informationen finden Sie unter [DNS](#) im AWS Outposts-Benutzerhandbuch.

- Wenn Sie bei Netzwerkunterbrechungen mit einem Anstieg des Anwendungsdatenverkehrs rechnen, können Sie in Ihrem Cluster bei Verbindung mit der Cloud freie Rechenkapazität bereitstellen. EC2 Amazon-Instances sind im Preis von AWS Outposts enthalten. Das Ausführen von Ersatz-Instances wirkt sich also nicht auf Ihre AWS Nutzungskosten aus.
- Während Netzwerkunterbrechungen, die das Erstellen, Aktualisieren und Skalieren von Workloads ermöglichen, müssen die Container-Images Ihrer Anwendung über das lokale Netzwerk zugänglich sein und Ihr Cluster muss über genügend Kapazität verfügen. Lokale Cluster hosten keine Container-Registry für Sie. Wenn die Pods zuvor auf diesen Knoten ausgeführt wurden, werden Container-Images auf den Knoten zwischengespeichert. Wenn Sie die Container-Images Ihrer Anwendung in der Regel aus Amazon ECR in der Cloud beziehen, sollten Sie erwägen, einen lokalen Cache oder eine lokale Registry auszuführen. Ein lokaler Cache oder eine lokale Registry ist hilfreich, wenn Sie während einer Netzwerkunterbrechung Workload-Ressourcen erstellen, aktualisieren und skalieren müssen.
- Lokale Cluster verwenden Amazon EBS als Standardspeicherklasse für persistente Volumes und den Amazon-EBS-CSI-Treiber, um den Lebenszyklus persistenter Amazon-EBS-Volumes zu verwalten. Bei Netzwerkunterbrechungen können Pods, die von Amazon EBS unterstützt werden, nicht erstellt, aktualisiert oder skaliert werden. Dies liegt daran, dass diese Vorgänge Aufrufe an die Amazon-EBS-API in der Cloud erfordern. Wenn Sie statusbehaftete Workloads auf lokalen Clustern bereitstellen und während Netzwerkunterbrechungen Erstellungs-, Aktualisierungs- oder Skalierungsvorgänge benötigen, sollten Sie die Verwendung eines alternativen Speichermechanismus in Betracht ziehen.
- Amazon EBS-Snapshots können nicht erstellt oder gelöscht werden, wenn AWS Outposts nicht auf die entsprechende AWS Region zugreifen können APIs (z. B. APIs für Amazon EBS oder Amazon S3).
- Bei der Integration von ALB (Ingress) mit AWS Certificate Manager (ACM) werden Zertifikate übertragen und im Speicher der AWS Outposts ALB Compute-Instanz gespeichert. Die aktuelle TLS-Terminierung funktioniert weiterhin, falls die Verbindung zur Region getrennt wird. AWS Mutationsvorgänge in diesem Kontext schlagen fehl (z. B. neue Eingangsdefinitionen, neue API-Vorgänge für ACM-basierte Zertifikate, ALB-Rechenskalierung oder Zertifikatsrotation). Weitere Informationen finden Sie unter [Problembehandlung bei der verwalteten Zertifikatserneuerung](#) im AWS Certificate Manager Manager-Benutzerhandbuch.
- Die Protokolle der Amazon EKS-Kontrollebene werden bei Netzwerkunterbrechungen lokal auf den Kubernetes-Steuerebenen-Instances zwischengespeichert. Bei der erneuten Verbindung werden

die Protokolle an Logs in der übergeordneten Region CloudWatch gesendet. AWS Sie können die Partnerlösungen von [Prometheus](#), [Grafana](#) oder Amazon EKS verwenden, um den Cluster lokal mithilfe des Metriken-Endpunkts des Kubernetes-API-Servers oder Fluent Bit für Protokolle zu überwachen.

- Wenn Sie den Load AWS Balancer Controller auf Outposts für Anwendungsdatenverkehr verwenden, empfangen bestehende Pods, denen der Load AWS Balancer Controller vorangestellt ist, auch während Netzwerkunterbrechungen weiterhin Datenverkehr. Neue Pods, die bei Netzwerkunterbrechungen erstellt werden, empfangen erst dann Traffic, wenn der Outpost wieder mit der Cloud verbunden ist. AWS Erwägen Sie, die Anzahl der Replikate für Ihre Anwendungen festzulegen, während Sie mit der AWS Cloud verbunden sind, um Ihren Skalierungsanforderungen bei Netzwerkunterbrechungen gerecht zu werden.
- [Das Amazon VPC CNI-Plugin für Kubernetes verwendet standardmäßig den sekundären IP-Modus](#). Es ist mit `WARM_ENI_TARGET = 1` konfiguriert, was es dem Plugin ermöglicht, „eine vollständige elastic network interface“ mit verfügbaren IP-Adressen verfügbar zu halten. Erwägen Sie, `WARM_ENI_TARGET`-, `WARM_IP_TARGET`- und `MINIMUM_IP_TARGET`-Werte entsprechend Ihren Skalierungsanforderungen während eines getrennten Zustands zu ändern. Weitere Informationen finden Sie in der [Readme-Datei](#) für das Plugin unter GitHub. Eine Liste der maximalen Anzahl von Pods, die von den einzelnen Instanztypen unterstützt werden, finden Sie in der [eni-max-pods.txt-Datei](#) unter. GitHub

Authentifizierung bei Ihrem lokalen Cluster während einer Netzwerkunterbrechung

AWS Identity and Access Management (IAM) ist bei Netzwerkunterbrechungen nicht verfügbar. Sie können sich nicht mit IAM-Anmeldeinformationen bei Ihrem lokalen Cluster authentifizieren, wenn die Verbindung unterbrochen ist. Sie können jedoch über Ihr lokales Netzwerk mithilfe von x509-Zertifikaten eine Verbindung zu Ihrem Cluster herstellen, wenn die Verbindung getrennt ist. Sie müssen ein Client X509-Zertifikat herunterladen und speichern, das Sie während der Verbindungstrennung verwenden können. In diesem Thema erfahren Sie, wie Sie das Zertifikat erstellen und verwenden, um sich bei Ihrem Cluster zu authentifizieren, wenn dieser getrennt ist.

1. Erstellen einer Zertifikatssignierungsanforderung

- a. Generieren einer Zertifikatssignierungsanforderung.

```
openssl req -new -newkey rsa:4096 -nodes -days 365 \
-keyout admin.key -out admin.csr -subj "/CN=admin"
```

- b. Erstellen Sie eine Anforderung zum Signieren eines Zertifikats in Kubernetes.

```
BASE64_CSR=$(cat admin.csr | base64 -w 0)
cat << EOF > admin-csr.yaml
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  name: admin-csr
spec:
  signerName: kubernetes.io/kube-apiserver-client
  request: ${BASE64_CSR}
  usages:
    - client auth
EOF
```

2. Erstellen einer Zertifikatssignierungsanforderung mit `kubectl`.

```
kubectl create -f admin-csr.yaml
```

3. Überprüfen Sie den Status der Zertifikatssignierungsanforderung.

```
kubectl get csr admin-csr
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	AGE	REQUESTOR	CONDITION
admin-csr	11m	kubernetes-admin	Pending

Kubernetes hat die Anforderung zum Signieren des Zertifikats erstellt.

4. Genehmigen Sie die Zertifikatssignieranforderung.

```
kubectl certificate approve admin-csr
```

5. Überprüfen Sie erneut den Status der Anfrage zum Signieren des Zertifikats auf Genehmigung.

```
kubectl get csr admin-csr
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	AGE	REQUESTOR	CONDITION
admin-csr	11m	kubernetes-admin	Approved

6. Rufen Sie das Zertifikat ab und überprüfen Sie es.

a. Rufen Sie das Zertifikat ab.

```
kubectl get csr admin-csr -o jsonpath='{.status.certificate}' | base64 --decode > admin.crt
```

b. Überprüfen Sie das Zertifikat.

```
cat admin.crt
```

7. Erstellen Sie eine Cluster-Rollenbindung für einen admin-Benutzer.

```
kubectl create clusterrolebinding admin --clusterrole=cluster-admin \
  --user=admin --group=system:masters
```

8. Generieren Sie eine kubeconfig mit Benutzerbereich für einen getrennten Status.

Sie können eine kubeconfig-Datei mit den heruntergeladenen admin-Zertifikaten generieren. Ersetzen Sie *my-cluster* und *apiserver-endpoint* in den folgenden Befehlen.

```
aws eks describe-cluster --name my-cluster \
  --query "cluster.certificateAuthority" \
  --output text | base64 --decode > ca.crt
```

```
kubectl config --kubeconfig admin.kubeconfig set-cluster my-cluster \
  --certificate-authority=ca.crt --server apiserver-endpoint --embed-certs
```

```
kubectl config --kubeconfig admin.kubeconfig set-credentials admin \
  --client-certificate=admin.crt --client-key=admin.key --embed-certs
```

```
kubectl config --kubeconfig admin.kubeconfig set-context admin@my-cluster \
  --cluster my-cluster --user admin
```

```
kubectl config --kubeconfig admin.kubeconfig use-context admin@my-cluster
```

9. Ziehen Sie Ihre kubeconfig-Datei an.

```
kubectl get nodes --kubeconfig admin.kubeconfig
```

10. Wenn Sie bereits über Services in Produktion auf Ihrem Outpost verfügen, überspringen Sie diesen Schritt. Wenn Amazon EKS der einzige Dienst ist, der auf Ihrem Outpost läuft und der Outpost derzeit nicht in Betrieb ist, können Sie eine Netzwerkunterbrechung simulieren. Bevor Sie mit Ihrem lokalen Cluster in die Produktion gehen, simulieren Sie eine Unterbrechung, um sicherzustellen, dass Sie auf Ihren Cluster zugreifen können, wenn er unterbrochen ist.
- Wenden Sie Firewall-Regeln auf die Netzwerkgeräte an, die Ihren Outpost mit der AWS Region verbinden. Dadurch wird der Service-Link des Outposts getrennt. Sie können keine neuen Instanzen erstellen. Derzeit ausgeführte Instances verlieren die Konnektivität zur AWS Region und zum Internet.
 - Sie können die Verbindung zu Ihrem lokalen Cluster testen, während die Verbindung getrennt ist, indem Sie das `x509`-Zertifikat verwenden. Stellen Sie sicher, dass Sie Ihr `kubeconfig` in das `admin.kubeconfig` ändern, das Sie in einem vorherigen Schritt erstellt haben. `my-cluster` Ersetzen Sie es durch den Namen Ihres lokalen Clusters.

```
kubectl config use-context admin@my-cluster --kubeconfig admin.kubeconfig
```

Wenn Sie Probleme mit Ihren lokalen Clustern feststellen, während diese getrennt sind, empfehlen wir, ein Support-Ticket zu eröffnen.

Wählen Sie Instance-Typen und Platzierungsgruppen für Amazon EKS-Cluster auf AWS Outposts basierend auf Kapazitätsüberlegungen aus

Dieses Thema enthält Anleitungen zur Auswahl des Instance-Typs der Kubernetes-Steuerebene und (optional) zur Verwendung von Platzierungsgruppen, um die Hochverfügbarkeitsanforderungen für Ihren lokalen Amazon EKS-Cluster auf einem Outpost zu erfüllen.

Bevor Sie einen Instanztyp (wie `m5`, oder `t5`) auswählen, der für die Kubernetes-Steuerebene Ihres lokalen Clusters in Outposts verwendet werden soll, überprüfen Sie die Instance-Typen, die in Ihrer Outpost-Konfiguration verfügbar sind. Nachdem Sie die verfügbaren Instance-Typen identifiziert haben, wählen Sie die Instance-Größe (z. B. `large`, `xlarge`, oder `2xlarge`) basierend auf der Anzahl der Knoten, die Ihr Workload benötigt. Die folgende Tabelle enthält Empfehlungen für die Auswahl einer Instance-Größe.

Note

Die Instance-Größen müssen auf Ihren Outposts eingestellt werden. Stellen Sie sicher, dass Sie über genügend Kapazität für drei Instances der auf Ihren Outposts verfügbaren Größe für

die Lebensdauer Ihres lokalen Clusters verfügen. Eine Liste der verfügbaren EC2 Amazon-Instance-Typen finden Sie in den Abschnitten Compute und Storage unter [AWS Outposts Rack-Funktionen](#).

Anzahl der Knoten	Instance-Größe der Kubernetes-Steuerebene
1–20	large
21–100	xlarge
101–250	2xlarge
251–500	4xlarge

Der Speicher für die Kubernetes-Steuerebene benötigt 246 GB Amazon EBS-Speicher für jeden lokalen Cluster, um die erforderlichen IOPS für zu erfüllen. etcd Bei der Erstellung des lokalen Clusters werden die Amazon-EBS-Volumes automatisch für Sie bereitgestellt.

Platzierung der Steuerebene

Wenn Sie mit der `OutpostConfig.ControlPlanePlacement.GroupName` Eigenschaft keine Platzierungsgruppe angeben, wird für die EC2 Amazon-Instances, die für Ihre Kubernetes-Kontrollebene bereitgestellt werden, keine spezifische Hardwareplatzierung für die zugrunde liegende Kapazität, die auf Ihrem Outpost verfügbar ist, erzwungen.

Sie können Platzierungsgruppen verwenden, um die Hochverfügbarkeitsanforderungen für Ihren lokalen Amazon EKS-Cluster auf einem Outpost zu erfüllen. Indem Sie bei der Clustererstellung eine Platzierungsgruppe angeben, beeinflussen Sie die Platzierung der Kubernetes-Steuerebenen-Instances. Die Instances sind auf unabhängige zugrundeliegende Hardware (Racks oder Hosts) verteilt, wodurch die Auswirkungen korrelierter Instances bei Hardwareausfällen minimiert werden.

Die Art der Verteilung, die Sie konfigurieren können, hängt von der Anzahl der Outpost-Racks in Ihrer Bereitstellung ab.

- Bereitstellungen mit einem oder zwei physischen Racks in einem einzigen logischen Outpost — Sie müssen über mindestens drei Hosts verfügen, die mit dem Instance-Typ konfiguriert sind, den Sie für Ihre Kubernetes-Steuerebene-Instances auswählen. Eine Spread-Placement-Gruppe, die

Spread auf Host-Ebene verwendet, stellt sicher, dass alle Kubernetes-Steuerungsinstanzen auf unterschiedlichen Hosts innerhalb der zugrunde liegenden Racks ausgeführt werden, die in Ihrer Outpost-Bereitstellung verfügbar sind.

- Bereitstellungen mit drei oder mehr physischen Racks in einem einzigen logischen Outpost — Sie müssen mindestens drei Hosts mit dem Instance-Typ konfiguriert haben, den Sie für Ihre Kubernetes-Steuerebenen-Instances wählen. Eine Spread-Placement-Gruppe, die Spread auf Rack-Ebene verwendet, stellt sicher, dass alle Kubernetes-Steuerungsinstanzen auf unterschiedlichen Racks in Ihrer Outpost-Bereitstellung ausgeführt werden. Sie können alternativ die auf Host-Ebene verteilte Platzierungsgruppe verwenden, wie in der vorherigen Option beschrieben.

Sie sind für die Erstellung der gewünschten Platzierungsgruppe verantwortlich. Sie geben die Platzierungsgruppe an, wenn Sie die `CreateCluster`-API aufrufen. Weitere Informationen zu Placement-Gruppen und deren Erstellung finden Sie unter [Placement-Gruppen](#) im EC2 Amazon-Benutzerhandbuch.

- Wenn eine Platzierungsgruppe angegeben wird, muss verfügbare Slot-Kapazität auf Ihrem Outpost vorhanden sein, um erfolgreich einen lokalen Amazon-EKS-Cluster zu erstellen. Die Kapazität variiert je nachdem, ob Sie den Host- oder Rack-Spread-Typ verwenden. Wenn nicht genügend Kapazität vorhanden ist, verbleibt der Cluster im `Creating` Status. Sie können das `Insufficient Capacity Error` auf dem Zustandsfeld der [DescribeCluster](#)-API-Antwort überprüfen. Sie müssen Kapazität freigeben, damit der Erstellungsprozess fortgesetzt werden kann.
- Während der lokalen Clusterplattform- und Versionsupdates von Amazon EKS werden die Kubernetes-Steuerebenen-Instances aus Ihrem Cluster durch neue Instances ersetzt, die eine fortlaufende Aktualisierungsstrategie verwenden. Während dieses Ersetzungsprozesses wird jede Instance der Steuerebene beendet, wodurch ihr jeweiliger Slot freigegeben wird. Eine neue aktualisierte Instance wird an ihrer Stelle bereitgestellt. Die aktualisierte Instance wird möglicherweise in den freigegebenen Slot platziert. Wenn der Slot von einer anderen unabhängigen Instance verbraucht wird und keine Kapazität mehr vorhanden ist, die die erforderliche verteilte Topologieanforderung erfüllt, verbleibt der Cluster im `Updating`-Zustand. Sie können das entsprechende `Insufficient Capacity Error` im Zustandsfeld der [DescribeCluster](#)-API-Antwort anzeigen. Sie müssen Kapazitäten freigeben, damit der Aktualisierungsprozess fortschreiten und vorherige Hochverfügbarkeitsniveaus wiederherstellen kann.

- Sie können in jeder AWS Region maximal 500 Platzierungsgruppen pro Konto erstellen. Weitere Informationen finden Sie unter [Allgemeine Regeln und Einschränkungen](#) im EC2 Amazon-Benutzerhandbuch.

Fehlerbehebung bei lokalen Amazon EKS-Clustern auf AWS Outposts

In diesem Thema werden einige häufige Fehler behandelt, die bei der Verwendung lokaler Cluster auftreten können, und wie Sie diese beheben können. Lokale Cluster ähneln Amazon EKS-Clustern in der Cloud, es gibt jedoch einige Unterschiede in der Art und Weise, wie sie von Amazon EKS verwaltet werden.

Important

Beenden Sie niemals eine verwaltete lokale Kubernetes EKS-Cluster-Steuerebeneninstanz, die auf Outpost ausgeführt wird, es sei denn, Sie werden ausdrücklich vom Support dazu aufgefordert. AWS Das Beenden dieser Instanzen birgt ein Risiko für die Verfügbarkeit des lokalen Clusterdienstes, einschließlich des Verlusts des lokalen Clusters, falls mehrere Instanzen gleichzeitig beendet werden. Instanzen der lokalen Kubernetes EKS-Cluster-Steuerebene werden durch das Tag `eks-local:controlplane-name` auf der EC2 Instanzkonsole identifiziert.

API-Verhalten

Lokale Cluster werden über die Amazon-EKS-API erstellt, aber asynchron ausgeführt. Dies bedeutet, dass Anforderungen an die Amazon-EKS-API für lokale Cluster sofort zurückgegeben werden. Diese Anforderungen können jedoch erfolgreich sein, aufgrund von Eingabvalidierungsfehlern schnell scheitern oder fehlschlagen und beschreibende Validierungsfehler aufweisen. Dieses Verhalten ähnelt der Kubernetes-API.

Lokale Cluster gehen nicht in einen FAILED Status über. Amazon EKS versucht, den Cluster-Status kontinuierlich mit dem vom Benutzer angeforderten gewünschten Status abzugleichen. Infolgedessen kann ein lokaler Cluster für längere Zeit im CREATING-Status verbleiben, bis das zugrunde liegende Problem behoben ist.

Beschreibung des Bereichs Cluster-Integrität

Probleme mit lokalen Clustern können mit dem Amazon [AWS EKS-CLI-Befehl describe-cluster](#) erkannt werden. Probleme mit lokalen Clustern werden im `cluster.health` Antwortfeld des

`describe-cluster` Befehls angezeigt. Die in diesem Feld enthaltene Meldung enthält einen Fehlercode, eine beschreibende Meldung und eine zugehörige Ressource. IDs Diese Informationen sind nur über die Amazon EKS-API und AWS CLI verfügbar. Im folgenden Beispiel ersetzen Sie es *my-cluster* durch den Namen Ihres lokalen Clusters.

```
aws eks describe-cluster --name my-cluster --query 'cluster.health'
```

Eine Beispielausgabe sieht wie folgt aus.

```
{
  "issues": [
    {
      "code": "ConfigurationConflict",
      "message": "The instance type 'm5.large' is not supported in Outpost 'my-outpost-arn'.",
      "resourceIds": [
        "my-cluster-arn"
      ]
    }
  ]
}
```

Wenn das Problem nicht behoben werden kann, müssen Sie möglicherweise den lokalen Cluster löschen und einen neuen erstellen. Beispiel: Sie versuchen, einen Cluster mit einem Instance-Typ bereitzustellen, der in Ihrem Outpost nicht verfügbar ist. Die folgende Tabelle enthält allgemeine Fehler im Zusammenhang mit der Integrität.

Fehlerszenario	Code	Fehlermeldung	ResourceIds
Die angegebenen Subnetze konnten nicht gefunden werden.	ResourceNotFound	The subnet ID <i>subnet-id</i> does not exist	Alle bereitgestellten Subnetze IDs
Vorausgesetzt, Subnetze gehören nicht zu derselben VPC.	ConfigurationConflict	Subnets specified must belong to the same VPC	Alle bereitgestellten Subnetze IDs

Fehlerszenario	Code	Fehlermeldung	ResourceIds
Einige bereitgestellte Subnetze gehören nicht zum angegebenen Outpost.	ConfigurationConflict	Subnet <i>subnet-id</i> expected to be in <i>outpost-arn</i> , but is in <i>other-outpost-arn</i>	Problematische Subnetz-ID
Einige der bereitgestellten Subnetze gehören zu keinem Outpost.	ConfigurationConflict	Subnet <i>subnet-id</i> is not part of any Outpost	Problematische Subnetz-ID
Einige bereitgestellte Subnetze verfügen nicht über genügend freie Adressen, um elastische Netzwerkschnittstellen für Kontrollebeneninstanzen zu erstellen.	ResourceLimitExceeded	The specified subnet does not have enough free addresses to satisfy the request.	Problematische Subnetz-ID
Der angegebene Instance-Typ der Kontrollebene wird auf Ihrem Outpost nicht unterstützt.	ConfigurationConflict	The instance type <i>type</i> is not supported in Outpost <i>outpost-arn</i>	Cluster-ARN

Fehlerszenario	Code	Fehlermeldung	ResourceIds
Sie haben eine EC2 Amazon-Instance auf Kontrollebene beendet oder <code>run-instance</code> waren erfolgreich, aber der beobachtete Status hat sich geändert <code>Terminated</code> . Dies kann für einen bestimmten Zeitraum passieren, nachdem Ihr Outpost wieder eine Verbindung hergestellt hat und interne Amazon EBS-Fehler dazu führen, dass ein EC2 interner Amazon-Workflow fehlschlägt.	<code>InternalFailure</code>	EC2 instance state "Terminated" is unexpected	Cluster-ARN
Sie verfügen über unzureichende Kapazität auf Ihrem Outpost. Dies kann auch passieren, wenn ein Cluster erstellt wird und ein Outpost von der Region getrennt wird. AWS	<code>ResourceLimitExceeded</code>	There is not enough capacity on the Outpost to launch or start the instance.	Cluster-ARN
Ihr Konto hat das Kontingent Ihrer Sicherheitsgruppe überschritten.	<code>ResourceLimitExceeded</code>	Von der Amazon EC2 API zurückgegebene Fehlermeldung	Ziel-VPC-ID

Fehlerszenario	Code	Fehlermeldung	ResourceIds
Ihr Konto hat Ihr Kontingent für die elastische Netzwerkschnittstelle überschritten.	ResourceLimitExceeded	Von der Amazon EC2 API zurückgegebene Fehlermeldung	Ziel-Subnetz-ID
Instanzen der Kontrollebene waren über AWS Systems Manager nicht erreichbar. Informationen zur Lösung finden Sie unter the section called “Instanzen der Kontrollebene sind über AWS Systems Manager nicht erreichbar” .	ClusterUnreachable	Amazon-EKS-Steuerbene-Instances sind nicht über SSM erreichbar. Bitte überprüfen Sie Ihre SSM- und Netzwerkkonfiguration und lesen Sie die Dokumentation zur Fehlerbehebung bei EKS on Outposts.	EC2 Amazon-Instanz IDs
Beim Abrufen von Details für eine verwaltete Sicherheitsgruppe oder eine elastische Netzwerkschnittstelle ist ein Fehler aufgetreten.	Basiert auf dem EC2 Amazon-Client-Fehlercode.	Von der Amazon EC2 API zurückgegebene Fehlermeldung	Alle verwalteten Sicherheitsgruppen IDs

Fehlerszenario	Code	Fehlermeldung	ResourceIds
Beim Autorisieren oder Widerrufen von Eingangsregeln für Sicherheitsgruppen ist ein Fehler aufgetreten. Dies gilt sowohl für die Sicherheitsgruppen des Clusters als auch der Steuerebene.	Basiert auf dem EC2 Amazon-Client-Fehlercode.	Von der Amazon EC2 API zurückgegebene Fehlermeldung	Problematische Sicherheitsgruppen-ID
Beim Löschen einer elastischen Netzwerkschnittstelle für eine Instance der Steuerebene ist ein Fehler aufgetreten.	Basiert auf dem EC2 Amazon-Client-Fehlercode.	Von der Amazon EC2 API zurückgegebene Fehlermeldung	Problematische ID der Elastic-Netzwerkschnittstelle

In der folgenden Tabelle sind Fehler anderer AWS Dienste aufgeführt, die im Feld „Integrität“ der `describe-cluster` Antwort aufgeführt sind.

EC2 Amazon-Fehlercode	Code für Cluster-Integritätsprobleme	Beschreibung
AuthFailure	AccessDenied	Dieser Fehler kann aus einer Vielzahl von Gründen auftreten. Der häufigste Grund ist, dass Sie versehentlich ein Tag entfernt haben, das der Service verwendet, um die Richtlinie für die mit dem Service verknüpfte Rolle von der Steuerebene herabzustufen. In diesem

EC2 Amazon-Fehlercode	Code für Cluster-Integritätsprobleme	Beschreibung
		Fall kann Amazon EKS diese AWS Ressourcen nicht mehr verwalten und überwachen.
UnauthorizedOperation	AccessDenied	Dieser Fehler kann aus einer Vielzahl von Gründen auftreten. Der häufigste Grund ist, dass Sie versehentlich ein Tag entfernt haben, das der Service verwendet, um die Richtlinie für die mit dem Service verknüpfte Rolle von der Steuerebene herabzustufen. In diesem Fall kann Amazon EKS diese AWS Ressourcen nicht mehr verwalten und überwachen.
InvalidSubnetID.NotFound	ResourceNotFound	Dieser Fehler tritt auf, wenn die Subnetz-ID für die Eingangsregeln einer Sicherheitsgruppe nicht gefunden werden kann.
InvalidPermission.NotFound	ResourceNotFound	Dieser Fehler tritt auf, wenn die Berechtigungen für die Eingangsregeln einer Sicherheitsgruppe nicht korrekt sind.
InvalidGroup.NotFound	ResourceNotFound	Dieser Fehler tritt auf, wenn die Gruppe der Eingangsregeln einer Sicherheitsgruppe nicht gefunden werden kann.

EC2 Amazon-Fehlercode	Code für Cluster-Integritätsprobleme	Beschreibung
InvalidNetworkInterfaceID.NotFound	ResourceNotFound	Dieser Fehler tritt auf, wenn die Netzwerkschnittstellen-ID für die Eingangsregeln einer Sicherheitsgruppe nicht gefunden werden kann.
InsufficientFreeAddressesInSubnet	ResourceLimitExceeded	Dieser Fehler tritt auf, wenn das Kontingent der Subnetzressourcen überschritten wird.
InsufficientCapacityOnOutpost	ResourceLimitExceeded	Dieser Fehler tritt auf, wenn das Kapazitätskontingent des Außenpostens überschritten wird.
NetworkInterfaceLimitExceeded	ResourceLimitExceeded	Dieser Fehler tritt auf, wenn das Kontingent der elastischen Netzwerkschnittstelle überschritten wird.
SecurityGroupLimitExceeded	ResourceLimitExceeded	Dieser Fehler tritt auf, wenn das Kontingent der Sicherheitsgruppe überschritten wird.

EC2 Amazon-Fehlercode	Code für Cluster-Integrität probleme	Beschreibung
VcpuLimitExceeded	ResourceLimitExceeded	Dies wird beobachtet, wenn eine EC2 Amazon-Instance in einem neuen Konto erstellt wird. Die Fehlermeldung könnte ähnlich wie die folgende lauten: „You have requested more vCPU capacity than your current vCPU limit of 32 allows for the instance bucket that the specified instance type belongs to. Please visit http://aws.amazon.com/contact-us/ec2-request to request an adjustment to this limit.“
InvalidParameterValue	ConfigurationConflict	Amazon EC2 gibt diesen Fehlercode zurück, wenn der angegebene Instance-Typ im Outpost nicht unterstützt wird.
Alle anderen Fehler	InternalFailure	Keine

Cluster können nicht erstellt oder geändert werden

Lokale Cluster erfordern andere Berechtigungen und Richtlinien als Amazon-EKS-Cluster, die in der Cloud gehostet werden. Wenn ein Cluster nicht erstellt werden kann und ein InvalidPermissions Fehler auftritt, überprüfen Sie, ob der Cluster-Rolle, die Sie verwenden, die von [Amazon EKSLocal OutpostClusterPolicy](#) verwaltete Richtlinie zugeordnet ist. Alle anderen API-Aufrufe erfordern dieselben Berechtigungen wie Amazon-EKS-Cluster in der Cloud.

Cluster bleibt im **CREATING**-Zustand hängen

Die Zeit, die zum Erstellen eines lokalen Clusters benötigt wird, hängt von mehreren Faktoren ab. Zu diesen Faktoren gehören Ihre Netzwerkkonfiguration, Outpost-Konfiguration und die Konfiguration des Clusters. Im Allgemeinen wird ein lokaler Cluster erstellt und wechselt innerhalb von 15–20 Minuten in den ACTIVE-Status. Wenn ein lokaler Cluster im CREATING-Status bleibt, können Sie `describe-cluster` aufrufen, um Informationen über die Ursache im `cluster.health-`Ausgabefeld abzurufen.

Die am häufigsten auftretenden Probleme sind:

- Ihr Cluster kann von der AWS Region aus, in der sich Systems Manager befindet, keine Verbindung zur Kontrollebeneninstanz herstellen. Sie können dies überprüfen, indem Sie `aws ssm start-session --target instance-id` von einem Bastion-Host in der Region aufrufen. Wenn dieser Befehl nicht funktioniert, überprüfen Sie, ob Systems Manager auf der Steuerungsebeneninstanz ausgeführt wird. Eine andere Möglichkeit besteht darin, den Cluster zu löschen und ihn dann neu zu erstellen.
- Die Instanzen der Steuerungsebene können aufgrund von KMS-Schlüsselberechtigungen für EBS-Volumes nicht erstellt werden. Bei benutzerverwalteten KMS-Schlüsseln für verschlüsselte EBS-Volumes werden die Instanzen der Kontrollebene beendet, wenn auf den Schlüssel nicht zugegriffen werden kann. Wenn die Instances beendet werden, wechseln Sie entweder zu einem AWS verwalteten KMS-Schlüssel oder stellen Sie sicher, dass Ihre Richtlinie für benutzerverwaltete Schlüssel der Clusterrolle die erforderlichen Berechtigungen gewährt.
- Instances auf der Steuerebene von Systems Manager haben möglicherweise keinen Zugriff auf das Internet. Überprüfen Sie, ob das Subnetz, das Sie beim Erstellen des Clusters angegeben haben, über ein NAT-Gateway und eine VPC mit einem Internet-Gateway verfügt. Verwenden Sie VPC Reachability Analyzer, um zu überprüfen, ob die Instance der Steuerebene das Internet-Gateway erreichen kann. Weitere Informationen finden Sie unter [Erste Schritte mit VPC Reachability Analyzer](#).
- Der von Ihnen angegebene Rollen-ARN enthält keine Richtlinien. Prüfen Sie, ob die [AWS verwaltete Richtlinie: Amazon](#) aus der Rolle entfernt EKSLocal OutpostClusterPolicy wurde. Dies kann auch passieren, wenn ein AWS CloudFormation Stack falsch konfiguriert ist.
- Alle bereitgestellten Subnetze müssen demselben Outpost zugeordnet sein und sich gegenseitig erreichen. Wenn beim Erstellen eines Clusters mehrere Subnetze angegeben werden, versucht Amazon EKS, die Instances der Steuerebene auf mehrere Subnetze zu verteilen.

- Amazon-EKS-verwaltete Sicherheitsgruppen werden auf die Elastic-Network-Schnittstelle angewendet. Andere Konfigurationselemente wie NACL-Firewall-Regeln könnten jedoch mit den Regeln für die elastische Netzwerkschnittstelle in Konflikt geraten.

VPC- und Subnetz-DNS-Konfiguration ist falsch konfiguriert oder fehlt

Lesen [Sie den Artikel VPC und Subnetze für Amazon EKS-Cluster auf AWS Outposts erstellen](#).

Cluster bleibt im **UPDATING**-Zustand hängen

Amazon EKS aktualisiert automatisch alle vorhandenen lokalen Cluster auf die neuesten Plattformversionen für die entsprechende Kubernetes-Nebenversion. Weitere Informationen zu Plattformversionen finden Sie unter [the section called “Versionen der EKS-Plattform”](#)

Während eines automatischen Rollouts einer Plattformversion ändert sich der Clusterstatus auf **UPDATING**. Der Aktualisierungsprozess besteht darin, alle Instanzen der Kubernetes-Steuerebene durch neue Instanzen zu ersetzen, die die neuesten Sicherheitspatches und Bugfixes enthalten, die für die jeweilige Kubernetes-Nebenversion veröffentlicht wurden. Im Allgemeinen wird ein lokaler Clusterplattform-Aktualisierungsprozess innerhalb von weniger als 30 Minuten abgeschlossen und der Cluster wechselt wieder in den Status **ACTIVE**. Bleibt ein lokaler Cluster über einen längeren Zeitraum im **UPDATING** Status, können Sie anrufen, `describe-cluster` um im `cluster.health` Ausgabefeld nach Informationen zur Ursache zu suchen.

