



Benutzer-Leitfaden

AWS Transformieren



AWS Transformieren: Benutzer-Leitfaden

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. 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

Was ist AWS Transformieren?	1
Terminologie	1
Erste Schritte	4
Einrichtung	4
Bevor Sie beginnen	4
Melden Sie sich an für ein AWS-Konto	4
Erste Schritte mit Access IAM-only	4
Verwenden von IAM-Anmeldeinformationen	5
Erste Schritte mit AWS Organizations	6
Erste Schritte mit AWS IAM Identity Center	7
Verwendung von Identitätsanbietern von Drittanbietern	8
Onboarding	11
Verwenden Sie Ihren eigenen S3-Bucket	13
Aktivieren AWS Transformieren	22
Schnellstart: Ich versuche es AWS Transformieren	24
Verwalten von Benutzern	24
Benutzer im IAM Identity Center hinzufügen	24
Benutzer hinzufügen zu AWS Transformieren	25
Benutzer mit IAM-only Zugriff verwalten	26
Grundlegendes zu den Berechtigungen von Mitarbeitern	26
AWS Transformieren Sie die Umgebung	29
Spracheinstellungen	31
Starte dein Projekt	32
AWS Verwandeln Sie den Chat	32
Entwicklertools	34
Kiro Power	34
Agenten-Plugin	34
IDE-Plugin	35
MCP-Server	35
Authentifizierung	36
Erstellen Sie benutzerdefinierte Agenten für AWS Transformieren	37
Bewertungen der Migration	38
Voraussetzungen	38
Wie funktionieren Migrationsbewertungen	38

Inventardaten hochladen	39
Überprüfung der Discovery-Ergebnisse	40
Verwaltung des Inventarumfangs	40
Konfiguration von Bewertungsszenarien	40
Bewertungsmöglichkeiten	41
Amazon EC2 richtig dimensionieren	41
Amazon EBS-Speicher	41
Amazon FSx	41
Amazon RDS für SQL Server	42
Amazon EC2-SQL-Server	42
On-premises Preisgestaltung	43
Nachhaltigkeit	43
Bewertung des Geschäftswerts	43
Netzwerkkosten	44
Kosten für den Support	44
Endbenutzer-Datenverarbeitung	44
Mithilfe von Chat-basierten Bewertungen	44
Grobe Schätzung mit begrenzten Daten	44
Inventar per Chat hinzufügen	45
Kosten ändern und Dienste hinzufügen	45
Szenarien vergleichen	45
Szenarien erstellen	45
Vergleiche werden ausgeführt	46
What-if Analyse	46
Generierung von Ergebnissen	46
Verwandte Themen	47
Benutzerdefiniert	48
Was ist AWS Benutzerdefiniert transformieren?	48
Die wichtigsten Funktionen	48
Transformationsmuster	48
Wie AWS Transformieren Sie benutzerdefinierte Werke	51
Wichtige -Konzepte verstehen	52
Transformationsdefinitionen	52
Transformationsregister	53
Entwurf und veröffentlichte Transformationen	53
Referenzen im Vergleich zu Lektionen	54

Befehle zum Erstellen und Überprüfen	55
Kontinuierliches Lernen	55
Client-Side Fähigkeiten	56
Erste Schritte	56
Voraussetzungen	57
Installieren von AWS CLI transformieren	57
Konfigurieren der Authentifizierung	58
Konfigurieren AWS Region	60
Führen Sie Ihre erste Transformation durch	64
Transformationsergebnisse verstehen	64
Eine benutzerdefinierte Transformation erstellen	65
AWS Webanwendung transformieren (optional)	65
Einführung in benutzerdefinierte Transformationsbefehle	66
Arbeitsabläufe	67
Transformationen ausführen	67
Kontinuierliches Lernen	73
Erweiterte Konfiguration	74
Erstellen Sie benutzerdefinierte Transformationen	88
Befehlsreferenz	92
Interaktive Befehle	92
Befehle zur Transformationsdefinition	92
Befehle der Lektion	96
Befehle taggen	97
Befehle aktualisieren	97
MCP-Befehle	97
AWS-Verwaltete Transformationen	98
-Übersicht	98
Available (Verfügbar) AWS-Verwaltete Transformationen	98
Anpassen AWS-Verwaltete Transformationen	116
Häufige Anwendungsfälle	116
Lambda-Runtime-Upgrades	116
VPC-Endpunkte (AWS PrivateLink)	118
Überlegungen zu AWS Transform benutzerdefinierte VPC-Endpunkte	119
Voraussetzungen	119
Erstellen eines Schnittstellen-VPC-Endpunkts für AWS Transform benutzerdefiniert	119
Erstellen einer VPC-Endpunktrichtlinie für AWS Transform benutzerdefiniert	120

Verwenden eines lokalen Computers zum Herstellen einer Verbindung zu einem AWS	
Transform Benutzerdefinierter Endpunkt	121
Fehlerbehebung	121
Speicherorte protokollieren	121
Häufige Fehler	122
Supportanfragen	124
Probleme mit dem S3-Zugriff	124
CLI-Versionshistorie	126
Kontinuierliche Modernisierung	137
Was ist AWS Kontinuierliche Modernisierung transformieren?	137
Die wichtigsten Funktionen	137
Arten von Analysen	138
Verständnis wichtiger Konzepte	139
Quellen	139
Repositorien	140
Analysen	140
Ergebnisse	140
Abhilfemaßnahmen	140
Definitionen der Transformation	140
Wie AWS Transformation: Kontinuierliche Modernisierung funktioniert	141
Rechenoptionen	141
Einrichtung des Security Agents	143
Erste Schritte	144
Voraussetzungen	144
Schnellstart	145
Arbeiten mit kontinuierlicher Modernisierung	145
Quellenverwaltung	145
Entdeckung und Verwaltung von Repositorien	147
Analyse wird ausgeführt	147
Verwaltung der Erkenntnisse	148
Erstellung von Abhilfemaßnahmen	148
AWS Webanwendung transformieren (optional)	149
Entwicklertools	150
Agenten-Skills	150
CLI-Referenz	151
Fehlerbehebung	154

Tool zur Entdeckung	156
Workflow	156
Richten Sie das Discovery-Tool ein	157
Voraussetzungen	157
Auf VMware bereitstellen	159
Bereitstellen auf Hyper-V	161
Auf Linux bereitstellen	161
Konfigurieren Sie das Discovery-Tool	164
Erforderliche Berechtigungen	178
VMware vCenter	178
Hyper-V Hosts (Windows)	179
Linux-Server (SSH)	180
Windows-Server (WinRM) — Betriebssystemmetriken	181
Windows-Server (WinRM) — SQL Server-Sammlung	183
Oracle-Datenbank (SQL)	184
Erfassung im Netzwerk	184
Kurzreferenz: Mindestberechtigungen nach Anwendungsfall	185
Datenerfassung	186
Zeitplan für die Abholung	186
Inventar entdeckt	188
OS-related Daten	193
Sicherheitsüberlegungen	212
Sicherung der Discovery-Tool-VM	212
Anmeldeinformationen sichern	212
Speicherung von Anmeldeinformationen	214
Auto-Connect Funktion mit Vorsicht verwenden	214
Sicherheit beim CSV-Import	216
Überlegungen zum Widerrufen des Zugriffs	217
Beheben Sie Fehler beim Discovery-Tool	217
Überprüfen der Konnektivität des Discovery-Tools mit vCenter	217
WinRM-Problembehandlung	219
Kerberos-Fehlerbehebung	219
Fehlerbehebung bei der Oracle-Datenbank	224
SNMP-Fehlerbehebung	225
Fehler bei der Netzwerkerfassung	226
Fehler beim Sammeln von Betriebssystem-Metriken	227

Probleme beim Zugriff auf das Inventar „Ermittelt“	227
Fehlerbehebung bei der SSH-Schlüsselauthentifizierung	228
Fehlerbehebung beim Linux-Installationsprogramm	229
Häufige Fehlermeldungen	229
Versionshinweise	231
Konnektoren	237
Rückverfolgbarkeit durch Benutzer für behördliche Abläufe	237
Konnektoren verwalten	239
Migrationen (einschließlich VMware)	241
Funktionen und Hauptmerkmale	241
Architektur	241
Jobs im Bereich Migration	242
Einen Workspace einrichten	242
Arten von Job	243
Einen Job erstellen und starten	244
Einen Workspace-Übersichtsbericht herunterladen	244
Einschränkungen	245
Entdecken Sie die Quelldaten	245
Erstellen Sie einen Migrationsplan	246
Workflow	248
7R-Empfehlungen	251
Diagramme und Berichte	252
Ziel Connect AWS-Konto s und Regionen	253
Schritt 1: Auswahl des Migrationstyps	253
Schritt 2: MAP-Vereinbarung	254
Schritt 3: Konfiguration des Connectors	254
landing zone bauen	260
Einrichtung des Konnektors	261
Einrichtung der Stiftung	262
Entwurf des Workload-Kontos	266
IaC-Formate	268
Genehmigungsverfahren für die Bereitstellung	269
Tag: Ressourcen für die landing zone	269
Änderungen rückgängig machen	270
Zugehörige Ressourcen	270
Migrieren Sie Ihr Netzwerk zu AWS	271