Amazon EKS stellt sicher, dass mindestens 2 von 3 Kubernetes-Control-Plane-Instances fehlerfrei und betriebsbereit sind, um die lokale Clusterverfügbarkeit aufrechtzuerhalten und Serviceunterbrechungen zu verhindern. Wenn ein lokaler Cluster blockiert ist, liegt dies in **UPDATING** der Regel daran, dass ein Infrastruktur- oder Konfigurationsproblem vorliegt, das verhindert, dass die Mindestverfügbarkeit der beiden Instanzen garantiert werden kann, falls der Prozess fortgesetzt wird. Der Aktualisierungsvorgang wird also gestoppt, um die Unterbrechung des lokalen Clusterdienstes zu verhindern.

Es ist wichtig, Fehler bei einem lokalen Cluster, der im **UPDATING** Status hängen geblieben ist, zu beheben und die Ursache zu beheben, damit der Aktualisierungsprozess abgeschlossen und der lokale Cluster wieder **ACTIVE** mit der Hochverfügbarkeit von 3 Kubernetes-Steuerungsinstanzen wiederhergestellt werden kann.

Beenden Sie keine verwalteten lokalen Kubernetes EKS-Clusterinstanzen auf Outposts, sofern Sie nicht ausdrücklich vom AWS Support dazu aufgefordert werden. Dies ist besonders wichtig für lokale

Cluster, die im UPDATING Status feststecken, da die Wahrscheinlichkeit hoch ist, dass ein anderer Knoten auf der Kontrollebene nicht vollständig funktionsfähig ist und das Beenden der falschen Instanz zu Betriebsunterbrechungen und dem Risiko eines Datenverlusts im lokalen Cluster führen kann.

Die am häufigsten auftretenden Probleme sind:

- Eine oder mehrere Instanzen der Kontrollebene können aufgrund einer Änderung der Netzwerkkonfiguration seit der ersten Erstellung des lokalen Clusters keine Verbindung zu System Manager herstellen. Sie können dies überprüfen, indem Sie `aws ssm start-session --target instance-id` von einem Bastion-Host in der Region aufrufen. Wenn dieser Befehl nicht funktioniert, überprüfen Sie, ob Systems Manager auf der Steuerungsebeneninstanz ausgeführt wird.
- Neue Instanzen der Steuerungsebene können aufgrund von KMS-Schlüsselberechtigungen für EBS-Volumes nicht erstellt werden. Bei benutzerverwalteten KMS-Schlüsseln für verschlüsselte EBS-Volumes werden die Instanzen der Kontrollebene beendet, wenn auf den Schlüssel nicht zugegriffen werden kann. Wenn die Instances beendet werden, wechseln Sie entweder zu einem AWS verwalteten KMS-Schlüssel oder stellen Sie sicher, dass Ihre Richtlinie für benutzerverwaltete Schlüssel der Clusterrolle die erforderlichen Berechtigungen gewährt.
- Die Instanzen der Systems Manager Manager-Steuerungsebene haben möglicherweise den Internetzugang verloren. Überprüfen Sie, ob das Subnetz, das bei der Erstellung des Clusters bereitgestellt wurde, über ein NAT-Gateway und eine VPC mit einem Internet-Gateway verfügt. Verwenden Sie VPC Reachability Analyzer, um zu überprüfen, ob die Instance der Steuerebene das Internet-Gateway erreichen kann. Weitere Informationen finden Sie unter [Erste Schritte mit VPC Reachability Analyzer](#). Wenn Ihre privaten Netzwerke keine ausgehende Internetverbindung haben, stellen Sie sicher, dass alle erforderlichen VPC-Endpunkte und Gateway-Endpunkte weiterhin im regionalen Subnetz Ihres Clusters vorhanden sind (siehe). [the section called “Subnetzzugriff auf Dienste AWS”](#)
- Der von Ihnen angegebene Rollen-ARN enthält keine Richtlinien. Prüfen Sie, ob die [AWS verwaltete Richtlinie: Amazon](#) nicht aus der Rolle entfernt EKSLocal OutpostClusterPolicy wurde.
- Bei einer der neuen Kubernetes-Steuerungsinstanzen ist möglicherweise ein unerwarteter Bootstrapping-Fehler aufgetreten. Bitte reichen Sie ein Ticket beim [AWS Support Center](#) ein, um weitere Informationen zur Fehlerbehebung und zur Erfassung von Protokollen in diesem Ausnahmefall zu erhalten.

Knoten können nicht zu einem Cluster hinzugefügt werden

- AMI-Probleme:
 - Sie verwenden ein AMI, das nicht unterstützt wird. Sie müssen [v20220620](#) oder höher für das [Erstellen von Knoten mit optimiertem Amazon Linux, Amazon EKS-optimierte AMIs Amazon Linux](#) verwenden.
 - Wenn Sie zum Erstellen Ihrer Knoten eine AWS CloudFormation Vorlage verwendet haben, stellen Sie sicher, dass sie kein nicht unterstütztes AMI verwendet.
- Fehlt der AWS IAM-Authenticator ConfigMap — Falls er fehlt, müssen Sie ihn erstellen. Weitere Informationen finden Sie unter [the section called “Anwenden von aws-authConfigMap auf Ihren Cluster”](#).
- Die falsche Sicherheitsgruppe wird verwendet – Stellen Sie sicher, dass Sie `eks-cluster-sg-cluster-name-uniqueid` für die Sicherheitsgruppe Ihrer Worker-Knoten verwenden. Die ausgewählte Sicherheitsgruppe wird geändert AWS CloudFormation , sodass bei jeder Verwendung des Stacks eine neue Sicherheitsgruppe zulässig ist.
- Unerwartete VPC-Schritte für private Links – Falsche CA-Daten (`--b64-cluster-ca`) oder API-Endpoint (`--apiserver-endpoint`) sind bestanden.

Sammeln von Protokollen

Wenn ein Outpost von der AWS Region getrennt wird, der er zugeordnet ist, funktioniert der Kubernetes-Cluster wahrscheinlich weiterhin normal. Wenn der Cluster jedoch nicht ordnungsgemäß funktioniert, folgen Sie den Schritten zur Fehlerbehebung unter [Lokale Amazon EKS-Cluster auf AWS Outposts für Netzwerkunterbrechungen vorbereiten](#). Wenn Sie auf andere Probleme stoßen, wenden Sie sich an den AWS Support. AWS Der Support kann Sie beim Herunterladen und Ausführen eines Tools zur Protokollerfassung unterstützen. Auf diese Weise können Sie Protokolle von Ihren Kubernetes-Cluster-Steuerungsebeneninstanzen sammeln und sie zur weiteren Untersuchung an den AWS Support senden.

Instanzen der Kontrollebene sind über AWS Systems Manager nicht erreichbar

Wenn die Amazon EKS Control Plane Instances nicht über AWS Systems Manager (Systems Manager) erreichbar sind, zeigt Amazon EKS den folgenden Fehler für Ihren Cluster an.

```
Amazon EKS control plane instances are not reachable through SSM. Please verify your SSM and network configuration, and reference the EKS on Outposts troubleshooting documentation.
```

Um dieses Problem zu beheben, stellen Sie sicher, dass Ihre VPC und Subnetze die Anforderungen unter [Erstellen einer VPC und Subnetze für Amazon EKS-Cluster auf AWS Outposts](#) erfüllen und dass Sie die Schritte unter [Setup Session Manager im Systems Manager Manager-Benutzerhandbuch](#) ausgeführt haben. AWS

Amazon Linux-Knoten auf AWS Outposts erstellen

Dieses Thema beschreibt Hinweise zum Starten von Auto-Scaling-Gruppen von Amazon-Linux-Knoten auf einem Outpost, die mit Ihrem Amazon-EKS-Cluster registriert sind. Der Cluster kann sich in der AWS Cloud oder in einem Outpost befinden.

- Ein vorhandener Outpost. Weitere Informationen finden Sie unter [Was sind AWS Outposts](#).
- Ein vorhandener Amazon-EKS-Cluster. Informationen zur Bereitstellung eines Clusters in der AWS Cloud finden Sie unter [the section called “Erstellen eines -Clusters”](#). Informationen zum Bereitstellen eines Clusters in einem Outpost finden Sie unter [the section called “Führen Sie lokale Cluster aus”](#).
- Angenommen, Sie erstellen Ihre Knoten in einem Cluster in der AWS Cloud und Sie haben Subnetze in der AWS Region, in der Sie AWS Outposts, AWS Wavelength oder AWS Local Zones aktiviert haben. Diese Subnetze dürfen dann bei der Erstellung Ihres Clusters nicht angegeben worden sein. Wenn Sie Ihre Knoten in einem Cluster auf einem Outpost erstellen, müssen Sie bei der Erstellung Ihres Clusters ein Outpost-Subnetz eingegeben haben.
- (Empfohlen für Cluster in der AWS Cloud) Das Amazon VPC CNI-Plug-In für Kubernetes ist mit einer eigenen IAM-Rolle konfiguriert, der die erforderliche IAM-Richtlinie zugeordnet ist. Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#). Lokale Cluster unterstützen keine IAM-Rollen für Service-Konten.

Sie können eine selbstverwaltete Amazon Linux-Knotengruppe mit `eksctl` oder AWS Management Console (mit einer AWS CloudFormation Vorlage) erstellen. Sie können auch Terraform verwenden.

Sie können eine selbstverwaltete Knotengruppe für einen lokalen Cluster mit den folgenden auf dieser Seite beschriebenen Tools erstellen:

- [the section called “eksctl”](#)
- [the section called “AWS Management Console”](#)

Important

- Die selbstverwaltete Knotengruppe umfasst EC2 Amazon-Instances in Ihrem Konto. Diese Instances werden nicht automatisch aktualisiert, wenn Sie oder Amazon EKS die Version der Kontrollebene in Ihrem Namen aktualisieren. Bei einer selbstverwalteten Knotengruppe wird in der Konsole nicht angezeigt, dass sie aktualisiert werden muss. Sie können die auf einem Knoten installierte kubelet-Version anzeigen, indem Sie den Knoten in der Liste Knoten auf der Registerkarte Übersicht Ihres Clusters auswählen, um zu bestimmen, welche Knoten aktualisiert werden müssen. Sie müssen die Knoten manuell aktualisieren. Weitere Informationen finden Sie unter [the section called “Update-Methoden”](#).
- Die von Kubelet auf Ihren selbstverwalteten Knoten verwendeten Zertifikate werden mit einer Laufzeit von einem Jahr ausgestellt. [Standardmäßig ist die Zertifikatsrotation nicht aktiviert \(siehe: \[https://kubernetes.io/docs/reference/config-api/kubelet-config.v1beta1/# kubelet-config-k 8 s-io-v 1beta1- KubeletConfiguration\]\(https://kubernetes.io/docs/reference/config-api/kubelet-config.v1beta1/#kubelet-config-k8s-io-v1beta1-KubeletConfiguration\)\)](#), das heißt, wenn Sie einen selbstverwalteten Knoten haben, der länger als ein Jahr läuft, kann er sich nicht mehr bei der Kubernetes-API authentifizieren.
- Als bewährte Methode empfehlen wir Kunden, ihre selbstverwalteten Knotengruppen regelmäßig zu aktualisieren, um Sicherheitspatches von den neuesten für Amazon EKS optimierten AMI zu erhalten CVEs . Das Aktualisieren von AMI, das in selbstverwalteten Knotengruppen verwendet wird, löst auch die Neuerstellung von Knoten aus und stellt sicher, dass diese nicht aufgrund abgelaufener Kubelet-Zertifikate auf Probleme stoßen.
- [Alternativ können Sie auch die Rotation von Client-Zertifikaten aktivieren \(siehe: <https://kubernetes.io/docs/tasks/tls/certificate-rotation/>\)](#) beim Erstellen der selbstverwalteten Knotengruppen, um sicherzustellen, dass Kubelet-Zertifikate erneuert werden, wenn das aktuelle Zertifikat bald abläuft.

eksctl

Um selbstverwaltete Linux-Knoten zu starten mit **eksctl**

1. Installieren Sie die Version 0.210.0 oder höher des auf Ihrem Gerät installierten eksctl Befehlszeilentools oder AWS CloudShell. Informationen zum Installieren und Aktualisieren von eksctl finden Sie in der Dokumentation zu eksctl unter [Installation](#).
2. Wenn sich Ihr Cluster in der AWS Cloud befindet und die von AmazonEKS_CNI_Policy verwaltete IAM-Richtlinie mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie](#)

[stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Dienstkonto zuordnen. aws-node Weitere Informationen finden Sie unter [the section called “Für IRSA konfigurieren”](#). Wenn sich Ihr Cluster in Ihrem Outpost befindet, muss die Richtlinie an Ihre Knotenrolle angehängt sein.

3. Der folgende Befehl erstellt eine Knotengruppe in einem bestehenden Cluster. Der Cluster muss mit eksctl erstellt worden sein. Ersetzen Sie *al-nodes* durch einen Namen für Ihre Knotengruppe. Der Name der Knotengruppe darf nicht länger als 63 Zeichen sein. Er muss mit einem Buchstaben oder einer Ziffer beginnen, kann danach aber auch Bindestriche und Unterstriche enthalten. Ersetzen Sie *my-cluster* mit dem Namen Ihres Clusters. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein. Wenn Ihr Cluster auf einem Outpost existiert, ersetzen Sie *id* mit der ID eines Outpost-Subnetzes. Wenn Ihr Cluster in der AWS Cloud existiert, *id* ersetzen Sie ihn durch die ID eines Subnetzes, das Sie bei der Erstellung Ihres Clusters nicht angegeben haben. Ersetzen Sie *instance-type* durch einen Instance-Typ, der von Ihrem Outpost unterstützt wird. Ersetzen Sie den Rest der *example values* durch Ihre eigenen Werte. Die Knoten werden standardmäßig mit derselben Kubernetes-Version wie die Steuerungsebene erstellt.

Ersetzen Sie *instance-type* durch einen Instance-Typ, der auf Ihrem Outpost verfügbar ist.

my-key Ersetzen Sie es durch den Namen Ihres EC2 Amazon-Schlüsselpaars oder öffentlichen Schlüssels. Dieser Schlüssel wird für den SSH-Zugriff zu Ihren Knoten verwendet, nachdem diese gestartet wurden. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch.

Erstellen Sie Ihre Knoten-Gruppe mit dem folgenden Befehl.

```
eksctl create nodegroup --cluster my-cluster --name al-nodes --node-type instance-type \
    --nodes 3 --nodes-min 1 --nodes-max 4 --managed=false --node-volume-type gp2 --
subnet-ids subnet-id
```

Wenn Ihr Cluster in der AWS Cloud bereitgestellt ist:

- Die Knotengruppe, die Sie bereitstellen, kann Pods IPv4 Adressen aus einem anderen CIDR-Block als dem der Instanz zuweisen. Weitere Informationen finden Sie unter [the section called “Benutzerdefinierte Netzwerke”](#).

- Die Knotengruppe, die Sie bereitstellen, benötigt keinen ausgehenden Internetzugang. Weitere Informationen finden Sie unter [the section called “Private Cluster”](#).

Eine vollständige Liste aller verfügbaren Optionen und Standardeinstellungen finden Sie in der Dokumentation unter [AWS Outposts Support](#). `eksctl`

- Wenn Knoten dem Cluster nicht beitreten können, finden Sie weitere Informationen unter [the section called “Knoten können nicht mit dem Cluster verknüpft werden” Beheben von Problemen mit Amazon EKS-Clustern und -Knoten](#) und unter [Problembehandlung the section called “Knoten können nicht zu einem Cluster hinzugefügt werden” bei lokalen Amazon EKS-Clustern auf AWS Outposts](#).
- Eine Beispielausgabe sieht wie folgt aus. Mehrere Zeilen werden ausgegeben, während die Knoten erstellt werden. Die letzte Ausgabezeile ähnelt der folgenden Beispielzeile.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

4. (Optional) [???](#) Stellen Sie eine Beispielanwendung bereit, um Ihren Cluster und Ihre Linux-Worker-Knoten zu testen.

AWS Management Console

Schritt 1: Starten Sie selbstverwaltete Linux-Knoten mit AWS Management Console

1. Laden Sie die neueste Version der AWS CloudFormation Vorlage herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/  
amazon-eks-nodegroup.yaml
```

2. Öffnen Sie die [AWS CloudFormation -Konsole](#).
3. Wählen Sie Create stack (Stack erstellen) und dann With new resources (standard) (Mit neuen Ressourcen [Standard]) aus.
4. Wählen Sie für Specify template (Vorlage festlegen) Upload a template file (Vorlagendatei hochladen) aus und wählen Sie dann Choose file (Datei wählen). Wählen Sie die `amazon-eks-nodegroup.yaml`-Datei aus, die Sie in einem vorherigen Schritt heruntergeladen haben, und wählen Sie dann Next (Weiter) aus.
5. Geben Sie auf der Seite Specify stack details (Stack-Details angeben) die folgenden Parameter ein und klicken Sie dann auf Next (Weiter):

- **Stack-Name:** Wählen Sie einen Stack-Namen für Ihren AWS CloudFormation Stack. Sie können ihn beispielsweise *a1-nodes* nennen. Der Name darf nur alphanumerische Zeichen (wobei die Groß- und Kleinschreibung beachtet werden muss) und Bindestriche enthalten. Er muss mit einem alphanumerischen Zeichen beginnen und darf nicht länger als 100 Zeichen sein. Der Name muss innerhalb der AWS Region und des AWS Kontos, in dem Sie den Cluster erstellen, eindeutig sein.
- **ClusterName:** Geben Sie den Namen Ihres Clusters ein. Wenn dieser Name nicht mit Ihrem Clusternamen übereinstimmt, können Ihre Knoten dem Cluster nicht beitreten.
- **ClusterControlPlaneSecurityGroup:** Wählen Sie den SecurityGroupsWert aus der AWS CloudFormation Ausgabe aus, die Sie bei der Erstellung Ihrer [VPC](#) generiert haben.

Die folgenden Schritte zeigen einen Vorgang zum Abrufen der entsprechenden Gruppe.

- i. Öffnen Sie die [Amazon-EKS-Konsole](#).
 - ii. Wählen Sie den Namen des Clusters.
 - iii. Wählen Sie die Registerkarte Network (Network) aus.
 - iv. Verwenden Sie den Wert Zusätzliche Sicherheitsgruppen als Referenz, wenn Sie aus der ClusterControlPlaneSecurityGroupDropdownliste auswählen.
- **NodeGroupName:** Geben Sie einen Namen für Ihre Knotengruppe ein. Dieser Name kann später verwendet werden, um die Auto Scaling-Knotengruppe zu identifizieren, die für Ihre Knoten erstellt wurde.
 - **NodeAutoScalingGroupMinSize:** Geben Sie die Mindestanzahl von Knoten ein, auf die Ihre Auto Scaling Scaling-Gruppe für Knoten skalieren kann.
 - **NodeAutoScalingGroupDesiredCapacity:** Geben Sie die gewünschte Anzahl von Knoten ein, auf die bei der Erstellung Ihres Stacks skaliert werden soll.
 - **NodeAutoScalingGroupMaxSize:** Geben Sie die maximale Anzahl von Knoten ein, auf die Ihre Auto Scaling Scaling-Gruppe für Knoten skalieren kann.
 - **NodeInstanceType:** Wählen Sie einen Instance-Typ für Ihre Knoten. Wenn Ihr Cluster in der AWS Cloud läuft, finden Sie weitere Informationen unter [the section called “EC2 Amazon-Instance-Typen”](#). Wenn Ihr Cluster auf einem Outpost ausgeführt wird, können Sie nur einen Instance-Typ auswählen, der auf Ihrem Outpost verfügbar ist.
 - **NodeImageIdSSMParam:** Vorab mit dem Amazon EC2 Systems Manager Manager-Parameter eines kürzlich für Amazon EKS optimierten AMI für eine variable Kubernetes-Version gefüllt. Um eine andere Kubernetes-Nebenversion zu verwenden, die von Amazon EKS unterstützt wird,

ersetzen Sie **1.XX** durch eine andere [unterstützte Version](#). Wir empfehlen, dieselbe Kubernetes-Version wie Ihr Cluster anzugeben.

Um ein für Amazon EKS optimiertes beschleunigtes AMI zu verwenden, **amazon-linux-2** ersetzen Sie es durch `amazon-linux-2-gpu`. Um ein für Amazon EKS optimiertes Arm-AMI zu verwenden, **amazon-linux-2** ersetzen Sie es durch `amazon-linux-2-arm64`.

 Note

Die Amazon EKS-Knoten AMIs basieren auf Amazon Linux. Sie können Sicherheits- oder Datenschutzereignisse für Amazon Linux im [Amazon Linux-Sicherheitszentrum](#) verfolgen, indem Sie den Tab für Ihre gewünschte Version auswählen. Sie können auch den entsprechenden RSS-Feed abonnieren. Sicherheits- oder Datenschutzereignisse enthalten eine Übersicht über das Problem, welche Pakete betroffen sind und wie Sie Ihre Instances aktualisieren, um das Problem zu beheben.

- **NodeImageId:** (Optional) Wenn Sie Ihr eigenes benutzerdefiniertes AMI (anstelle eines für Amazon EKS optimierten AMI) verwenden, geben Sie eine Knoten-AMI-ID für Ihre AWS Region ein. Wenn Sie hier einen Wert angeben, überschreibt dieser alle Werte im `NodeImageIdSSMParamField`.
- **NodeVolumeSize:** Geben Sie eine Root-Volume-Größe für Ihre Knoten in GiB an.
- **NodeVolumeType:** Geben Sie einen Root-Volume-Typ für Ihre Knoten an.
- **KeyName:** Geben Sie den Namen eines Amazon EC2 SSH-Schlüsselpaars ein, mit dem Sie nach dem Start über SSH eine Verbindung zu Ihren Knoten herstellen können. Wenn Sie noch kein EC2 Amazon-Schlüsselpaar haben, können Sie eines in der erstellen AWS Management Console. Weitere Informationen finden Sie unter [EC2 Amazon-Schlüsselpaare](#) im EC2 Amazon-Benutzerhandbuch.

 Note

Wenn Sie hier kein key pair angeben, schlägt die AWS CloudFormation Stack-Erstellung fehl.

- **BootstrapArguments:** Es gibt mehrere optionale Argumente, die Sie an Ihre Knoten übergeben können. Weitere Informationen finden Sie in den [Bootstrap-Skript-Nutzungsinformationen](#) auf GitHub. Wenn Sie Knoten zu einem lokalen Amazon EKS-Cluster auf AWS Outposts hinzufügen (wo die Kubernetes-Steuerplane-Instances auf AWS Outposts ausgeführt werden)

und der Cluster keine Eingangs- und Ausgangsinternetverbindung hat (auch als private Cluster bezeichnet), müssen Sie die folgenden Bootstrap-Argumente (als einzelne Zeile) angeben.

```
--b64-cluster-ca ${CLUSTER_CA} --apiserver-endpoint https://${APISERVER_ENDPOINT}
--enable-local-outpost true --cluster-id ${CLUSTER_ID}
```

Führen Sie die folgenden AWS CLI-Befehle CLUSTER_ID aus CLUSTER_CAAPISERVER_ENDPOINT, um die Werte für, und Ihres lokalen Amazon EKS-Clusters abzurufen. Ersetzen Sie cluster-name durch den Namen Ihres Clusters und die Region (z. B. us-east-1) durch die Region Ihres Clusters. AWS

```
echo "CLUSTER_CA=$(aws eks describe-cluster --name cluster-name --region region --
query cluster.certificateAuthority.data --output text)"

echo "APISERVER_ENDPOINT=$(aws eks describe-cluster --name cluster-name --region
region --query cluster.endpoint --output text)"

echo "CLUSTER_ID=$(aws eks describe-cluster --name cluster-name --region region --
query cluster.id --output text)"
```

- Deaktivieren IMDSv1: Standardmäßig unterstützt jeder Knoten den Instanz-Metadatendienst Version 1 () und. IMDSv1 IMDSv2 Sie können deaktivieren IMDSv1. Um zu verhindern, dass future Knoten und Pods in der Knotengruppe verwendet werden IMDSv1, setzen Sie Disable IMDSv1 auf true. Weitere Informationen finden Sie unter [Konfiguration des Instance-Metadatenservice](#). Weitere Informationen zum Einschränken des Zugriffs darauf auf Ihre Knoten finden Sie unter [Beschränken Sie den Zugriff auf das Instance-Profil, das dem Worker-Knoten zugewiesen ist](#).
 - VpcId: Geben Sie die ID für die [VPC](#) ein, die Sie erstellt haben. Bevor Sie sich für eine VPC entscheiden, sollten Sie sich die [VPC-Anforderungen und Überlegungen ansehen](#).
 - Subnets (Subnetze): Wenn sich Ihr Cluster auf einem Outpost befindet, wählen Sie mindestens ein privates Subnetz in Ihrer VPC. Bevor Sie Subnetze auswählen, überprüfen Sie die [Anforderungen und Überlegungen zu Subnetzen](#). Sie können sehen, welche Subnetze privat sind, indem Sie den jeweiligen Subnetzlink in der Registerkarte Networking (Netzwerk) Ihres Clusters öffnen.
6. Treffen Sie die gewünschte Auswahl auf der Seite Configure stack options (Stackoptionen konfigurieren) und wählen Sie dann Next (Weiter) aus.
 7. Aktivieren Sie das Kontrollkästchen links neben Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden. , und wählen Sie dann Stapel erstellen aus.

8. Wenn Ihr Stack fertig erstellt wurde, wählen Sie ihn in der Konsole aus und klicken Sie auf Outputs (Ausgaben).
9. Notieren Sie das `NodeInstanceRole` für die Knotengruppe, die erstellt wurde. Sie benötigen diese, wenn Sie Ihre Amazon-EKS--Arbeitsknoten konfigurieren.

Schritt 2: Ermöglichen Sie den Knoten, Ihrem Cluster beizutreten

1. Überprüfen Sie, ob Sie bereits über eine `aws-auth ConfigMap` verfügen.

```
kubectl describe configmap -n kube-system aws-auth
```

2. Wenn eine `aws-auth ConfigMap` angezeigt wird, aktualisieren Sie sie nach Bedarf.
 - a. Öffnen Sie `ConfigMap` zum Bearbeiten.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Fügen Sie nach Bedarf einen neuen `mapRoles`-Eintrag hinzu. Setzen Sie den `roleARN` Wert auf den `NodeInstanceRole` Wert, den Sie im vorherigen Verfahren aufgezeichnet haben.

```
[...]
data:
  mapRoles: |
    - roleARN: <ARN of instance role (not instance profile)>
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
[...]
```

- c. Speichern Sie die Datei und beenden Sie den Text-Editor.
3. Wenn die Fehlermeldung `Error from server (NotFound): configmaps "aws-auth" not found` angezeigt wird, wenden Sie die standardmäßige `ConfigMap` an.
 - a. Laden Sie die Konfigurationszuordnung herunter.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/
aws-auth-cm.yaml
```

- b. Stellen Sie in der `aws-auth-cm.yaml` Datei `rolearn` den `NodeInstanceRole`Wert ein, den Sie im vorherigen Verfahren aufgezeichnet haben. Hierzu können Sie einen Texteditor verwenden oder `my-node-instance-role` ersetzen und den folgenden Befehl ausführen:

```
sed -i.bak -e 's|<ARN of instance role (not instance profile)>|my-node-instance-role|' aws-auth-cm.yaml
```

- c. Wenden Sie die Konfiguration an. Die Ausführung dieses Befehls kann einige Minuten dauern.

```
kubectl apply -f aws-auth-cm.yaml
```

4. Sehen Sie sich den Status Ihrer Knoten an und warten Sie, bis diese in den Ready-Status eintreten.

```
kubectl get nodes --watch
```

Geben Sie `Ctrl+C` ein, um zu einer Shell-Eingabeaufforderung zurückzukehren.

Note

Wenn Sie Autorisierungs- oder Ressourcenfehler erhalten, finden Sie weitere Informationen unter [the section called “Nicht autorisiert oder Zugriff verweigert \(kubectl\)”](#) im Thema zur Fehlerbehebung.

Wenn Knoten dem Cluster nicht beitreten können, finden Sie weitere Informationen unter [the section called “Knoten können nicht mit dem Cluster verknüpft werden”](#) [Beheben von Problemen mit Amazon EKS-Clustern und -Knoten](#) und unter [Problembehandlung the section called “Knoten können nicht zu einem Cluster hinzugefügt werden”](#) bei lokalen Amazon EKS-Clustern auf AWS [Outposts](#).

5. Installieren Sie den Amazon-EBS-CSI-Treiber. Weitere Informationen finden Sie unter [Installation](#) am GitHub. Stellen Sie im Abschnitt Einrichten der Treiberberechtigung sicher, dass Sie die Anweisungen für die Option Verwenden des IAM-Instance-Profils befolgen. Sie müssen die gp2-Speicherklasse verwenden. Die gp3 Speicherklasse wird nicht unterstützt.

Führen Sie die folgenden Schritte aus, um eine gp2-Speicherklasse auf Ihrem Cluster zu erstellen.

- a. Führen Sie den folgenden Befehl aus, um die Datei `gp2-storage-class.yaml` zu erstellen.

```
cat >gp2-storage-class.yaml <<EOF
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
  name: ebs-sc
provisioner: ebs.csi.aws.com
volumeBindingMode: WaitForFirstConsumer
parameters:
  type: gp2
  encrypted: "true"
allowVolumeExpansion: true
EOF
```

b. Wenden Sie das Manifest auf Ihren Cluster an.

```
kubectl apply -f gp2-storage-class.yaml
```

6. (Nur GPU-Knoten) Wenn Sie einen GPU-Instance-Typ und ein für Amazon EKS optimiertes beschleunigtes AMI ausgewählt haben, müssen Sie das [NVIDIA-Geräte-Plug-In für Kubernetes](#) als DaemonSet auf Ihrem Cluster anwenden. Ersetzen Sie es `vX.X.X` durch die gewünschte [s-device-pluginNVIDIA/K8-Version](#), bevor Sie den folgenden Befehl ausführen.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/
deployments/static/nvidia-device-plugin.yml
```

Schritt 3: Zusätzliche Aktionen

1. (Optional) [???](#) Stellen Sie eine Beispielanwendung bereit, um Ihren Cluster und Ihre Linux-Worker-Knoten zu testen.
2. Wenn Ihr Cluster auf einem Outpost bereitgestellt wird, überspringen Sie diesen Schritt. Wenn Ihr Cluster in der AWS Cloud bereitgestellt wird, sind die folgenden Informationen optional. Wenn die von AmazonEKS_CNI_Policy verwaltete IAM-Richtlinie mit Ihrer [Amazon EKS-Knoten-IAM-Rolle verknüpft ist, empfehlen wir, sie stattdessen einer IAM-Rolle](#) zuzuweisen, die Sie dem Kubernetes-Servicekonto zuordnen. aws-node Weitere Informationen finden Sie unter [the section called "Für IRSA konfigurieren"](#).

Überblick über Machine Learning auf Amazon EKS

Amazon Elastic Kubernetes Service (EKS) ist eine verwaltete Kubernetes-Plattform, die es Unternehmen ermöglicht, KI- und ML-Workloads (Machine Learning) mit beispielloser Flexibilität und Kontrolle bereitzustellen, zu verwalten und zu skalieren. EKS basiert auf dem Open-Source-Kubernetes-Ökosystem und ermöglicht es Ihnen, Ihr vorhandenes Kubernetes-Fachwissen zu nutzen und sich gleichzeitig nahtlos in Open-Source-Tools und -Services zu integrieren. AWS

Ganz gleich, ob Sie groß angelegte Modelle trainieren, Online-Inferenzen in Echtzeit ausführen oder generative KI-Anwendungen einsetzen, EKS bietet die Leistung, Skalierbarkeit und Kosteneffizienz, die Ihre KI/ML-Projekte benötigen.

Warum sollten Sie sich für EKS für KI/ML entscheiden?

EKS ist eine verwaltete Kubernetes-Plattform, mit der Sie komplexe KI/ML-Workloads bereitstellen und verwalten können. Sie basiert auf dem Open-Source-Kubernetes-Ökosystem, lässt sich in AWS Dienste integrieren und bietet so die Kontrolle und Skalierbarkeit, die für fortgeschrittene Projekte erforderlich sind. Für Teams, die mit KI/ML-Implementierungen noch nicht vertraut sind, werden vorhandene Kubernetes-Fähigkeiten direkt übertragen, was eine effiziente Orchestrierung mehrerer Workloads ermöglicht.

EKS unterstützt alles, von Betriebssystemanpassungen bis hin zur Rechenskalierung, und seine Open-Source-Grundlage fördert technologische Flexibilität, sodass die Wahlmöglichkeiten für future Infrastrukturentscheidungen gewahrt bleiben. Die Plattform bietet die Leistungs- und Optimierungsoptionen, die für KI/ML-Workloads erforderlich sind, und unterstützt Funktionen wie:

- Vollständige Clusterkontrolle zur Feinabstimmung von Kosten und Konfigurationen ohne versteckte Abstraktionen
- Latenz von weniger als einer Sekunde für Inferenz-Workloads in Echtzeit in der Produktion
- Erweiterte Anpassungen wie Multi-Instance- und Multi-Cloud-Strategien GPUs und Tuning auf Betriebssystemebene
- Möglichkeit, Workloads mithilfe von EKS als einheitlichem Orchestrator für alle KI/ML-Pipelines zu zentralisieren

Wichtige Anwendungsfälle

Amazon EKS bietet eine robuste Plattform für eine Vielzahl von KI/ML-Workloads und unterstützt verschiedene Technologien und Bereitstellungsmuster:

- (Online-) Inferenz in Echtzeit: [EKS ermöglicht mithilfe von Tools wie Triton Inference Server und Amazon EC2 Inf1- und Inf2-Instances sofortige Vorhersagen zu eingehenden Daten TorchServe, z. B. zur Betrugserkennung, mit einer Latenz von weniger als einer Sekunde.](#) Diese Workloads profitieren von der dynamischen Skalierung mit [Karpenter](#) und [KEDA](#) und nutzen gleichzeitig [Amazon EFS](#) für das modellübergreifende Sharding. [Amazon ECR Pull Through Cache \(PTC\)](#) beschleunigt Modellaktualisierungen, und [Bottlerocket-Datenvolumes](#) mit [Amazon EBS-optimierten](#) Volumes sorgen für schnellen Datenzugriff.
- Allgemeines Modelltraining: [Organizations nutzen EKS, um komplexe Modelle mit großen Datensätzen über längere Zeiträume zu trainieren, indem sie die Kubeflow Training Operator \(KRO\), Ray Serve und Torch Distributed Elastic auf Amazon EC2 P4d- und Amazon Trn1-Instances verwenden. EC2 Diese Workloads werden durch Batch-Planung mit Tools wie Volcano, Unikorn und Kueue unterstützt. Amazon EFS ermöglicht die gemeinsame Nutzung von Modellprüfpunkten, und Amazon S3 übernimmt den Modellimport/-export mit Lebenszyklusrichtlinien für die Versionsverwaltung.](#)
- RAG-Pipelines (Retrieval Augmented Generation): EKS verwaltet Chatbots und ähnliche Anwendungen für den Kundensupport, indem es Abruf- und Generierungsprozesse integriert. [Diese Workloads verwenden häufig Tools wie Argo Workflows und Kubeflow für die Orchestrierung, Vektordatenbanken wie Pinecone, Weaviate oder Amazon und stellen Anwendungen Benutzern über den Application Load OpenSearch Balancer Controller \(LBC\) zur Verfügung. NVIDIA NIM optimiert die GPU-Auslastung, während Prometheus und Grafana die Ressourcennutzung überwachen.](#)
- Einsatz generativer KI-Modelle: [Unternehmen setzen mithilfe von Ray Serve, vLLM und Triton Inference Server auf Amazon EC2 G5 - und Inferentia-Beschleunigern Dienste zur Erstellung von Inhalten in Echtzeit auf EKS ein, z. B. Text- oder Bildgenerierung.](#) Diese Implementierungen optimieren die Leistung und die Speichernutzung für groß angelegte Modelle. [JupyterHub](#) ermöglicht iterative Entwicklung, [Gradio](#) bietet einfache Weboberflächen und der [S3 Mountpoint CSI-Treiber](#) ermöglicht das Mounten von S3-Buckets als Dateisysteme für den Zugriff auf große Modelldateien.
- Batch- (Offline-) Inferenz: [Organizations verarbeiten große Datenmengen effizient durch geplante Jobs mit AWS Batch oder Volcano.](#) Diese Workloads verwenden häufig [Inf1- und EC2 Inf2-Instances](#) für AWS [Inferentia-Chips](#), Amazon EC2 [G4dn-Instances](#) für NVIDIA T4 oder [c5-](#)

und c6i-CPU-Instances GPUs, wodurch die Ressourcennutzung außerhalb der Spitzenzeiten für Analyseaufgaben maximiert wird. Das AWS Neuron SDK und die NVIDIA-GPU-Treiber optimieren die Leistung, während MIG/TS die gemeinsame Nutzung von GPU ermöglicht. Zu den Speicherlösungen gehören Amazon S3 und Amazon EFS sowie FSx für Lustre mit CSI-Treibern für verschiedene Speicherklassen. Das Modellmanagement nutzt Tools wie Kubeflow Pipelines, Argo Workflows und Ray Cluster, während die Überwachung von Prometheus, Grafana und benutzerdefinierten Modellüberwachungstools übernommen wird.

Fallstudien

Kunden entscheiden sich aus verschiedenen Gründen für Amazon EKS, z. B. um die GPU-Nutzung zu optimieren oder Inferenz-Workloads in Echtzeit mit Latenz unter einer Sekunde auszuführen, wie in den folgenden Fallstudien gezeigt wird. Eine Liste aller Fallstudien für Amazon EKS finden Sie unter [AWS Kundenerfolgsgeschichten](#).

- [Unitary](#) verarbeitet täglich 26 Millionen Videos mithilfe von KI für die Moderation von Inhalten, was Inferenzen mit hohem Durchsatz und geringer Latenz erfordert, und hat die Startzeiten von Containern um 80% reduziert, sodass bei schwankendem Datenverkehr schnell auf Skalierungsereignisse reagiert werden kann.
- [Miro](#), die Plattform für visuelle Zusammenarbeit, die 70 Millionen Benutzer weltweit unterstützt, verzeichnete eine Senkung der Rechenkosten um 80% im Vergleich zu ihren früheren selbstverwalteten Kubernetes-Clustern.
- [Synthesia](#), das generative KI-Videoerstellung als Service für Kunden anbietet, um realistische Videos anhand von Textansagen zu erstellen, erzielte eine 30-fache Verbesserung des Durchsatzes beim Training mit ML-Modellen.
- [Harri, Anbieter von HR-Technologie für das Gastgewerbe, erzielte als Reaktion auf Nachfragespitzen eine um 90% schnellere Skalierung und senkte seine Rechenkosten durch die Migration auf Graviton-Prozessoren um 30%.AWS](#)
- [Ada Support](#), ein KI-gestütztes Unternehmen für Kundenservice-Automatisierung, erzielte eine Senkung der Rechenkosten um 15% bei gleichzeitiger Steigerung der Recheneffizienz um 30%.
- [Snorkel AI](#), das Unternehmen in die Lage versetzt, Basismodelle und umfangreiche Sprachmodelle zu entwickeln und anzupassen, erzielte durch die Implementierung intelligenter Skalierungsmechanismen für ihre GPU-Ressourcen Kosteneinsparungen von über 40%

Beginnen Sie mit der Nutzung von Machine Learning auf EKS

Um mit der Planung und Nutzung von Plattformen und Workloads für Machine Learning auf EKS in der AWS Cloud zu beginnen, fahren Sie mit dem [the section called “Fangen Sie mit ML an”](#) Abschnitt fort.

Erste Schritte mit ML

Um in Machine Learning auf EKS einzusteigen, wählen Sie zunächst eines dieser präskriptiven Muster aus, um schnell einen EKS-Cluster sowie ML-Software und -Hardware für die Ausführung von ML-Workloads vorzubereiten. Die meisten dieser Muster basieren auf Terraform-Blueprints, die auf der Website [Data on Amazon](#) EKS verfügbar sind. Bevor Sie beginnen, sollten Sie einige Dinge beachten:

- GPUs oder Neuron-Instanzen sind erforderlich, um diese Prozeduren auszuführen. Mangelnde Verfügbarkeit dieser Ressourcen kann dazu führen, dass diese Verfahren bei der Clustererstellung oder der automatischen Knotenskalierung fehlschlagen.
- Neuron SDK (Trainium- und Inferentia-basierte Instances) kann Geld sparen und ist verfügbarer als NVIDIA. GPUs Wenn Ihre Workloads dies zulassen, empfehlen wir Ihnen, die Verwendung von Neuron für Ihre Machine Learning Learning-Workloads in Betracht zu ziehen (siehe [Willkommen AWS bei Neuron](#)).
- Für einige der ersten Erfahrungen hier ist es erforderlich, dass Sie Daten über Ihr eigenes [Hugging Face Face-Konto](#) abrufen.

Wählen Sie zunächst eines der folgenden Muster aus, die Ihnen den Einstieg in die Infrastruktur für die Ausführung Ihrer Machine Learning Learning-Workloads erleichtern sollen:

- [JupyterHub auf EKS](#): Erkunden Sie den [JupyterHub Blueprint](#), in dem Time Slicing- und MIG-Funktionen sowie mandantenfähige Konfigurationen mit Profilen vorgestellt werden. Dies ist ideal für die Bereitstellung großer JupyterHub Plattformen auf EKS.
- [Große Sprachmodelle auf AWS Neuron und RayServe](#): Verwenden Sie [AWS Neuron](#), um große Sprachmodelle (LLMs) auf Amazon EKS und AWS Trainium- und Inferentia-Beschleunigern auszuführen. AWS Anweisungen zum Einrichten einer Plattform für Inferenzanfragen [LLMs mit folgenden Komponenten finden Sie unter Serving with RayServe und vLLM AWS on Neuron](#)
 - AWS Neuron SDK-Toolkit für Deep Learning
 - AWS Inferentia- und Trainium-Beschleuniger

- [vLLM — Sprachmodell mit variabler Länge \(siehe die vLLM-Dokumentationsseite\)](#)
- RayServe Bibliothek zur Bereitstellung skalierbarer Modelle (siehe Website [Ray Serve: Scalable and Programmable Serving](#))
- Llama-3-Sprachmodell mit Ihrem eigenen [Hugging](#) Face Face-Konto.
- Beobachtbarkeit mit einem Neuron Monitor AWS CloudWatch
- WebUI öffnen
- [Große Sprachmodelle auf NVIDIA und Triton](#): Stellen Sie mehrere große Sprachmodelle (LLMs) auf Amazon EKS und NVIDIA GPUs bereit. Anweisungen zum Einrichten einer Plattform für Inferenzanfragen [mit folgenden Komponenten finden Sie unter Bereitstellen mehrerer großer Sprachmodelle mit NVIDIA Triton Server und vLLM](#)
- [NVIDIA Triton Inference Server \(siehe die Triton Inference Server-Website\)](#) GitHub
- [vLLM — Sprachmodell mit variabler Länge \(siehe die vLLM-Dokumentationsseite\)](#)
- Zwei Sprachmodelle: mistralai/Mistral-7B-Instruct-v0.2 and meta-llama/Llama -2-7b-chat-hf, mit deinem eigenen [Hugging](#) Face Face-Konto.

Weiter mit ML auf EKS

Neben der Auswahl aus den auf dieser Seite beschriebenen Blueprints gibt es auch andere Möglichkeiten, wie Sie die Dokumentation zu ML on EKS durchgehen können, wenn Sie dies bevorzugen. Beispielsweise ist Folgendes möglich:

- Probieren Sie Tutorials für ML auf EKS aus — Führen Sie andere end-to-end Tutorials zum Erstellen und Ausführen Ihrer eigenen Machine-Learning-Modelle auf EKS durch. Siehe [the section called “Probieren Sie Tutorials für ML auf EKS aus”](#).

Informationen zur Verbesserung Ihrer Arbeit mit ML auf EKS finden Sie in den folgenden Abschnitten:

- Bereiten Sie sich auf ML vor — Erfahren Sie, wie Sie sich mit Funktionen wie benutzerdefinierten Reservierungen AMLs und GPU-Reservierungen auf ML auf EKS vorbereiten können. Siehe [the section called “Bereiten Sie sich auf ML vor”](#).

Bereiten Sie sich auf ML-Cluster vor

Es gibt Möglichkeiten, wie Sie Ihre Erfahrung mit Machine Learning auf EKS verbessern können. Die folgenden Seiten in diesem Abschnitt helfen Ihnen dabei:

- Machen Sie sich mit Ihren Optionen für die Verwendung von ML auf EKS vertraut und
- Hilfe bei der Vorbereitung Ihrer EKS- und ML-Umgebung.

Dies wird Ihnen insbesondere helfen:

- Wählen Sie AMIs: AWS bietet mehrere maßgeschneiderte Lösungen AMIs für die Ausführung von ML-Workloads auf EKS. Siehe [the section called “Führen Sie Linux GPU aus AMIs”](#) und [the section called “Führen Sie Windows GPU aus AMIs”](#).
- Anpassen AMIs: Sie können die AWS benutzerdefinierte Version weiter modifizieren AMIs , um weitere Software und Treiber hinzuzufügen, die Sie für Ihre speziellen Anwendungsfälle benötigen. Siehe [the section called “Reservieren Sie GPUs für SMN”](#).
- Reservieren GPUs: Aufgrund der Nachfrage können GPUs Sie die benötigten Artikel im Voraus reservieren GPUs, um sicherzustellen, dass die von Ihnen benötigten Artikel zur Verfügung stehen, wenn GPUs Sie sie benötigen. Siehe [the section called “Verfälschen Sie GPU-Knoten”](#).
- EFA hinzufügen: Fügen Sie den Elastic Fabric-Adapter hinzu, um die Netzwerkleistung für die Cluster-Kommunikation zwischen Knoten zu verbessern. Siehe [the section called “Trainingscluster mit EFA”](#).
- AWSInferentia Workloads verwenden: Erstellen Sie einen EKS-Cluster mit Amazon EC2 Inf1-Instances. Siehe [the section called “Bereiten Sie Inferentia-Cluster vor”](#).

Themen

- [GPU-beschleunigte Container ausführen \(Linux auf\) EC2](#)
- [GPU-beschleunigte Container ausführen \(Windows auf G-Series\) EC2](#)
- [Erstellen Sie eine verwaltete Knotengruppe mit Capacity Blocks for ML](#)
- [Erstellen Sie selbstverwaltete Knoten mit Capacity Blocks for ML](#)
- [Verhindern, dass Pods auf bestimmten Knoten geplant werden](#)
- [Führen Sie Machine-Learning-Schulungen auf Amazon EKS mit Elastic Fabric Adapter durch](#)
- [Verwenden Sie AWS Inferentia-Instances mit Amazon EKS für Machine Learning](#)

GPU-beschleunigte Container ausführen (Linux auf) EC2

Das für Amazon EKS optimierte beschleunigte Amazon Linux AMIs basiert auf dem standardmäßigen Amazon EKS-optimierten Amazon Linux AMIs. Einzelheiten zu diesen finden AMIs Sie unter [the section called “Amazon EKS hat Amazon Linux optimiert und beschleunigt AMIs”](#). Im folgenden Text wird beschrieben, wie AWS Neuron-basierte Workloads aktiviert werden.

Um auf AWS Neuron (ML Accelerator) basierende Workloads zu aktivieren

Einzelheiten zu Trainings- und Inferenz-Workloads mit Neuron in Amazon EKS finden Sie in den folgenden Referenzen:

- [Container — Kubernetes — Erste Schritte](#) in der Neuron-Dokumentation AWS
- [Schulung](#) mit AWS Neuron EKS-Proben am GitHub
- [Bereitstellen von ML-Inferenz-Workloads AWSInferentia auf Amazon EKS](#)

Das folgende Verfahren beschreibt, wie Sie einen Workload auf einer GPU-basierten Instance mit Amazon EKS optimierter und beschleunigter Ausführung ausführen AMIs.

1. Nachdem Ihre GPU-Knoten Ihrem Cluster beigetreten sind, müssen Sie das [NVIDIA-Geräte-Plug-In für Kubernetes](#) als DaemonSet auf Ihrem Cluster anwenden. Ersetzen Sie es `vX.X.X` durch die gewünschte [s-device-pluginNVIDIA/K8-Version](#), bevor Sie den folgenden Befehl ausführen.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/
deployments/static/nvidia-device-plugin.yml
```

2. Mit dem folgenden Befehl können Sie überprüfen, ob Ihre Knoten über GPUs Allocatable verfügen.

```
kubectl get nodes "-o=custom-
columns=NAME:.metadata.name,GPU:.status.allocatable.nvidia\.com/gpu"
```

3. Erstellen Sie eine Datei mit dem Namen `nvidia-smi.yaml` und dem folgenden Inhalt. [Ersetzen Sie es `tag` durch das gewünschte Tag für `nvidia/cuda`](#). Dieses Manifest startet einen [NVIDIA CUDA-Container](#), der auf einem Knoten ausgeführt wird. `nvidia-smi`

```
apiVersion: v1
kind: Pod
metadata:
  name: nvidia-smi
```

```
spec:
  restartPolicy: OnFailure
  containers:
  - name: nvidia-smi
    image: nvidia/cuda:tag
    args:
    - "nvidia-smi"
    resources:
      limits:
        nvidia.com/gpu: 1
```

4. Wenden Sie das Manifest mit dem folgenden Befehl an.

```
kubectl apply -f nvidia-smi.yaml
```

5. Nachdem der Pod fertig ausgeführt wurde, können Sie seine Protokolle mit dem folgenden Befehl anzeigen.

```
kubectl logs nvidia-smi
```

Eine Beispielausgabe sieht wie folgt aus.

```
Mon Aug  6 20:23:31 20XX
+-----+
| NVIDIA-SMI  XXX.XX                Driver Version:  XXX.XX                |
+-----+-----+-----+-----+-----+-----+
| GPU  Name            Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
|=====+=====+=====+=====+=====+=====+
|   0   Tesla V100-SXM2...    On   | 00000000:00:1C.0 Off  |                 0    |
| N/A   46C    P0      47W / 300W |  0MiB / 16160MiB |      0%    Default  |
+-----+-----+-----+-----+-----+-----+
+-----+
| Processes:                                                       GPU Memory |
|  GPU       PID    Type    Process name                       Usage    |
+-----+-----+-----+-----+-----+-----+
| No running processes found                                         |
+-----+
```

GPU-beschleunigte Container ausführen (Windows auf G-Series) EC2

Important

Das [Kubernetes Device Plugin für DirectX](#) von TensorWorks ist ein Drittanbieter-Tool, das nicht von empfohlen, unterstützt oder verwaltet wird. AWS übernimmt keine Verantwortung für die Sicherheit, Zuverlässigkeit oder Leistung dieses Plugins.

Erfahren Sie, wie Sie GPU-beschleunigte Windows-Container-Workloads auf Amazon EKS (Elastic Kubernetes Service) mithilfe von NVIDIA GPUs mit dem Kubernetes Device Plugin für DirectX von ausführen. TensorWorks Weitere Informationen finden Sie unter [Kubernetes Device Plugin für DirectX](#).

Es gibt zwei Hauptansätze für die Einrichtung der GPU-Beschleunigung für Ihre Windows-Container:

- Option 1: [Erstellen Sie ein benutzerdefiniertes für Windows optimiertes EKS-AMI](#) mit den erforderlichen vorinstallierten GPU-Treibern.
 - Verwenden Sie diesen Ansatz, wenn Sie eine konsistente, vorkonfigurierte Umgebung benötigen, in der GPU-beschleunigte Windows-Container ausgeführt werden können, und Sie den zusätzlichen Aufwand in die Erstellung und Wartung des benutzerdefinierten AMI investieren können.
- Option 2: Installieren Sie nach dem Start Ihrer Instance die erforderlichen GPU-Treiber auf Ihren EKS-Worker-Knoten.
 - Verwenden Sie diesen Ansatz, wenn Sie einen einfacheren Einrichtungsprozess wünschen und es Ihnen nichts ausmacht, die GPU-Treiber auf jedem neuen Worker-Knoten zu installieren. Eher für eine Entwicklungsumgebung geeignet, wenn Sie GPU-beschleunigte Workloads evaluieren oder Prototypen entwickeln.

Beide Ansätze können mithilfe der in diesem Handbuch beschriebenen Schritte genutzt werden.

Überlegungen

Dieses Handbuch enthält Schritte zur Installation und Einrichtung der GPU-Beschleunigung für Ihre Windows-Container mithilfe von NVIDIA GPUs, NVIDIA GRID-Treibern und dem [Kubernetes Device Plugin für DirectX](#) von. TensorWorks Die Schritte wurden getestet und verifiziert, um GPU-Beschleunigung für Ihre Windows-Container-Workloads auf Amazon EKS bereitzustellen. [the section](#)

[called “Bekannte Beschränkungen”](#) Weitere Informationen zu kompatiblen Treibern und Geräte-Plugins finden Sie unter. Bevor Sie fortfahren, beachten Sie Folgendes:

- Nur Instance-Typen der G-Familie mit [NVIDIA GRID-Treibern](#) wurden getestet und verifiziert, dass sie mit diesem Handbuch funktionieren. Andere Instance-Typen und Treiberkombinationen können zwar auch GPU-beschleunigte Windows-Container ausführen, sie erfordern jedoch möglicherweise zusätzliche Konfigurationsschritte, die in diesem Handbuch nicht behandelt werden.
- Nur DirectX-basierte Workloads wurden getestet und verifiziert, dass sie mit diesem Handbuch funktionieren. Während andere GPUs APIs wie OpenGL, Vulkan und OpenCL möglicherweise kompatibel sind, um GPU-beschleunigte Windows-Container auszuführen, erfordern sie möglicherweise zusätzliche Konfigurationsschritte, die in diesem Handbuch nicht behandelt werden.
- Es gibt einige bekannte Einschränkungen, die Sie beachten sollten, bevor Sie GPU-beschleunigte Windows-Container ausführen. Weitere Informationen finden Sie im [the section called “Bekannte Beschränkungen”](#) Abschnitt.

Voraussetzungen

Um die GPU-Beschleunigung für Ihre Windows-Container auf Amazon EKS zu aktivieren, müssen Sie die folgenden Anforderungen vorbereiten, bevor Sie fortfahren:

- Starten Sie einen Amazon EKS-Cluster mit Kubernetes v1.27 oder neuer.
- Stellen Sie Windows-Knoten mit Windows Server 2022 oder neuer bereit.
- [Stellen Sie Windows-Knoten der Instance-Typen der G-Familie bereit, z. B. G4 oder G5.](#)
- Stellen Sie Windows-Knoten eine Container-Runtime mit containerd 1.7.x oder 2.x.x bereit. (Informationen [the section called “Versionsinformationen abrufen”](#) zur Überprüfung der Container-Version in Ihrem Amazon EKS-optimierten AMI finden Sie unter.)

Installieren Sie den GPU-Treiber auf jedem Windows-Worker-Knoten

Um die NVIDIA GRID-Treiber auf Ihren EKS-Worker-Knoten zu installieren, folgen Sie den Schritten unter [NVIDIA-Treiber für Ihre EC2 Amazon-Instance](#). Navigieren Sie zu [Installationsoptionen — Option 3: GRID-Treiber](#) und folgen Sie den Installationsschritten.

Für Windows Server Core installieren

Für Windows Server Core, das kein Desktop-Erlebnis bietet, installieren Sie NVIDIA GRID-Treiber im Hintergrund mit den folgenden Befehlen:

```
$nvidiaInstallerFilePath = nvidia-driver-installer.exe # Replace with path to installer
$installerArguments = "-s -clean -noreboot -noeula"
Start-Process -FilePath $nvidiaInstallerFilePath -ArgumentList $installerArguments -
Wait -NoNewWindow -PassThru
```

Überprüfen Sie Ihre Installation

Führen Sie den folgenden PowerShell Befehl aus, um Diagnoseinformationen GPUs zur Instanz anzuzeigen:

```
nvidia-smi
```

Mit diesem Befehl werden die NVIDIA-Treiberversion sowie Informationen zur GPU-Hardware angezeigt. Stellen Sie sicher, dass die Ausgabe dieses Befehls der NVIDIA GRID-Treiberversion entspricht, die Sie voraussichtlich installiert haben.

Stellen Sie das GPU-Geräte-Plugin auf jedem Knoten bereit

Um die Erkennung und Bereitstellung der GPU-Ressourcen in Containern auf Ihren Windows-Knoten zu ermöglichen, benötigen Sie ein Geräte-Plug-In. Stellen Sie das [DirectX Device Plugin](#) von Tensorworks auf jedem Worker-Knoten bereit, indem Sie es als DaemonSet in Ihrem EKS-Cluster ausführen. Folgen Sie der in der [README.md](#) angegebenen Installationsanleitung, die die folgenden Schritte umfasst. Es wird empfohlen:

- Stellen Sie das Geräte-Plugin im kube-system Namespace bereit.
- Legen Sie entsprechende Ressourcenlimits für das fest DaemonSet , um sicherzustellen, dass es keine übermäßigen Ressourcen auf Ihren Knoten verbraucht.

Note

Das Geräte-Plug-In DaemonSet wird auf jedem Knoten als Host-Prozesscontainer mit erhöhten Rechten ausgeführt. Es wird empfohlen, RBAC-Steuerungen zu implementieren, um den Zugriff darauf einzuschränken, DaemonSet sodass nur autorisierte Benutzer privilegierte Befehle ausführen können.

Beim Ausführen von GPU-beschleunigten Containern unterstützt das Geräte-Plugin zwei Modi:

- **Single-Tenancy-Modus:** In diesem Modus werden alle GPU-Ressourcen einem einzelnen Container auf der Instance zugewiesen. Installieren Sie die Geräte-Plugins mit Single-Tenancy-Unterstützung mithilfe des folgenden Befehls. Weitere Informationen finden Sie unter README.md.

```
kubectl apply -f "https://raw.githubusercontent.com/TensorWorks/directx-device-plugins/main/deployments/default-daemonsets.yml"
```

- **Mehrmandantenmodus:** Dieser Modus ermöglicht die gemeinsame Nutzung von GPU-Ressourcen durch mehrere Container auf der Instance. Installieren Sie die Geräte-Plugins mit Multi-Tenancy-Unterstützung mit dem folgenden Befehl. Weitere Informationen finden Sie unter README.md.

```
kubectl apply -f "https://raw.githubusercontent.com/TensorWorks/directx-device-plugins/main/deployments/multitenancy-inline.yml"
```

Verwenden Sie alternativ a, um die ConfigMap Mehrmandantenfähigkeit anzugeben.

```
kubectl apply -f "https://raw.githubusercontent.com/TensorWorks/directx-device-plugins/main/deployments/multitenancy-configmap.yml"
```

Die Bereitstellung des Geräte-Plug-ins wird überprüft

Nachdem Sie das Geräte-Plug-In bereitgestellt haben, ersetzen Sie den folgenden Befehl `<namespace>` und führen Sie ihn aus, um sicherzustellen, dass das DirectX-Geräte-Plug-In auf all Ihren Windows-Knoten ordnungsgemäß ausgeführt wird.

```
kubectl get ds device-plugin-wddm -n <namespace>
```

Es wird überprüft, ob die Container bereit für die Bereitstellung sind

Sobald das Geräte-Plug-In auf den GPU-betriebenen Windows-Worker-Knoten ausgeführt wird, überprüfen Sie mit dem folgenden Befehl, ob für jeden Knoten eine Zuweisung möglich ist. GPUs Die entsprechende Zahl sollte der Anzahl der DirectX-Geräte auf jedem Knoten entsprechen.

```
kubectl get nodes "-o=custom-columns=NAME:.metadata.name,DirectX:.status.allocatable.directx\.microsoft\.com/display"
```

Windows-Container mit GPU-Beschleunigung ausführen

Bevor Sie Ihre Pods starten, geben Sie den Ressourcennamen in `an.directx.microsoft.com/display.spec.containers[].resources`. Dies weist darauf hin, dass Ihre Container GPU-fähige Funktionen benötigen, und `kube-scheduler` werden versuchen, Ihre Pods auf Ihrem vorkonfigurierten Windows-Knoten mit verfügbaren GPU-Ressourcen zu platzieren.

Sehen Sie sich als Beispiel den folgenden Beispielbefehl an, der `a` startet, Job um eine Monte-Carlo-Simulation auszuführen, um den Wert von Pi zu schätzen. Dieses Beispiel stammt aus dem GitHub Repository [Kubernetes Device Plugins for DirectX](#), das [mehrere Beispiele](#) zur Auswahl hat, die Sie ausführen können, um die GPU-Fähigkeiten Ihres Windows-Knotens zu testen.

```
cat <<EOF | kubectl apply -f -
apiVersion: batch/v1
kind: Job
metadata:
  name: example-cuda-montecarlo-wddm
spec:
  template:
    spec:
      containers:
      - name: example-cuda-montecarlo-wddm
        image: "index.docker.io/tensorworks/example-cuda-montecarlo:0.0.1"
        resources:
          limits:
            directx.microsoft.com/display: 1
      nodeSelector:
        "kubernetes.io/os": windows
      restartPolicy: Never
    backoffLimit: 0
EOF
```

Bekannte Beschränkungen

Alle sind nutzbar GPUs

Alle GPUs auf der Instance befindlichen Container können von jedem laufenden Container auf dem Host verwendet werden, auch wenn Sie eine bestimmte Anzahl von GPUs für einen bestimmten Container anfordern. Darüber hinaus ist das Standardverhalten, dass alle Container, die auf dem Host ausgeführt werden, die GPU mit dem Index 0 verwenden, auch wenn mehrere auf dem Knoten GPUs verfügbar sind. Damit Aufgaben mit mehreren GPUs ordnungsgemäß ausgeführt werden

können, müssen Sie das spezifische GPU-Gerät, das im Code Ihrer Anwendung verwendet werden soll, explizit angeben.

Die genaue Implementierung, mit der ein Gerät für die Anwendung zugewiesen wird, hängt von der verwendeten Programmiersprache oder dem verwendeten Framework ab. Wenn Sie beispielsweise die CUDA-Programmierung verwenden, um eine bestimmte GPU auszuwählen, können Sie das Gerät, das in Ihrem Anwendungscode verwendet werden soll, mithilfe der Funktion [cudaSetDevice\(\)](#) explizit angeben.

Die Notwendigkeit, das Gerät explizit anzugeben, ist auf ein bekanntes Problem zurückzuführen, das Windows-Container betrifft. Sie können den Fortschritt bei der Lösung dieses Problems in der [Microsoft/Windows-Container-Ausgabe #333](#) nachverfolgen. Die folgende Tabelle stellt eine visuelle Darstellung und ein praktisches Beispiel für dieses Verhalten bei der GPU-Zuweisung dar.

Stellen Sie sich ein Szenario vor, in dem es einen einzelnen Windows-Knoten vom EC2 Instanztyp `g4dn.12xlarge`, der aus vier besteht GPUs. Stellen Sie sich ein Szenario vor, in dem drei Pods auf dieser Instanz gestartet werden. Die Tabelle zeigt, dass unabhängig von der Anzahl der von jedem Container GPUs angeforderten Pods alle drei Pods Zugriff auf alle vier GPUs auf der Instance haben und standardmäßig die GPU mit dem Geräteindex 0 verwenden.

Pod	Angefragt GPUs	Tatsächlicher GPU-Zugriff	Standard-GPU-Nutzung	Verfügbare GPU-Indizes	Instanz insgesamt GPUs
Kapsel 1	1 GPU	Alle 4 GPUs	GPU mit Index 0	0, 1, 2, 3	4
Kapsel 2	2 GPUs	Alle 4 GPUs	GPU mit Index 0	0, 1, 2, 3	4
Kapsel 3	1 GPU	Alle 4 GPUs	GPU mit Index 0	0, 1, 2, 3	4

Unterstützung für Kubernetes-Geräte-Plugins

Die offizielle Implementierung des [Kubernetes-Geräte-Plugins von NVIDIA unterstützt Windows](#) nicht. Sie können den Fortschritt beim Hinzufügen der offiziellen Windows-Unterstützung in der [NVIDIA/K8s-Ausgabe #419 s-device-plugin](#) verfolgen.

Einschränkungen der GPU-Recheninstanz

Abhängig von Ihrer AWS Kontokonfiguration gelten möglicherweise Servicebeschränkungen für die Anzahl und Art der Amazon EC2 GPU-Recheninstanzen, die Sie starten können. Wenn Sie zusätzliche Kapazität benötigen, können Sie [eine Erhöhung des Kontingents beantragen](#).

Muss ein GPU-optimiertes Windows-AMI erstellen

Es gibt keine verwaltete EKS-Komponente für Windows GPU Optimized AMI oder EC2 Image Builder, die von Amazon EKS bereitgestellt werden. Sie müssen die Schritte in diesem Handbuch befolgen, um ein benutzerdefiniertes Windows-optimiertes EKS-AMI mit den erforderlichen GPU-Treibern zu erstellen, oder die erforderlichen GPU-Treiber nach dem Start Ihrer Instances auf Ihren EKS-Worker-Knoten installieren.

Inferentia und Trainium werden nicht unterstützt

AWS Workloads, die auf [Inferentia](#) und AWS [Trainium](#) basieren, werden unter Windows nicht unterstützt.

Erstellen Sie eine verwaltete Knotengruppe mit Capacity Blocks for ML

Kapazitätsblöcke für Machine Learning (ML) ermöglichen es Ihnen, GPU-Instances zu einem zukünftigen Zeitpunkt zu reservieren, um Ihre ML-Workloads mit kurzer Dauer zu unterstützen. Weitere Informationen finden Sie unter [Capacity Blocks for ML](#) im EC2 Amazon-Benutzerhandbuch für Linux-Instances.

Überlegungen

Important

- Kapazitätsblöcke sind nur für bestimmte EC2 Amazon-Instance-Typen und AWS Regionen verfügbar. Informationen zur Kompatibilität finden Sie unter [Voraussetzungen für das Arbeiten mit Kapazitätsblöcken](#) im EC2 Amazon-Benutzerhandbuch für Linux-Instances.
- Weitere Informationen finden Sie unter [Verwenden von Kapazitätsblöcken für Machine-Learning-Workloads](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Verwaltete Knotengruppen mit Kapazitätsblöcken können nur mit benutzerdefinierten Startvorlagen erstellt werden.

- Wenn Sie verwaltete Knotengruppen mit Kapazitätsblöcken aktualisieren, stellen Sie sicher, dass die gewünschte Größe der Knotengruppe auf eingestellt ist0.

Erstellen Sie eine verwaltete Knotengruppe mit Amazon EC2 Capacity Blocks

Sie können Capacity Blocks mit von Amazon EKS verwalteten Knotengruppen für die Bereitstellung und Skalierung von GPU-beschleunigten Worker-Knoten verwenden. Die folgenden AWS CloudFormation Vorlagenbeispiele decken nicht alle Aspekte ab, die in Produktionsclustern benötigt werden. In der Regel benötigen Sie auch ein Bootstrapping-Skript, um den Knoten mit dem Cluster zu verbinden und ein Amazon EKS-beschleunigtes AML anzugeben. Weitere Informationen finden Sie unter [the section called "Erstellen"](#).

1. Erstellen Sie eine Startvorlage, die für Ihre Workloads geeignet ist und mit von Amazon EKS verwalteten Knotengruppen funktioniert. Weitere Informationen finden Sie unter [the section called "Startvorlagen"](#).

Stellen Sie zusätzlich zu den Anforderungen in den oben genannten Verfahren sicher, dass Folgendes Folgendes LaunchTemplateData umfasst:

- InstanceMarketOptions mit der Einstellung "capacity-block" für MarketType
- CapacityReservationSpecification: CapacityReservationTarget mit CapacityReservationId Einstellung auf den Capacity-Block (zum Beispiel: `cr-02168da1478b509e0`)
- InstanceType auf einen Instance-Typ gesetzt, der Capacity-Blöcke unterstützt (zum Beispiel: `p5.48xlarge`)

Im Folgenden finden Sie einen Auszug aus einer CloudFormation Vorlage, mit der eine Startvorlage für einen Kapazitätsblock erstellt wird. Um eine benutzerdefinierte AML-verwaltete Knotengruppe zu erstellen, können Sie ImageId auch UserData Parameter hinzufügen.

```
NodeLaunchTemplate:
  Type: "AWS::EC2::LaunchTemplate"
  Properties:
    LaunchTemplateData:
      InstanceMarketOptions:
        MarketType: "capacity-block"
      CapacityReservationSpecification:
        CapacityReservationTarget:
```

```
CapacityReservationId: "cr-02168da1478b509e0"  
InstanceType: p5.48xlarge
```

2. Verwenden Sie die Startvorlage, um eine verwaltete Knotengruppe zu erstellen.

Im Folgenden finden Sie ein Beispiel für den Befehl zum Erstellen einer Knotengruppe für Kapazitätsblöcke. *example-values* Ersetzen Sie sie durch diejenigen, die für Ihren Cluster gelten.