Schritt 1: Zuordnung des Quellnetzwerks	271
Schritt 2: Zusätzliche Konfigurationsdateien	273
Schritt 3: Netzwerktopologien	273
Schritt 4: Zuordnung von Sicherheitsgruppen	277
Schritt 5: Überprüfen und optimieren Sie Ihr Netzwerk	279
Schritt 6: Netzwerkdiagramm	284
Schritt 7: Konfigurieren Sie das Ressourcen-Tagging	284
Schritt 8: Stellen Sie Ihr Netzwerk bereit	286
Löscht bereitgestellte Netzwerkressourcen	287
Extrahieren der Konfigurationsdatei	288
Server migrieren	289
Voraussetzungen und Konfiguration der Standardeinstellungen für die Migration	290
Schritt 1: Migrationswelle einrichten	293
Schritt 2: Inventar validieren und bestätigen	296
Schritt 3: Replikationsagenten bereitstellen	297
Schritt 4: Datenreplikation	305
Schritt 5: Testen	306
Schritt 5b: Markieren Sie Anwendungen als bereit für die Umstellung	306
Schritt 6: Umstellung	307
Status des Serverlebenszyklus	308
Genehmigungen für die Bereitstellung	309
Versionshinweise	309
Juni 2026	309
Mai 2026	310
April 2026	310
März 2026	310
Februar 2026	310
Januar 2026	311
Dezember 2025	311
Oktober 2025	311
September 2025	311
August 2025	312
Mai 2025	312
Containerisierung des Quellcodes	313
Funktionen und Hauptmerkmale	313
Wie funktioniert die Containerisierung	314

Voraussetzungen	314
Arbeitsablauf bei der Containerisierung	315
Starten eines Containerisierungsjobs	315
Berechtigungen	316
Basisrichtlinie	316
Netzwerkrichtlinie	317
Speicherrichtlinie	317
AWS KMS policy	318
Amazon ECS-Richtlinie	318
Amazon EKS-Richtlinie	318
Schritt 1: Sicherheitsausschluss	319
Was der Haftungsausschluss abdeckt	319
Wichtige Informationen	319
Schritt 2: Quellcode klonen	320
Option 1: Git-Repositoryen	320
Option 2: Hochladen einer Zip-Datei	321
Optional: Konfigurieren Sie private Abhängigkeiten	321
Bestätigung der Einstellungen für die Containerisierung	322
Schritt 3: Containerisieren	322
Was passiert bei der Containerisierung	322
Unterstützte Anwendungstypen	323
Wichtige Informationen	323
Schritt 4: Artefakte überprüfen	323
Änderungen aus Git-Repositorys überprüfen	324
Änderungen aus ZIP-Uploads überprüfen	324
Änderungen anfordern	324
Schritt 5: Bilder veröffentlichen	324
Was passiert beim Veröffentlichen	325
Wichtige Informationen	325
Schritt 6: IaC generieren	326
Amazon Elastic Kubernetes Service (Kubernetes)	326
Amazon Elastic Container Service (Terraform)	326
Automatisierte Validierung und Sicherheitsscans	327
IaC wird ohne veröffentlichte Bilder generiert	327
Wichtige Informationen	327
Schritt 7: Stellen Sie die Testinfrastruktur bereit	328

Was passiert während der Testbereitstellung	328
Wichtige Informationen	328
Iteration an der Infrastruktur	329
Wiederherstellung der Sitzung	329
Schritt 8: Bereinigen Sie die Testinfrastruktur	329
Wichtige Informationen	329
Schritt 9: Implementieren Sie die Umstellungsinfrastruktur	330
Wichtige Informationen	330
Wiederherstellung von Sitzungen	331
Mainframe-Modernisierung	332
Funktionen und Hauptmerkmale	332
High-level Komplettlösung	333
Der Mensch ist auf dem Laufenden (HITL)	333
Unterstützte Dateitypen für die Transformation von Mainframe-Anwendungen	334
Unterstützte Regionen und Kontingente für AWS Transformieren Sie den Mainframe	335
Der Weg zur Modernisierung	335
Phase 1: Beurteilen	335
Phase 2: Mobilisieren	336
Phase 3: Migration und Modernisierung	337
Phase 4: Betrieb, Optimierung und Innovation	339
Transformation des Workflows für Mainframe-Anwendungen	340
Voraussetzung: Bereiten Sie die Projekteingaben in S3 vor	340
Sammlung von Mainframe-Quellartefakten	341
Sign-in und erstelle einen Job	350
Den Fortschritt der Transformation verfolgen	351
Richten Sie einen Konnektor ein	351
Beurteilen und überdenken Sie den Stellenplan	356
Stellen Sie sich den Jobplan neu vor	362
Benutzerdefinierter Jobplan	362
Erstellen und implementieren Sie eine modernisierte Anwendung	395
Voraussetzungen	395
Schritt 1: Rufen Sie den modernisierten Code ab	396
Schritt 2: Erstellen Sie die modernisierte Anwendung	396
Schritt 3: Konfigurieren Sie die Testumgebung	397
Schritt 4: Stellen Sie die modernisierte Anwendung bereit	398
Schritt 5: Testen Sie die modernisierte Anwendung	399

Weiteres Beispiel	399
Full-stack Windows-Modernisierung	400
.NET	400
Umgebungen	400
Fähigkeiten und Hauptmerkmale	401
Unterstützte Versionen und Projekttypen	401
Einschränkungen	402
Menschliches Eingreifen	403
Weitere Informationen	403
.NET-Web-App	403
.NET-IDE	421
Portierung von Code auf UI-Ebene	430
Berichte über die Transformation	432
Bewährte Methoden	434
Modernisierung von SQL Server	440
Unterstützte -Regionen	441
Funktionen und Hauptmerkmale	441
Unterstützte Versionen und Projekttypen	442
Anforderungen für SQL Server	446
Anforderungen an die Bewerbung	447
Anforderungen an die Infrastruktur	448
Anforderungen an das Repository	448
SQL Server-Setup	448
AWS Transformieren Sie das Setup	457
Erstellen Sie einen Auftrag zur Modernisierung von SQL Server	457
Workflow zur Modernisierung von SQL Server	464
Testen und implementieren Sie nach der Transformation	497
Bewährte Methoden und Problembehebung	499
Sicherheit	505
Datenschutz	506
Cross-region Verarbeitung	507
Datenverschlüsselung	516
Verbesserung der Services	527
Identity and Access Management	528
Zielgruppe	529
Authentifizierung mit Identitäten	529

Verwalten des Zugriffs mit Richtlinien	531
Wie AWS Transform funktioniert mit IAM	532
Identity-based politische Beispiele	538
Fehlerbehebung	548
Verwenden von servicegebundenen Rollen	550
AWS verwaltete Richtlinien	557
AWS Referenz zu Transformationsberechtigungen	574
Compliance-Validierung	576
Ausfallsicherheit	576
VPC-Endpunkte (AWS PrivateLink)	577
Überlegungen zu AWS Transform VPC-Endpunkte	577
Voraussetzungen	577
Erstellen eines Schnittstellen-VPC-Endpunkts für AWS Transform	578
Verwenden Sie einen lokalen Computer, um eine Verbindung zu einem herzustellen AWS Transform Endpunkt	579
VPC-Zugriff auf Webanwendungen	579
Funktionsweise	579
Architektur	580
Voraussetzungen	581
Konfiguration der VPC-Endpunkttrichtlinie	581
Einrichtung eines kontrollierten Internetausgangs	582
Verifizierung	589
Fehlerbehebung	590
Kostenüberlegungen	591
Bereinigen	591
Überwachen	593
CloudTrail Logs	594
AWS Verwandeln Sie Informationen in CloudTrail	594
Verständnis AWS Logdateieinträge transformieren	595
Benachrichtigungen	595
E-Mail-Benachrichtigungen	595
Kontingente	598
Unterstützte Regionen	604
Unterstützt AWS-Regionen (standardmäßig aktiviert)	604
Support	606
Voraussetzungen	606

Support Case Management aktivieren	606
Einen Support-Fall erstellen	606
Supportfälle anzeigen	607
Mitteilungen zu einem Fall hinzufügen	608
Einen Fall lösen	608
Support Case Management deaktivieren	608
Nutzungsstelemetrie	609
Operative Daten	610
Änderungsprotokoll	611
Dokumentverlauf	636
.....	dcxlv

Was ist AWS Transformieren?

AWS Transform ist ein Service, der Ihnen hilft, die Transformation von Infrastruktur, Anwendungen und Code mit einem agentischen KI-Erlebnis zu beschleunigen und zu vereinfachen. Er bietet spezielle Tools zur Optimierung der Modernisierungs- und Migrationsbemühungen für verschiedene Workloads.

Mit AWS Transform können Sie:

- Modernisieren und migrieren Sie IBM z/OS und Fujitsu GS21 auf AWS
- Migrieren Sie VMware-Workloads zu Amazon EC2
- Modernisieren Sie .NET-Anwendungen auf plattformübergreifendes .NET Linux-ready
- Beurteilen Sie die Bereitschaft der Workloads zur Migration

AWS Transform hilft Ihnen dabei, arbeitsintensive, komplexe Transformationsaufgaben in der Erkennungs-, Planungs- und Ausführungsphase an KI-Agenten mit Fachkenntnissen in Sprachen, Frameworks und Infrastruktur auszulagern. Dieser Ansatz ermöglicht es Ihren Teams, sich auf Innovationen zu konzentrieren und gleichzeitig komplexe, umfangreiche Projekte durch ein einheitliches Weberlebnis effizient zu transformieren.

Für die Nutzung von AWS Transform fallen keine zusätzlichen Gebühren an.

Terminologie

In diesem Abschnitt steht Kursivschrift für einen offiziellen Begriff innerhalb der Definition eines anderen Begriffs.

Verbindung zum Konto

Ein Konto ist in diesem Zusammenhang ein allgemeiner Verweis auf einen kundeneigenen Container oder eine Sicherheitsgrenze für Ressourcen im AWS oder Remote-Service, z. B. ein AWS-Konto Oder-Konto. GitHub

Artifact

Ein von Transform erstelltes Ergebnis. AWS

Administrator

Administratoren können alles im Workspace lesen und mutieren. Sie können Chats mit AWS Transform beginnen, Jobs und upload/download Artefakte starten und beenden. Administratoren können mit laufenden Jobs interagieren, um HITL-Aktionen (Human-in-the-Loop) durchzuführen, und sie können kritische HITL-Aktionen wie die Zusammenführung zu Main, die Graphzerlegung oder die Bereitstellung von Code in Produktionsumgebungen genehmigen. [Administratoren können Workspaces, Konnektoren und Benutzer mutieren.](#)

Agent

Ein aufgabenspezifischer Dienst, der einen bestimmten Transformationstyp ausführt. Zum Beispiel VMware-Migrationen.