Gehen Sie beim Erstellen der verwalteten Knotengruppe Capacity Block wie folgt vor:

- Legen Sie den Wert für `capacity-type` auf `"CAPACITY_BLOCK"` fest. Wenn der Kapazitätstyp nicht auf `"CAPACITY_BLOCK"` oder einer der anderen oben genannten erforderlichen Werte für die Startvorlage fehlt, wird die Erstellungsanforderung abgelehnt.
- Achten Sie bei der Angabe `subnets` in der Erstellungsanforderung darauf, nur das Subnetz in derselben Availability Zone wie die Kapazitätsreservierung anzugeben.
- Wenn Sie `desiredSize` in der Erstellungsanforderung einen Wert ungleich Null angeben, berücksichtigt Amazon EKS dies bei der Erstellung der Auto Scaling Scaling-Gruppe (ASG). Wenn die Erstellungsanforderung jedoch gestellt wird, bevor die Kapazitätsreservierung aktiv ist, kann die ASG EC2 Amazon-Instances erst starten, wenn sie aktiv wird. Infolgedessen wird es bei ASG-Skalierungsaktivitäten zu Startfehlern kommen. Immer wenn die Reservierung aktiv wird, ist der Start der Instances erfolgreich und die ASG wird auf die bei der `desiredSize` Erstellung angegebene Größe hochskaliert.

```
aws eks create-nodegroup \  
  --cluster-name my-cluster \  
  --nodegroup-name my-mng \  
  --node-role node-role-arn \  
  --region region-code \  
  --subnets subnet-id \  
  --scaling-config minSize=node-group-min-size,maxSize=node-group-max-  
size,desiredSize=node-group-desired-size \  
  --ami-type "AL2023_x86_64_NVIDIA" \  
  --capacity-type "CAPACITY_BLOCK" \  
  --launch-template id="lt-id",version=1
```

3. Stellen Sie sicher, dass sich die Knoten nach der Skalierung verbinden. Amazon EKS-Cluster, die verwaltete Knotengruppen mit Kapazitätsblöcken verwenden, führen keine Überprüfungen durch, ob gestartete Instances tatsächlich dem Cluster beitreten und sich dort registrieren.

4. Wenn Sie 0 bei der Erstellung `desiredSize` die Option auswählen, haben Sie verschiedene Optionen, um die Knotengruppe zu vergrößern, wenn die Kapazitätsreservierung aktiv wird:
 - Erstellen Sie eine geplante Skalierungsrichtlinie für die ASG, die sich an der Startzeit der Kapazitätsblockreservierung orientiert. Weitere Informationen finden Sie unter [Geplante Skalierung für Amazon EC2 Auto Scaling](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
 - Verwenden Sie die Amazon EKS-Konsole oder `eks update-nodegroup-config` aktualisieren Sie die Skalierungskonfiguration und legen Sie die gewünschte Größe der Knotengruppe fest.
 - Verwenden Sie den Kubernetes Cluster Autoscaler. [Weitere Informationen finden Sie unter Cluster Autoscaler on. AWS](#)
5. Die Knotengruppe ist jetzt bereit für die Planung von Workloads und Pods.
6. Damit Ihre Pods vor Ablauf der Reservierung ordnungsgemäß geleert werden können, verwendet Amazon EKS eine geplante Skalierungsrichtlinie, um die Größe der Knotengruppe auf zu reduzieren. 0 Für diese geplante Skalierung wird ein Name mit dem Titel festgelegt. Amazon EKS Node Group Capacity Scaledown Before Reservation End Wir empfehlen, diese Aktion nicht zu bearbeiten oder zu löschen.

Amazon EC2 beginnt 30 Minuten vor dem Ende der Reservierung mit dem Herunterfahren der Instances. Aus diesem Grund richtet Amazon EKS 40 Minuten vor Ende der Reservierung ein geplantes Herunterfahren der Knotengruppe ein, um Pods sicher und ordnungsgemäß zu entfernen.

Erstellen Sie selbstverwaltete Knoten mit Capacity Blocks for ML

Kapazitätsblöcke für Machine Learning (ML) ermöglichen es Ihnen, GPU-Instances zu einem zukünftigen Zeitpunkt zu reservieren, um Ihre ML-Workloads mit kurzer Dauer zu unterstützen. Weitere Informationen finden Sie unter [Capacity Blocks for ML](#) im EC2 Amazon-Benutzerhandbuch für Linux-Instances.

Überlegungen

Important

- Kapazitätsblöcke sind nur für bestimmte EC2 Amazon-Instance-Typen und AWS Regionen verfügbar. Informationen zur Kompatibilität finden Sie unter [Voraussetzungen für das Arbeiten mit Kapazitätsblöcken](#) im EC2 Amazon-Benutzerhandbuch für Linux-Instances.
- Kapazitätsblöcke können derzeit nicht mit Karpenter verwendet werden.
- Wenn Sie eine selbstverwaltete Knotengruppe erstellen, bevor die Kapazitätsreservierung aktiv wird, legen Sie die gewünschte Kapazität auf fest. 0
- Um genügend Zeit zu haben, den/die Knoten ordnungsgemäß zu entleeren, empfehlen wir, die Skalierung so zu planen, dass sie mehr als 30 Minuten vor der Endzeit der Kapazitätsblock-Reservierung auf Null skaliert.
- Damit Ihre Pods ordnungsgemäß entleert werden können, empfehlen wir Ihnen, den AWS Node Termination Handler einzurichten, wie in den Beispielschritten beschrieben.

Verwenden Sie Capacity Blocks mit selbstverwalteten Knoten

Sie können Kapazitätsblöcke mit Amazon EKS für die Bereitstellung und Skalierung Ihrer selbstverwalteten Knoten verwenden. Die folgenden Schritte geben einen allgemeinen Beispielüberblick. Die AWS CloudFormation Vorlagenbeispiele decken nicht alle Aspekte ab, die für einen Produktionsworkload erforderlich sind. In der Regel benötigen Sie auch ein Bootstrapping-Skript, um den Knoten mit dem Cluster zu verbinden, ein Amazon EKS-beschleunigtes AMI und ein geeignetes Instance-Profil für den Beitritt zum Cluster anzugeben. Weitere Informationen finden Sie unter [the section called "Amazon Linux"](#).

1. Erstellen Sie eine Startvorlage, die für Ihren Workload geeignet ist. Weitere Informationen finden Sie unter [Verwenden von Kapazitätsblöcken für Machine-Learning-Workloads](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Stellen Sie sicher, dass LaunchTemplateData dies Folgendes beinhaltet:

- InstanceMarketOptions mit der Einstellung "capacity-block" für MarketType
- CapacityReservationSpecification: CapacityReservationTarget mit CapacityReservationId Einstellung auf den Capacity-Block (zum Beispiel: `cr-02168da1478b509e0`)

- `IamInstanceProfile` wobei der Wert auf den entsprechenden Wert Arn eingestellt ist *iam-instance-profile-arn*
- `ImageId` auf das Zutreffende setzen *image-id*
- `InstanceType` auf einen Instance-Typ gesetzt, der Capacity Blocks unterstützt (zum Beispiel: *p5.48xlarge*)
- `SecurityGroupIds` auf den zutreffenden Wert gesetzt IDs (zum Beispiel: *sg-05b1d815d1EXAMPLE*)
- `UserData` auf die *user-data* für Ihre selbstverwaltete Knotengruppe zutreffende Einstellung setzen

Im Folgenden finden Sie einen Auszug aus einer CloudFormation Vorlage, mit der eine Startvorlage für einen Kapazitätsblock erstellt wird.

```
NodeLaunchTemplate:
  Type: "aws::EC2::LaunchTemplate"
  Properties:
    LaunchTemplateData:
      InstanceMarketOptions:
        MarketType: "capacity-block"
      CapacityReservationSpecification:
        CapacityReservationTarget:
          CapacityReservationId: "cr-02168da1478b509e0"
      IamInstanceProfile:
        Arn: iam-instance-profile-arn
      ImageId: image-id
      InstanceType: p5.48xlarge
      KeyName: key-name
      SecurityGroupIds:
        - sg-05b1d815d1EXAMPLE
      UserData: user-data
```

Sie müssen das Subnetz in der Availability Zone übergeben, in der die Reservierung vorgenommen wurde, da Kapazitätsblöcke zonal sind.

2. Verwenden Sie die Startvorlage, um eine selbstverwaltete Knotengruppe zu erstellen. Wenn Sie dies tun, bevor die Kapazitätsreservierung aktiv wird, setzen Sie die gewünschte Kapazität auf 0. Achten Sie beim Erstellen der Knotengruppe darauf, dass Sie nur das entsprechende Subnetz für die Availability Zone angeben, in der die Kapazität reserviert ist.

Im Folgenden finden Sie eine CloudFormation Beispielvorlage, auf die Sie zurückgreifen können, wenn Sie eine Vorlage erstellen, die für Ihren Workload geeignet ist. In diesem Beispiel wird das LaunchTemplateId Ende Version der `AWS::Amazon::EC2::LaunchTemplate` Ressource abgerufen, die im vorherigen Schritt angezeigt wurde. Sie erhält auch die Werte für `DesiredCapacity`, `MaxSize`, `MinSize`, und `VPCZoneIdentifier`, die an anderer Stelle in derselben Vorlage deklariert sind.

```
NodeGroup:
  Type: "AWS::AutoScaling::AutoScalingGroup"
  Properties:
    DesiredCapacity: !Ref NodeAutoScalingGroupDesiredCapacity
    LaunchTemplate:
      LaunchTemplateId: !Ref NodeLaunchTemplate
      Version: !GetAtt NodeLaunchTemplate.LatestVersionNumber
    MaxSize: !Ref NodeAutoScalingGroupMaxSize
    MinSize: !Ref NodeAutoScalingGroupMinSize
    VPCZoneIdentifier: !Ref Subnets
  Tags:
    - Key: Name
      PropagateAtLaunch: true
      Value: !Sub ${ClusterName}-${NodeGroupName}-Node
    - Key: !Sub kubernetes.io/cluster/${ClusterName}
      PropagateAtLaunch: true
      Value: owned
```

3. Nachdem die Knotengruppe erfolgreich erstellt wurde, stellen Sie sicher, dass Sie die `NodeInstanceRole` für die Knotengruppe aufzeichnen, die erstellt wurde. Sie benötigen dies, um sicherzustellen, dass bei der Skalierung der Knotengruppe die neuen Knoten dem Cluster beitreten und Kubernetes die Knoten erkennen kann. Weitere Informationen finden Sie in den AWS Management Console Anweisungen unter [Selbstverwaltete Amazon Linux-Knoten erstellen](#).
4. Wir empfehlen Ihnen, eine geplante Skalierungsrichtlinie für die Auto-Scaling-Gruppe zu erstellen, die sich an den Reservierungszeiten für Kapazitätsblöcke orientiert. Weitere Informationen finden Sie unter [Geplante Skalierung für Amazon EC2 Auto Scaling](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Sie können alle von Ihnen reservierten Instances bis 30 Minuten vor Ablauf der Endzeit des Kapazitätsblocks verwenden. Instances, die zu diesem Zeitpunkt noch laufen, werden beendet. Um genügend Zeit zu haben, den/die Knoten ordnungsgemäß zu entleeren, empfehlen wir, die

Skalierung so zu planen, dass sie mehr als 30 Minuten vor der Endzeit der Kapazitätsblock-Reservierung auf Null skaliert.

Wenn Sie stattdessen manuell skalieren möchten, wann immer die Kapazitätsreservierung erfolgt, müssen Sie die gewünschte Kapazität der Auto Scaling Group zum Startzeitpunkt der Kapazitätsblockreservierung aktualisieren. Dann müssten Sie auch mehr als 30 Minuten vor dem Ende der Kapazitätsblock-Reservierung manuell herunterskalieren.

5. Die Knotengruppe ist jetzt bereit für die Planung von Workloads und Pods.
6. Damit Ihre Pods ordnungsgemäß entleert werden können, empfehlen wir Ihnen, den AWS Node Termination Handler einzurichten. Dieser Handler kann mithilfe von Amazon EC2 Auto Scaling nach „ASG Scale-in“-Lebenszykluseignissen Ausschau halten EventBridge und es der Kubernetes-Steuerebene ermöglichen, die erforderlichen Maßnahmen zu ergreifen, bevor die Instance nicht verfügbar ist. Andernfalls bleiben Ihre Pods und Kubernetes-Objekte im Status „Ausstehend“ hängen. Weitere Informationen finden Sie unter [AWS Node Termination Handler on GitHub](#)

Wenn Sie keinen Node Termination Handler einrichten, empfehlen wir, dass Sie mit der manuellen Entleerung Ihrer Pods beginnen, bevor Sie das 30-Minuten-Zeitfenster erreichen, damit sie genügend Zeit haben, um ordnungsgemäß entleert zu werden.

Verhindern, dass Pods auf bestimmten Knoten geplant werden

Der Betrieb von Knoten mit speziellen Prozessoren kann teurer sein als der Betrieb von Knoten GPUs, die auf Standardcomputern ausgeführt werden. Aus diesem Grund sollten Sie diese Knoten vor Workloads schützen, für deren Bereitstellung keine spezielle Hardware erforderlich ist. Eine Möglichkeit, dies zu tun, sind Taints.

Amazon EKS unterstützt die Konfiguration von Kubernetes-Taints über verwaltete Knotengruppen. Taints und Tolerations arbeiten zusammen, um sicherzustellen, dass Pods nicht auf unangemessene Knoten eingeplant werden. Ein oder mehrere Taints können auf einen Knoten angewendet werden. Dies bedeutet, dass der Knoten keine Pods akzeptieren sollte, die die Taints nicht tolerieren. Toleranzen werden auf Pods angewendet und ermöglichen es den Pods, Knoten mit entsprechenden Taints zuzuordnen, müssen aber nicht. Weitere Informationen finden Sie unter [Taints and Tolerations](#) in der Kubernetes-Dokumentation.

Kubernetes-Knotenfehler können mithilfe der AWS Management Console oder über die Amazon EKS-API auf neue und bestehende verwaltete Knotengruppen angewendet werden.

- Informationen zum Erstellen einer Knotengruppe mit einem Taint mithilfe von finden Sie unter. AWS Management Console [the section called “Erstellen”](#)
- Im Folgenden finden Sie ein Beispiel für die Erstellung einer Knotengruppe mit einem Taint mithilfe der AWS CLI:

```
aws eks create-nodegroup \
  --cli-input-json '
{
  "clusterName": "my-cluster",
  "nodegroupName": "node-taints-example",
  "subnets": [
    "subnet-1234567890abcdef0",
    "subnet-abcdef01234567890",
    "subnet-021345abcdef67890"
  ],
  "nodeRole": "arn:aws:iam::111122223333:role/AmazonEKSNodeRole",
  "taints": [
    {
      "key": "dedicated",
      "value": "gpuGroup",
      "effect": "NO_SCHEDULE"
    }
  ]
}'
```

Weitere Informationen und Anwendungsbeispiele finden Sie unter [Taint](#) in der Kubernetes-Referenzdokumentation.

Note

- Taints können aktualisiert werden, nachdem Sie die Knotengruppe mit dem UpdateNodegroupConfig-API erstellen.
- Der Taint-Schlüssel muss mit einem Buchstaben oder einer Zahl beginnen. Es kann Buchstaben, Zahlen, Bindestriche (-), Punkte (.) und Unterstriche (_) enthalten. Er kann bis zu 63 Zeichen lang sein.
- Optional kann der Taint-Schlüssel mit einem DNS-Subdomänenpräfix und einem einzelnen / beginnen. Wenn er mit einem DNS-Subdomänenpräfix beginnt, kann er 253 Zeichen lang sein.

- Der Wert ist optional und muss mit einem Buchstaben oder einer Zahl beginnen. Es kann Buchstaben, Zahlen, Bindestriche (-), Punkte (.) und Unterstriche (_) enthalten. Er kann bis zu 63 Zeichen lang sein.
- Wenn Sie Kubernetes direkt oder das verwenden, muss der Taint-Effekt AWS Management Console,, oder sein. NoSchedule PreferNoSchedule NoExecute Bei Verwendung der AWS CLI oder API muss der Taint-Effekt jedoch NO_SCHEDULE,PREFER_NO_SCHEDULE, oder NO_EXECUTE sein.
- Für eine Knotengruppe sind maximal 50 Taints zulässig.
- Wenn Taints, die mithilfe einer verwalteten Knotengruppe erstellt wurden, manuell von einem Knoten entfernt werden, fügt Amazon EKS die Taints dem Knoten nicht wieder hinzu. Dies gilt auch dann, wenn die Taints in der Konfiguration der verwalteten Knotengruppe angegeben sind.

Sie können den [AWS eks update-nodegroup-config](#) AWS CLI-Befehl verwenden, um Taints für verwaltete Knotengruppen hinzuzufügen, zu entfernen oder zu ersetzen.

Führen Sie Machine-Learning-Schulungen auf Amazon EKS mit Elastic Fabric Adapter durch

In diesem Thema wird beschrieben, wie Sie den Elastic Fabric Adapter (EFA) in Pods integrieren, die in Ihrem Amazon EKS-Cluster bereitgestellt werden. Elastic Fabric Adapter (EFA) ist eine Netzwerkschnittstelle für EC2 Amazon-Instances, mit der Sie Anwendungen ausführen können, die ein hohes Maß an Kommunikation zwischen Knoten erfordern, in großem Umfang. AWS Die speziell für die Umgehung von Betriebssystemen entwickelte Hardware-Schnittstelle verbessert die Leistung der Instance-übergreifenden Kommunikation, was für die Skalierung dieser Anwendungen von entscheidender Bedeutung ist. Mit EFA können High Performance Computing (HPC) -Anwendungen, die das Message Passing Interface (MPI) verwenden, und Machine Learning (ML) -Anwendungen, die die NVIDIA Collective Communications Library (NCCL) verwenden, auf Tausende von oder skalieren. CPUs GPUs Dadurch erhalten Sie die Anwendungsleistung von lokalen HPC-Clustern mit der On-Demand-Elastizität und Flexibilität der Cloud. AWS Durch die Integration von EFA in Anwendungen, die auf Amazon-EKS-Clustern ausgeführt werden, können Sie die Zeit für die Durchführung umfangreicher verteilter Schulungs-Workloads verkürzen, ohne dass zusätzliche Instances zu Ihrem Cluster hinzugefügt werden müssen. Weitere Informationen zu EFA finden Sie unter [Elastic Fabric Adapter](#).

Instanztypen mit EFA

Das AWS EFA Kubernetes Device Plugin unterstützt alle EC2 Amazon-Instance-Typen, die EFA haben. Eine Liste aller Instance-Typen mit EFA finden Sie unter [Unterstützte Instance-Typen](#) im EC2 Amazon-Benutzerhandbuch. Um ML-Anwendungen schnell auszuführen, empfehlen wir jedoch, dass eine Instance zusätzlich zu [AWS EFA über Hardwarebeschleunigungschips wie nVidia GPUs, Inferentia-Chips](#) oder [AWS Trainium-Chips](#) verfügt. Eine Liste der Instance-Typen mit Hardwarebeschleunigungschips und EFA finden Sie unter [Accelerated Computing](#) im EC2 Amazon-Benutzerhandbuch.

Wenn Sie Instance-Typen vergleichen, um zwischen ihnen zu wählen, sollten Sie die Anzahl der für diesen Instance-Typ verfügbaren EFA-Netzwerkkarten sowie die Anzahl der Beschleunigerkarten, die CPU-Menge und die Speichermenge berücksichtigen. Sie können bis zu einem EFA pro Netzwerkkarte zuweisen. Eine EFA zählt als Netzwerkschnittstelle. Wie viele EFA für jeden Instance-Typ mit EFA verfügbar sind, finden Sie in der Liste der [Netzwerkkarten](#) im EC2 Amazon-Benutzerhandbuch.

EFA- und reine EFA-Schnittstellen

Ein Elastic Fabric Adapter (EFA) ist eine Netzwerkschnittstelle, die die Funktionen eines Elastic Network Adapters (ENA) und einer OS-Bypass-Schnittstelle kombiniert und auf dem Scalable AWS Reliable Datagram (SRD) -Protokoll basiert. Die EFA-Funktionen ermöglichen Anwendungen die direkte Kommunikation mit der Hardware für den Transport mit niedriger Latenz. Sie können sich dafür entscheiden, nur über reine EFA-Schnittstellen auf die EFA-Funktionen zuzugreifen und so die Kommunikation auf Schnittstellen innerhalb derselben Availability Zone zu beschränken.

Um Knoten zu erstellen, die nur über EFA-Schnittstellen verfügen können, müssen Sie eine benutzerdefinierte EC2 Startvorlage verwenden und den Wert auf `InterfaceType efa-only` setzen. In Ihrer benutzerdefinierten Startvorlage können Sie die Netzwerkkarte nicht `0` auf eine reine EFA-Schnittstelle festlegen, da dies die primäre Netzwerkkarte und Netzwerkschnittstelle der Instance ist. Für reine EFA-Schnittstellen benötigen Sie die VPC CNI-Version `1.18.5` oder höher. Wenn Sie Amazon Linux 2 verwenden, muss die ami-Version `v20240928` oder höher für reine EFA-Schnittstellen sein.

Das folgende Verfahren führt Sie zum Erstellen eines EKS-Clusters `eksctl` mit Knoten, die über NVIDIA GPUs - und EFA-Schnittstellen verfügen. Sie können `eksctl` damit keine Knoten und Knotengruppen erstellen, die reine EFA-Schnittstellen verwenden.

Voraussetzungen

- Ein vorhandener Amazon-EKS-Cluster. Wenn Sie noch keinen Cluster haben, erstellen Sie einen mit. [Erste Schritte](#) Ihr Cluster muss in einer VPC bereitgestellt werden, in der mindestens ein privates Subnetz mit genügend verfügbaren IP-Adressen zum Bereitstellen von Knoten vorhanden sind. Das private Subnetz muss über einen ausgehenden Internetzugang verfügen, der von einem externen Gerät, z. B. einem NAT-Gateway, bereitgestellt wird.

Wenn Sie planen, `eksctl` zu verwenden, um Ihre Knotengruppe zu erstellen, kann `eksctl` auch einen Cluster für Sie erstellen.

- Version 2.12.3 oder höher oder Version 1.27.160 oder höher der auf Ihrem Gerät installierten und konfigurierten AWS Befehlszeilenschnittstelle (AWS CLI) oder AWS CloudShell. Um Ihre aktuelle Version zu überprüfen, verwenden Sie `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Paketmanager wie `yum` oder `apt-get`, oder Homebrew für macOS liegen oft mehrere Versionen hinter der neuesten Version der AWS CLI. Informationen zur Installation der neuesten Version finden Sie unter [Installation](#) und [Schnellkonfiguration mit aws configure](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. Die AWS CLI-Version, in der installiert ist, AWS CloudShell kann auch mehrere Versionen hinter der neuesten Version liegen. Informationen zur Aktualisierung finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CLI in Ihrem Home-Verzeichnis installieren](#).
- Das `kubectl`-Befehlszeilen-Tool ist auf Ihrem Gerät oder in der AWS CloudShell installiert. Die Version kann mit der Kubernetes-Version Ihres Clusters identisch oder bis zu einer Nebenversion sein, die vor oder nach der Kubernetes-Version liegt. Wenn Ihre Clusterversion beispielsweise 1.29 ist, können Sie `kubectl`-Version 1.28, 1.29, oder 1.30 damit verwenden. Informationen zum Installieren oder Aktualisieren von `kubectl` finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Sie müssen das Amazon VPC CNI-Plug-In für Kubernetes in der Version 1.7.10 oder höher installiert haben, bevor Sie Worker-Knoten starten können, die mehrere Elastic Fabric-Adapter unterstützen, z. B. den oder. p4d p5 Weitere Informationen zur Aktualisierung Ihrer Amazon VPC CNI-Plug-in-Version für Kubernetes finden Sie unter. [the section called “Amazon VPC CNI”](#)

Important

Eine wichtige Überlegung, die für die Übernahme von EFA mit Kubernetes erforderlich ist, ist die Konfiguration und Verwaltung von Huge Pages als Ressource im Cluster. Weitere Informationen dazu finden Sie unter [Manage Huge Pages](#) in der Kubernetes-Dokumentation.

EC2 Amazon-Instances, auf denen der EFA-Treiber installiert ist, weisen 5128 Huge Pages mit 2 MiB vorab zu, die Sie als Ressourcen anfordern können, die Sie in Ihren Jobspezifikationen nutzen können.

Knotengruppen erstellen

Das folgende Verfahren hilft Ihnen dabei, eine Knotengruppe mit einer `p4d.24xlarge` gesicherten Knotengruppe mit EFA-Schnittstellen und GPUDirect RDMA zu erstellen und einen Beispieltest der NVIDIA Collective Communications Library (NCCL) für die NCCL-Leistung mit mehreren Knoten durchzuführen. EFAs Das Beispiel kann als Vorlage für verteiltes Deep-Learning-Training auf Amazon EKS verwendet EFAs werden.

1. Ermitteln Sie, welche EC2 Amazon-Instance-Typen, die EFA unterstützen, in der AWS Region verfügbar sind, in der Sie Knoten bereitstellen möchten. `region-code` Ersetzen Sie es durch die AWS Region, in der Sie Ihre Knotengruppe bereitstellen möchten.

```
aws ec2 describe-instance-types --region region-code \
  --filters Name=network-info.efa-supported,Values=true \
  --query "InstanceTypes[*].InstanceType" --output text
```

Wenn Sie Knoten bereitstellen, muss der Instance-Typ, den Sie bereitstellen möchten, in der AWS Region verfügbar sein, in der sich Ihr Cluster befindet.

2. Bestimmen Sie, in welchen Availability Zones der Instance-Typ bereitgestellt werden soll. In diesem Tutorial wird der `p5.48xlarge` Instance-Typ verwendet und muss in der Ausgabe für die AWS Region zurückgegeben werden, die Sie im vorherigen Schritt angegeben haben. Wenn Sie Knoten in einem Produktionscluster bereitstellen, `p5.48xlarge` ersetzen Sie ihn durch einen beliebigen Instance-Typ, der im vorherigen Schritt zurückgegeben wurde.

```
aws ec2 describe-instance-type-offerings --region region-code \
  --location-type availability-zone --filters Name=instance-
type,Values=p4d.24xlarge,p5.48xlarge \
  --query 'InstanceTypeOfferings[*].Location' --output text
```

Eine Beispielausgabe sieht wie folgt aus.

```
us-west-2a    us-west-2c    us-west-2b
```

Beachten Sie, dass Availability Zones zur Verwendung in späteren Schritten zurückgegeben wurden. Wenn Sie Knoten in einem Cluster bereitstellen, muss Ihre VPC über Subnetze mit verfügbaren IP-Adressen in einer der in der Ausgabe zurückgegebenen Availability Zones verfügen.

3. Erstellen Sie eine Knotengruppe mit `eksctl`. Sie benötigen eine Version `0.210.0` oder eine neuere Version des `eksctl` Befehlszeilentools, das auf Ihrem Gerät installiert ist oder AWS CloudShell. Informationen zum Installieren und Aktualisieren von `eksctl` finden Sie in der Dokumentation zu `eksctl` unter [Installation](#).
- a. Kopieren Sie den folgenden Inhalt in eine Datei namens `efa-cluster.yaml`. Ersetzen Sie das `example values` durch Ihr eigenes. Sie können `p5.48xlarge` mit einer anderen Instance ersetzen. Wenn Sie dies tun, stellen Sie sicher, dass die Werte für `availabilityZones` Availability Zones sind, die in Schritt 1 für den Instance-Typ zurückgegeben wurden.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-efa-cluster
  region: region-code
  version: "1.XX"

iam:
  withOIDC: true

availabilityZones: ["us-west-2a", "us-west-2c"]

managedNodeGroups:
- name: my-efa-ng
  instanceType: p5.48xlarge
  minSize: 1
  desiredCapacity: 2
  maxSize: 3
  availabilityZones: ["us-west-2a"]
  volumeSize: 300
  privateNetworking: true
  efaEnabled: true
```

- b. Erstellen einer verwalteten Knotengruppe in einem bestehenden Cluster

```
eksctl create nodegroup -f efa-cluster.yaml
```

Wenn Sie noch keinen Cluster haben, können Sie den folgenden Befehl ausführen, um einen Cluster und die Knotengruppe zu erstellen.

```
eksctl create cluster -f efa-cluster.yaml
```

Note

Da der in diesem Beispiel verwendete Instance-Typ GPUs, installiert `eksctl` automatisch das NVIDIA Kubernetes-Geräte-Plug-In auf jeder Instance für Sie, wenn Sie Amazon Linux 2 verwenden. Dies ist für Bottlerocket nicht erforderlich, da das NVIDIA-Geräte-Plugin in die EKS-NVIDIA-Variante von Bottlerocket integriert ist. Wenn `true` in der Nodegroup-Konfiguration auf eingestellt `efaEnabled` ist, `eksctl` wird auch das EFA-Geräte-Plugin automatisch auf den Knoten bereitgestellt.

Bottlerocket mit EFA verwenden

Bottlerocket AMI Version 1.28.0 und höher beinhalten offizielle Unterstützung für EFA. Um Bottlerocket für EFA-fähige Knoten zu verwenden, geben Sie dies in Ihrer Konfiguration an. `amiFamily: Bottlerocket` Wenn Sie eine benutzerdefinierte AMI-ID verwenden müssen, müssen Sie `nodeGroups` stattdessen `Standard` verwenden `managedNodeGroups`.

Hier ist eine Beispielkonfiguration:

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-efa-bottlerocket-cluster
  region: region-code
  version: "1.XX"

iam:
  withOIDC: true

availabilityZones: ["us-west-2a", "us-west-2c"]
```

```

managedNodeGroups:
  - name: my-efa-bottlerocket-ng
    instanceType: p5.48xlarge
    minSize: 1
    desiredCapacity: 2
    maxSize: 3
    availabilityZones: ["us-west-2a"]
    volumeSize: 300
    privateNetworking: true
    efaEnabled: true
    amiFamily: Bottlerocket
    bottlerocket:
      enableAdminContainer: true
      settings:
        kernel:
          sysctl:
            "vm.nr_hugepages": "3000" # Configures 3000 * 2Mi = 6000Mi hugepages

```

Die obige `vm.nr_hugepages` `sysctl`-Einstellung konfiguriert die Anzahl der 2Mi-Hugepages. In diesem Beispiel bedeutet `3000 3000 * 2 Mi = 6000 Mi` an riesigen Seiten.

Überprüfen Sie die Installation des EFA-Geräte-Plugins

Wenn Sie eine Knotengruppe mit `createEfaEnabled: true`, `eksctl` wird das EFA-Kubernetes-Geräte-Plugin automatisch für Sie bereitgestellt. Sie können überprüfen, ob das Geräte-Plugin installiert ist und ordnungsgemäß funktioniert:

1. Überprüfen Sie den DaemonSet Status:

```
kubectl get daemonsets -n kube-system
```

Beispielausgabe:

NAME	AVAILABLE	NODE SELECTOR	AGE	DESIRED	CURRENT	READY	UP-TO-DATE
aws-efa-k8s-device-plugin-daemonset	2	<none>	6m16s	2	2	2	2
...							

Hier läuft das EFA-Geräte-Plugin DaemonSet auf zwei Knoten. Beide sind **BEREIT** und **VERFÜGBAR**.

2. Überprüfen Sie als Nächstes die Pods, die erstellt wurden von DaemonSet:

```
kubectl get pods -n kube-system -l name=aws-efa-k8s-device-plugin
```

Beispielausgabe:

NAME	READY	STATUS	RESTARTS	AGE
aws-efa-k8s-device-plugin-daemonset-d68bs	1/1	Running	0	6m16s
aws-efa-k8s-device-plugin-daemonset-w4l8t	1/1	Running	0	6m16s

Die EFA-Geräte-Plug-in-Pods befinden sich im Status Running, was bestätigt, dass das Plugin erfolgreich bereitgestellt wurde und betriebsbereit ist.

3. Überprüfen Sie die Ressourcenregistrierung:

Sie können bestätigen, dass die `vpc.amazonaws.com/efa` Ressource im Kubelet registriert ist, indem Sie die Knoten beschreiben:

```
kubectl describe nodes
```

Wenn die EFA-Ressource ordnungsgemäß registriert ist, wird sie unter Kapazität und Zuweisbare Ressourcen des Knotens aufgeführt. Zum Beispiel:

```
Capacity:
...
vpc.amazonaws.com/efa: 4
Allocatable:
...
vpc.amazonaws.com/efa: 4
```

Diese Ausgabe bestätigt, dass der Knoten die EFA-Ressource erkennt, sodass sie für Pods verfügbar ist, die sie anfordern.

(Optional) Testen Sie die Leistung der EFA

Wir empfehlen Ihnen, das EFA-Setup zu testen. Sie können die [NCCL-Tests](#) im Repository am `aws-samples/awesome-distributed-training` verwenden. GitHub [NCCL-Tests](#) bewerten die Leistung des Netzwerks mithilfe der Nvidia Collective Communication Library. Mit den folgenden Schritten werden NCCL-Tests auf Amazon EKS eingereicht.

1. Stellen Sie den Kubeflow MPI Operator bereit:

Für die NCCL-Tests können Sie den Kubeflow MPI Operator anwenden. Der MPI Operator macht es einfach, auf Kubernetes verteiltes Training im Allreduce-Stil durchzuführen. Weitere Informationen finden Sie unter [MPI Operator on. GitHub](#)

2. Führen Sie den NCCL-Leistungstest mit mehreren Knoten aus, um RDMA/EFA zu überprüfen: GPUDirect

Führen Sie den standardmäßigen NCCL-Leistungstest aus, um die NCCL-Leistung mit GPUDirect RDMA over EFA zu überprüfen. [Weitere Informationen finden Sie im offiziellen NCCL-Tests-Repo unter. GitHub](#)

Führen Sie die folgenden Schritte aus, um einen NCCL-Leistungstest mit zwei Knoten auszuführen. Im Beispiel für einen NCCL-Testjob fordert jeder Worker acht GPUs, 5210 Mi, vier und 8000 Mi Arbeitsspeicher an EFAs, was praktisch bedeutet, dass jeder Worker alle Ressourcen einer Instanz verbraucht. `hugepages-2Mi p5.48xlarge`

a. Erstellen Sie das Manifest: MPIJob

Kopieren Sie Folgendes in eine Datei mit dem Namen `nccl-tests.yaml`:

```
apiVersion: kubeflow.org/v2beta1
kind: MPIJob
metadata:
  name: nccl-tests
spec:
  runPolicy:
    cleanPodPolicy: Running
    backoffLimit: 20
  slotsPerWorker: 8
  mpiReplicaSpecs:
    Launcher:
      replicas: 1
      template:
        spec:
          restartPolicy: OnFailure
          containers:
            - image: public.ecr.aws/hpc-cloud/nccl-tests:latest
              imagePullPolicy: IfNotPresent
              name: test-nccl-launcher
              env:
                - name: PATH
```

```

        value: $PATH:/opt/amazon/efa/bin:/usr/bin
    - name: LD_LIBRARY_PATH
      value: /opt/amazon/openmpi/lib:/opt/nccl/build/lib:/opt/amazon/efa/
lib:/opt/aws-ofi-nccl/install/lib:/usr/local/nvidia/lib:$LD_LIBRARY_PATH
    - name: NCCL_DEBUG
      value: INFO
    - name: NCCL_BUFFSIZE
      value: '8388608'
    - name: NCCL_P2P_NET_CHUNKSIZE
      value: '524288'
    - name: NCCL_TUNER_PLUGIN
      value: /opt/aws-ofi-nccl/install/lib/libnccl-ofi-tuner.so
  command:
  - /opt/amazon/openmpi/bin/mpirun
  - --allow-run-as-root
  - --tag-output
  - -np
  - "16"
  - -N
  - "8"
  - --bind-to
  - none
  - -x
  - PATH
  - -x
  - LD_LIBRARY_PATH
  - -x
  - NCCL_DEBUG=INFO
  - -x
  - NCCL_BUFFSIZE
  - -x
  - NCCL_P2P_NET_CHUNKSIZE
  - -x
  - NCCL_TUNER_PLUGIN
  - --mca
  - pml
  - ^cm,ucx
  - --mca
  - btl
  - tcp,self
  - --mca
  - btl_tcp_if_exclude
  - lo,docker0,veth_def_agent
  - /opt/nccl-tests/build/all_reduce_perf

```

- -b
- "8"
- -e
- "16G"
- -f
- "2"
- -g
- "1"
- -c
- "1"
- -n
- "100"

Worker:

replicas: 2

template:

spec:

nodeSelector:

node.kubernetes.io/instance-type: "p5.48xlarge"

containers:

- image: public.ecr.aws/hpc-cloud/nccl-tests:latest

imagePullPolicy: IfNotPresent

name: nccl-tests-worker

volumeMounts:

- name: shm

mountPath: /dev/shm

resources:

limits:

nvidia.com/gpu: 8

hugepages-2Mi: 5120Mi

vpc.amazonaws.com/efa: 32

memory: 32000Mi

requests:

nvidia.com/gpu: 8

hugepages-2Mi: 5120Mi

vpc.amazonaws.com/efa: 32

memory: 32000Mi

volumes:

- name: shm

hostPath:

path: /dev/shm

b. Wenden Sie die NCCL-Tests MPIJob an:

Reichen Sie das ein, MPIJob indem Sie das Manifest anwenden. Dadurch werden zwei p5.48xlarge EC2 Amazon-Instances erstellt.

```
kubectl apply -f nccl-tests.yaml
```

Eine Beispielausgabe sieht wie folgt aus.

```
mpijob.kubeflow.org/nccl-tests created
```

- c. Stellen Sie sicher, dass der Job Pods gestartet hat:

Sehen Sie sich Ihre laufenden Pods an.

```
kubectl get pods
```

Eine Beispielausgabe sieht wie folgt aus.

NAME	READY	STATUS	RESTARTS	AGE
nccl-tests-launcher-nbql9	0/1	Init:0/1	0	2m49s
nccl-tests-worker-0	1/1	Running	0	2m49s
nccl-tests-worker-1	1/1	Running	0	2m49s

Der MPI-Operator erstellt einen Launcher-Pod und 2 Worker-Pods (einen auf jedem Knoten).

- d. Stellen Sie anhand der Protokolle sicher, dass der Job erfolgreich ausgeführt wird:

Sehen Sie sich das Protokoll für den nccl-tests-launcher Pod an. Ersetzen Sie **nbql9** mit dem Wert aus Ihrer Ausgabe.

```
kubectl logs -f nccl-tests-launcher-nbql9
```

Wenn der Test erfolgreich abgeschlossen wurde, können Sie Ihre Anwendungen bereitstellen, die die Nvidia Collective Communication Library verwenden.

Verwenden Sie AWS Inferentia-Instances mit Amazon EKS für Machine Learning

In diesem Thema wird beschrieben, wie Sie einen Amazon EKS-Cluster mit Knoten erstellen, auf denen [Amazon EC2 Inf1-Instances](#) ausgeführt werden, und (optional) eine Beispielanwendung bereitstellen. Amazon EC2 Inf1-Instances werden mit [AWS Inferentia-Chips](#) betrieben, die speziell für hohe Leistung und kostengünstigste Inferenz in der Cloud entwickelt wurden. AWS Modelle für maschinelles Lernen werden mithilfe von [AWS Neuron](#), einem speziellen Software Development Kit (SDK), das aus Compiler-, Runtime- und Profiling-Tools besteht, in Containern bereitgestellt, die die Inferenzleistung von Inferentia-Chips für maschinelles Lernen optimieren. AWS Neuron unterstützt beliebte Frameworks für maschinelles Lernen wie, und. TensorFlow PyTorch MXNet

Note

Das logische Neuron-Gerät IDs muss zusammenhängend sein. Wenn ein Pod, der mehrere Neuron-Geräte anfordert, für einen `inf1.24xlarge` Instanztyp `inf1.6xlarge` oder geplant ist (der mehr als ein Neuron-Gerät hat), kann dieser Pod nicht gestartet werden, wenn der Kubernetes-Scheduler ein nicht zusammenhängendes Gerät auswählt. IDs [Weitere Informationen finden Sie unter Das logische Gerät muss zusammenhängend sein. IDs](#) [GitHub](#)

Voraussetzungen

- `eksctl` ist auf Ihrem Computer installiert. Wenn Sie es nicht installiert haben, finden Sie in der Dokumentation weitere Informationen unter [Installation](#). `eksctl`
- Installieren Sie `kubectl` auf Ihrem Computer. Weitere Informationen finden Sie unter [the section called “Richten Sie kubectl und eksctl ein”](#).
- Installieren Sie `python3` auf Ihrem Computer (optional). Wenn Sie es nicht installiert haben, finden Sie Installationsanweisungen unter [Python-Downloads](#).

Erstellen eines -Clusters

1. Erstellen Sie einen Cluster mit EC2 Inf1-Amazon-Instance-Knoten. Sie können `inf1.2xlarge` mit jedem [Inf1-Instance-Typ](#) ersetzen. Das `eksctl` Hilfsprogramm erkennt, dass Sie eine

Knotengruppe mit einem Inf1 Instance-Typ starten, und startet Ihre Knoten mit einem der für Amazon EKS optimierten beschleunigten Amazon Linux AMIs.

 Note

Sie können [IAM-Rollen nicht für Dienstknoten](#) bei TensorFlow Serving verwenden.

```
eksctl create cluster \  
  --name inferentia \  
  --region region-code \  
  --nodegroup-name ng-inf1 \  
  --node-type inf1.2xlarge \  
  --nodes 2 \  
  --nodes-min 1 \  
  --nodes-max 4 \  
  --ssh-access \  
  --ssh-public-key your-key \  
  --with-oidc
```

 Note

Notieren Sie den Wert der folgenden Ausgabezeile. Es wird in einem späteren (optionalen) Schritt verwendet.

```
[9] adding identity "arn:aws:iam::111122223333:role/eksctl-inferentia-nodegroup-ng-  
in-NodeInstanceRole-FI7HIYS3BS09" to auth ConfigMap
```

Beim Starten einer Knotengruppe mit Inf1 Instanzen `eksctl` wird automatisch das AWS Neuron Kubernetes-Geräte-Plugin installiert. Dieses Plugin zeigt die Kubernetes-Scheduler-Neuron-Geräte als Systemressourcen an, die von einem Container angefordert werden können. Zusätzlich zu den Standardrichtlinien für Amazon-EKS-Knoten wird die IAM-Richtlinie für den schreibgeschützten Zugriff von Amazon S3 hinzugefügt. So kann die in einem späteren Schritt behandelte Beispielanwendung ein trainiertes Modell aus Amazon S3 laden.

2. Stellen Sie sicher, dass alle Pods korrekt gestartet wurden.

```
kubectl get pods -n kube-system
```

Gekürzte Ausgabe:

NAME	READY	STATUS	RESTARTS	AGE
[...]				
neuron-device-plugin-daemonset-6djhp	1/1	Running	0	5m
neuron-device-plugin-daemonset-hwjsj	1/1	Running	0	5m

(Optional) Stellen Sie ein TensorFlow Serving-Anwendungsimage bereit

Ein trainiertes Modell muss für ein Inferentia-Ziel zusammengetragen werden, bevor es auf Inferentia-Instances bereitgestellt werden kann. Um fortzufahren, benötigen Sie ein für [Neuron optimiertes TensorFlow](#) Modell, das in Amazon S3 gespeichert ist. Falls Sie noch keines haben SavedModel, folgen Sie bitte dem Tutorial zum [Erstellen eines Neuron-kompatiblen ResNet 50-Modells und laden Sie das Ergebnis SavedModel auf S3 hoch](#). ResNet-50 ist ein beliebtes Modell für maschinelles Lernen, das für Bilderkennungsaufgaben verwendet wird. Weitere Informationen zur Kompilierung von Neuron-Modellen finden Sie unter [The AWS Inferentia Chip With DLAMI](#) im Deep Learning Developer Guide. AWS AMIs

Das Beispiel-Deployment-Manifest verwaltet einen vorgefertigten Inferenz-Serving-Container, der von AWS Deep Learning Containers TensorFlow bereitgestellt wird. Im Container befinden sich die AWS Neuron Runtime und die TensorFlow Serving-Anwendung. Eine vollständige Liste der vorgefertigten, für Neuron optimierten Deep Learning Containers finden Sie GitHub unter [Verfügbare Images](#). Beim Start ruft der DLC Ihr Modell von Amazon S3 ab, startet Neuron TensorFlow Serving mit dem gespeicherten Modell und wartet auf Vorhersageanfragen.

Die Anzahl der Neuron-Geräte, die Ihrer Serving-Anwendung zugewiesen sind, kann angepasst werden, indem Sie die `aws.amazon.com/neuron`-Ressource in der Bereitstellung yaml verändern. Bitte beachten Sie, dass die Kommunikation zwischen TensorFlow Serving und der Neuron-Laufzeit über GRPC erfolgt, weshalb die Fähigkeit an den `IPC_LOCK` Container übergeben werden muss.

1. Fügen Sie die `AmazonS3ReadOnlyAccess` IAM-Richtlinie der Knoteninstanzrolle hinzu, die in Schritt 1 von Cluster [erstellen](#) erstellt wurde. Dies ist notwendig, damit die Beispielanwendung ein trainiertes Modell aus Amazon S3 laden kann.

```
aws iam attach-role-policy \
```

```
--policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess \  
--role-name eksctl-inferentia-nodegroup-ng-in-NodeInstanceRole-FI7HIYS3BS09
```

2. Erstellen Sie eine Datei mit dem Namen `rn50_deployment.yaml` und dem folgenden Inhalt. Aktualisieren Sie den Regions-Code und den Modellpfad entsprechend den gewünschten Einstellungen. Der Modellname dient zu Identifikationszwecken, wenn ein Client eine Anfrage an den TensorFlow Server stellt. In diesem Beispiel wird ein Modellname verwendet, der einem Beispiel-Clientskript von ResNet 50 entspricht, das in einem späteren Schritt zum Senden von Vorhersageanforderungen verwendet wird.

```
aws ecr list-images --repository-name neuron-rtd --registry-id 790709498068 --region  
us-west-2
```

```
kind: Deployment  
apiVersion: apps/v1  
metadata:  
  name: eks-neuron-test  
  labels:  
    app: eks-neuron-test  
    role: master  
spec:  
  replicas: 2  
  selector:  
    matchLabels:  
      app: eks-neuron-test  
      role: master  
  template:  
    metadata:  
      labels:  
        app: eks-neuron-test  
        role: master  
    spec:  
      containers:  
        - name: eks-neuron-test  
          image: 763104351884.dkr.ecr.us-east-1.amazonaws.com/tensorflow-inference-  
neuron:1.15.4-neuron-py37-ubuntu18.04  
          command:  
            - /usr/local/bin/entrypoint.sh  
          args:  
            - --port=8500  
            - --rest_api_port=9000  
            - --model_name=resnet50_neuron
```

```

      - --model_base_path=s3://${your-bucket-of-models}/resnet50_neuron/
ports:
  - containerPort: 8500
  - containerPort: 9000
imagePullPolicy: IfNotPresent
env:
  - name: AWS_REGION
    value: "us-east-1"
  - name: S3_USE_HTTPS
    value: "1"
  - name: S3_VERIFY_SSL
    value: "0"
  - name: S3_ENDPOINT
    value: s3.us-east-1.amazonaws.com
  - name: AWS_LOG_LEVEL
    value: "3"
resources:
  limits:
    cpu: 4
    memory: 4Gi
    aws.amazon.com/neuron: 1
  requests:
    cpu: "1"
    memory: 1Gi
securityContext:
  capabilities:
    add:
      - IPC_LOCK

```

3. Stellen Sie das Modell bereit.

```
kubectl apply -f rn50_deployment.yaml
```

4. Erstellen Sie eine Datei mit dem Namen `rn50_service.yaml` und dem folgenden Inhalt. Die HTTP- und gRPC-Ports werden für die Annahme von Prognoseanforderungen geöffnet.

```

kind: Service
apiVersion: v1
metadata:
  name: eks-neuron-test
  labels:
    app: eks-neuron-test
spec:

```

```
type: ClusterIP
ports:
  - name: http-tf-serving
    port: 8500
    targetPort: 8500
  - name: grpc-tf-serving
    port: 9000
    targetPort: 9000
selector:
  app: eks-neuron-test
  role: master
```

5. Erstellen Sie einen Kubernetes-Service für Ihre TensorFlow Model Serving-Anwendung.

```
kubectl apply -f rn50_service.yaml
```

(Optional) Treffen Sie Prognosen für Ihren Serving-Service TensorFlow

1. Um dies lokal zu testen, leiten Sie den gRPC-Port an den Service eks-neuron-test weiter.

```
kubectl port-forward service/eks-neuron-test 8500:8500 &
```

2. Erstellen Sie das Python-Skript namens `tensorflow-model-server-infer.py` mit folgendem Inhalt. Dieses Skript führt die Inferenz über gRPC (Service-Framework) aus.

```
import numpy as np
import grpc
import tensorflow as tf
from tensorflow.keras.preprocessing import image
from tensorflow.keras.applications.resnet50 import preprocess_input
from tensorflow_serving.apis import predict_pb2
from tensorflow_serving.apis import prediction_service_pb2_grpc
from tensorflow.keras.applications.resnet50 import decode_predictions

if __name__ == '__main__':
    channel = grpc.insecure_channel('localhost:8500')
    stub = prediction_service_pb2_grpc.PredictionServiceStub(channel)
    img_file = tf.keras.utils.get_file(
        "./kitten_small.jpg",
        "https://raw.githubusercontent.com/aws-labs/mxnet-model-server/master/docs/
images/kitten_small.jpg")
```

```
img = image.load_img(img_file, target_size=(224, 224))
img_array = preprocess_input(image.img_to_array(img)[None, ...])
request = predict_pb2.PredictRequest()
request.model_spec.name = 'resnet50_inf1'
request.inputs['input'].CopyFrom(
    tf.make_tensor_proto(img_array, shape=img_array.shape))
result = stub.Predict(request)
prediction = tf.make_ndarray(result.outputs['output'])
print(decode_predictions(prediction))
```

3. Führen Sie das Skript aus, um Prognosen an den Service zu senden.

```
python3 tensorflow-model-server-infer.py
```

Eine Beispielausgabe sieht wie folgt aus.

```
[[('n02123045', 'tabby', 0.68817204), ('n02127052', 'lynx', 0.12701613),
 ('n02123159', 'tiger_cat', 0.08736559), ('n02124075', 'Egyptian_cat',
 0.063844085), ('n02128757', 'snow_leopard', 0.009240591)]]
```

Probieren Sie Tutorials zum Bereitstellen von Machine Learning Learning-Workloads auf EKS aus

Wenn Sie daran interessiert sind, Plattformen und Frameworks für Machine Learning in EKS einzurichten, schauen Sie sich die auf dieser Seite beschriebenen Tutorials an. Diese Tutorials decken alles ab, von Mustern für die optimale Nutzung von GPU-Prozessoren über die Auswahl von Modellierungstools bis hin zur Erstellung von Frameworks für spezielle Branchen.

Erstellen Sie generative KI-Plattformen auf EKS

- [Generative KI-Modelle auf Amazon EKS bereitstellen](#)
- [Aufbau von JupyterHub Multi-Tenant-Plattformen auf Amazon EKS](#)

Führen Sie spezielle generative KI-Frameworks auf EKS aus

- [Beschleunigen Sie Ihre verteilten Trainingsworkloads mit generativer KI mit dem NVIDIA NeMo Framework auf Amazon EKS](#)

- [Wird TorchServe auf Amazon Elastic Kubernetes Service ausgeführt](#)

Maximieren Sie die NVIDIA-GPU-Leistung für ML auf EKS

- Implementieren Sie GPU-Sharing, um NVIDIA effizient GPUs für Ihre EKS-Cluster zu nutzen:

[GPU-Sharing auf Amazon EKS mit NVIDIA Timeslicing und beschleunigten Instances EC2](#)

- Verwenden Sie Multi-Instance- GPUs (MIGs) und NIM-Mikroservices, um mehr Pods pro GPU auf Ihren EKS-Clustern auszuführen:

[Maximierung der GPU-Auslastung mit der Multi-Instance-GPU \(MIG\) von NVIDIA auf Amazon EKS: Ausführung von mehr Pods pro GPU für mehr Leistung](#)

- [Erstellen und implementieren Sie ein skalierbares System für maschinelles Lernen auf Kubernetes mit aktiviertem Kubeflow AWS](#)

Führen Sie Videokodierungs-Workloads auf EKS aus

- [Bereitstellung von Videoinhalten mit fraktionierten GPUs Containern auf Amazon EKS](#)

Beschleunigen Sie das Laden von Bildern für Inferenz-Workloads

- [Wie H2O.ai seine KI/ML-Infrastruktur mit Karpenter und Bottlerocket optimiert und gesichert hat](#)

Überwachung von ML-Workloads

- [Überwachung von GPU-Workloads auf Amazon EKS mithilfe AWS verwalteter Open-Source-Dienste](#)
- [Pod-basierte GPU-Metriken in Amazon aktivieren CloudWatch](#)

Ankündigungen für ML auf EKS

- [Bottlerocket-Unterstützung für NVIDIA GPUs](#)
- [Verwendung von NVIDIA Multi-Instance-GPU \(MIG\) in Amazon EC2 P4d-Instances auf Amazon Elastic Kubernetes Service](#)

- [Bereitstellung verwalteter P4d-Instances in Amazon Elastic Kubernetes Service mit NVIDIA RDMA GPUDirect](#)

Erweitern Sie die Funktionen von Amazon EKS mit Open-Source-Projekten

Diese Open-Source-Projekte erweitern die Funktionalität von Kubernetes-Clustern, die auf oder außerhalb von laufen AWS, einschließlich Clustern, die von Amazon EKS verwaltet werden.

Support für Software, die auf EKS bereitgestellt wird

Wenn Sie sich die Amazon EKS-Dokumente ansehen, werden Sie in unseren Verfahren und Beispielen auf Verweise auf verschiedene Open-Source-Tools und -Software stoßen. [Zu diesen Tools gehören der Kubernetes Metrics Server und der Cert Manager.](#)

Bitte beachten Sie, dass jegliche Drittanbieter- oder Open-Source-Software, die Sie bereitstellen, nicht in den Geltungsbereich Ihrer AWS Support-Verträge fällt. Ein Vorteil der Verwendung von Kubernetes ist die aktive Open-Source-Community. Wir empfehlen, direkt mit den entsprechenden Open-Source-Communities und Projektbetreuern zusammenzuarbeiten, um geeignete Supportkanäle für solche Komponenten einzurichten. Weitere Informationen finden Sie in den Abschlussprojekten [und im Aufbau befindlichen Projekten](#) der Cloud Native Computing Foundation (CNCF).

Das Kubernetes-Ökosystem umfasst zahlreiche Projekte und Komponenten mit unterschiedlichem Maß an Community-Support, Reaktionszeiten und vorgesehenen Anwendungsfällen. Stellen Sie bei der Implementierung dieser Technologien zusammen mit EKS sicher, dass Sie die Support-Matrix für jede Komponente verstehen.

AWS verwaltet die Open-Source-Komponenten, die wir in die EKS-Steuerebene integrieren. Dazu gehört unsere umfassende Sicherheitspipeline, die Build-Verifizierung, Schwachstellen-Scans, Validierungstests und Patch-Management für alle Container-Images und -Binärdateien, die wir vertreiben, umfasst. AWS ist beispielsweise für den [Kubernetes-API-Server](#) verantwortlich. Der Kubernetes-API-Server ist durch das [Amazon EKS Service Level](#) Agreement abgedeckt. Sie können Ihren [Amazon Web Services Services-Supportplan](#) verwenden, um Probleme mit dem Kubernetes-API-Server zu lösen oder allgemeine Hinweise zu erhalten.

Sie müssen den Support, der für verschiedene Amazon EKS-Add-Ons angeboten wird, sorgfältig prüfen. AWS Add-Ons sind die einzige Art von Amazon EKS-Add-on, die vollständig von unterstützt werden AWS. AWS Marketplace-Add-Ons werden hauptsächlich von AWS Partnern unterstützt. Community-Add-ons erhalten grundlegenden Lebenszyklus-Support von AWS. Weitere Informationen finden Sie unter [Support für Zusatzmodule](#).

Jedes EKS-Add-on, unabhängig vom Typ, erhält grundlegenden Lebenszyklus-Support von EKS, einschließlich Marketplace-Add-Ons. Der grundlegende Lebenszyklus-Support umfasst die Installation und Deinstallation des Add-ons. Weitere Informationen zu den verfügbaren Amazon EKS-Add-ons und den zugehörigen Support-Stufen finden Sie unter [Umfang des Supports für Amazon EKS-Add-Ons](#). Add-Ons, die vollständig von unterstützt werden AWS, finden Sie unter [Amazon Web Services Services-Add-Ons](#).

- Weitere Informationen zu unseren Sicherheitspraktiken und Support-Grenzen finden Sie unter [Sicherheit in Amazon EKS](#).
- Weitere Informationen zu Community- und AWS Marketplace-Add-ons, die über Amazon EKS Add-ons erhältlich sind, finden Sie unter [EKS Add-ons Support](#).

Verwaltungs-Tools

Verwandte Verwaltungs-Tools für Amazon EKS und Kubernetes-Cluster.

eksctl

`eksctl` ist ein einfaches CLI-Tool zum Erstellen von Clustern in Amazon EKS.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)
- AWS Open-Source-Blog: [eksctl: Amazon EKS-Cluster mit einem Befehl](#)

AWS Controller für Kubernetes

Mit AWS Controllern für Kubernetes können Sie AWS Ressourcen direkt von Ihrem Kubernetes-Cluster aus erstellen und verwalten.

- [Projekt-URL](#)
- AWS Open-Source-Blog: [AWS Service Operator](#) für Kubernetes jetzt verfügbar

Flux CD

Flux ist ein Tool, mit dem Sie Ihre Cluster-Konfiguration mit Git verwalten können. Es verwendet einen Operator im Cluster, um Bereitstellungen innerhalb von Kubernetes auszulösen. Weitere Informationen zu Operatoren finden Sie unter [OperatorHub.io](#) auf GitHub

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)

CDK für Kubernetes

Mit dem CDK für Kubernetes (cdk8s) können Sie Kubernetes-Apps und Komponenten mit vertrauten Programmiersprachen definieren. Cdk8s-Apps synthetisieren zu Standard-Kubernetes-Manifests, die auf jeden Kubernetes-Cluster angewendet werden können.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)
- AWS Container-Blog: [Wir stellen vor: cdk8s+](#): Intent-Driven für Kubernetes-Objekte APIs

Netzwerk

Verwandte Netzwerkprojekte für Amazon EKS und Kubernetes-Cluster.

Amazon-VPC-CNI-Plug-In für Kubernetes

Amazon EKS unterstützt native VPC-Netzwerke über das Amazon-VPC-CNI-Plug-In für Kubernetes. Das Plugin weist jedem Pod eine IP-Adresse von Ihrer VPC zu.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)

AWS Load Balancer Controller für Kubernetes

Der Load AWS Balancer Controller hilft bei der Verwaltung von AWS Elastic Load Balancers für einen Kubernetes-Cluster. Er erfüllt die Anforderungen der Kubernetes Ingress-Ressourcen durch die Bereitstellung von Application Load Balancers. AWS Es erfüllt die Anforderungen der Kubernetes-Serviceressourcen durch die Bereitstellung von Network Load Balancers. AWS

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)

ExternalDNS

ExternalDNS synchronisiert exponierte Kubernetes-Dienste und -Ingresses mit DNS-Anbietern wie Amazon Route 53 und Service Discovery. AWS

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)

Machine Learning

Verwandte Machine-Learning-Projekte für Amazon EKS und Kubernetes-Cluster.

Kubeflow

Ein Machine-Learning-Toolkit für Kubernetes.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)
- AWS Open-Source-Blog: [Kubeflow auf Amazon EKS](#)

Auto Scaling

Verwandte Auto-Scaling-Projekte für Amazon EKS und Kubernetes-Cluster.

Cluster Autoscaler

Cluster Autoscaler ist ein Tool, das die Größe des Kubernetes-Clusters automatisch an die CPU- und Speicher-Auslastung anpasst.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)
- Amazon EKS-Workshop: [Cluster-Autoscaler](#)

Karpenter

Karpenter ist ein Kubernetes Node Autoscaler, der auf Flexibilität, Leistung und Einfachheit ausgelegt ist.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)
- Amazon EKS-Werkstatt: [Karpenter](#)

Escalator

Escalator ist ein Batch- oder Auftrag-optimiertes Tool zur automatischen horizontalen Skalierung für Kubernetes.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)

Überwachung

Verwandte Überwachungs-Projekte für Amazon EKS und Kubernetes-Cluster.

Prometheus

Prometheus ist ein Open-Source-Toolkit zur Überwachung und Benachrichtigung für Systeme.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)
- Amazon EKS-Workshop: https://eksworkshop.com/intermediate/240_Monitoring/

Fortlaufende Integration/Fortlaufende Bereitstellung

Verwandte CI/CD-Projekte (Continuous Integration/Continuous Deployment) für Amazon-EKS- und Kubernetes-Cluster.

Jenkins X

CI/CD-Lösung für moderne Cloud-Anwendungen auf Amazon-EKS- und Kubernetes-Clustern.

- [Projekt-URL](#)
- [Projekt-Dokumentation](#)

Erfahren Sie mehr über die neuen Funktionen und die Roadmap von Amazon EKS

Sie können sich über die neuen Funktionen von Amazon EKS informieren, indem Sie auf der AWS Seite [Was gibt's Neues mit](#) zum Feed „Neuigkeiten“ scrollen. Sie können sich auch die [Roadmap ansehen](#) GitHub, die Sie über bevorstehende Funktionen und Prioritäten informiert, sodass Sie planen können, wie Sie Amazon EKS in future verwenden möchten. Sie können uns direktes Feedback zu den Roadmap-Prioritäten geben.

Dokumentverlauf

In der folgenden Tabelle werden einige der wichtigsten Updates und neuen Funktionen für das Amazon EKS-Benutzerhandbuch beschrieben. Um Benachrichtigungen zu erhalten, wenn diese Tabelle einen neuen Eintrag erhält, können Sie die folgende URL mit einem RSS-Reader abonnieren:

<https://docs.aws.amazon.com/eks/latest/userguide/doc-history.rss>

Änderung	Beschreibung	Datum
Inhaltsupdate zur Fehlerbehebung bei VPC CNI	Die Seite zur Fehlerbehebung für die Kubernetes-Netzwerkrichtlinie in der VPC-CNI wurde erweitert. Die Berechtigungen CRDs und die RBAC-Berechtigungen sowie 12 bekannte Probleme wurden hinzugefügt.	30. Juni 2025
Aktualisierung der Amazon-EKS-Plattformversion	Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. In dieser Plattformversion gibt es keine neuen Patch-Versionen von Kubernetes.	26. Juni 2025
AWS verwaltete Richtlinienaktualisierungen	<code>ssmmessages:OpenDataChannel</code> Erlaubnis zu hinzugefügt <code>AmazonEKSLocalOutpostServiceRolePolicy</code> .	26. Juni 2025
AWS verwaltete Richtlinienaktualisierungen	Es wurden Berechtigungen hinzugefügt, <code>AmazonEKSServiceRolePolicy</code> <code>AmazonEKSComputePolicy</code> um Amazon EKS	20. Juni 2025

Auto Mode das Starten von Instances mithilfe der EC2 On-Demand-Kapazitätsreservierungen in Ihrem Konto zu ermöglichen. Außerdem wurden die Berechtigungen `AmazonEKSCoordinateInstances` für Amazon EKS hinzugefügt, um die mit dem EC2 Spot-Dienst verknüpfte Rolle in Ihrem Namen zu erstellen.

[Verwaltete Richtlinienaktualisierungen](#)

AmazonEKSDashboard ConsoleReadOnly Richtlinie hinzugefügt. 19. Juni 2025

[Aktualisierung des automatischen Modus von Amazon EKS auf NodeClass](#)

Die NodeClass Vorlage für Knoten im automatischen Modus fügte eine Konfiguration für separate Pod-Subnetze hinzu. Dadurch werden die optionalen Schlüssel hinzugefügt `podSubnetSelectorTerms` und `podSecurityGroupSelectorTerms` die Subnetze und Sicherheitsgruppen für die Pods festgelegt. 13. Juni 2025

[Mit EKS Pod Identities zielen Sie auf sekundäre und kontoübergreifende Rollen ab](#)

Amazon EKS fügt EKS Pod Identities Ziel-IAM-Rollen für eine automatisierte Rollenverkettung hinzu. Sie können dies verwenden, um automatisch eine Rolle in einem anderen Konto zu übernehmen, und EKS Pod Identity wechselt die temporären Anmeldeinformationen. Jede Pod Identity-Zuordnung muss über eine IAM-Rolle in demselben Konto verfügen, um sie zuerst übernehmen zu können. Anschließend verwendet sie diese Rolle, um die Zielrolle zu übernehmen.

11. Juni 2025

[Aktualisierung der Amazon-EKS-Plattformversion](#)

Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. In dieser Plattformversion gibt es keine neuen Patch-Versionen von Kubernetes.

11. Juni 2025

[Erweiterung der Amazon AWS EKS-Region](#)

Amazon EKS ist jetzt in der AWS Region Asien-Pazifik (Taipeh) (ap-east-2) verfügbar.

6. Juni 2025

[IPv6Zugriffskontrolle für öffentliche Dual-Stack-Endpunkte für neue Cluster IPv6](#)

5. Juni 2025

[Aktualisierung der Amazon-EKS-Plattformversion](#)

Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Dazu gehören neue Patch-Versionen von Kubernetes 1.32.5, und 1.31.9 1.30.13

30. Mai 2025

[Neue Cluster-Einblicke für EKS-Hybridknoten](#)

Amazon EKS bietet neue Cluster-Einblicke, die die Konfiguration Ihrer Hybridknoten überprüfen. Diese Insight-Checks warnen Sie vor Problemen mit lokalen Knoten und Pods sowie der Remote-Netzwerkkonfiguration des Clusters.

29. Mai 2025

[Kubernetes-Version 1.33](#)

1.33 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.

29. Mai 2025

[Zusätzliche Unterstützung für den Amazon FSx CSI-Treiber](#)

Sie können jetzt die AWS Management Console, AWS CLI und API verwenden, um den Amazon FSx CSI-Treiber zu verwalten.

23. Mai 2025

[Prometheus-Scraper in der Konsole bearbeiten](#)

Sie können jetzt Amazon Managed Service für Prometheus-Scraper in der Amazon EKS-Konsole bearbeiten.

22. Mai 2025

<u>Verwaltete Richtlinienaktualisierungen</u>	AmazonEKSDashboard ServiceRolePolicy Richtlinie hinzugefügt.	21. Mai 2025
<u>Aktualisierung der Amazon-EKS-Plattformversion</u>	Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. In diesen Plattformversionen gibt es keine neuen Patch-Versionen von Kubernetes.	16. Mai 2025
<u>Neue Seiten für Amazon FSx for Lustre Performance</u>	Es wurden neue Themen mit Details zur Optimierung der Leistung von Amazon FSx for Lustre hinzugefügt.	2. Mai 2025
<u>Aktualisierung des automatischen Modus von Amazon EKS auf NodeClass</u>	Die NodeClass Vorlage für Knoten im automatischen Modus fügte eine Konfiguration für Forward-Netzwerk-Proxys hinzu. Dadurch wird der optionale Schlüssel advancedNetworking zum Einstellen Ihres HTTPS-Proxys hinzugefügt.	30. April 2025
<u>Bottlerocket für Hybridknoten</u>	Bottlerocket ist jetzt für EKS-Hybridknoten verfügbar.	29. April 2025
<u>Aktualisierung der Amazon-EKS-Plattformversion</u>	Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. In diesen Plattformversionen gibt es keine neuen Patch-Versionen von Kubernetes.	29. April 2025

[Seiten mit neuen Konzepten
für hybride Netzwerke](#)

Seiten für Konzepte von EKS-Hybridknoten hinzugefügt. Diese behandeln die lokalen und Cloud-Netzwerke im Detail anhand von Diagrammen.

18. April 2025

[AWS verwaltete Richtlinienaktualisierungen](#)

Es wurden Berechtigungen hinzugefügt, AmazonEKS ClusterPolicy um Amazon EKS den Zugriff auf elastische Netzwerkschnittstellen zu ermöglichen, die von der VPC CNI erstellt wurden. Dies ist erforderlich, damit EKS elastische Netzwerkschnittstellen bereinigen kann, die zurückbleiben, wenn das VPC-CNI unerwartet beendet wird.