Genehmiger

Genehmiger haben ähnliche Rechte wie Administratoren, mit der Ausnahme, dass sie nicht berechtigt sind, Workspaces, Connectors oder Benutzer zu mutieren. [Genehmiger können keine Workspaces, Connectors oder Benutzer mutieren.](#)

Anlage

Eingabe für einen [Transformationsjob](#). Zum Beispiel Quellcode, Server, Datenbank, Netzwerk des Kunden. Auf Ressourcen wird über einen [Konnektor](#) zugegriffen.

Anfrage eines Mitarbeiters

Eine Aufgabe, bei der AWS Transform einen Menschen auffordert, etwas zu tun.

Anschluss

Konnektoren sind Asset-Anbieter, die den Zugriff auf kundeneigene Ressourcen in einem System außerhalb von AWS Transform ermöglichen.

Wenn Sie einen Connector einrichten, muss der Administrator des Kontos, zu dem Sie eine Verbindung herstellen, die Verbindung akzeptieren. Um die Verbindung akzeptieren zu können, müssen sie über die in [der Connector-Akzeptorrichtlinie](#) festgelegten Berechtigungen verfügen.

Die folgenden beiden Konten müssen entweder identisch sein oder derselben AWS Organizations Organisation angehören:

- Das Konto, von dem aus der AWS Transform-Administrator den Dienst aktiviert.
- Das Konto, das auf der Empfängerseite Ihrer Transformation sein wird. Diesem Konto muss eine IAM-Rolle zugewiesen werden, die es ihm ermöglicht, einen [Connector](#) zu verwenden.

Mitwirkender

Mitwirkende können alles im Workspace lesen. Sie können Chats mit AWS Transform beginnen, Jobs starten und beenden, Artefakte hoch- oder herunterladen und mit laufenden [Jobs](#) für HITL-Aktionen interagieren. Sie können jedoch keine kritischen HITL-Aktionen wie das Zusammenführen zu den Hauptfunktionen, die Graphzerlegung oder die Bereitstellung von Code in Produktionsumgebungen ausführen. [Mitwirkende können auch keine Arbeitsbereiche, Konnektoren oder Benutzer mutieren.](#)

Zielsetzung

Ein benutzerdefinierter Endzustand, auf den AWS Transform hinarbeitet. Benutzer schreiben dies, und AWS Transform wandelt das Ziel dann in eine Reihe von Aufgaben um, die es bei Bedarf gemeinsam mit den Benutzern ausführt.

Job

Ein lang andauernder Prozess (weeks/months+), an dem AWS Transform arbeitet, um ein von einem Benutzer definiertes [Ziel](#) zu erreichen. Bestehend aus mehreren [Aufgaben](#) und Anfragen von [Mitarbeitern](#).

Planen

Eine Liste von [Aufgaben](#), die AWS Transform (mit Hilfe von menschlichen Benutzern) zur Verfolgung eines [Ziels](#) übernimmt.

Leser

Leser können den Status und die Ergebnisse der AWS Transform-Jobs einsehen, aber keine Änderungen vornehmen. Sie können alles im [Workspace](#) lesen, Artefakte herunterladen, [Jobs](#) ansehen und sich Human-in-the-Loop (HITL) -Aktionen (Human-in-the-Loop) ansehen. Leser können in Transform jedoch keine mutierenden Aktionen ausführen. AWS

Aufgabe

Eine einzelne Arbeitseinheit, die Teil eines [Jobs](#) ist.

Arbeitsprotokoll

Ein Protokoll darüber, welche Aktionen AWS Transform und Benutzer im Rahmen eines [Jobs](#) ausgeführt haben.

Arbeitsbereich

Eine AWS Transform-Ressource, die andere Ressourcen wie [Konnektoren](#) und [Jobs](#) enthält. Ein [Workspace](#) dient als Grenze für Berechtigungen.

Erste Schritte mit AWS Transformieren

Topics

- [Einrichtung AWS Transformieren](#)
- [Aktivieren AWS Transformieren](#)
- [Schnellstart: Ich versuche es AWS Transformieren](#)
- [Verwalten von Benutzern](#)
- [AWS Transformieren Sie die Umgebung](#)

Einrichtung AWS Transformieren

Bevor Sie beginnen

Bevor Sie AWS Transform einrichten, stellen Sie sicher, dass Sie über ein AWS Konto mit Administratorzugriff verfügen

Note

Wenn Sie AWS Transform als Machbarkeitsnachweis oder für Testumgebungen ausprobieren möchten, finden Sie weitere Informationen unter [Schnellstart: Transform ausprobieren](#). AWS

Melden Sie sich an für ein AWS-Konto

Um loszulegen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter [Erste Schritte mit einem AWS-Konto](#) im AWS -Kontenverwaltung Referenzhandbuch.

Erste Schritte mit Access IAM-only

Beim IAM-only Zugriff authentifizieren sich Benutzer mit ihren vorhandenen AWS Anmeldeinformationen.

So richten Sie den IAM-only Zugriff ein:

1. Navigieren Sie in der AWS Konsole zu AWS Transform und wählen Sie Get started aus.

2. Schließen Sie die Konfiguration der Kontoeinstellungen ab.
3. Wählen Sie unter Benutzerzugriff die Option IAM-only Zugriff aus.
4. Wählen Sie Aktivieren, um Ihr Profil zu erstellen.

Benutzer melden sich über bei der AWS Transform-Webanwendung an [AWS Sign-In](#). Ihre Benutzer-ID in der Webanwendung basiert auf ihrem IAM-Prinzipal.

Important

Nach Abschluss der Einrichtung können Sie keinen Identitätsanbieter hinzufügen. Um Benutzer mit IAM Identity Center oder einem vorhandenen Identitätsanbieter zu verwalten, wählen Sie bei der Ersteinrichtung eine dieser Optionen aus.

Mit IAM-only Zugriff kann jeder IAM-Prinzipal mit der `transform:AccessTransformProfile` Berechtigung für die Profilressource auf Transform zugreifen AWS . Sie verwalten den Benutzerzugriff über IAM-Richtlinien und nicht über Benutzerzuweisungen von Identitätsanbietern.

Die `transform:AccessTransformProfile` Aktion gewährt nur Zugriff auf AWS Transform. Sobald sie sich in AWS Transform befinden, steuern Workspace-Rollen, welche Aktionen ein Benutzer ausführen kann. Zu diesen Rollen gehören Admin, Contributor, Approver und Read-only Workspace-Rollen gelten unabhängig davon, wie sich der Benutzer authentifiziert hat.

Verwenden von IAM-Anmeldeinformationen

Umgang mit Benutzerinformationen

Wenn IAM-Prinzipale auf AWS Transform zugreifen, behandelt der Dienst die Benutzeridentität anders als beim Zugriff auf Identitätsanbieter.

Benutzeridentität

[IAM-Benutzer werden anhand ihres IAM-Prinzipals identifiziert.](#)

Doppelte Identität

Ein Benutzer, der sowohl über eine Identitätsanbieter-Identität (wie IAM Identity Center) als auch über eine IAM-Sitzung verfügt, wird in AWS Transform als zwei separate Benutzer angezeigt. Ihre Arbeit steht in keinem Zusammenhang zwischen den beiden Identitäten.

E-Mail-Benachrichtigungen

E-Mail-Benachrichtigungen sind nur für SSO-Benutzer aktiviert. IAM-Prinzipale können weiterhin zu Workspaces hinzugefügt werden, sie erhalten jedoch keine E-Mail-Benachrichtigungen.

Audit

IAM-API-Aufrufe werden AWS CloudTrail mit der IAM-Identität des Anrufers angemeldet.

Aktionen, die von IAM-Benutzern in einem Job ausgeführt werden, können auch in Transform-Worklogs nachverfolgt werden. AWS

Aktivierung des IAM-Zugriffs zusammen mit einem Identitätsanbieter

Wenn Sie AWS Transform mit IAM Identity Center oder einem externen Identitätsanbieter einrichten, können Sie den IAM-Zugriff auch als zusätzliche Authentifizierungsmethode aktivieren. Auf diese Weise können IAM-Prinzipale zusammen mit Ihren bestehenden Identity AWS Provider-Benutzern auf Transform zugreifen.

Der IAM-Zugriff ist standardmäßig aktiviert, wenn Sie ein Profil mit IAM Identity Center oder einem externen Identitätsanbieter erstellen. So können Sie den IAM-Zugriff jederzeit aktivieren oder deaktivieren:

1. Navigieren Sie in der AWS Transform-Konsole zu Einstellungen.
2. Aktivieren oder deaktivieren Sie unter Mit IAM-Anmeldeinformationen auf AWS Transformation zugreifen die Option IAM-Zugriff aktivieren.

Wenn der IAM-Zugriff aktiviert ist, können sowohl Identity Provider-Benutzer als auch IAM-Prinzipale Transform verwenden. AWS IAM-Benutzer und Identity Provider-Benutzer können im selben Workspace zusammenarbeiten.

Erste Schritte mit AWS Organizations

Gehen Sie wie folgt vor, um AWS Transform einzurichten:

1. Melden Sie sich bei Ihrem AWS Organisationsverwaltungskonto an.
2. Navigieren Sie zum AWS Transform-Dienst.
3. Wählen Sie Dienst aktivieren für Ihre Organisation aus, um AWS Transform zu verwenden.
4. Konfigurieren Sie die erforderlichen Berechtigungen für Mitgliedskonten der Organisation.
5. Greifen Sie von Ihren Mitgliedskonten aus auf das AWS Transform-Weberlebnis zu.