16. April 2025

[AWS verwaltete Richtlinienaktualisierungen](#)

Es wurden Berechtigungen hinzugefügt AmazonEKS ServiceRolePolicy , um AI/ML EKS-Kunden das Hinzufügen von Ausgangsregeln zur standardmäßigen EKS-Cluster-Sicherheitsgruppe zu ermöglichen.

14. April 2025

Zustand der Knoten für EKS-Hybridknoten

Sie können es ab Version `eks-node-monitoring-agent` auf Hybridknoten verwenden `1.2.0-eks-build.1`. Wird `eks-node-monitoring-agent` als Amazon EKS-Add-on ausgeführt, um Gesundheitsprobleme zu erkennen und anzuzeigen.

31. März 2025

EKS-Hybridknoten für bestehende Cluster

Sie können jetzt die Konfiguration der Hybridknoten vorhandener Cluster hinzufügen, ändern oder entfernen. Bisher konnten Sie die Konfiguration der Hybridknoten nur zu neuen Clustern hinzufügen, wenn Sie sie erstellt hatten. Mit Amazon EKS Hybrid Nodes können Sie Ihre lokale Infrastruktur und Ihre Edge-Infrastruktur als Knoten in Amazon EKS-Clustern verwenden. AWS verwaltet die AWS gehostete Kubernetes-Steuerebene des Amazon EKS-Clusters, und Sie verwalten die Hybridknoten, die in Ihren lokalen oder Edge-Umgebungen ausgeführt werden.

31. März 2025

[Rollback: Vermeiden Sie versehentliche Upgrades mit Cluster-Erkenntnissen](#)

Amazon EKS hat vorübergehend eine Funktion zurückgesetzt, bei der Sie bei bestimmten Cluster-Insight-Problemen ein `--force` Flag verwenden müssten, um Ihren Cluster zu aktualisieren. Weitere Informationen finden Sie unter [Vorübergehendes Rollback der Durchsetzung von Upgrade-Erkenntnissen bei der Aktualisierung der Cluster-Version auf](#). [GitHub](#)

28. März 2025

[Bottlerocket FIPS AMIs](#)

Bottlerocket FIPS AMIs sind jetzt in standardmäßigen verwalteten Knotengruppen verfügbar.

27. März 2025

[AWS verwaltete Richtlinienaktualisierungen](#)

Es wurden Berechtigungen hinzugefügt, AmazonEKS ServiceRolePolicy um Amazon EKS das Beenden von EC2 Instances zu ermöglichen, die im automatischen Modus erstellt wurden. Es wurden Berechtigungen hinzugefügt, AmazonEKS ServiceRolePolicy um Amazon EKS das Beenden von EC2 Instances zu ermöglichen, die im automatischen Modus erstellt wurden.

28. Februar 2025

[Aktualisieren Sie die Strategie n für verwaltete Knotengru ppen](#)

Sie können jetzt Aktualisierungsstrategien verwenden , um den Versionsupdate-Prozess für verwaltete Knotengruppen zu konfigurieren. Damit wird die Minimalaktualisierungsstrategie eingeführt, bei der Knoten beendet werden, bevor neue erstellt werden, was in Umgebungen mit eingeschränkter Kapazität nützlich ist. Die Standard-Aktualisierungsstrategie setzt das bestehende Verhalten fort.

27. Januar 2025

[Kubernetes-Version 1.32](#)

1.32 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.

23. Januar 2025

[Erweiterung der Amazon AWS EKS-Region](#)

Amazon EKS ist jetzt in den AWS Regionen Asien-Pazifik (Thailand) (ap-southeast-7) und Mexiko (Zentral) (mx-central-1) verfügbar. Der automatische EKS-Modus und VPC-Endpunkte für die EKS-API sind in keiner der beiden Regionen verfügbar.

14. Januar 2025

<u>AWS verwaltete Richtlinienaktualisierungen</u>	Es wurden mehrere Berechtigungen hinzugefügt <code>AmazonEBS CSI Driver Policy</code> , damit der Amazon EBS CSI-Treiber alle Snapshots wiederherstellen, Fast Snapshot Restore (FSR) auf EBS-Volumes aktivieren und Tags auf Volumes ändern kann.	13. Januar 2025
<u>AWS verwaltete Richtlinienaktualisierungen</u>	Berechtigungen wurden hinzugefügt zu <code>AmazonEKS LoadBalancingPolicy</code> .	26. Dezember 2024
<u>Die Cluster-Einblicke wurden aktualisiert</u>	Amazon EKS Upgrade Insights warnt nun vor weiteren Problemen mit dem Clusterstatus und der Versionskompatibilität. Es kann Probleme zwischen verschiedenen Kubernetes- und Amazon EKS-Komponenten wie <code>kubelet</code> <code>kube-proxy</code> , und Amazon EKS-Add-Ons erkennen.	20. Dezember 2024
<u>Agent zur Knotenüberwachung und auto Reparatur</u>	Sie können das neue Add-on <code>eks-node-monitoring-agent</code> als Amazon EKS verwenden, um Gesundheitsprobleme zu erkennen und anzuzeigen. Sie können auch die auto Knotenreparatur aktivieren, um Knoten automatisch zu ersetzen, wenn Probleme erkannt werden.	16. Dezember 2024

[Amazon EKS-Hybridknoten](#)

Sie können jetzt Knoten lokal ausführen, die mit Amazon EKS-Clustern verbunden sind. Mit Amazon EKS Hybrid Nodes können Sie Ihre lokale Infrastruktur und Ihre Edge-Infrastruktur als Knoten in Amazon EKS-Clustern verwenden. AWS verwaltet die AWS gehostete Kubernetes-Steuerebene des Amazon EKS-Clusters, und Sie verwalten die Hybridknoten, die in Ihren lokalen oder Edge-Umgebungen ausgeführt werden.

01. Dezember 2024

[Automatischer Amazon EKS-Modus](#)

Amazon EKS Auto Mode automatisiert die Verwaltung der Kubernetes-Cluster-Infrastruktur für Datenverarbeitung, Speicherung und Netzwerke vollständig. AWS Es vereinfacht das Kubernetes-Management durch die automatische Bereitstellung der Infrastruktur, die Auswahl optimaler Recheninstanzen, die dynamische Skalierung von Ressourcen, die kontinuierliche Optimierung der Kosten, das Patchen von Betriebssystemen und die Integration mit Sicherheitsservices. AWS

01. Dezember 2024

[Aktualisierung der Amazon-EKS-Plattformversion](#)

Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Dies schließt neue Patch-Versionen von Kubernetes 1.31.2, 1.30.6, 1.29.10 und 1.28.15 mit ein.

22. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

Aus `AWSServiceRoleForAmazonEKSNodegroup` Gründen der Kompatibilität mit China Regionen aktualisiert.

22. November 2024

[Kubernetes Version 1.30 ist jetzt für lokale Cluster auf Outposts verfügbar AWS](#)

Sie können jetzt mit Kubernetes Version 1.30 einen lokalen Amazon EKS-Cluster auf einem AWS Outposts erstellen.

21. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat die AWS verwaltete Richtlinie `AmazonEKSLocalOutpostsClusterPolicy` aktualisiert. Es wurde eine `ec2:DescribeAvailabilityZones` Berechtigung hinzugefügt, damit der AWS Cloud Controller Manager auf der Cluster-Steuerebene die Availability Zone identifizieren kann, in der sich jeder Knoten befindet.

21. November 2024

[Bottlerocket, die FIPS AMIs 140-3 verwenden](#)

Bottlerocket AMIs sind verfügbar, die für die Verwendung von FIPS 140-3-validierten kryptografischen Modulen vorkonfiguriert sind. Dazu gehören das Amazon Linux 2023 Kernel Cryptographic API Cryptographic Module und das AWS-LC Cryptographic Module.

20. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

Die `AWSServiceRoleForAmazonEKSNodegroup` Richtlinie wurde aktualisiert, `ec2:RebootInstances` um Instances zuzulassen, die von Amazon EKS verwalteten Knotengruppen erstellt wurden. Die `ec2:CreateTags` Berechtigungen für EC2 Amazon-Ressourcen wurden eingeschränkt.

20. November 2024

[Dashboard zur Beobachtbarkeit](#)

Das Observability-Dashboard hilft Ihnen dabei, Probleme schnell zu erkennen, zu beheben und zu beheben. Im Namespace sind auch [CloudWatch neue Metriken](#) verfügbar. AWS/EKS

18. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat die AWS verwaltete Richtlinienaktualisierung `AmazonEKSServiceRolePolicy` . Es wurden Berechtigungen für EKS-Zugriffsrichtlinien, Load Balancer-Management und automatische Cluster-Ressourcenbereinigung hinzugefügt.

16. November 2024

[Neue Rollenerstellung in der Konsole für Add-Ons, die EKS Pod Identities unterstützen](#)

Bei der Verwendung der Konsole zum Erstellen oder Aktualisieren von Add-Ons, die EKS Pod Identities unterstützen, gibt es neue Schritte, mit denen Sie automatisch IAM-Rollen mit dem entsprechenden Namen, der Rollenrichtlinie und der Vertrauensrichtlinie für das Add-on generieren können.

15. November 2024

[Verwaltete Knotengruppen in AWS Local Zones](#)

Verwaltete Knotengruppen können jetzt in AWS Local Zones erstellt werden.

15. November 2024

[Neue Metriken sind verfügbar](#)

In der API-Gruppe sind neue Metriken verfügbar `metrics.eks.amazonaws.com` .

11. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat die AWS verwaltete Richtlinie aktualisiert `AmazonEKSClusterPolicy`. Die Ressourcenerweiterungen für die `iam:AddRoleToInstanceProfile` Aktion wurden aktualisiert.

7. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt: `AmazonEKSClusterPolicy`

1. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

Berechtigungen wurden hinzugefügt zu `AmazonEKSClusterPolicy`. Es wurde die `ec2:DescribeInstancesTopology` Berechtigung hinzugefügt, damit Amazon EKS Topologieinformationen als Labels an den Knoten anhängen kann.

1. November 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt: `AmazonEKSElasticBlockStorePolicy`

30. Oktober 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt: `AmazonEKSElasticLoadBalancingPolicy`

30. Oktober 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

Es wurden `cloudwatch:PutMetricData` Berechtigungen hinzugefügt, `AmazonEKSServiceRolePolicy` die es Amazon EKS ermöglichen, Metriken auf Amazon zu veröffentlichen CloudWatch.

29. Oktober 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt: `AmazonEKSNetworkingPolicy`

28. Oktober 2024

[Dual-Stack-Endpunkte für neue Cluster IPv6](#)

Stellen Sie eine Connect zu neuen IPv6 Clustern mit einem `eks-cluster.region.api.aws` Dual-Stack-Endpunkt her. Dieser Endpunkt wird zurückgegeben, wenn Sie diese Cluster beschreiben. `kubectl` und andere Kubernetes-API-Clients in IPv4IPv6, oder Dual-Stack-Umgebungen können diese Endpunkte für öffentliche oder private Cluster auflösen und eine Verbindung zu ihnen herstellen.

21. Oktober 2024

[AWS verwaltete Richtlinienaktualisierungen](#)

Es wurden autoscaling:ResumeProcesses und autoscaling:SuspendProcesses , und zugehörige Berechtigungen für die Integration mit Amazon Application Recovery Controller for EKS AWSServiceRoleForAmazonEKSNodegroup in den Regionen China hinzugefügt. Keine Änderungen an anderen Regionen.

21. Oktober 2024

[AL2023 beschleunigt AMIs](#)

Sie können jetzt beschleunigte NVIDIA und AWS Neuron-Instances für verwenden, die auf AMIs 023 basieren. AL2

11. Oktober 2024

[Neues Quellformat](#)

Wir haben mit einigen Layoutänderungen auf ein neues Quellformat umgestellt. Es gibt vorübergehend kleinere Formatierungsprobleme, die wir beheben werden.

10. Oktober 2024

[AWS verwaltete Richtlini
enaktualisierungen](#)

Berechtigungen für AmazonEKSServicePolicy und hinzugefügt AmazonEKSServiceRolePolicy. Tag-Berechtigungen wurden hinzugefügt ec2:GetSecurityGroupsForVpc und verknüpft, damit EKS Sicherheitsgruppeninformationen lesen und zugehörige Tags aktualisieren kann.

10. Oktober 2024

[AWS verwaltete Richtlini
enaktualisierungen — Neue
Richtlinie](#)

EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt.

3. Oktober 2024

[Kubernetes-Version 1.31](#)

1.31 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.

24. September 2024

[AWS verwaltete Richtlini
enaktualisierungen — Aktualisi
erung einer bestehenden
Richtlinie](#)

Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.

21. August 2024

[Kubernetes Version 1.29 ist
jetzt für lokale Cluster auf
Outposts verfügbar AWS](#)

Sie können jetzt mit Kubernetes Version 1.29 einen lokalen Amazon EKS-Cluster auf einem AWS Outposts erstellen.

20. August 2024

[EKS-Pod-Identität in \(USA\)
AWS GovCloud](#)

Amazon EKS Pod Identität
s verknüpfen eine IAM-Rolle
mit einem Kubernetes-Service
konto. Mit diesem Feature
müssen Sie der Knoten-
IAM-Rolle keine erweitert
en Berechtigungen mehr
bereitstellen. Auf diese Weise
können Pods auf diesem
Knoten aufrufen. AWS APIs
Im Gegensatz zu IAM-Rollen
für Dienstkonten befinden sich
EKS-Pod-Identitäten vollständ
ig in EKS. Sie benötigen
keinen OIDC-Identitätsanb
ieter.

14. August 2024

[Szenariogesteuerte Inhaltsak
tualisierungen](#)

Wir haben die Themen
umbenannt und aktualisi
ert, sodass sie im gesamten
Leitfaden stärker von
Szenarien abhängen.

9. August 2024

[Dual-Stack-VPC-Schnittstell
en-Endpunkte für Amazon
EKS](#)

Sie können jetzt Dual-Stack-
VPC-Schnittstellenendpunk
te für Amazon EKS mit IPv6
IP-Adressen IPv4 und DNS-
Namen erstellen.

7. August 2024

[Neue Dual-Stack-Endpunkte für Amazon EKS APIs mit Adressen IPv6](#)

Die EKS-API für die Erstellung und Verwaltung von Clustern und der OIDC-Issuer URLs für Cluster verfügen über neue Dual-Stack-Endpunkte. Der neue DNS-Name für die Amazon EKS-API lautet `eks.region.api.aws`, der in IPv4 Adressen und IPv6 Adressen aufgelöst wird. Neue Cluster haben eine neue Dual-Stack-OIDC-Aussteller-URL (`.oidc-eks.region.api.aws`).

1. August 2024

[Kapazitätsblöcke für verwaltete Knotengruppen](#)

Sie können jetzt Kapazitätsblöcke für verwaltete Knotengruppen verwenden.

1. Juli 2024

[Die Erfassung von Auto Scaling Group-Metriken ist standardmäßig aktiviert](#)

Für von Amazon EKS verwaltete Knotengruppen sind jetzt standardmäßig Amazon EC2 Auto Scaling Scaling-Gruppenmetriken ohne zusätzliche Kosten aktiviert. Bisher mussten Sie mehrere Schritte ausführen, um diese Funktion zu aktivieren.

28. Juni 2024

[AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie](#)

Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.

27. Juni 2024

[Kubernetes-Version 1.26](#)

Die Kubernetes-Version 1.26 wird jetzt erweitert.

12. Juni 2024

Verbesserungen der AMI-Informationsreferenzen	Wir haben die AMI-Informationsreferenzen verbessert, insbesondere für Bottlerocket.	12. Juni 2024
Kubernetes-Version 1.30	1.30 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	23. Mai 2024
Automatische CoreDNS-Skalierung	CoreDNS Autoscaler passt die Anzahl der Replikate der CoreDNS in einem EKS-Cluster dynamisch an die Anzahl der Knoten und CPU-Kerne an. Diese Funktion funktioniert für CoreDNS v1.9 und die neueste Plattformversion der EKS-Release-Version 1.25 und höher.	14. Mai 2024
Aktualisierung der Amazon-EKS-Plattformversion	Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Dies beinhaltet neue Patch-Versionen von Kubernetes 1.29.4, und 1.28.9 1.27.13	14. Mai 2024
CloudWatch Container Insights-Unterstützung für Windows	Das Amazon CloudWatch Observability Operator-Add-on ermöglicht jetzt auch Container Insights auf Windows-Worker-Knoten im Cluster.	10. April 2024
Kubernetes-Konzepte	Neues Thema zu Kubernetes-Konzepten hinzugefügt.	5. April 2024

[Restrukturieren Sie Access und IAM-Inhalte](#)

Verschieben Sie bestehende Seiten, die sich auf Access- und IAM-Themen beziehen, wie z. B. Auth Config Map, Zugriffseinträge, Pod-ID und IRSA, in einen neuen Abschnitt. Überarbeiten Sie den Inhalt der Übersicht.

2. April 2024

[Bottlerocket OS-Unterstützung für den Amazon S3 CSI-Treiber](#)

Der Mountpoint for Amazon S3 CSI-Treiber ist jetzt mit Bottlerocket kompatibel.

13. März 2024

[AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie](#)

Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.

4. März 2024

[Amazon Linux 2023](#)

Amazon Linux 2023 (AL2023) ist ein neues Linux-basiertes Betriebssystem, das eine sichere, stabile und leistungsstarke Umgebung für Ihre Cloud-Anwendungen bietet.

29. Februar 2024

[EKS Pod Identity und IRSA unterstützen Sidecars in Kubernetes 1.29](#)

In Kubernetes sind 1.29 Sidecar-Container in Amazon EKS-Clustern verfügbar. Sidecar-Container werden mit IAM-Rollen für Dienstkonten oder EKS Pod Identity unterstützt. Weitere Informationen zu Sidecars finden Sie unter [Sidecar](#) Containers in der Kubernetes-Dokumentation.

26. Februar 2024

Kubernetes-Version 1.29	1.29 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	23. Januar 2024
Vollständige Version: Amazon EKS Extended Support für Kubernetes-Versionen	Die erweiterte Unterstützung für Kubernetes-Versionen ermöglicht es Ihnen, länger als 14 Monate bei einer bestimmten Kubernetes-Version zu bleiben.	16. Januar 2024
Zustandserkennung von Amazon EKS-Clustern in der AWS Cloud	Amazon EKS erkennt Probleme mit Ihren Amazon EKS-Clustern und der Infrastruktur der Cluster-Voraussetzungen in der Cluster-Integrität. Sie können die Probleme mit Ihren EKS-Clustern im AWS Management Console und im Cluster in health der EKS-API einsehen. Diese Probleme werden zusätzlich zu den Problemen erkannt, die von der Konsole erkannt und angezeigt werden. Bisher war die Clusterintegrität nur für lokale Cluster auf AWS Outposts verfügbar.	28. Dezember 2023
Einblicke in Cluster	Sie können jetzt Empfehlungen für Ihren Cluster erhalten, die auf wiederkehrenden Prüfungen basieren.	20. Dezember 2023

[Erweiterung der Amazon AWS EKS-Region](#)

Amazon EKS ist jetzt in der AWS Region Kanada West (Calgary) (ca-west-1) verfügbar.

20. Dezember 2023

[Sie können jetzt mithilfe von Zugriffseinträgen IAM-Rollen und -Benutzern Zugriff auf Ihren Cluster gewähren.](#)

Vor der Einführung von Zugriffseinträgen haben Sie IAM-Rollen und -Benutzern Zugriff auf Ihren Cluster gewährt, indem Sie Einträge zu aws-auth ConfigMap hinzugefügt haben. Jetzt verfügt jeder Cluster über einen Zugriffsmodus und Sie können nach Ihrem eigenen Zeitplan auf die Verwendung von Zugriffseinträgen umsteigen. Nachdem Sie den Modus gewechselt haben, können Sie Benutzer hinzufügen, indem Sie Zugriffseinträge in der AWS CLI AWS CloudFormation, und dem hinzufügen AWS SDKs.

18. Dezember 2023

[Aktualisierung der Amazon-EKS-Plattformversion](#)

Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Dies schließt neue Patch-Versionen von Kubernetes 1.28.4, 1.27.8, 1.26.11 und 1.25.16 mit ein.

12. Dezember 2023

[Mountpoint für Amazon S3 CSI-Treiber](#)

Sie können jetzt den Mountpoint for Amazon S3 CSI-Treiber auf Amazon EKS-Clustern installieren.

8. November 2023

[Prometheus-Metriken beim Erstellen eines Clusters aktivieren](#)

In der AWS Management Console können Sie jetzt Prometheus-Metriken aktivieren, wenn Sie einen Cluster erstellen. Sie können die Details zum Prometheus-Scraper auch auf der Registerkarte Observability anzeigen.

26. November 2023

[Amazon-EKS-Pod-Identitäten](#)

Amazon EKS Pod Identitäten verknüpfen eine IAM-Rolle mit einem Kubernetes-Servicekonto. Mit diesem Feature müssen Sie der Knoten-IAM-Rolle keine erweiterten Berechtigungen mehr bereitstellen. Auf diese Weise können Pods auf diesem Knoten aufrufen. AWS APIs Im Gegensatz zu IAM-Rollen für Dienstkonten befinden sich EKS-Pod-Identitäten vollständig in EKS. Sie benötigen keinen OIDC-Identitätsanbieter.

26. November 2023

[AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie](#)

Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.

26. November 2023

CSI-Snapshot-Controller	Sie können den CSI-Snapshot-Controller jetzt für die Verwendung mit kompatiblen CSI-Treibern wie dem Amazon-EBS-CSI-Treiber installieren.	17. November 2023
Neuverfassung des Themas „ADOT Operator“	Der Bereich Amazon EKS-Add-On-Unterstützung für ADOT Operator war zusammen mit der AWS Distribution zur OpenTelemetry Dokumentation überflüssig. Wir haben die verbleibenden wichtigen Informationen auf diese Ressource migriert, um veraltete und inkonsistente Informationen zu reduzieren.	14. November 2023
CoreDNS EKS-Add-On-Unterstützung für Prometheus-Metriken	Die v1.8.7-eksbuild.8 Versionen v1.10.1-eksbuild.5 v1.9.3-eksbuild.9 , und des EKS-Add-ons für CoreDNS machen den Port, für den CoreDNS Metriken veröffentlicht hat, im Service verfügbar. kube-dns Dies macht es einfacher , die CoreDNS-Metriken in Ihre Überwachungssysteme aufzunehmen.	10. November 2023
Amazon EKS CloudWatch Observability Operator-Add-on	Die Amazon EKS CloudWatch Observability Operator-Seite wurde hinzugefügt.	6. November 2023

[Kapazitätsblöcke für selbstverwaltete P5-Instances in USA Ost \(Ohio\)](#)

In USA Ost (Ohio) können Sie Kapazitätsblöcke jetzt für selbstverwaltete P5-Instances verwenden.

31. Oktober 2023

[Cluster unterstützen das Ändern von Subnetzen und Sicherheitsgruppen](#)

Sie können den Cluster aktualisieren, um zu ändern, welche Subnetze und Sicherheitsgruppen der Cluster verwendet. Sie können von der AWS Management Console, der neuesten Version der AWS CLI AWS CloudFormation, und `eksctl` Version `v0.164.0-rc.0` oder höher aus aktualisieren. Möglicherweise müssen Sie dies tun, um Subnetzen mehr verfügbare IP-Adressen zur Verfügung zu stellen, damit eine Clusterversion erfolgreich aktualisiert werden kann.

24. Oktober 2023

[Die Clusterrolle und die Rolle der verwalteten Knotengruppe unterstützen vom Kunden verwaltete AWS Identity and Access Management Zugriffsverwaltungsrichtlinien](#)

Sie können anstelle der von [Amazon Policy AWS verwalteten Richtlinie eine benutzerdefinierte EKSCluster IAM-Richtlinie für](#) die Cluster-Rolle verwenden. Außerdem können Sie anstelle der von [Amazon](#) verwalteten Richtlinie eine benutzerdefinierte IAM-Richtlinie für die Knotenrolle in einer EKSWorker NodePolicy AWS verwalteten Knotengruppe verwenden. Auf diese Weise können Sie eine Richtlinie mit der geringsten Berechtigung erstellen, um strenge Compliance-Anforderungen zu erfüllen.

23. Oktober 2023

[Link zur Installation von eksctl korrigiert](#)

Korrigiert den Installationslink für eksctl, nachdem die Seite verschoben wurde.

06. Oktober 2023

[Vorabversion: Amazon EKS Extended Support für Kubernetes-Versionen](#)

Die erweiterte Unterstützung für Kubernetes-Versionen ermöglicht es Ihnen, länger als 14 Monate bei einer bestimmten Kubernetes-Version zu bleiben.

04. Oktober 2023

[Verweise auf die AWS App Mesh Mesh-Integration entfernen](#)

Amazon EKS-Integrationen mit AWS App Mesh stehen weiterhin nur bestehenden Kunden von App Mesh zur Verfügung.

29. September 2023

Kubernetes-Version 1.28	1.28 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	26. September 2023
Bestehende Cluster unterstützen die Durchsetzung von Kubernetes-Netzwerkrichtlinien im Amazon VPC CNI-Plugin für Kubernetes	Sie können die Kubernetes-Netzwerkrichtlinie in vorhandenen Clustern mit dem Amazon VPC CNI-Plugin für Kubernetes verwenden, anstatt eine Drittanbieterlösung zu benötigen. Sie können die Kubernetes-Netzwerkrichtlinie in vorhandenen Clustern mit dem Amazon VPC CNI-Plugin für Kubernetes verwenden, anstatt eine Drittanbieterlösung zu benötigen.	15. September 2023
Das CoreDNS Amazon EKS Add-on unterstützt das Ändern von PDB	Sie können das PodDisruptionBudget EKS-Add-On für CoreDNS in Versionen v1.9.3-eksbuild.7 und höher v1.10.1-eksbuild.4 und später ändern.	15. September 2023
Amazon-EKS-Unterstützung für gemeinsam genutzte Subnetze	Neue Anforderungen und Überlegungen für gemeinsam genutzte Subnetze für die Erstellung von Amazon-EKS-Clustern in gemeinsam genutzten Subnetzen.	07. September 2023

Aktualisierungen an „Was ist Amazon EKS?“	Neue Themen in Häufige Anwendungsfälle und Architektur hinzugefügt. Andere Themen wurden aktualisiert.	6. September 2023
Durchsetzung von Kubernetes-Netzwerkrichtlinien im Amazon VPC CNI-Plugin für Kubernetes	Sie können die Kubernetes-Netzwerkrichtlinie mit dem Amazon VPC CNI-Plugin für Kubernetes verwenden, anstatt eine Drittanbieterlösung zu benötigen. Sie können die Kubernetes-Netzwerkrichtlinie mit dem Amazon VPC CNI-Plugin für Kubernetes verwenden, anstatt eine Drittanbieterlösung zu benötigen.	29. August 2023
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Israel (Tel Aviv) (il-central-1) verfügbar.	1. August 2023
Konfigurierbarer flüchtiger Speicher für Fargate	Sie können die Gesamtmenge an flüchtigem Speicher für jeden Pod erhöhen, der auf Amazon EKS Fargate ausgeführt wird.	31. Juli 2023
Add-on-Support für Amazon-EFS-CSI-Treiber	Sie können jetzt die AWS CLI und die AWS Management Console API verwenden, um den Amazon EFS CSI-Treiber zu verwalten.	26. Juli 2023
AWS verwaltete Richtlinienaktualisierungen — Neue Richtlinie	Amazon EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt.	26. Juli 2023

Kubernetes-Versionsupdates für 1.27, 1.26, 1.25 und 1.24 sind jetzt für lokale Cluster auf Outposts verfügbar AWS	Kubernetes-Versionsupdates auf 1.27.3, 1.26.6, 1.25.11 und 1.24.15 sind jetzt für lokale Cluster auf Outposts verfügbar AWS	20. Juli 2023
Unterstützung von IP-Präfixen für Windows-Knoten	Durch die Zuweisung von IP-Präfixen zu Ihren Knoten können Sie eine deutlich höhere Anzahl von Pods auf Ihren Knoten hosten, als wenn Sie Ihren Knoten einzelne sekundäre IP-Adressen zuweisen.	6. Juli 2023
Amazon FSx für OpenZFS CSI-Treiber	Sie können jetzt den Amazon FSx for OpenZFS CSI-Treiber auf Amazon EKS-Clustern installieren.	30. Juni 2023
Pods auf Linux-Knoten in IPv4 Clustern können jetzt mit IPv6 Endpunkten kommunizieren.	Nachdem Sie Ihrem Knoten eine IPv6 Adresse zugewiesen haben, ist die Adresse Ihrer Pods eine IPv4 Netzwerkadresse, die in die IPv6 Adresse des Knotens übersetzt wird, auf dem sie ausgeführt werden.	19. Juni 2023
Von Windows verwaltete Knotengruppen in Regionen AWS GovCloud (USA)	In den Regionen AWS GovCloud (USA) können verwaltete Amazon EKS-Knotengruppen jetzt Windows-Container ausführen.	30. Mai 2023

Kubernetes-Version 1.27	1.27 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	24. Mai 2023
Kubernetes-Version 1.26	1.26 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	11. April 2023
Domainlose GmSA	Sie können jetzt domänenloses GmSA mit Windows Pods verwenden.	27. März 2023
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Asien-Pazifik (Melbourne) (ap-southeast-4) verfügbar.	10. März 2023
CSI-Treiber für Amazon File Cache	Sie können jetzt den CSI-Treiber für Amazon File Cache in Amazon-EKS-Clustern installieren.	3. März 2023
Kubernetes Version 1.25 ist jetzt für lokale Cluster auf Outposts verfügbar AWS	Sie können jetzt mithilfe der Kubernetes-Versionen — einen lokalen Amazon EKS-Cluster auf einem Outpost erstellen. 1.22 1.25	1. März 2023
Kubernetes-Version 1.25	1.25 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	22. Februar 2023

AWS verwaltete Richtlinie enaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	07. Februar 2023
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in den AWS Regionen Asien-Pazifik (Hyderabadap-south-2), Europa (Zürich) (eu-central-2) und Europa (Spanien) (eu-south-2) verfügbar.	06. Februar 2023
Kubernetes-Versionen 1.21 — 1.24 sind jetzt für lokale Cluster auf AWS Outposts verfügbar.	Sie können jetzt mithilfe der Kubernetes-Versionen — einen lokalen Amazon EKS-Cluster auf einem Outpost erstellen. 1.21 1.24 Bisher war nur die Version 1.21 verfügbar.	17. Januar 2023
Amazon EKS unterstützt jetzt AWS PrivateLink	Sie können eine verwenden AWS PrivateLink , um eine private Verbindung zwischen Ihrer VPC und Amazon EKS herzustellen.	16. Dezember 2022
Windows-Unterstützung für verwaltete Knotengruppen	Sie können jetzt Windows für von Amazon EKS verwaltete Knotengruppen verwenden.	15. Dezember 2022
Amazon EKS-Add-Ons von unabhängigen Softwareanbietern sind jetzt im AWS Marketplace erhältlich	Sie können jetzt Amazon EKS-Add-Ons von unabhängigen Softwareanbietern über den AWS Marketplace durchsuchen und abonnieren.	28. November 2022

AWS verwaltete Richtlinie enaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	17. November 2022
Kubernetes-Version 1.24	1.24 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	15. November 2022
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Naher Osten (VAE) (me-central-1) verfügbar.	03. November 2022
AWS verwaltete Richtlinie enaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	24. Oktober 2022
AWS verwaltete Richtlinie enaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	20. Oktober 2022
Lokale Cluster auf AWS Outposts sind jetzt verfügbar	Sie können jetzt einen lokalen Amazon-EKS-Cluster auf einem Outpost erstellen.	19. September 2022
vCPU-basierte Kontingente in Fargate	Fargate stellt von Pod-basierten auf vCPU-basierte Kontingente um.	8. September 2022
AWS verwaltete Richtlinie enaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	31. August 2022

Kostenüberwachung	Amazon EKS unterstützt jetzt Kubecost, sodass Sie die Kosten nach Kubernetes-Ressourcen wie Pods, Knoten, Namespaces und Labels aufgeschlüsselt überwachen können.	24. August 2022
AWS verwaltete Richtlinienaktualisierungen — Neue Richtlinie	Amazon EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt.	24. August 2022
AWS verwaltete Richtlinienaktualisierungen — Neue Richtlinie	Amazon EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt.	23. August 2022
Markieren von Ressourcen für die Fakturierung	Unterstützung für ein von <code>aws:eks:cluster-name</code> generiertes Kostenzuweisungstag wurde für alle Cluster hinzugefügt.	16. August 2022
Fargate-Profil-Platzhalter	Unterstützung für Fargate-Profil-Platzhalter in den Selektorkriterien für Namespaces, Labelschlüssel und Labelwerte wurde hinzugefügt.	16. August 2022
Kubernetes-Version 1.23	1.23 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	11. August 2022

Sehen Sie sich die Kubernetes-Ressourcen an im AWS Management Console	Sie können jetzt Informationen zu den in Ihrem Cluster bereitgestellten Kubernetes-Ressourcen mithilfe von anzeigen. AWS Management Console	3. Mai 2022
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Asien-Pazifik (Jakarta) (ap-southeast-3) verfügbar.	2. Mai 2022
Seite „Beobachtbarkeit“ und ADOT-Add-on-Unterstützung	Die Observability-Seite und die AWS Distribution für OpenTelemetry (ADOT) wurden hinzugefügt.	21. April 2022
Kubernetes-Version 1.22	1.22Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	4. April 2022
AWS verwaltete Richtlinienaktualisierungen — Neue Richtlinie	Amazon EKS hat eine neue AWS verwaltete Richtlinie hinzugefügt.	4. April 2022
Patch-Details für Fargate Pod hinzugefügt	Beim Upgrade von Fargate Pods versucht Amazon EKS zunächst, Pods auf der Grundlage Ihrer Budgets für Pod-Unterbrechungen zu entfernen. Sie können Ereignisregeln erstellen , um auf fehlgeschlagene Räumungen zu reagieren , bevor die Pods gelöscht werden.	1. April 2022

Vollständiger Release: Add-on-Support für Amazon-EBS-CSI-Treiber	Sie können jetzt die AWS CLI und die AWS Management Console API verwenden, um den Amazon EBS CSI-Treiber zu verwalten.	31. März 2022
AWS Aktualisierung der Inhalte von Outposts	Anweisungen zur Bereitstellung eines Amazon EKS-Clusters auf AWS Outposts.	22. März 2022
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	21. März 2022
Windows containerd - Unterstützung	Sie können jetzt die containerd -Laufzeit für Windows-Knoten auswählen.	14. März 2022
Überlegungen zum Amazon EKS Connector zur Sicherheitsdokumentation hinzugefügt	Beschreibt das Modell der gemeinsamen Verantwortung in Bezug auf verbundene Cluster.	25. Februar 2022
Weisen Sie Ihren Pods und Diensten IPv6 Adressen zu	Sie können jetzt einen 1.21 oder einen späteren Cluster erstellen, der Ihren Pods und Diensten IPv6 Adressen zuweist.	6. Januar 2022
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Amazon EKS hat eine bestehende AWS verwaltete Richtlinie aktualisiert.	13. Dezember 2021

[Vorversion: Add-on-Support für Amazon-EBS-CSI-Treiber](#)

Sie können jetzt eine Vorschau anzeigen AWS Management Console, indem Sie die AWS CLI und die API verwenden, um den Amazon EBS CSI-Treiber zu verwalten.

9. Dezember 2021

[Support von Karpenter Autoscaler](#)

Sie können jetzt das Karpenter -Open-Source-Projekt verwenden, um Ihre Knoten automatisch zu skalieren.

29. November 2021

[Support für Fluent-Bit-Kubernetes-Filter bei der Fargate-Protokollierung](#)

Sie können jetzt den Fluent-Bit-Kubernetes-Filter mit Fargate-Protokollierung verwenden.

10. November 2021

[Windows-Support in der Steuerebene verfügbar](#)

Windows-Support ist jetzt in Ihrer Steuerebene verfügbar. Sie müssen ihn nicht mehr in Ihrer Datenebene aktivieren.

9. November 2021

[Bottlerocket wurde als AMI-Typ für verwaltete Knotengruppen hinzugefügt](#)

Zuvor war Bottlerocket nur als Option für selbstverwaltete Knoten verfügbar. Jetzt kann es als verwaltete Knotengruppe konfiguriert werden, wodurch der Aufwand zur Erfüllung der Knoten-Compliance-Anforderungen reduziert wird.

28. Oktober 2021

<u>DL1 Treiber-Unterstützung</u>	Benutzerdefiniertes Amazon Linux unterstützt AMIs jetzt Deep-Learning-Workloads für Amazon Linux 2. Diese Aktivierung ermöglicht eine generische On-Premises- oder Cloud-Baseline-Konfiguration.	25. Oktober 2021
<u>VT1 Video-Unterstützung</u>	Benutzerdefiniertes Amazon Linux unterstützt AMIs VT1 jetzt einige Distributionen. Diese Aktivierung bewirbt Xilinx U30-Geräte in Ihrem Amazon-EKS-Cluster.	13. September 2021
<u>Amazon EKS Connector ist jetzt verfügbar</u>	Sie können Amazon EKS Connector verwenden, um jeden konformen Kubernetes-Cluster zu registrieren und zu verbinden AWS und ihn in der Amazon EKS-Konsole zu visualisieren.	8. September 2021
<u>Amazon EKS Anywhere ist jetzt verfügbar</u>	Amazon EKS Anywhere ist eine neue Bereitstellungsoption für Amazon EKS, mit der Sie Kubernetes-Cluster vor Ort erstellen und betreiben können.	8. September 2021
<u>Amazon FSx für NetApp ONTAP CSI-Treiber</u>	Es wurde ein Thema hinzugefügt, das den Amazon FSx for NetApp ONTAP CSI-Treiber zusammenfasst und Links zu anderen Referenzen enthält.	2. September 2021

[Verwaltete Knotengruppen berechnen jetzt automatisch die von Amazon EKS empfohlene maximale Anzahl an Pods für Knoten](#)

Verwaltete Knotengruppen berechnen jetzt automatisch die maximale Anzahl an Amazon EKS-Pods für Knoten, die Sie ohne Startvorlage oder mit einer Startvorlage bereitstellen, in der Sie keine AMI-ID angegeben haben.

30. August 2021

[Amazon-EKS-Verwaltung der Add-on-Einstellungen entfernen, ohne die Amazon-EKS-Add-on-Software zu entfernen](#)

Sie können jetzt ein Amazon-EKS-Add-on entfernen, ohne die Add-on-Software aus Ihrem Cluster zu entfernen.

20. August 2021

[Erstellen mehrfach vernetzter Pods mit Multus](#)

Sie können jetzt mit Multus mehrere Netzwerkschnittstellen zu einem Pod hinzufügen.

2. August 2021

[Fügen Sie Ihren EC2 Linux-Amazon-Knoten weitere IP-Adressen hinzu](#)

Sie können Ihren EC2 Linux-Amazon-Knoten jetzt deutlich mehr IP-Adressen hinzufügen. Das bedeutet, dass Sie auf jedem Knoten eine höhere Dichte an Pods ausführen können. Sie können Ihren EC2 Linux-Amazon-Knoten jetzt deutlich mehr IP-Adressen hinzufügen. Das bedeutet, dass Sie auf jedem Knoten eine höhere Dichte an Pods ausführen können.

27. Juli 2021

[containerd -Laufzeit-Bootstrap](#)

Das für Amazon EKS optimierte, beschleunigte Amazon Linux Amazon Machine Image (AMI) enthält jetzt ein Bootstrap-Flag, mit dem Sie die containerd Laufzeit in Amazon EKS Optimized und AMIs Bottlerocket aktivieren können. Dieses Flag ist in allen unterstützten Kubernetes-Versionen des AMI verfügbar.

19. Juli 2021

[Kubernetes-Version 1.21](#)

Unterstützung für die Kubernetes-Version hinzugefügt. 1.21

19. Juli 2021

[Thema zu verwalteten Richtlinien hinzugefügt](#)

Eine Liste aller von Amazon EKS IAM verwalteten Richtlinien und Änderungen, die seit dem 17. Juni 2021 daran vorgenommen wurden.

17. Juni 2021

[Verwenden Sie Sicherheitsgruppen für Pods mit Fargate](#)

Sie können jetzt Sicherheitsgruppen für Pods mit Fargate verwenden, zusätzlich zu deren Verwendung mit EC2 Amazon-Knoten.

1. Juni 2021

[CoreDNS- und kube-proxy -Amazon EKS-Add-ons hinzugefügt](#)

Amazon EKS kann Ihnen jetzt bei der Verwaltung der CoreDNS- und kube-proxy -Amazon-EKS-Add-ons für Ihren Cluster helfen.

19. Mai 2021

Kubernetes-Version 1.20	1.20 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	18. Mai 2021
AWS Load Balancer Controller veröffentlicht 2.2.0	Sie können jetzt den Load AWS Balancer Controller verwenden, um Elastic Load Balancer mithilfe von Instance- oder IP-Zielen zu erstellen.	14. Mai 2021
Knoten-Taints für verwaltete Knoten-Gruppen	Amazon EKS unterstützt jetzt das Hinzufügen von Notizmarkierungen zu verwalteten Knotengruppen.	11. Mai 2021
Geheimnisverschlüsselung für vorhandene Cluster	Amazon EKS unterstützt jetzt das Hinzufügen von Geheimnis-Verschlüsselung zu vorhandenen Clustern.	26. Februar 2021
Kubernetes-Version 1.19	1.19 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	16. Februar 2021
Amazon EKS unterstützt jetzt OpenID Connect (OIDC)-Identitätsanbieter als Methode zur Authentifizierung von Benutzern bei Clustern mit Version 1.16 oder höher.	OIDC-Identitätsanbieter können zusammen mit oder als Alternative zu AWS Identity and Access Management (IAM) verwendet werden.	12. Februar 2021

[Sehen Sie sich Knoten- und Workload-Ressourcen an im AWS Management Console](#)

Sie können jetzt Details zu Ihren verwalteten, selbstverwalteten und Fargate-Knoten sowie zu Ihren bereitgestellten Kubernetes-Workloads in der anzeigen. AWS Management Console

1. Dezember 2020

[Spot-Instance-Typen in einer verwalteten Knotengruppe bereitstellen](#)

Sie können nun mehrere Spot- oder On-Demand-Instance-Typen für eine verwaltete Knotengruppe bereitstellen.

1. Dezember 2020

[Amazon EKS kann jetzt spezifische Add-ons für Ihren Cluster verwalten](#)

Sie können Add-Ons selbst verwalten oder Amazon EKS erlauben, den Start und die Version eines Add-Ons über die Amazon-EKS-API zu steuern.

1. Dezember 2020

[Teilen Sie eine ALB über mehrere Ingresses](#)

Sie können jetzt einen AWS Application Load Balancer (ALB) für mehrere Kubernetes-Ingresses gemeinsam nutzen. In der Vergangenheit mussten Sie für jeden Ingress eine separate ALB bereitstellen.

23. Oktober 2020

[Unterstützung von NLB-IP-Zielen](#)

Sie können jetzt einen Network Load Balancer (NLB) mit IP-Zielen bereitstellen. Das bedeutet, dass Sie einen NLB verwenden können, um den Netzwerkverkehr auf Fargate Pods und direkt auf Pods, die auf EC2 Amazon-Knoten laufen, zu verteilen.

23. Oktober 2020

Kubernetes-Version 1.18	1.18 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	13. Oktober 2020
Geben Sie einen benutzerdefinierten CIDR-Block für die Zuweisung der Kubernetes-Service-IP-Adresse an.	Sie können jetzt einen benutzerdefinierten CIDR-Block angeben, von dem Kubernetes-Service-IP-Adressen zuweist.	29. September 2020
Weisen Sie einzelnen Pods Sicherheitsgruppen zu	Sie können jetzt einigen der einzelnen Pods, die auf vielen EC2 Amazon-Instance-Typen ausgeführt werden, verschiedene Sicherheitsgruppen zuordnen.	9. September 2020
Stellen Sie Bottlerocket auf Ihren Knoten bereit	Sie können jetzt Knoten bereitstellen, auf denen Bottlerocket ausgeführt wird.	31. August 2020
Die Möglichkeit, Arm-Knoten zu starten, ist allgemein verfügbar	Sie können jetzt Arm-Knoten in verwalteten und selbstverwalteten Knotengruppen starten.	17. August 2020
Startvorlagen für verwaltete Knotengruppen und benutzerdefiniertes AMI	Sie können jetzt eine verwaltete Knotengruppe bereitstellen, die eine EC2 Amazon-Startvorlage verwendet. Die Startvorlage kann bei Bedarf ein benutzerdefiniertes AMI angeben.	17. August 2020
EFS-Unterstützung für AWS Fargate	Sie können jetzt Amazon EFS mit AWS Fargate verwenden.	17. August 2020

[Aktualisierung der Amazon-EKS-Plattformversion](#)

Dies ist eine neue Plattformversion mit Sicherheitsfixes und -verbesserungen. Dies beinhaltet die UDP-Unterstützung für Dienste des Typs, LoadBalancer wenn Network Load Balancers mit der Kubernetes-Version oder höher verwendet werden. 1.15 Weitere Informationen finden Sie unter dem Problem [UDP für AWS Network Load Balancer zulassen](#) unter GitHub.

12. August 2020

[Erweiterung der Amazon AWS EKS-Region](#)

Amazon EKS ist jetzt in den AWS Regionen Afrika (Kapstadt) (af-south-1) und Europa (Mailand) (eu-south-1) verfügbar.

6. August 2020

[Fargate-Nutzungskennzahlen](#)

AWS Fargate stellt CloudWatch Nutzungsmetriken bereit, die Aufschluss darüber geben, wie Ihr Konto die Fargate-On-Demand-Ressourcen nutzt.

3. August 2020

[Kubernetes-Version 1.17](#)

1.17 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.

10. Juli 2020

Erstellen und Verwalten von App-Mesh-Ressourcen aus Kubernetes mit dem App-Mesh-Controller für Kubernetes	Sie können App-Mesh-Ressourcen in Kubernetes erstellen und verwalten. Der Controller injiziert außerdem automatisch den Envoy-Proxy und die Init-Container in die von Ihnen bereitgestellten Pods.	18. Juni 2020
Amazon EKS unterstützt jetzt Amazon EC2 Inf1-Knoten	Sie können Ihrem Cluster Amazon EC2 Inf1-Knoten hinzufügen.	4. Juni 2020
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in den Regionen AWS GovCloud (US-Ost) (us-gov-east-1) und AWS GovCloud (US-West) (us-gov-west-1) AWS verfügbar.	13. Mai 2020
Kubernetes 1.12 wird auf Amazon EKS nicht mehr unterstützt	Die Kubernetes-Version 1.12 wird auf Amazon EKS nicht mehr unterstützt. Aktualisieren Sie alle 1.12-Cluster auf Version 1.13 oder höher, um Service-Unterbrechungen zu vermeiden.	12. Mai 2020
Kubernetes-Version 1.16	1.16Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	30. April 2020
Die dienstverknüpfte AWSServiceRoleForAmazonEKS-Rolle wurde hinzugefügt	Die dienstgebundene AWSServiceRoleForAmazonEKS-Rolle wurde hinzugefügt.	16. April 2020

Kubernetes-Version 1.15	1.15 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	10. März 2020
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in den AWS Regionen Peking (cn-north-1) und Ningxia (cn-northwest-1) verfügbar.	26. Februar 2020
FSx für den Lustre CSI-Treiber	Es wurde ein Thema für die Installation des FSx for Lustre CSI-Treibers auf Kubernetes 1.14 Amazon EKS-Clustern hinzugefügt.	23. Dezember 2019
Beschränken des Netzwerkzugriffs auf den öffentlichen Zugriffsendpunkt eines Clusters	Mit diesem Update können Sie Amazon EKS verwenden, um die CIDR-Bereiche einzuschränken, die mit dem öffentlichen Zugriffsendpunkt des Kubernetes-API-Servers kommunizieren können.	20. Dezember 2019
Auflösen der privaten Zugriffsendpunkt-Adresse für einen Cluster von außerhalb einer VPC	Mit diesem Update können Sie Amazon EKS verwenden , um den privaten Zugriffsendpunkt des Kubernetes-API-Servers von außerhalb einer VPC aufzulösen.	13. Dezember 2019
(Beta) Amazon EC2 A1 EC2 Amazon-Instanzknoten	Starten Sie Amazon EC2 EC2 A1-Amazon-Instance-Knoten , die sich bei Ihrem Amazon EKS-Cluster registrieren.	4. Dezember 2019

Einen Cluster auf AWS Outposts erstellen	Amazon EKS unterstützt jetzt die Erstellung von Clustern auf AWS Outposts.	3. Dezember 2019
AWS Fargate auf Amazon EKS	Amazon EKS Kubernetes-Cluster unterstützen jetzt die Ausführung von Pods auf Fargate.	3. Dezember 2019
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Kanada (Zentral) (ca-central-1) verfügbar.	21. November 2019
Verwaltete Knotengruppen	Von Amazon EKS verwaltete Knotengruppen automatisieren die Bereitstellung und das Lebenszyklusmanagement von Knoten (EC2 Amazon-Instances) für Amazon EKS Kubernetes-Cluster.	18. November 2019
Aktualisierung der Amazon-EKS-Plattformversion	Neue Plattformversionen zur Berücksichtigung von CVE-2019-11253 .	6. November 2019
Kubernetes 1.11 wird auf Amazon EKS nicht mehr unterstützt	Die Kubernetes-Version 1.11 wird auf Amazon EKS nicht mehr unterstützt. Bitte aktualisieren Sie alle 1.11-Cluster auf Version 1.12 oder höher, um Service-Unterbrechungen zu vermeiden.	4. November 2019
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Südamerika (São Paulo) (sa-east-1) verfügbar.	16. Oktober 2019

Windows-Unterstützung	Amazon EKS-Cluster, auf denen die Kubernetes-Version ausgeführt wird, unterstützen 1.14 jetzt Windows-Workloads.	7. Oktober 2019
Auto Scaling	Es wurde ein Kapitel hinzugefügt, in dem einige der verschiedenen Arten von Kubernetes-Auto Scaling behandelt werden, die auf Amazon-EKS-Clustern unterstützt werden.	30. September 2019
Aktualisierung des Kubernetes-Dashboards	Das Thema zur Installation des Kubernetes-Dashboards auf Amazon EKS-Clustern zur Verwendung der Beta-Version 2.0 wurde aktualisiert.	28. September 2019
Amazon EFS-CSI-Treiber	Es wurde ein Thema für die Installation des Amazon EFS CSI-Treibers auf 1.14 Kubernetes-Amazon-EKS-Clustern hinzugefügt.	19. September 2019
Amazon EC2 Systems Manager Manager-Parameter für Amazon EKS-optimierte AMI-ID	Es wurde ein Thema zum Abrufen der für Amazon EKS optimierten AMI-ID mithilfe eines Amazon EC2 Systems Manager Manager-Parameters hinzugefügt. Mit diesem Parameter müssen Sie nicht mehr nach AMI suchen IDs.	18. September 2019
Amazon EKS-Resource-Tagging	Sie können die Markierung Ihrer Amazon-EKS-Cluster verwalten.	16. September 2019

Amazon-EBS-CSI-Treiber	Es wurde ein Thema für die Installation des Amazon EBS CSI-Treibers auf 1.14 Kubernetes-Amazon-EKS-Clustern hinzugefügt.	9. September 2019
Neues Amazon-EKS-optimiertes AMIs für CVE-2019-9512 und CVE-2019-9514 gepatcht	Amazon EKS hat das für Amazon-EKS-optimierte AMI aktualisiert, um CVE-2019-9512 und CVE-2019-9514 zu adressieren.	6. September 2019
Ankündigung der Einstellung von 1.11 Kubernetes in Amazon EKS	Amazon EKS hat die Unterstützung für die Kubernetes-Version 1.11 am 4. November 2019 eingestellt.	4. September 2019
Kubernetes-Version 1.14	1.14Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	03. September 2019
IAM-Rollen für Servicekonten	Mit IAM-Rollen für Servicekonten auf Amazon-EKS-Clustern können Sie eine IAM-Rolle mit einem Kubernetes-Servicekonto verknüpfen. Mit diesem Feature müssen Sie der Knoten-IAM-Rolle keine erweiterten Berechtigungen mehr bereitstellen. Auf diese Weise können Pods auf diesem Knoten aufrufen. AWS APIs	03. September 2019

Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Naher Osten (Bahrain) (me-south-1) verfügbar.	29. August 2019
Aktualisierung der Amazon-EK S-Plattformversion	Neue Plattformversionen für Adresse CVE-2019-9512 und CVE-2019-9514 .	28. August 2019
Aktualisierung der Amazon-EK S-Plattformversion	Neue Plattformversionen für Adresse CVE-2019-11247 und CVE-2019-11249 .	5. August 2019
Erweiterung der Amazon-EKS-Region	Amazon EKS ist jetzt in der AWS Region Asien-Pazifik (Hongkong) (ap-east-1) verfügbar.	31. Juli 2019
Kubernetes wird auf 1.10 Amazon EKS nicht mehr unterstützt	Die Kubernetes-Version 1.10 wird auf Amazon EKS nicht mehr unterstützt. Aktualisieren Sie alle 1.10-Cluster auf Version 1.11 oder höher, um Service-Unterbrechungen zu vermeiden.	30. Juli 2019
Thema über ALB Ingress Controller hinzugefügt	Der AWS ALB Ingress Controller für Kubernetes ist ein Controller, der bewirkt, dass bei der Erstellung von Ingress-Ressourcen ein ALB erstellt wird.	11. Juli 2019
Neues Amazon-EKS-optimiertes AMIs	kubect1Unnötige AMIs Binärdatei wird entfernt von.	3. Juli 2019

Kubernetes-Version 1.13	1.13 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.	18. Juni 2019
Neues Amazon-EKS-optimiertes AMIs für AWS-2019-005 gepatcht	Amazon EKS hat das für Amazon EKS optimierte AMI aktualisiert, um die Sicherheitslücken zu beheben, die unter AWS link:security/security-bulletins/ -2019-005/ [-2019-005, type="marketing "] beschrieben sind. AWS	17. Juni 2019
Ankündigung der Einstellung der Unterstützung von 1.10 Kubernetes in Amazon EKS	Amazon EKS hat die Unterstützung der Kubernetes-Version 1.10 am 22. Juli 2019 eingestellt.	21. Mai 2019
Aktualisierung der Amazon-EKS-Plattformversion	Neue Plattformversion für Kubernetes 1.11 und 1.10 Cluster zur Unterstützung benutzerdefinierter DNS-Namen im kubelet Zertifikat und zur Verbesserung der Leistung. etcd	21. Mai 2019

Erste Schritte mit eksctl

In diesem Leitfaden für die ersten Schritte wird beschrieben, wie Sie alle erforderlichen Ressourcen installieren können, um mit Amazon EKS mit eksctl zu beginnen. Dies ist ein einfaches Befehlszeilen-Dienstprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.

10. Mai 2019

AWSget-token CLI-Befehl

Der `aws eks get-token` Befehl wurde der AWS CLI hinzugefügt. Sie müssen den AWS IAM Authenticator für Kubernetes nicht mehr installieren, um Client-Sicherheitstoken für die Cluster-API-Serverkommunikation zu erstellen. Aktualisieren Sie Ihre AWS CLI-Installation auf die neueste Version, um diese neue Funktionalität nutzen zu können. Weitere Informationen finden Sie unter [Installation der AWS Befehlszeilenschnittstelle](#) im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

10. Mai 2019

[Aktualisierung der Amazon-EKS-Plattformversion](#)

Neue Plattformversion für 1.12 Kubernetes-Cluster zur Unterstützung benutzerdefinierter DNS-Namen im kubelet Zertifikat und zur Verbesserung etcd der Leistung. Dadurch wird ein Fehler behoben, durch den bedingt kubelet-Daemons von Knoten alle paar Sekunden ein neues Zertifikat angefordert haben.

8. Mai 2019

[Prometheus-Tutorial](#)

Thema zur Bereitstellung von Prometheus auf Ihrem Amazon-EKS-Cluster hinzugefügt.

5. April 2019

[Amazon-EKS-Steuerebenen-Protokollierung](#)

Mit diesem Update können Sie Audit- und Diagnoseprotokolle direkt aus dem Amazon-EKS-Steuerungsbereich abrufen. Sie können diese CloudWatch Protokolle in Ihrem Konto als Referenz für die Sicherung und Ausführung von Clustern verwenden.

4. April 2019

[Kubernetes-Version 1.12](#)

1.12 Unterstützung der Kubernetes-Version für neue Cluster und Versionsupgrades hinzugefügt.

28. März 2019

[Einführungsleitfaden für App Mesh hinzugefügt](#)

Dokumentation für den Einstieg mit App Mesh und Kubernetes hinzugefügt.

27. März 2019

<u>Privater Amazon-EKS-API-Server-Endpunktzugriff</u>	Dokumentation zur Deaktivierung des öffentlichen Zugriffs für den Kubernetes-API-Serverendpunkt Ihres Amazon EKS-Clusters hinzugefügt.	19. März 2019
<u>Thema zur Installation des Kubernetes Metrics Servers hinzugefügt</u>	Der Kubernetes-Metrik-Server ist ein Aggregator für Ressourcenverbrauchsdaten in Ihrem Cluster.	18. März 2019
<u>Liste der zugehörigen Open-Source-Projekte hinzugefügt.</u>	Diese Open-Source-Projekte erweitern die Funktionalität von Kubernetes-Clustern AWS, auf denen sie ausgeführt werden, einschließlich Clustern, die von Amazon EKS verwaltet werden.	15. März 2019
<u>Thema zur lokalen Installation von Helm hinzugefügt.</u>	Der helm-Paketmanager für Kubernetes unterstützt Sie bei der Installation und Verwaltung von Anwendungen in Ihrem Kubernetes-Cluster. In diesem Thema wird gezeigt, wie die helm- und tiller-Binärdateien lokal installiert und ausgeführt werden. Auf diese Weise können Sie Diagramme mit der Helm-CLI auf Ihrem lokalen System installieren und verwalten.	11. März 2019

Aktualisierung der Amazon-EKS-Plattformversion	Neue Plattformversion, die Amazon EKS 1.11 Kubernetes-Cluster auf Patch-Ebene aktualisiert, um CVE-2019-1002100 1.11.8 zu adressieren.	8. März 2019
Erhöhtes Cluster-Limit	Amazon EKS hat die Anzahl der Cluster, die Sie in einer AWS Region erstellen können, von 3 auf 50 erhöht.	13. Februar 2019
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in den AWS Regionen Europa (London) (eu-west-2), Europa (Paris) (eu-west-3) und Asien-Pazifik (Mumbai) (ap-south-1) verfügbar.	13. Februar 2019
Neues Amazon-EKS-optimiertes AMIs für ALAS-2019-1156 gepatcht	Amazon EKS hat das für Amazon EKS optimierte AMI aktualisiert, um die in ALAS-2019-1156 beschriebene Sicherheitsanfälligkeit zu beheben.	11. Februar 2019
Neues Amazon-EKS-optimiertes AMIs für ALAS2-2019-1141 gepatcht	Amazon EKS hat das für Amazon EKS optimierte AMI aktualisiert, um die Probleme zu beheben, auf CVEs die in ALAS2-2019-1141 verwiesen wird.	9. Januar 2019
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Asien-Pazifik (Seoul) (ap-northeast-2) verfügbar.	9. Januar 2019

Erweiterung der Amazon-EKS-Region	Amazon EKS ist jetzt in den folgenden zusätzlichen AWS Regionen verfügbar: Europa (Frankfurt) (eu-central-1), Asien-Pazifik (Tokio) (ap-northeast-1), Asien-Pazifik (Singapur) (ap-southeast-1) und Asien-Pazifik (Sydney) (ap-southeast-2).	19. Dezember 2018
Amazon EKS-Cluster-Aktualisierungen	Dokumentation für Amazon-EKS- Cluster Kubernetes-Versionupdates und Knotenaustausch hinzugefügt.	12. Dezember 2018
Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der AWS Region Europa (Stockholm) (eu-north-1) verfügbar.	11. Dezember 2018
Aktualisierung der Amazon-EKS-Plattformversion	Neue Plattformversion, die Kubernetes auf Patch-Ebene aktualisiert, um den folgenden Link 1.10.11 zu adressieren:AWS security/security-bulletins/ -2018-020 / [CVE-2018-1002105, type="marketing "].	4. Dezember 2018
Support für Version1.0.0 für den ALB-Controller für eingehenden Datenverkehr hinzugefügt	Der ALB 1.0.0 AWS Ingress Controller veröffentlicht eine Version mit formeller Unterstützung von.	20. November 2018

<u>Unterstützung der CNI-Netzwerk-konfiguration hinzugefügt</u>	Die Version des Amazon VPC CNI-Plug-ins für Kubernetes unterstützt 1.2.1 jetzt die benutzerdefinierte Netzwerkkonfiguration für sekundäre Pod-Netzwerkschnittstellen.	16. Oktober 2018
<u>Unterstützung für MutatingAdmissionWebhook und ValidatingAdmissionWebhook hinzugefügt</u>	Die Amazon-EKS-Plattformversion 1.10-eks.2 unterstützt jetzt die Zulassung des Controller MutatingAdmissionWebhook und ValidatingAdmissionWebhook.	10. Oktober 2018
<u>Partner-AMI-Informationen hinzugefügt.</u>	Canonical hat sich mit Amazon EKS zusammengetan, um Knoten zu erstellen AMIs, die Sie in Ihren Clustern verwenden können.	3. Oktober 2018
<u>Anweisungen für den AWSupdate-kubeconfig CLI-Befehl hinzugefügt</u>	Amazon EKS hat das update-kubeconfig zur AWS CLI hinzugefügt, um das Erstellen einer kubeconfig Datei für den Zugriff auf Ihren Cluster zu vereinfachen.	21. September 2018
<u>Neues Amazon EKS optimiert AMIs</u>	Amazon EKS hat Amazon EKS optimiert AMIs (mit und ohne GPU-Unterstützung) aktualisiert, um verschiedene Sicherheitskorrekturen und AMI-Optimierungen bereitzustellen.	13. September 2018

Erweiterung der Amazon AWS EKS-Region	Amazon EKS ist jetzt in der Region Europa (Irland) (eu-west-1) verfügbar.	5. September 2018
Aktualisierung der Amazon-EKS-Plattformversion	Neue Plattformversion mit Unterstützung für die Kubernetes- Aggregatenebene und den Horizontal Pod Autoscaler (HPA).	31. August 2018
Neue Amazon EKS-optimierte Version AMIs und GPU-Unterstützung	Amazon EKS hat das für Amazon EKS optimierte AMI aktualisiert, sodass es eine neue AWS CloudFormation Knotenvorlage und ein neues Bootstrap-Skript verwendet . Außerdem ist ein neues Amazon-EKS-optimiertes AMI mit GPU-Unterstützung verfügbar.	22. August 2018
Neues Amazon-EKS-optimiertes AMIs für ALAS2-2018-1058 gepatcht	Amazon EKS hat das für Amazon EKS optimierte AMI aktualisiert, um die Probleme zu beheben, auf CVEs die in ALAS2-2018-1058 verwiesen wird.	14. August 2018
Amazon-EKS-optimierte AMI-Build-Skripts	Amazon EKS hat die Build-Skripts, die zum Erstellen des Amazon-EKS-optimierten AMI verwendet werden, als Open-Source-Software zur Verfügung gestellt. Diese Build-Skripte sind jetzt auf verfügbar. GitHub	10. Juli 2018

[Erstveröffentlichung von
Amazon EKS](#)

Erste Dokumentation für den
Servicestart

5. Juni 2018

Tragen Sie zum EKS-Benutzerhandbuch bei

AWS hat ein verbessertes Beitragserlebnis für das EKS-Benutzerhandbuch eingeführt.

Sie können die Quelle des EKS-Benutzerhandbuchs jetzt direkt auf bearbeiten GitHub.

Die Dokumente verwenden jetzt eine leistungsstarke Autorensprache AsciiDoc, die Markdown ähnelt. AsciiDoc kombiniert einfache Syntax mit Funktionen für Unternehmensdokumentationen wie erweiterte Formatierung, Querverweise und Sicherheitskontrollen.

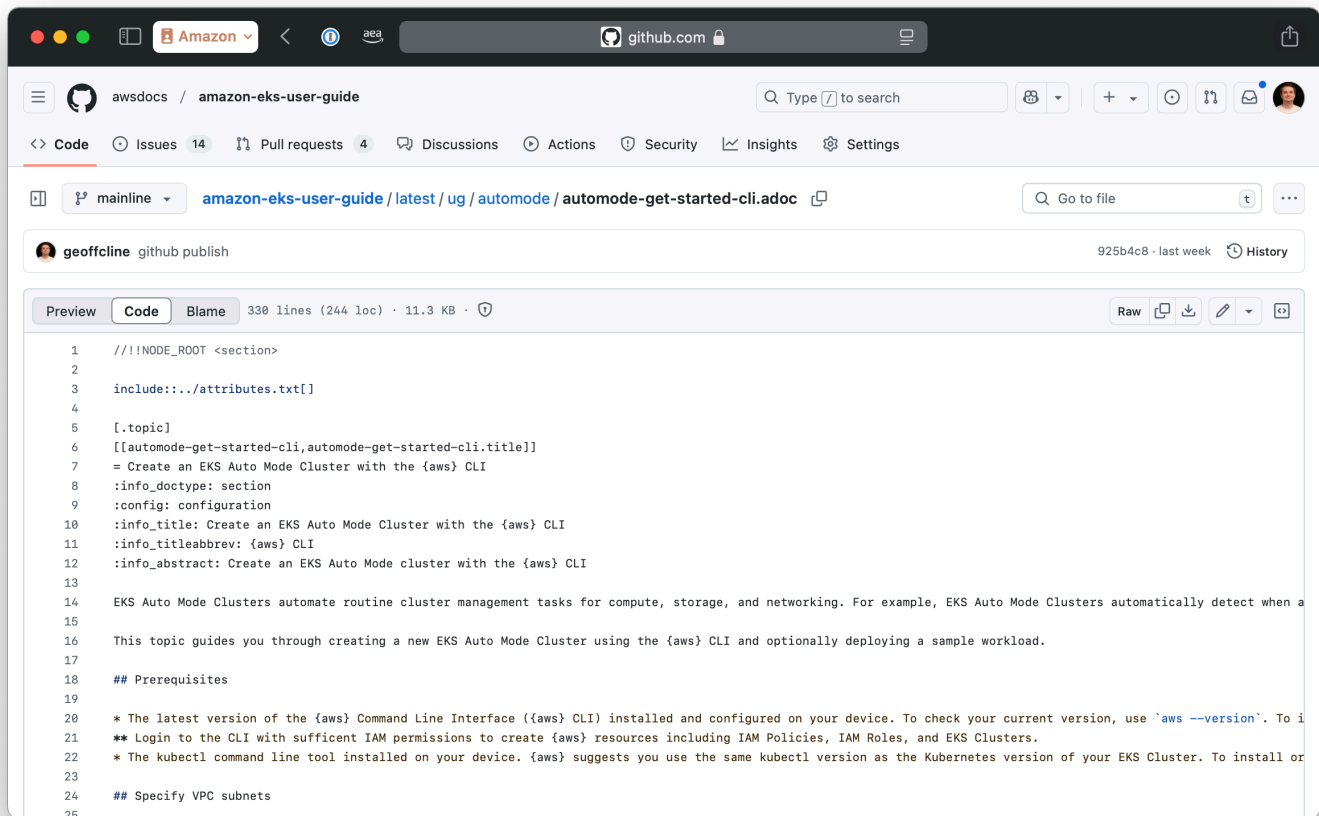
Sie können die EKS-Dokumente jetzt direkt auf bearbeiten. GitHub Unser optimierter Prozess umfasst:

- Schnellere Verarbeitung von Pull-Requests
- Weniger manuelle Schritte
- Automatisierte Qualitätsprüfungen von Inhalten

Wir freuen uns auf Ihre Beiträge.

Bearbeiten Sie eine einzelne Seite in einem Webbrowser

Sie können eine einzelne Seite im EKS-Benutzerhandbuch ganz einfach direkt über Ihren Webbrowser bearbeiten.



Wenn Sie mehrere Seiten in Ihrem Webbrowser bearbeiten möchten, finden Sie weitere Informationen unter [the section called “Bearbeiten Sie Dateien mit GitHub”](#).

Voraussetzungen

- Die zu ändernde Dokumentenseite wurde im Webbrowser geöffnet.
- Eingeloggt GitHub.