 Note

Um die landing zone Accelerator (LZA) AWS On-Lösung zum Aufbau Ihrer Landing Zone zusammen mit den Migrationsfunktionen von AWS Transform zu verwenden, müssen sich Ihr AWS Transform-Konto und Ihre LZA-Installation in derselben AWS Organisation befinden. Die Verwendung separater Organisations-IDs für LZA- und AWS Transform-Bereitstellungen wird nicht unterstützt, da dies zu Inkonsistenzen bei der Organisationsverwaltung und der Ressourcenbereitstellung führen kann. Informationen zur Einrichtung Ihrer LZA-Installation mithilfe von Organizations finden Sie unter [Bereitstellen einer Cloud-Grundlage zur Unterstützung stark regulierter Workloads und komplexer Compliance-Anforderungen](#) im Benutzerhandbuch von Landing Zone Accelerator on AWS Implementation Guide.

Erste Schritte mit AWS IAM Identity Center

Gehen Sie wie folgt vor, um IAM Identity Center for AWS Transform zu verwenden und Benutzer und Gruppen hinzuzufügen.

Standardmäßig haben keine Benutzer Zugriff auf AWS Transform, wenn Sie es zum ersten Mal aktivieren.

 Note

IAM Identity Center ist nicht auf die Region beschränkt, in der es eingerichtet ist. Wenn Sie IAM Identity Center bereits in einer Region eingerichtet haben, die von AWS Transform nicht unterstützt wird, können Sie es für AWS Transform verwenden.

1. Richten Sie IAM Identity Center gemäß den Anweisungen unter [So aktivieren Sie eine Instanz von IAM Identity Center](#) ein.

Konfigurieren Sie IAM Identity Center für die Verwendung eines externen Unternehmensidentitätsanbieters und replizieren Sie dessen Benutzer- und Gruppeninformationen in IAM Identity Center.

2. Wählen Sie in der AWS Konsole AWS Transform und anschließend Get started aus.
3. Wählen Sie Dienst aktivieren für Ihre Organisation aus, um AWS Transform zu verwenden.
4. Wählen Sie einen Verschlüsselungsschlüssel aus. Die Standardauswahl ist ein AWS verwalteter Schlüssel. Um einen benutzerdefinierten Schlüssel zu verwenden:

- a. Wählen Sie unter Verschlüsselungsschlüssel die Option Verschlüsselungseinstellungen anpassen aus.
- b. Wählen Sie AWS KMS-Schlüssel verwenden aus.
- c. Wählen Sie einen vorhandenen Schlüssel oder erstellen Sie einen neuen.
- d. Wählen Sie „Senden“, um Ihre Änderungen zu übernehmen, und wählen Sie dann „AWS Transformation aktivieren“.

Wählen Sie „Profil anzeigen“, um die Konfiguration anzuzeigen. Die URL der Webanwendung wird von Ihren Benutzern für den Zugriff auf das einheitliche Weberlebnis von AWS Transform verwendet.

5. Wählen Sie im Navigationsbereich Benutzer aus und wählen Sie Benutzer oder Gruppen zuweisen aus.
6. Suchen Sie nach dem Namen des Benutzers oder der Gruppen, die Sie zur Verwendung von AWS Transform autorisieren möchten. Die Suche verweist auf Benutzer und Gruppen, die von Ihrem Identitätsanbieter weitergegeben wurden.
7. Wählen Sie eine Gruppe oder einen Benutzer aus, wählen Sie Fertig und dann Zuweisen aus. Diese Benutzer sind berechtigt, die einheitliche Weboberfläche von AWS Transform zu verwenden.

Verwendung von Identitätsanbietern von Drittanbietern

AWS Transform unterstützt die Integration mit Identitätsanbietern von Drittanbietern (IdPs) wie Azure Active Directory (Entra ID) und Okta Workforce Identity. Auf diese Weise können Sie Ihr vorhandenes Identitätsverwaltungssystem für die Benutzerauthentifizierung verwenden.

Voraussetzungen

Stellen Sie vor der Konfiguration der Integration eines externen Identitätsanbieters sicher, dass für die Benutzer Ihres Identitätsanbieters die Attribute Name, E-Mail und Benutzername konfiguriert sind

Gespeicherte Informationen

Wenn Sie AWS Transform mit verwenden IdPs, AWS werden nur minimale Benutzerinformationen gespeichert, die verschlüsselt und gesichert sind:

Gespeicherte Benutzerinformationen

AWS Transform speichert bei der ersten Anmeldung grundlegende Benutzerprofilinformationen, darunter den Anzeigenamen, die E-Mail-Adresse, den Benutzernamen (`preferred_username`) und eine eindeutige Benutzerkennung. Diese Informationen werden je nach Konfiguration des Transform-Profiles des Kunden entweder mit einem kundeneigenen KMS-Schlüssel oder einem diensteigenen Schlüssel verschlüsselt. Die Daten werden in der Authentifizierungsdatenbank von AWS Transform gespeichert und nur während der ersten Anmeldesitzung gesammelt. Dadurch werden die Suchergebnisse aufgefüllt, wenn andere Benutzer in einen Workspace eingeladen werden.

Datenlebenszyklus

Benutzerinformationen werden nur für Benutzer gespeichert, die sich mindestens einmal bei der AWS Transform-Web-App angemeldet haben. Sie können veraltet sein, wenn Benutzer ihre Informationen in ihrem Identitätsanbieter aktualisieren, ohne sich erneut bei AWS Transform anzumelden. Alle gespeicherten Benutzerinformationen werden gelöscht, wenn das AWS Transform-Profil gelöscht wird.

Geheimer Speicher des Kunden

Das bei der Einrichtung angegebene geheime Kundegeheimnis wird AWS Secrets Manager mithilfe eines Service Linked Secret (SLS) in Ihrem Konto gespeichert.

Umgang mit Benutzerkennungen

Geben Sie ein

Verwendet den „oid“-Anspruch (Object Identifier) als eindeutige Benutzer-ID, die unveränderlich ist und Benutzer im gesamten Microsoft-Mandanten eindeutig identifiziert. Dieser Wert ist für Kunden in der Entra-Konsole sichtbar und erscheint in CloudTrail den Protokollen.

Okta Workforce Identity

Verwendet je nach Tokentyp unterschiedliche Ansprüche für die Benutzeridentifikation — den „Sub“-Anspruch bei ID-Token und den „UID“-Anspruch bei Zugriffstoken. AWS Transform überprüft, ob beide Ansprüche bei der Authentifizierung denselben Wert enthalten. Dieser Wert ist für Kunden in der Okta-Konsole sichtbar und erscheint in CloudTrail den Protokollen.

Azure Active Directory einrichten (Entra ID)

So konfigurieren Sie die Azure Active Directory-Integration mit AWS Transform:

1. Navigieren Sie zum Azure-Portal und wählen Sie Azure Active Directory aus.
2. Wählen Sie im linken Navigationsbereich Verwalten > App-Registrierungen aus.
3. Wählen Sie + Neue Registrierung.
4. Geben Sie einen Anwendungsnamen ein, wählen Sie Ihren unterstützten Kontotyp aus, lassen Sie die Umleitungs-URI leer und wählen Sie Registrieren.
5. Wählen Sie in der linken Navigationsleiste „Verwalten“ > „Manifest“.
6. Aktualisieren Sie `requestedAccessTokenVersion` von `null` bis 2 und wählen Sie Speichern.
7. Wählen Sie „Verwalten“ > „Eine API verfügbar machen“ und wählen Sie „Bereich hinzufügen“.
8. Erstellen Sie einen Anwendungs-ID-URI mit der Standardstruktur `api://<client-id>`.
9. Fügen Sie den Bereich hinzu `transform:read_write`.
10. Wählen Sie Zertifikat oder Geheimnis hinzufügen und erstellen Sie ein neues Client-Geheimnis. Speichern Sie diesen Wert so, wie er für die Profilerstellung benötigt wird.
11. Suchen Sie die Aussteller-URL, indem Sie Endpoints und dann das OpenID Connect-Metadaten-Dokument auswählen. Das Feld „Aussteller“ in den Metadaten ist Ihre Aussteller-URL.
12. Erstellen Sie in der AWS Transform-Konsole ein Profil mit der Client-ID, dem geheimen Clientschlüssel und der Aussteller-URL.
13. Fügen Sie nach der Profilerstellung eine Umleitungs-URI hinzu, indem Sie Plattform hinzufügen, Web auswählen und eingeben `<web-application-url>/login/callback`.

Okta Workforce Identity einrichten

So konfigurieren Sie die Integration von Okta Workforce Identity mit AWS Transform:

1. Navigieren Sie zu Ihrer Okta Workforce Identity-Konsole.
2. Wählen Sie „Anwendungen“ > „Anwendungen“ und dann „Anwendungsintegration erstellen“.
3. Wählen Sie OIDC — OpenID Connect and Web Application und dann Weiter.
4. Geben Sie Ihrer Anwendung einen Namen, lassen Sie den Grant Type als Autorisierungscode stehen, lassen Sie die Weiterleitungs-URIs leer, konfigurieren Sie Benutzerzuweisungen und wählen Sie Speichern.

5. Navigieren Sie zur Registerkarte „Anmelden“ und geben Sie als Aussteller Okta-URL statt „Dynamisch“ ein.
6. Kopieren Sie die Client-ID und konfigurieren Sie sie als Zielgruppe für Ihren Autorisierungsserver, indem Sie zu Sicherheit > API gehen und einen Autorisierungsserver hinzufügen.
7. Fügen Sie im Autorisierungsserver den Bereich auf der `transform:read_write` Registerkarte Bereiche hinzu.
8. Fügen Sie eine Zugriffsrichtlinie hinzu, die es der OIDC-Anwendung ermöglicht, diesen Autorisierungsserver zu verwenden, und konfigurieren Sie eine Regel für die Richtlinie.
9. Notieren Sie sich auf der Seite mit den Einstellungen des Autorisierungservers die Aussteller-URL für die Profilerstellung in Transform. AWS
10. Erstellen Sie in AWS Transform ein Profil mit der Aussteller-URL, der Client-ID und dem geheimen Clientschlüssel aus den Anwendungseinstellungen.
11. Fügen Sie `<web-application-url>/login/callback` nach der Profilerstellung auf der Registerkarte Allgemein der Anwendung eine Umleitungs-URL hinzu.