Verfahren

1. Navigieren Sie im Amazon EKS-Benutzerhandbuch zu der Seite, die Sie bearbeiten möchten.
2. Wählen Sie im rechten Bereich den GitHub Link Diese Seite bearbeiten auf.
3. Sobald diese Option aktiviert GitHub ist, öffnen Sie den Editor auf eine der folgenden Arten:
 - Drücken Sie die e Taste auf Ihrer Tastatur.

- Klicken Sie auf das Stiftsymbol und wählen Sie im Drop-down-Menü die Option An Ort und Stelle bearbeiten aus.
 - Wenn Sie keine Bearbeitungsoption haben, müssen Sie sich GitHub bei anmelden. Ihr GitHub Konto benötigt keine besonderen Berechtigungen, um Änderungen vorzuschlagen. Interne Amazon-Mitwirkende sollten jedoch ihr GitHub Profil verlinken.
4. Nehmen Sie die erforderlichen Änderungen am Inhalt im GitHub Editor vor.
 - Der Editor bietet Funktionen zur Syntaxhervorhebung und Vorschau.
 - Sie können AsciiDoc Markup verwenden, um Ihre Änderungen zu formatieren.
 - Sie können es verwenden `ctrl-f`, um eine Suchen/Ersetzen-Schnittstelle zu öffnen.
 5. (Optional) Zeigen Sie eine Vorschau Ihrer Änderungen an.
 - Verwenden Sie die `preview` Registerkarte, um eine Vorschau Ihrer Änderungen mit umfangreicher Formatierung anzuzeigen.
 - Verwenden Sie die `show diff` Option, um geänderte Abschnitte hervorzuheben. Entfernte Abschnitte haben einen roten Indikator am linken Rand. Neue Abschnitte haben eine grüne Anzeige am linken Rand.
 6. Wenn Sie mit der Bearbeitung fertig sind, klicken Sie oben im Editor auf die Schaltfläche Änderungen übernehmen...
 7. Gehen Sie im Commit-Dialog wie folgt vor:
 - Vergewissern Sie sich, dass Ihre E-Mail-Adresse korrekt ist.
 - Fügen Sie eine kurze, aber aussagekräftige Commit-Nachricht hinzu, in der Ihre Änderungen erläutert werden.
 - Fügen Sie optional bei Bedarf eine längere Beschreibung hinzu.
 - Wählen Sie diese Option, um eine neue Branch- und Pull-Anfrage zu erstellen.

Sie haben einen Pull-Request mit den vorgeschlagenen Änderungen erstellt.

Überblick über die Pull-Anfrage

Wenn du eine PR erstellst:

- Ihre Änderungen werden von den Repository-Betreuern zur Überprüfung eingereicht.
- Gutachter können Ihre Änderungen kommentieren und Änderungen beantragen.
- Automatisierte Tests können ausgeführt werden, um Ihre Änderungen zu validieren.

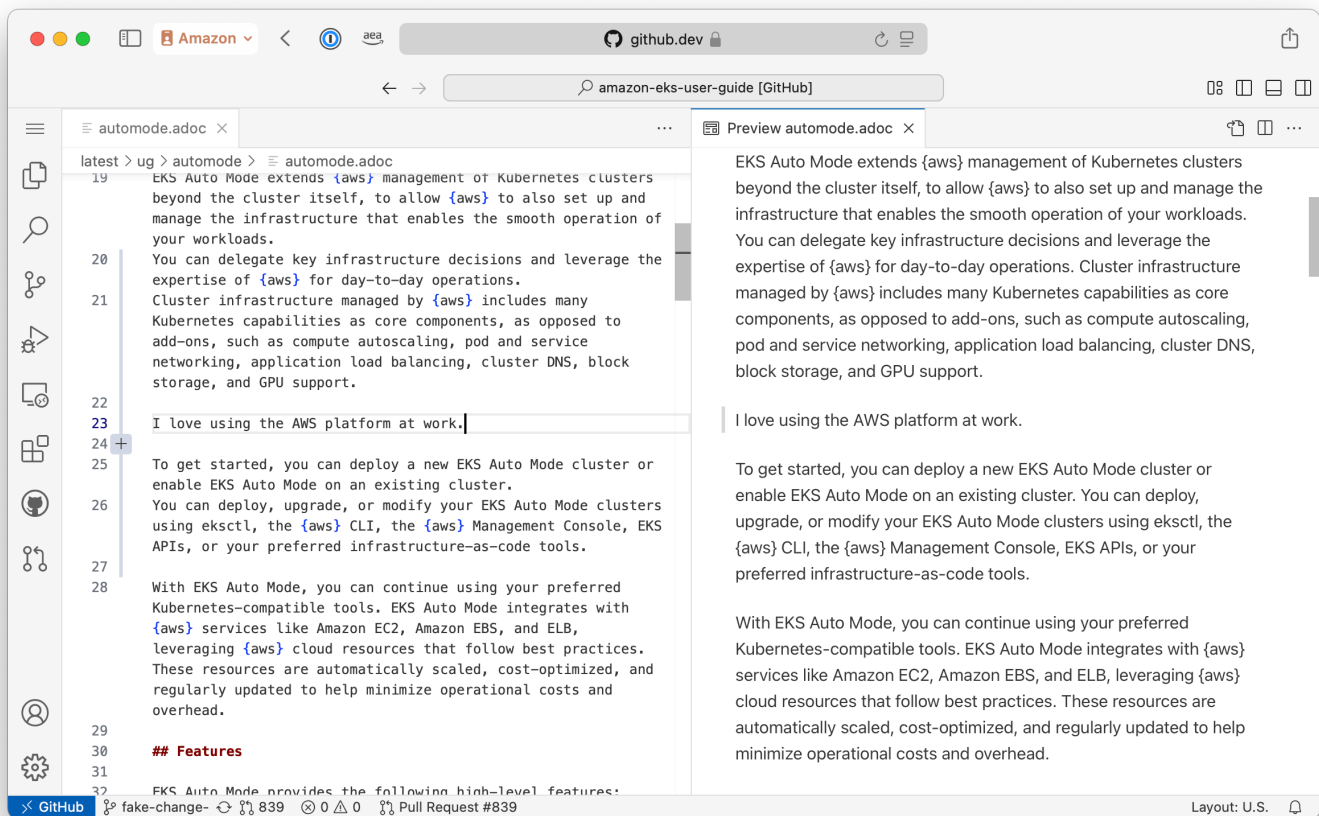
- Nach der Genehmigung können Ihre Änderungen mit dem Haupt-Repository zusammengeführt werden.

Pull-Requests tragen zur Qualitätssicherung bei und bieten die Möglichkeit, Änderungen zu besprechen, bevor sie integriert werden.

[In den GitHub Dokumenten erfährst du, wie Pull Requests geprüft und genehmigt werden.](#)

Bearbeiten Sie mehrere Dateien in einem Webbrowser mit dem GitHub Web Editor

Wenn Sie Änderungen an mehreren Seiten vorschlagen oder eine neue Dokumentseite erstellen möchten, verwenden Sie den GitHub .dev-Webeditor. Dieser Webeditor basiert auf dem beliebten Visual Studio Code-Texteditor.



Voraussetzungen

- Eingeloggt bei GitHub
- Vertrautheit mit dem Visual Studio Code-Editor
- Vertrautheit mit Git

Verfahren

Note

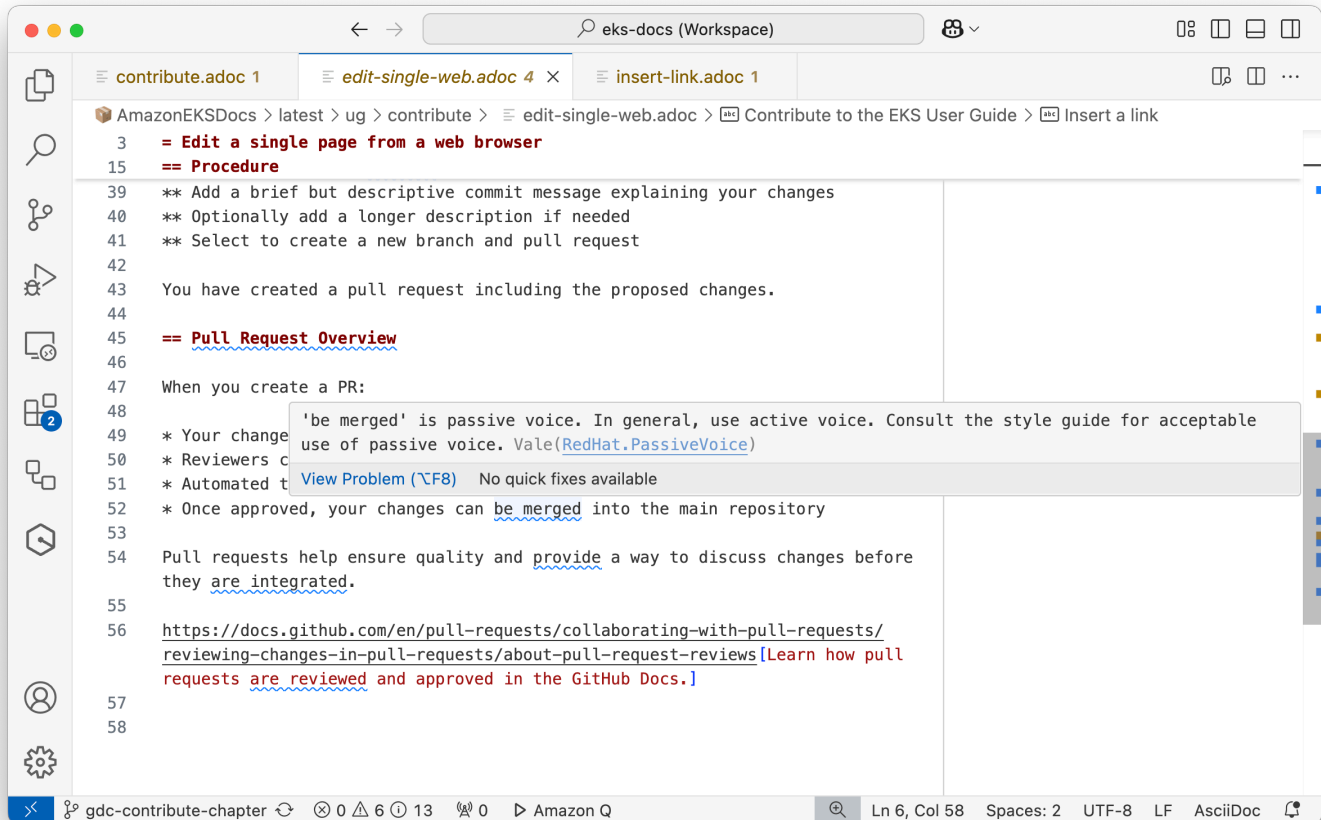
Das Team von EKS Docs hat eine Workspace-Datei erstellt, die Konfigurationsvorschläge für den Editor enthält, z. B. Textumbruch und AsciiDoc Syntaxhervorhebung. Wir empfehlen Ihnen, diese Workspace-Datei zu laden.

1. Öffne den [Workspace](https://github.dev/awsdocs/amazon-eks-user-guide/blob/mainline/eks-docs.code-workspace?workspace=true) auf GitHub .dev.
 - Sie können die URL mit einem Lesezeichen versehen <https://github.dev/awsdocs/amazon-eks-user-guide/blob/mainline/eks-docs.code-workspace?workspace=true>
2. (Nur bei der Erstinstallation) Möglicherweise werden Sie aufgefordert, einen Fork des Repos in Ihrem eigenen GitHub Konto zu erstellen. Akzeptieren Sie diese Aufforderung. Weitere Informationen finden Sie in der GitHub Dokumentation unter [About Forks](#).
3. (Nur bei der Erstinstallation) Akzeptieren Sie die Aufforderung unten rechts, um die AsciiDoc Erweiterung zu installieren.
4. Navigieren Sie zum Inhalt der Dokumente unter `latest/ug`.
 - Die Dokumentdateien sind nach ihrem Abschnitt auf oberster Ebene organisiert. Zum Beispiel haben Seiten im Kapitel „Sicherheit“ Quelldateien im Verzeichnis „security“.
5. Um eine Vorschau einer Dokumentseite anzuzeigen, klicken Sie oben rechts auf die Schaltfläche Seitenvorschau öffnen. Das Symbol enthält eine kleine Lupe.
6. Verwenden Sie die Registerkarte Quellcodeverwaltung auf der linken Seite, um Ihre Änderungen zu übernehmen. Weitere Informationen finden Sie in den Visual Studio Code-Dokumenten:
 - [Änderungen übernehmen](#)
 - [Erstellen einer Pull-Anforderung](#)

Nachdem du eine Pull-Anfrage erstellt hast, wird sie vom Docs-Team überprüft.

Lassen Sie sich während der Eingabe Feedback zum Stil anzeigen, indem Sie Vale lokal installieren

Während der Eingabe können Sie sich das Feedback zum Stil ansehen. Auf diese Weise können Sie unangenehmes Schreiben und Tippfehler erkennen.



Überblick:

- Die Vale-CLI lädt Styleguides und führt sie anhand von Quelldateien aus.
- Das EKS Docs-Repo enthält eine Vale-Konfigurationsdatei, die Styleguides und lokale Regeln lädt.
- Die Vale-Erweiterung für Visual Studio (VS) Code zeigt wertvolles Feedback im Editor an.

Installieren Sie Vale

Folgen Sie den Anweisungen in den Vale-CLI-Dokumenten, um [Vale mit einem Paketmanager zu installieren](#).

Installieren Sie die VS Code Vale-Erweiterung

1. Öffnen Sie VS Code.
2. Klicken Sie in der Aktivitätsleiste auf das Erweiterungssymbol (oder drücken Sie Strg+Shift+X).
3. Suchen Sie nach „Vale“.
4. Klicken Sie bei der Erweiterung „Vale VSCode“ von Chris Chinchilla auf Installieren.
5. Laden Sie den VS-Code neu, wenn Sie dazu aufgefordert werden.

Vale synchronisieren

Vale verwendet die `.vale.ini` Konfigurationsdatei in Ihrem Projektstamm, um zu bestimmen, welche Stilregeln angewendet werden sollen.

1. Öffnen Sie VS Code.
2. Klicken Sie auf Ansicht > Terminal (oder drücken Sie Strg+`).
3. Navigieren Sie bei Bedarf zum Stammverzeichnis Ihres Projekts.
4. Führen Sie den Befehl aus:

```
vale sync
```

5. Warten Sie, bis Vale das Herunterladen und Synchronisieren der Style-Regeln abgeschlossen hat

Stil-Feedback in VS Code anzeigen

1. Öffnen Sie einen Markdown oder eine AsciiDoc Datei in VS Code.
2. Die Vale-Erweiterung überprüft Ihren Text automatisch anhand der Stilregeln.
3. Stilprobleme werden im Editor unterstrichen.
4. Bewegen Sie den Mauszeiger über den unterstrichenen Text, um den jeweiligen Stilvorschlag zu sehen.

5. Behebt Probleme, indem ihr den Vorschlägen folgt oder den Styleguide konsultiert.

Eine neue Seite erstellen

Erfahren Sie, wie Sie eine neue Dokumentationsseite erstellen. Dieses Thema enthält Anweisungen zum Erstellen der Metadaten der ersten Seite und zum Hinzufügen der Seite zum Inhaltsverzeichnis des Leitfadens.

Seite erstellen

1. Navigieren Sie zum Kapitelverzeichnis. Wenn Sie beispielsweise im Bereich „Sicherheit“ eine neue Seite erstellen möchten, navigieren Sie zum `latest/ug/security` Verzeichnis.
2. Ermitteln Sie die Seiten-ID. Konventionell besteht die Seiten-ID ausschließlich aus Kleinbuchstaben und ist mit `segmentiert`. – Die ID dieser Seite lautet `create-page`.
3. Erstellen Sie eine neue Datei mit der Seiten-ID und der `adoc` Erweiterung. Beispiel, `create-page.adoc`.
4. Fügen Sie die Seitenmetadaten mithilfe dieser Vorlage ein:

```
include:../attributes.txt[]

[.topic]
[#unique-page-id]
= Page title
:info_titleabbrev: Short title

[abstract]
--
Brief summary of the page's content.
--

Introduction paragraph goes here.
```

Seite zur Navigation hinzufügen

1. Navigieren Sie zur übergeordneten Seite. Die übergeordnete Seite der Abschnitte auf oberster Ebene ist `book.adoc`.
2. Fügen Sie unten auf der übergeordneten Seite die untergeordnete Seite ein.

```
include::${filename}[leveloffset=+1]
```

Beispiel:

```
include::create-page.adoc[leveloffset=+1]
```

Fügen Sie einen Link ein

AsciiDoc unterstützt mehrere Arten von Links. Die Verwendung des richtigen Linktyps ist wichtig, damit der Link in verschiedenen Umgebungen ordnungsgemäß funktioniert.

Link zu einer Seite oder einem Abschnitt im EKS-Benutzerhandbuch

Verwenden Sie Querverweise (XRef), um Links zwischen Seiten oder Abschnitten innerhalb derselben Dokumentationsseite zu erstellen, z. B. im EKS-Benutzerhandbuch. Sie werden automatisch aktualisiert, wenn der Zielabschnitt verschoben oder umbenannt wird.

Verwenden Sie den Seitentitel als Linktext

Wenn Sie in diesem Benutzerhandbuch auf eine andere ID verlinken, gehen Sie in den meisten Fällen wie folgt vor, damit der Linktext bei Bedarf automatisch auf den neuesten Titel aktualisiert wird.

For more information, see <<page-or-section-id>>.

Definieren Sie benutzerdefinierten Linktext

Verwenden Sie für Fälle, in denen Sie einen benutzerdefinierten Linktext benötigen, das folgende Format.

Here's an example of a <<page-or-section-id,link with custom text>>.

Link zu einem anderen Leitfaden in den AWS Dokumenten

1. Finden Sie den Link zur AWS Dokumentationsseite.
2. Entfernen Sie das <https://docs.aws.amazon.com/> Präfix und behalten Sie nur den Pfad bei. Der Pfad sollte mit einem Buchstaben beginnen.
3. Erstellen Sie einen Link wie unten gezeigt:

```
link:AmazonS3/latest/userguide/create-bucket-overview.html[Create a bucket,  
type="documentation"]
```

Link zu einer externen Webseite

Dieses Format erstellt einen Standardlink zu einer Seite, die nicht von Amazon gehostet wird. Verwenden Sie dies beispielsweise für GitHub Links.

```
https://example.com[Link text]
```

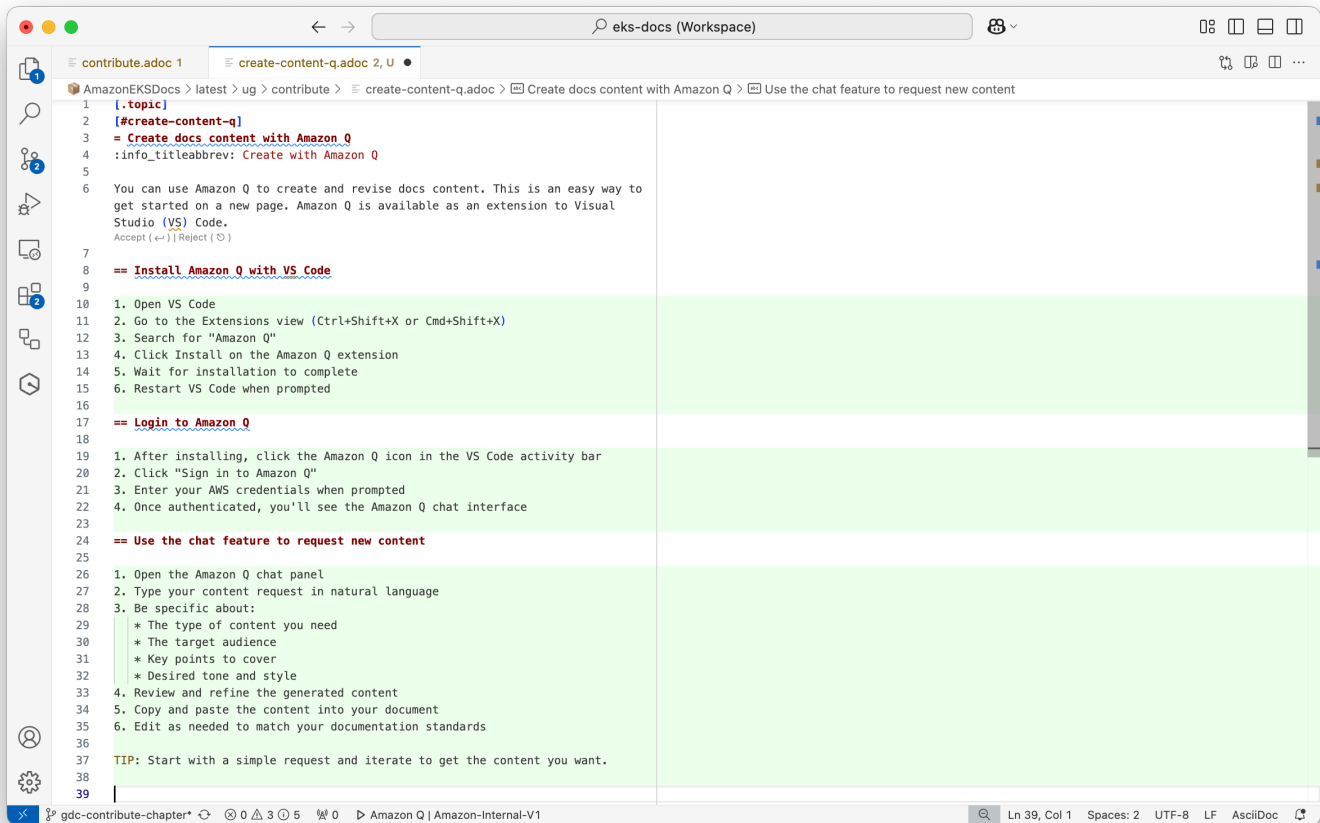
Note

Wir haben eine Zulassungsliste für externe Domains. Die Zulassungsliste befindet sich unter `vale/styles/EksDocs/ExternalDomains.yml`

Dokumentinhalte mit Amazon Q erstellen

Sie können Amazon Q verwenden, um Dokumentinhalte zu erstellen und zu überarbeiten. Dies ist eine einfache Möglichkeit, auf einer neuen Seite zu beginnen. Amazon Q ist als Erweiterung für Visual Studio (VS) Code verfügbar.

In der folgenden Abbildung hat Amazon Q die grün markierten Linien generiert.



Installieren Sie Amazon Q mit VS Code

1. Öffnen Sie VS Code
2. Gehen Sie zur Erweiterungsansicht (Strg+Shift+X oder Cmd+Shift+X)
3. Suche nach „Amazon Q“
4. Klicken Sie in der Amazon Q-Erweiterung auf Installieren
5. Warten Sie, bis die Installation abgeschlossen ist
6. Starten Sie VS Code neu, wenn Sie dazu aufgefordert werden

Melden Sie sich bei Amazon Q an

1. Wählen Sie nach der Installation das Amazon Q-Symbol in der VS Code-Aktivitätsleiste.
2. Wählen Sie Bei Amazon Q anmelden aus.
3. Geben Sie Ihre AWS Anmeldedaten ein, wenn Sie dazu aufgefordert werden.

4. Nach der Authentifizierung sehen Sie die Amazon Q-Chat-Oberfläche.

Verwenden Sie Amazon Q, um Inhalte zu erstellen

1. Öffnen Sie die Datei, die Sie bearbeiten möchten, in VS Code.
2. Wählen Sie den Text aus, den Sie überarbeiten möchten, oder den Speicherort für neue Inhalte.
3. Drücken Sie Strg+I oder Cmd+I.
4. Geben Sie in der Eingabeaufforderung Folgendes genau an:
 - Die Art des Inhalts, den Sie benötigen.
 - Die Zielgruppe.
 - Wichtige Punkte, die es zu behandeln gilt.
 - Gewünschter Ton und Stil.
5. Überprüfen Sie den generierten Inhalt in der Inline-Vorschau.
6. Verwenden Sie die Eingabetaste, um die Änderungen zu akzeptieren, oder ESC, um sie abzulehnen.
7. Bearbeiten Sie nach Bedarf weiter.

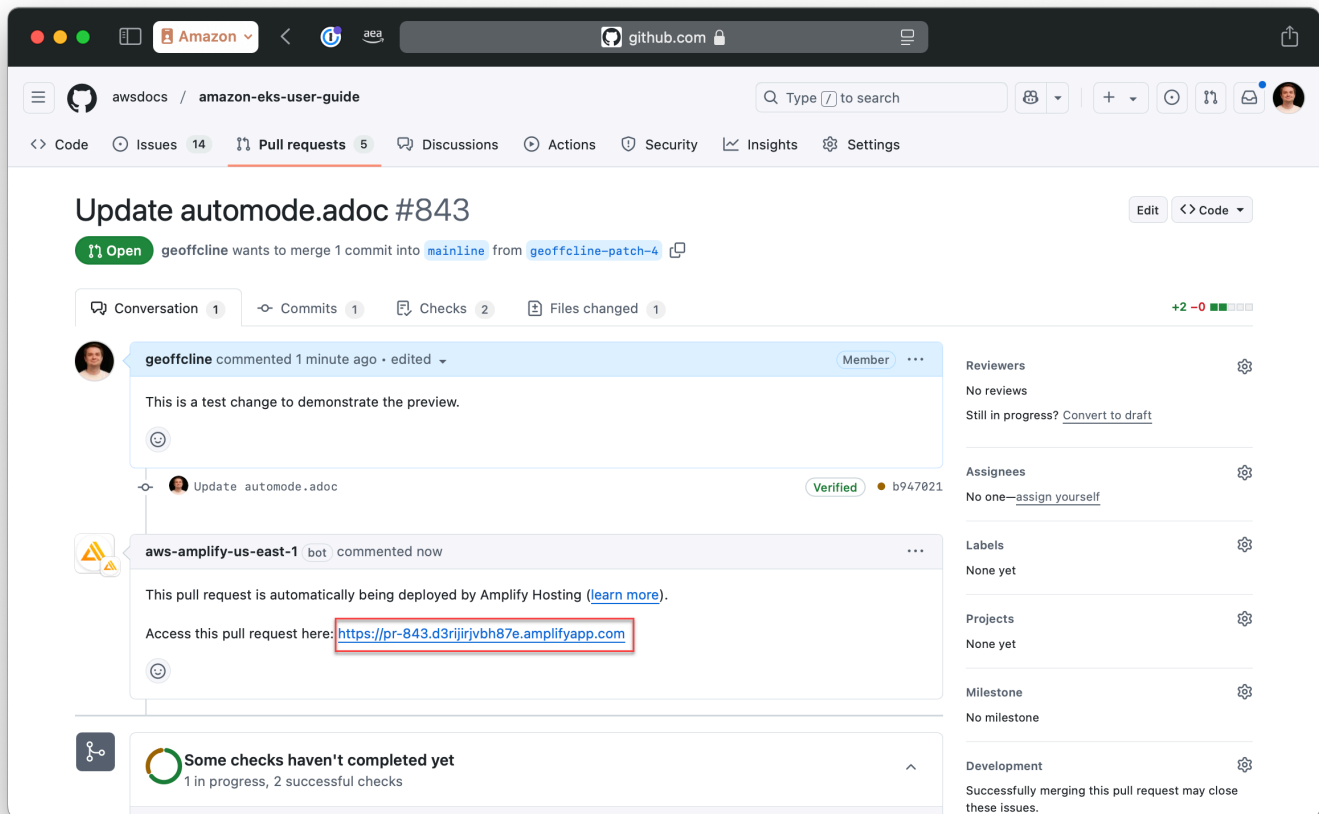
Tipps

- Beginnen Sie mit einer einfachen Anfrage und wiederholen Sie den Vorgang, bis Sie den gewünschten Inhalt erhalten.
- Erstellen Sie einen ersten Entwurf der Seitenüberschriften und bitten Sie Q dann, sie auszufüllen.
- Amazon Q gibt möglicherweise Markdown aus. Das ist in Ordnung. Das AsciiDoc Tool kann die meisten Markdown-Syntaxen verstehen.

Weitere Informationen zu Amazon Q Developer finden Sie unter [Amazon Q Developer in der IDE verwenden](#).

Eine Vorschau des Pull-Request-Inhalts anzeigen

Das Amazon EKS-Benutzerhandbuch GitHub ist so konfiguriert, dass es eine Vorschau der Docs-Website erstellt und generiert. Diese Vorschau enthält nicht das vollständige AWS Design, überprüft jedoch, ob der Inhalt ordnungsgemäß erstellt wurde und die Links funktionieren.



Diese Vorschau wird von AWS Amplify unter einer temporären URL gehostet.

Vorschau ansehen

Wenn Sie eine Pull-Anfrage einreichen, versucht AWS Amplify, eine Vorschau des Inhalts zu erstellen und bereitzustellen.

Wenn der Build erfolgreich ist, fügt aws-amplify-us-east-1 der Pull-Anfrage einen Kommentar hinzu, der einen Link zur Vorschau enthält. Wähle den Link rechts neben „Greifen Sie hier auf diesen Pull-Request zu“ (wie im Screenshot mit roter Umrandung dargestellt).

Wenn der Build fehlschlägt, können die Repo-Administratoren die Logs einsehen und Feedback geben.

 Note

Wenn Sie noch keinen Beitrag geleistet haben, muss möglicherweise ein Projektbetreuer die Ausführung des Builds genehmigen.

Einschränkungen in der Vorschau

Die Vorschau wird als einzelne große HTML-Datei erstellt. Sie wird bei der Veröffentlichung als mehrere Seiten angezeigt.

Was funktioniert:

- Querverweise (`xref`)
- Links zum Internet
- Bilder
- Inhalt gehostet von `samples/`

Was nicht funktioniert:

- Links zu anderen AWS Inhalten, `mittype="documentation"`. Das liegt daran, dass dieser Inhalt in der Vorschauumgebung nicht vorhanden ist.
- Das Attribut `{aws}` wird nicht richtig angezeigt. Der Wert dieses Werts ändert sich je nach Umgebung.

AsciiDoc Syntaxreferenz

AsciiDoc ist die bevorzugte Auszeichnungssprache für die AWS Dokumentation. Das Tool unterstützt zwar teilweise die Markdown-Syntax (wie Überschriften und Listen), wir empfehlen jedoch, die AsciiDoc Syntax für alle Inhalte zu verwenden, um Konsistenz und korrekte Darstellung zu gewährleisten.

Dieses Handbuch behandelt allgemeine Syntaxelemente, die Sie benötigen, wenn Sie zur Amazon EKS-Dokumentation beitragen. Eine fortgeschrittenere Syntax und detaillierte Informationen finden Sie in der [AsciiDoc Dokumentation](#).

Neue Seite

Jedes neue AsciiDoc Dokument sollte mit der Struktur beginnen, die in definiert ist [the section called “Seite erstellen”](#).

Überschriften

Verwenden Sie Überschriften, um Ihre Inhalte hierarchisch zu organisieren:

```
= Page/topic title (level 1)
== Section title (level 2)
=== Level 3 heading
==== Level 4 heading
===== Level 5 heading
===== Level 6 heading
```

Hinweis: Verwenden Sie für Überschriften in der Dokumentation immer die Groß-/Kleinschreibung.
AWS

Formatierung von Text

Formatieren Sie Text, um wichtige Informationen hervorzuheben:

```
Use *bold text* for UI labels.
Use _italic text_ for introducing terms or light emphasis.
Use `monospace text` for code, file names, and commands.
```

Listen

Ungeordnete Listen

Erstellen Sie Listen mit Aufzählungszeichen für Artikel ohne eine bestimmte Reihenfolge:

```
* First item
* Second item
** Nested item
** Another nested item
* Third item
```

Geordnete Listen

Erstellen Sie nummerierte Listen für aufeinanderfolgende Schritte oder priorisierte Elemente:

```
. First step
. Second step
.. Substep 1
.. Substep 2
. Third step
```

Links

Einzelheiten [the section called “Link einfügen”](#) zur korrekten Formatierung von Links finden Sie unter. Links im Markdown-Stil werden nicht unterstützt.

Codebeispiele

Inline-Code

Verwenden Sie Backticks für Inline-Code:

```
Use the `kubectl get pods` command to list all pods.
```

Codeblöcke

Erstellen Sie Codeblöcke mit Syntaxhervorhebung und Unterstützung für Attribute (ähnlich wie Entitäten):

```
[source,python,subs="verbatim,attributes"]
----
def hello_world():
    print("Hello, World!")
----
```

Bilder

Fügen Sie aus Gründen der Barrierefreiheit Bilder mit Alt-Text ein:

```
image::images/image-file.png[Alt text description]
```

Tabellen

Erstellen Sie Tabellen, um Informationen zu organisieren:

```
[%header,cols="2"]  
|===  
|Header 1  
|Header 2  
  
|Cell 1,1  
|Cell 1,2  
  
|Cell 2,1  
|Cell 2,2  
|===
```

Komplexere Tabellen finden Sie in der [AsciiDoc Tabellendokumentation](#).

Callouts

Verwenden Sie Beschriftungen, um wichtige Informationen und Ermahnungen hervorzuheben:

NOTE: This is a note callout for general information.

TIP: This is a tip callout for helpful advice.

IMPORTANT: This is an important callout for critical information.

Vorschau:

 Note

Dies ist ein Notiz-Callout.

Einschließlich anderer Dateien

Inhalte aus anderen Dateien einbeziehen:

```
include::filename.adoc[]
```

Attribute (ähnlich wie Entitäten)

Verwenden Sie vordefinierte Attribute, um die Konsistenz aufrechtzuerhalten. Insbesondere MÜSSEN Sie Attribute für AWS und verwenden `arn:aws:` .

```
{aws} provides Amazon EKS as a managed Kubernetes service.
```

```
[source,bash,subs="verbatim,attributes"]
----
aws iam attach-role-policy \
    --role-name AmazonEKSAutoClusterRole \
    --policy-arn {arn-aws}iam::aws:policy/AmazonEKSClusterPolicy
----
```

Eine Liste der Attribute finden Sie in der `../attributes.txt` Datei.

Verfahren

step-by-stepProzeduren formatieren:

```
To create an Amaozon EKS cluster. do the following steps.
```

- . Sign in to the {aws} Management Console.
- . Open the Amazon EKS console.
- . Choose *Create cluster*.

```
...
```