Note

Wenn Sie nach dem Abmelden zurück zur AWS Transform-Webanwendung weitergeleitet werden möchten, müssen Sie die URL Ihrer Webanwendung unter Sicherheit > API als vertrauenswürdigen Ursprung konfigurieren.

Onboarding von Benutzern

In diesem Abschnitt wird die Erfahrung für Benutzer beschrieben, denen Zugriff auf AWS Transform gewährt wurde.

Annahme der Einladung

Wenn ein Benutzer zu AWS Transform hinzugefügt wird, erhält er eine E-Mail-Einladung mit:

- Eine Begrüßung und Informationen zur Einladung
- Die URL der AWS Transform-Webanwendung
- Ihr Nutzernamen
- Ein Link, um die Einladung anzunehmen und ihr Passwort einzurichten

Um ihr Konto einzurichten:

1. Der Benutzer klickt in der E-Mail auf den Link „Einladung annehmen“.
2. Auf der Seite „Registrierung neuer Benutzer“ gibt er ein Passwort ein und bestätigt es.
3. Das Passwort muss die folgenden Sicherheitsanforderungen erfüllen:
 - Mindestens 8 Zeichen
 - Mindestens einen Großbuchstaben
 - Mindestens einen Kleinbuchstaben
 - Mindestens eine Zahl
 - Mindestens ein Sonderzeichen
4. Nachdem sie ein Passwort erstellt haben, erhalten sie eine Bestätigung, dass ihr Konto erfolgreich erstellt wurde.

Melden Sie sich an bei AWS Transformieren

Um dich bei AWS Transform anzumelden:

1. Navigieren Sie zur URL der AWS Transform-Webanwendung, die in der Einladungs-E-Mail angegeben ist.
2. Geben Sie den Nutzernamen ein.
3. Wählen Sie Weiter aus.
4. Geben Sie das Passwort ein.
5. Klicken Sie auf Sign in.

Willkommenes Erlebnis

Nach der ersten Anmeldung sehen Benutzer die AWS Transform-Willkommenseite mit:

- Eine personalisierte Begrüßung
- Verfügbare Transformationsfunktionen
- Option zum Erstellen eines Arbeitsbereichs

Auf der Willkommenseite finden Sie Informationen zu den in AWS Transform verfügbaren Transformationsfunktionen, darunter:

- Modernisieren Sie z/OS IBM-Migrationen zu AWS
- Migrieren Sie VMware-Workloads zu Amazon EC2
- Modernisieren Sie .NET-Anwendungen auf plattformübergreifendes .NET Linux-ready
- Beurteilen Sie die Bereitschaft der Workloads zur Migration

Benutzer können damit beginnen, einen Workspace zu erstellen oder ihr Team zu bitten, sie zu einem bestehenden Workspace hinzuzufügen.

Verwenden Sie Ihren eigenen Amazon S3 S3-Bucket

Standardmäßig verwendet AWS Transform einen vom Service verwalteten Amazon S3 S3-Bucket zum Speichern von Transformationsartefakten. Sie können stattdessen Ihren eigenen Amazon S3 S3-Bucket verwenden, um mehr Kontrolle über Datenspeicher-, Verschlüsselungs- und Zugriffsrichtlinien zu haben.

Note

Wenn Sie über einen Amazon S3 S3-Bucket für Mainframe-Transformationen verfügen, können Sie diesen S3-Connector weiterhin verwenden und müssen diese Funktionalität nicht verwenden.

Note

Ihr Amazon S3 S3-Bucket speichert nur die Uploads und Transformationsartefakte, mit denen Sie interagieren. Interne, vom System generierte Artefakte werden nicht in Ihrem Bucket gespeichert. Darüber hinaus AWS indexiert Transform die Artefakte in Ihrem Bucket. Es speichert die indexierten Daten in einer vom Service verwalteten Wissensdatenbank, die verwendet wird, um Ihnen ein erweitertes Chat-Erlebnis zu bieten.

Voraussetzungen

Bevor Sie Ihren eigenen Amazon S3 S3-Bucket konfigurieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Bucket muss sich in derselben AWS Region befinden, in der AWS Transform aktiviert ist.

- Die erforderliche Bucket-Richtlinie muss auf Ihren Bucket angewendet werden. Weitere Informationen finden Sie unter [the section called “Erforderliche Bucket-Richtlinie”](#).
- Wenn Sie die AWS Transform-Webanwendung verwenden, muss CORS in Ihrem Bucket konfiguriert sein. Weitere Informationen finden Sie unter [the section called “Erforderliche CORS-Konfiguration”](#).
- Wenn Sie einen benutzerdefinierten AWS KMS-Schlüssel verwenden, muss die erforderliche Schlüsselrichtlinie angewendet werden. Weitere Informationen finden Sie unter [the section called “KMS-Schlüsselrichtlinie \(optional\)”](#).

Unterstützte Verschlüsselungskonfigurationen

Ihr Bucket muss eine der folgenden Verschlüsselungskonfigurationen verwenden:

- SSE-S3 (AES256) — Lassen Sie das KMS-Schlüsselfeld leer. AWS Transform schreibt Objekte, ohne einen Verschlüsselungsheader anzugeben, und Amazon S3 wendet die Standardverschlüsselung des Buckets mit S3-managed Schlüsseln an. Weitere Informationen finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln \(SSE-S3\)](#) im Amazon S3 S3-Benutzerhandbuch.
- SSE-KMS mit einem vom Kunden verwalteten KMS-Schlüssel — Geben Sie den KMS-Schlüssel-ARN an. AWS Transform schreibt Objekte `x-amz-server-side-encryption: aws:kms` unter Verwendung des bereitgestellten Schlüssels. Befolgen Sie [the section called “KMS-Schlüsselrichtlinie \(optional\)”](#).

Folgendes wird nicht unterstützt:

- SSE-KMS mit einem AWS-verwalteten KMS-Schlüssel (zum Beispiel `aws/s3`)
- SSE-C
- DSSE-KMS
- Asymmetrische KMS-Schlüssel oder KMS-Schlüssel mit einer anderen Schlüsselspezifikation als `SYMMETRIC_DEFAULT`

 Warning

AWS-verwaltete KMS-Schlüssel werden nicht unterstützt. Wenn Ihr Bucket mit verschlüsselt ist `aws/s3`, migrieren Sie zu einem vom Kunden verwalteten Schlüssel oder SSE-S3 bevor Sie den Bucket mit AWS Transform verwenden.

Konfiguration Ihres Amazon S3 S3-Buckets

Sie können Transform von der AWS Transform-Konsole aus so konfigurieren, dass es Ihren eigenen Amazon S3 S3-Bucket verwendet. AWS

Um Ihren eigenen Amazon S3 S3-Bucket zu verwenden

1. Wählen Sie in der AWS Transform-Konsole Einstellungen aus.
2. Wählen Sie unter Artefaktspeicher die Option Meinen eigenen S3-Bucket verwenden aus. Sie können einen Bucket in Ihrem aktuellen Konto AWS-Konto oder in einem anderen Konto verwenden.
3. Geben Sie für Bucket die Amazon S3 S3-URI ein.
4. (Optional) Geben Sie für KMS-Schlüssel einen AWS KMS-Schlüssel-ARN ein, um Objekte im Bucket zu verschlüsseln. Wenn Sie dieses Feld leer lassen, schreibt AWS Transform Objekte ohne Verschlüsselungsheader, und Amazon S3 wendet die Standardverschlüsselungseinstellungen des Buckets an. Weitere Informationen finden Sie unter [Einstellung des standardmäßigen serverseitigen Verschlüsselungsverhaltens für Amazon S3 S3-Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

Wenn die Standardverschlüsselung Ihres Buckets lautet SSE-KMS, geben Sie den vom Kunden verwalteten KMS-Schlüssel-ARN in dieses Feld ein und aktualisieren Sie Ihre Schlüsselrichtlinie. Weitere Informationen finden Sie unter [the section called “KMS-Schlüsselrichtlinie \(optional\)”](#).

5. Wählen Sie Speichern. AWS Transform validiert die Bucket-Konfiguration und die Berechtigungen, bevor die Konfiguration angewendet wird.

Nachdem Sie die Konfiguration gespeichert haben, verwendet AWS Transform Ihren Bucket zum Speichern von Transformationsartefakten.

 Note

AWS Transform validiert Ihre Konfiguration nur, wenn Sie speichern. Wenn Sie später die Bucket-Richtlinie, die CORS-Konfiguration oder die KMS-Schlüsselrichtlinie ändern, speichern Sie Ihre Profileinstellungen erneut, um sie erneut zu validieren.

Erforderliche Bucket-Richtlinie

Sie müssen die Bucket-Richtlinie konfigurieren, um AWS Transform-Zugriff zu gewähren. Fügen Sie Ihrem Amazon S3 S3-Bucket die folgende Bucket-Richtlinie hinzu, damit der AWS Transform-Serviceprinzipal Transformationsartefakte lesen, schreiben, löschen und auflisten kann.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "transform.amazonaws.com"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:::bucket-name/AWSTransform/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "profile-account-id",
          "aws:SourceArn": "profile-arn"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": [
            "transform.amazonaws.com"
        ],
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:::bucket-name",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "profile-account-id",
                "aws:SourceArn": "profile-arn"
            }
        }
    }
}

```

Ersetzen Sie die folgenden Werte:

- *bucket-name*— Der Name Ihres Amazon S3 S3-Buckets.
- *profile-account-id*— Die mit Ihrem AWS Transform-Profil verknüpfte AWS-Konto ID.
- *profile-arn*— Der ARN Ihres AWS Transform-Profiles.

Erforderliche CORS-Konfiguration

Wenn Sie die AWS Transform-Webanwendung verwenden, müssen Sie Cross-Origin Resource Sharing (CORS) in Ihrem Amazon S3 S3-Bucket konfigurieren. Sie können die Webanwendungsdomäne finden, nachdem Sie AWS Transform aktiviert haben. Weitere Informationen finden Sie unter [Erste Schritte](#).

```

[
  {
    "AllowedHeaders": [
      "host",
      "content-type",
      "if-none-match",
      "x-amz-checksum-sha256",
      "x-amz-expected-bucket-owner",
      "x-amz-server-side-encryption",
      "x-amz-server-side-encryption-aws-kms-key-id",
      "x-amz-server-side-encryption-context",
      "x-amz-source-account",
    ]
  }
]

```

```
        "x-amz-source-arn"
    ],
    "AllowedMethods": [
        "GET",
        "PUT",
        "HEAD"
    ],
    "AllowedOrigins": [
        "webapp-domain"
    ],
    "ExposeHeaders": [
        "ETag",
        "x-amz-checksum-sha256",
        "x-amz-request-id",
        "x-amz-id-2"
    ],
    "MaxAgeSeconds": 3600
}
]
```

Ersetzen Sie die folgenden Werte:

- *webapp-domain*— Die Quell-URL Ihrer Webanwendung (z. B. `https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`), die Sie auf der Seite mit den AWS Transform-Einstellungen finden. Fügen Sie den abschließenden Schrägstrich nicht ein.

KMS-Schlüsselrichtlinie (optional)

Dieser Abschnitt gilt nur, wenn Ihr Bucket mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Wenn Ihr Bucket verwendet SSE-S3, überspringen Sie diesen Abschnitt.

Wenn Sie Ihren eigenen AWS KMS-Schlüssel für die Bucket-Verschlüsselung angeben, fügen Sie Ihrer Schlüsselrichtlinie die folgende Anweisung hinzu. AWS Transform verwendet Forward Access Sessions (FAS), um Grants für seinen Service Principal zu erstellen. Diese Grants werden verwendet, um Ihren Schlüssel und Ihre Zugriffsartefakte in Ihrem Amazon S3 S3-Bucket zu validieren.

```
{
  "Sid": "AllowAWSTransformServiceAccess",
  "Effect": "Allow",
  "Principal": {
```



```
    "AWS": "arn:aws:iam::key-owner-account-id:root"
  },
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "transform.region.amazonaws.com"
    }
  }
}
```

Ersetzen Sie die folgenden Werte:

- *key-owner-account-id*— Die AWS-Konto ID, der der KMS-Schlüssel gehört.
- *region*— Die AWS Region, in der AWS Transform aktiviert ist (z. B. *us-east-1*).

Zurück zum Standard-Bucket

Sie können jederzeit zum vom Service verwalteten Bucket zurückkehren.

Um zu wechseln AWS Transformieren Sie verwalteten Speicher

1. Wählen Sie in der AWS Transform-Konsole Einstellungen aus.
2. Wählen Sie unter Artefaktspeicher die Option Bearbeiten aus.
3. Wählen Sie Verwalteten Speicher AWS transformieren aus.
4. Wählen Sie Speichern.

Warning

Wenn Sie die Speicherkonfiguration wechseln, während Transformationsjobs ausgeführt werden, schlagen diese Jobs fehl. Auf alle Artefakte, die bereits durch diese laufenden Jobs generiert wurden, könnte ebenfalls nicht zugegriffen werden.

 Important

Wenn Sie zurück zum vom Service verwalteten Bucket wechseln, gehen Sie wie folgt vor:

- Artefakte in Ihrem Bucket werden nicht automatisch migriert. Um Artefakte beizubehalten, laden Sie sie aus Ihrem Amazon S3 S3-Bucket herunter und laden Sie sie über die AWS Transform-Webanwendung erneut in den Artefaktspeicher für den entsprechenden Workspace und Job hoch.
- AWS Transform zieht seinen Zuschuss für Ihren KMS-Schlüssel zurück. In Ihren Bucket geschriebene Objekte verbleiben in Ihrem Bucket. Löschen Sie sie manuell, wenn sie nicht mehr benötigt werden.

Dateien werden direkt in Ihren Bucket hochgeladen

Sie können Dateien direkt in Ihren Amazon S3 S3-Bucket hochladen, ohne die AWS Transform-Webanwendung zu verwenden. Um hochgeladene Dateien für Transformationsagenten verfügbar zu machen, laden Sie sie in den User Uploads Ordner für den Job hoch. Der Verzeichnispfad für diesen Ordner verwendet das folgende Format:

```
AWSTransform/Workspaces/workspace-id/Jobs/job-id/User Uploads/
```

Ersetzen Sie die folgenden Werte:

- *workspace-id*— Die ID Ihres AWS Transform-Workspace.
- *job-id*— Die ID des Transformationsjobs.

Jeder Job in AWS Transform hat seinen eigenen User Uploads Ordner. Dateien, die Sie in diesen Pfad hochladen, werden in der Webanwendung angezeigt und stehen Transformationsagenten zur Verfügung, während sie den Job abschließen.

Dateipfade dürfen keine führenden oder nachfolgenden Leerzeichen enthalten . . — Dateien, die diese Einschränkungen verletzen, sind für Agenten nicht sichtbar. //

 Important

Wenn Ihr Bucket verwendet SSE-KMS, fügen Sie bei jedem direkten Upload die folgenden Header hinzu:

```
x-amz-server-side-encryption: aws:kms  
x-amz-server-side-encryption-aws-kms-key-id: your-kms-key-arn
```

Objekte müssen mit dem KMS-Schlüssel verschlüsselt werden, der in Ihrem AWS Transform-Profil registriert ist. Objekte, die mit einem anderen Schlüssel verschlüsselt wurden, sind für AWS Transform nicht zugänglich.

Kompatibilitätsmatrix

Die folgende Tabelle fasst die Kompatibilität von AWS Transform mit den gängigen Amazon S3 S3-Bucket-Funktionen zusammen.

Feature	Kompatibilität	Hinweise
Bucket-Versioning	Unterstützt	Verwalten Sie nicht aktuelle Versionen mit einer Lebenszyklusregel.
Object Ownership	Erforderlich: Der Bucket-Besitzer wurde erzwungen	Bucket Owner Preferred und Object Writer werden nicht unterstützt.
ACL	Nicht unterstützt	ACLs müssen für den Bucket deaktiviert sein.
Objektsperre (Governance-Modus)	Teilweise unterstützt	Löschungen werden möglicherweise durch Aufbewahrungseinstellungen blockiert.
Objektsperre (Konformitätsmodus)	Nicht unterstützt	—
Block Public Access	Unterstützt	—
Zahlung durch den Anforderer	Nicht unterstützt	—
S3-Zugriffspunkte	Nicht unterstützt	Verwenden Sie den Bucket-Namen.

Feature	Kompatibilität	Hinweise
S3-Objekt-Lambda-Zugangspunkte	Nicht unterstützt	Verwenden Sie den Bucket-Namen.
S3 on Outposts	Nicht unterstützt	—
S3 Express One Zone (Verzeichnis-Buckets)	Nicht unterstützt	—
Cross-Region Eimer	Nicht unterstützt	—
Cross-account Eimer	Unterstützt	—
Cross-account KMS-Schlüssel	Nicht unterstützt	—
Lebenszyklusregel	Unterstützt	—
CloudTrail Datenereignisse	Unterstützt	—

Aktivieren AWS Transformieren

Um AWS Transform zu aktivieren:

1. Melden Sie sich bei der AWS Management Console an.
2. Suchen Sie in der Suchleiste oben in der Konsole nach AWS Transform.
3. Wählen Sie AWS in den Suchergebnissen die Option Transformieren aus.
4. Wählen Sie Erste Schritte, um den Dienst in Ihrer aktuellen Region zu aktivieren.
5. Optional: Konfigurieren Sie IAM Identity Center. In einem späteren Schritt können Sie sich auch dafür entscheiden, einen [externen Identitätsanbieter \(IdP\)](#) zu verwenden.
6. Wählen Sie einen Verschlüsselungsschlüssel: AWS verwalteter Standardschlüssel oder Verschlüsselungseinstellungen anpassen.
7. Optional: Verwenden Sie Ihren eigenen Amazon S3 S3-Bucket. Standardmäßig verwendet AWS Transform einen vom Service verwalteten Amazon S3 S3-Bucket zum Speichern von

Transformationsartefakten. Sie können sich dafür entscheiden, stattdessen Ihren eigenen Bucket zu verwenden. Weitere Informationen finden Sie unter [Verwenden Sie Ihren eigenen Amazon S3 S3-Bucket](#).

8. Wählen Sie aus, welche AWS Transform-Funktionen Sie aktivieren möchten:
 - Befehlszeilenschnittstelle (CLI), erforderlich, um [benutzerdefinierte Transformationen](#) zu erstellen und auszuführen. Um die CLI zu aktivieren, lesen und befolgen Sie die Download-Anweisungen.
 - Webanwendung, die zentrale Benutzeroberfläche für die Modernisierung. Wählen Sie Webanwendung aktivieren, um sie zu verwenden.
9. Wählen Sie „AWS Transformation aktivieren“.
10. Optional: Wählen Sie „Profil anzeigen“ aktivieren, um auf die Registerkarten „Benutzer AWS transformieren“, „Einstellungen“ und „Connectors“ zuzugreifen, oder „Benutzer verwalten“, um Benutzer zu verwalten.

Sie können jederzeit auf die Registerkarten „Benutzer“, „Einstellungen“ und „Connectors“ zugreifen, indem Sie auf das Menüsymbol in der oberen linken Ecke der Konsole klicken.

11. Konfigurieren Sie den Benutzerzugriff, indem Sie eine der folgenden Optionen wählen:
 - IAM Identity Center
 - Ein [externer Identitätsanbieter \(IdP\)](#)
 - [IAM-only Zugriff](#)

 Note

Diese Auswahl ist abgeschlossen und kann nicht geändert werden, wenn Sie AWS Transform aktivieren.

12. Wählen Sie Webanwendung aktivieren aus.
13. Das System zeigt „Enabling AWS Transform“ an, während es die erforderlichen Ressourcen erstellt.

Nach der Aktivierung von AWS Transform werden auf der Registerkarte „Einstellungen“ die folgenden Informationen angezeigt:

- URL der Webanwendung — Die URL für den Zugriff auf die AWS Transform-Webanwendung

- Start-URL für IDE — Die URL für den Zugriff auf AWS Transform in integrierten Entwicklungsumgebungen
- Region — Die AWS Region, in der AWS Transform aktiviert ist

Schnellstart: Ich versuche es AWS Transformieren

AWS Transform lässt sich am einfachsten mit einem eigenständigen AWS Konto ausprobieren. Möglicherweise möchten Sie dies als Machbarkeitsnachweis oder für Testumgebungen tun. Gehen Sie wie folgt vor:

1. Melden Sie sich bei der AWS Management Console an.
2. Navigieren Sie zum AWS Transform-Dienst.
3. Wählen Sie Erste Schritte aus, um den Dienst zu aktivieren.
4. Wählen Sie Ihren Identitätsanbieter aus und richten Sie ihn ein.
5. Weisen Sie dem AWS Transform-Dienst Benutzer zu.
6. Nachdem der Dienst aktiviert wurde, sehen Sie die URL der AWS Transform-Webanwendung.
7. Öffnen Sie diese URL in einem neuen Browserfenster, um auf das AWS Transform-Weberlebnis zuzugreifen.

Jetzt bist du bereit, deinen Workspace einzurichten.

Verwalten von Benutzern

Wie du den Benutzerzugriff auf AWS Transform verwaltest, hängt von dem Zugriffsmodell ab, das du bei der Einrichtung ausgewählt hast. Wenn Sie IAM Identity Center konfiguriert haben, fügen Sie Benutzer über IAM Identity Center hinzu. Wenn Sie einen externen Identitätsanbieter konfiguriert haben, verwalten Sie Benutzer in diesem Anbieter. Wenn Sie IAM-only den Zugriff ausgewählt haben, wird der Benutzerzugriff über IAM-Richtlinien verwaltet.

Benutzer im IAM Identity Center hinzufügen

So fügen Sie Benutzer im IAM Identity Center hinzu:

1. Navigieren Sie zur IAM Identity Center-Konsole.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).

3. Wählen Sie Benutzer hinzufügen.
4. Geben Sie die erforderlichen Informationen ein:
 - **Nutzername** — Eine eindeutige Kennung für den Benutzer (kann später nicht geändert werden)
 - **E-Mail-Adresse** — Die E-Mail-Adresse des Benutzers
 - **Vorname und Nachname** — Der Name des Benutzers
 - **Anzeigename** — Der Name, der in der Benutzerliste erscheint
5. Wählen Sie unter Passwort aus, wie der Benutzer sein Passwort erhält:
 - **Eine E-Mail senden** — Anweisungen zur Einrichtung per E-Mail senden
 - **Generieren Sie ein Einmalpasswort** — Erstellen Sie ein Passwort, das Sie manuell teilen möchten
6. Wählen Sie Weiter, um die Benutzerinformationen zu überprüfen.
7. Überprüfen Sie die Details und wählen Sie Benutzer hinzufügen.

Nachdem der Benutzer hinzugefügt wurde, erhält er eine E-Mail-Einladung zur Einrichtung seines IAM Identity Center-Kontos. Der Einladungslink ist 7 Tage gültig.

In diesem Video erfahren Sie auch mehr über die Arbeit mit IAM Identity Center und AWS Transform:

[VideoTitle](#)

Benutzer hinzufügen zu AWS Transformieren

Nachdem Sie Benutzer zu IAM Identity Center hinzugefügt haben, können Sie ihnen Zugriff auf AWS Transform gewähren:

1. Kehren Sie zur AWS Transform-Konsole zurück.
2. Wählen Sie im Navigationsbereich Benutzer und Gruppen aus.
3. Wählen Sie die Registerkarte Benutzer oder die Registerkarte Gruppen aus.
4. Suchen Sie im IAM Identity Center nach den Benutzern oder Gruppen, die Sie hinzufügen möchten, und wählen Sie sie aus.
5. Wählen Sie Benutzer und Gruppen zuweisen, um den ausgewählten Benutzern oder Gruppen Zugriff auf AWS Transform zu gewähren.

Nach dem Hinzufügen von Benutzern werden sie in der Benutzerliste mit dem Status „Ausstehend“ angezeigt, bis sie die Einladung annehmen und sich anmelden.

Benutzer mit IAM-only Zugriff verwalten

Wenn Sie AWS Transform mit IAM-only Zugriff konfiguriert haben, wird der Benutzerzugriff über IAM-Richtlinien verwaltet. Jeder IAM-Prinzipal mit der `transform:AccessTransformProfile` Berechtigung für die Profilressource kann auf Transform zugreifen AWS .

So gewähren Sie einem Benutzer oder einer Rolle Zugriff auf AWS Transform:

1. Navigieren Sie zur IAM-Konsole.
2. Fügen Sie dem IAM-Benutzer oder der IAM-Rolle eine Richtlinie hinzu, die die `transform:AccessTransformProfile` Aktion beinhaltet. Eine Beispielrichtlinie finden Sie unter [Benutzern den Zugriff auf AWS Transform mit IAM-Anmeldeinformationen ermöglichen](#).

Um den Zugriff zu widerrufen, entfernen Sie die Richtlinie für den IAM-Benutzer oder die IAM-Rolle.

Grundlegendes zu den Berechtigungen von Mitarbeitern

AWS Transform verwendet ein auf Workspace basierendes Berechtigungsmodell, um den Zugriff auf Ressourcen und Aktionen zu kontrollieren. Jedem Benutzer wird innerhalb eines Workspace eine bestimmte Rolle zugewiesen, die bestimmt, welche Aktionen er ausführen kann. Ein Benutzer kann in verschiedenen Arbeitsbereichen unterschiedliche Rollen haben.

Benutzerrollen

AWS Transform unterstützt fünf Benutzerrollen in jedem Arbeitsbereich. Diese Rollen gelten im Kontext eines Workspace, und einem Benutzer werden Rollen in jedem Workspace zugewiesen, in dem er Mitglied ist. Die für jede Rolle definierten Zugriffsberechtigungen sind unabhängig vom Arbeitsbereich, sodass Benutzer A mit der Administratorrolle in Arbeitsbereich A dieselben Rechte hat wie Benutzer B mit der Administratorrolle in Arbeitsbereich B.

Rollen-Berechtigungen

Detaillierte Berechtigungen für jede Rolle:

Action	ResourceType	Admin.	Genehmiger	Beitragender	ReadOnly
Create	Workspace	✓	✓	✓	✓
Auflisten	Workspace	✓	✓	✓	✓
Get	Workspace	✓	✓	✓	✓
Aktualisierung	Workspace	✓	x	x	x
Delete	Workspace	✓	x	x	x
Create	ChatMessage	✓	✓	✓	x
Lesen	ChatMessage	✓	✓	✓	✓
Create	RoleAssociation	✓	x	x	x
Lesen	RoleAssociation	✓	✓	✓	✓
Aktualisierung	RoleAssociation	✓	x	x	x
Delete	RoleAssociation	✓	x	x	x
Lesen	Aufgabe mit kritischem Treffer	✓	✓	✓	✓
Aktualisierung	Aufgabe mit kritischem Treffer	✓	✓	x	x
Delete	Aufgabe mit kritischem Treffer	✓	✓	x	x
Lesen	Treffer-Task	✓	✓	✓	✓
Aktualisierung	Drücken Sie Aufgabe	✓	✓	✓	x
Delete	Drücken Sie Aufgabe	✓	✓	✓	x

Action	ResourceType	Admin.	Genehmiger	Beitragender	ReadOnly
Create	Aufgabe	✓	✓	✓	x
Lesen	Aufgabe	✓	✓	✓	✓
Aktualisierung	Aufgabe	✓	✓	✓	x
Delete	Aufgabe	✓	✓	✓	x
Lesen	Arbeitsprotokoll	✓	✓	✓	✓
Create	Artefakt	✓	✓	✓	x
Lesen	Artefakt	✓	✓	✓	✓
Aktualisierung	Artefakt	✓	✓	✓	x
Delete	Artefakt	✓	✓	✓	x
Create	Konnektor	✓	✓	✓	x
Lesen	Konnektor	✓	✓	✓	✓
Aktualisierung	Konnektor	✓	✓	✓	x
Delete	Konnektor	✓	✓	✓	x

Human-in-the-loop (HITL) -Aktionen

AWS Transform bietet zwei Arten von HITL-Aktionen: Standardaktionen und kritische Aktionen:

Standard-HITL-Aktionen

Dies sind Routineaktionen, die von Benutzern mit den Rollen Mitwirkender, Genehmiger oder Administrator ausgeführt werden können.

Kritische HITL-Aktionen

Dies sind Aktionen mit erheblichen Auswirkungen und erfordern daher höhere Genehmigungsstufen. Zu den Beispielen gehören:

- Code mit Hauptzweigen zusammenführen
- Zerlegung von Graphen durchführen
- Bereitstellen von Code in Produktionsumgebungen

Kritische HITL-Aktionen können nur von Benutzern mit Genehmigungs- oder Administratorrollen ausgeführt werden.

Um sicherzustellen, dass in den AuthZ-Richtlinien zwischen Standard-HITL- und kritischen HITL-Aktionen unterschieden wird, bietet AWS Transform zwei separate HITL-APIs, eine für die Durchführung einer Standard-HITL-Aktion und eine für den Abschluss einer kritischen HITL-Aktion.

AWS Transformieren Sie die Umgebung

AWS Transform ist ein Agentendienst, der natürliche Sprachverarbeitung verwendet, um Sie bei der Planung und Ausführung Ihrer Workload-Transformationen zu unterstützen. Sie interagieren mit AWS Transform hauptsächlich über eine Konversationsoberfläche, in der sich der Service an den Kontext Ihrer Diskussion anpasst und reagiert. Sie können beispielsweise damit beginnen, Ihre aktuellen Architektur- und Transformationsziele in alltäglicher Sprache zu beschreiben, z. B. „Ich muss meine lokalen VMs auf EC2 migrieren“.

Während Sie mit AWS Transform sprechen, erstellt der Service einen maßgeschneiderten Arbeitsplan, der auf Ihre spezifischen Anforderungen zugeschnitten ist. Der Gesprächsablauf ist dynamisch und wird von Ihnen gesteuert, sodass Sie Ihren Transformationsplan iterativ verfeinern können. Sie können den Arbeitsplan während des Gesprächs ändern, indem Sie Anfragen wie „Fügen Sie eine Testphase vor der Produktionsumstellung hinzu“ oder „Entfernen Sie den Backup-Schritt, da wir bereits eine Lösung haben“, stellen. Sie können auch zu einer vorherigen Aufgabe zurückkehren und sie erneut ausführen. AWS Transform aktualisiert den Plan kontinuierlich auf der Grundlage Ihrer Eingaben und stellt so sicher, dass die endgültige Transformationsstrategie Ihren technischen und geschäftlichen Anforderungen entspricht.

Folgendes sehen Sie, wenn Sie AWS Transform öffnen.

- Kontrollbereich anzeigen: Dies ist der schmale Bereich auf der linken Seite von AWS Transform. Sie können eines der Symbole auswählen, um auszuwählen, welche Ansicht rechts neben dem

Kontrollbereich für Ansichten angezeigt wird. Bewegen Sie den Mauszeiger über die einzelnen Symbole, um einen Tooltip zu erhalten, der die Ansicht erklärt. Die fünf Standardansichten, von oben nach unten, sind:

- Stellenplan
- Dashboard
- Genehmigungen
- Artefakte
- Arbeitsprotokoll

Einige Workflows bieten zusätzliche Ansichten.

Wenn Sie an einem Jobplan arbeiten, gibt es folgende Ansichten:

- Chat
- Genehmigungen
- Laden für Artefakte
- Arbeitsprotokoll

Wenn Sie sich in einem Workspace befinden, befinden sich die Ansichten ganz oben:

- Aufträge
- Artefakte
- Mitarbeiter (Benutzer)
- Konnektoren
- Einstellungen
- Der Bereich Ansicht befindet sich neben den Steuerelementen für die Ansicht.
- Der Chat-Bereich befindet sich in der Mitte. Hier führen Sie Ihre Konversation mit AWS Transform.

 Note

Benutzer mit Leseberechtigungen können im Chat keine Nachrichten senden.

- Auf der rechten Seite befindet sich der Bereich Zusammenarbeit. Dies erscheint, wenn HITL-Aktivitäten (Human in the Loop) ausgeführt werden, wie z. B.:
 - Datendateien werden hochgeladen

Spracheinstellungen

AWS Transform unterstützt die Lokalisierung für ausgewählte Workflows. Sie können die Anzeigesprache der Webanwendung ändern, indem Sie oben rechts auf das Einstellungssymbol klicken und im Menü Sprache Ihre bevorzugte Sprache auswählen.

Die folgenden Sprachen werden unterstützt:

- Englisch (USA)
- Englisch (UK)
- Deutsch (Deutsch)
- Español (Spanisch)
- Français (Französisch)
- (Japanisch)
- Bahasa Indonesien (Indonesisch)
- Italiano (Italienisch)
- Português (Portugiesisch)
- (Koreanisch)
- () (Chinesisch vereinfacht)
- () (Traditionelles Chinesisch)
- Türkçe (Türkisch)

Die folgenden Workflows unterstützen die Lokalisierung:

- [Migrationen \(einschließlich VMware\)](#)

Note

Andere AWS Transform-Workflows sind derzeit nur auf Englisch verfügbar. Lokalisierungsunterstützung für zusätzliche Workflows kann in future Updates hinzugefügt werden.

Starte dein Projekt

AWS Transform führt Sie durch Ihre Modernisierungs- und Migrationsprojekte. Erste Schritte:

1. Richten Sie einen Workspace ein, in dem Sie Ihr Projekt hosten können. Wählen Sie auf der Seite Workspaces die Option Workspace erstellen aus. Folge den Anweisungen und öffne dann den Workspace.
2. Geben Sie im Chat-Bereich „Job erstellen“ ein
3. Wählen Sie einen Job aus und folgen Sie den Anweisungen von AWS Transform. Wenn Ihre Eingabe erforderlich ist, wird der Bereich Zusammenarbeit angezeigt, in dem erklärt wird, was erforderlich ist.

Flexibilität im Arbeitsablauf

Die Workflow-Umgebung von AWS Transform bietet Flexibilität bei der Weiterentwicklung Ihrer Modernisierungsprojekte. Wenn Sie natürliche Sprache im Chat-Bereich verwenden, können Sie:

- Versuchen Sie erneut, eine Aufgabe auszuführen, die AWS Transform bereits abgeschlossen hat, und geben Sie dabei unterschiedliche Eingaben durch den Benutzer ein.
- Führen Sie einen Job erneut aus, z. B. wenn sich Ihre Modernisierungsquellen geändert haben.

Chatten mit AWS Transformieren

AWS Transform Chat ist in jeder Phase Ihres Projekts verfügbar. Um den Chat zu öffnen, klicken Sie auf das lila sechseckige Symbol in der unteren rechten Ecke der Webkonsole.

Der Chat ist da, damit Sie alles fragen können. Sie können den Chat beispielsweise bitten, Konzepte zu erläutern, Sie durch einen Prozess zu führen, eine AWS Transform-Anfrage oder -Antwort zu erläutern oder einen AWS Transform-Bericht zu erläutern.

Note

Benutzer mit Leseberechtigungen können im Chat keine Nachrichten senden.

AWS Transformieren Sie Chat-Integrationen

AWS Transform Chat ist integriert in:

Experience-Based Beschleunigung

[Experience-Based Acceleration \(EBA\)](#) wird über den AWS Transform-Chat angeboten. Damit können Sie eine EBA-Bewertung für Windows-Workloads durchführen und einen Plan erstellen. Sie können damit beginnen, die Bewertungsergebnisse aus CAST zu importieren. Es hilft Ihnen dabei, Ihr Anwendungsportfolio zu ermitteln. Anschließend können Sie mithilfe von AWS Transform Chat Anwendungen auswählen, die Ihren Geschäftsanforderungen entsprechen (z. B. Anwendungen nach Komplexität oder Codezeilen filtern). Anschließend können Sie eine eingehendere Bewertung der ausgewählten Anwendung durchführen und einen Modernisierungsplan erstellen.

AWS Countdown Premium

[AWS Countdown Premium](#) (CDP), das in AWS Transform integriert ist, bietet nachhaltige, fachkundige Beratung mit spezieller technischer Unterstützung. AWS Ihr designierter CDP-Techniker befasst sich eingehend mit Ihrem Tech-Stack und bietet personalisierten, kontextsensitiven Support, wenn Probleme auftreten. Benutzer können AWS Transform nutzen, um ein Support-Ticket direkt von der Chat-Oberfläche aus zu erstellen. Das Support-Ticket enthält Details zum Arbeitsprotokoll und zum Jobplan, damit der Support den Kontext des Kunden besser verstehen kann. Wenn ein Kunde oder Partner am CDP-Programm teilnimmt, wird das Supportticket automatisch an den zuständigen CDP-Techniker weitergeleitet, der Ihnen bei der Fehlersuche, der Interpretation der Transformationsergebnisse und der Beschleunigung der Problemlösung behilflich sein kann. Beispiel:

- Hinsichtlich von .NET-Workloads kann CDP bei Problemen mit dem Repository-Connector, bei der Behebung von Abhängigkeiten und bei der Bereitstellung nach der Transformation behilflich sein.
- In Mainframe-Szenarien kann CDP bei der Behebung von Problemen mit umgestaltetem Java-Code, bei der Konfiguration von Datenbankmigrationstools und beim Aufbau von Pipelines helfen. CI/CD
- Bei VMware-Migrationen kann CDP die Netzwerkkonfiguration, das MGN-Setup und die Agenteninstallation beschleunigen.

AWS Skill Builder

[AWS Skill Builder](#) bietet relevante Lernmodule über den Chat. Sie können AWS Transform Chat nach Ihren Lernbedürfnissen fragen, und es präsentiert Ihnen den entsprechenden Kurskatalog. Skill Builder bietet kontextbezogene Mikrolernerfahrungen, während Sie die Transformationsphasen durchlaufen.

Entwicklertools

Sie können über Agenten-IDEs, Agent-Plug-ins und den MCP-Server auf AWS Transform-Agenten zugreifen. Wählen Sie die Oberfläche, die zu Ihrem Arbeitsablauf passt.

Note

Die Kiro Power- und Agent-Plugins installieren den MCP-Server automatisch. Sie müssen den MCP-Server nur manuell installieren, wenn Sie ihn ohne ein Kiro Power- oder Agent-Plugin verwenden möchten.

Kiro Power

Der [AWS Transform Kiro Power](#) bietet vollen Zugriff auf AWS Transform-Agenten von der Kiro IDE aus.

Um das zu installieren AWS Transformieren Sie Kiro Power

1. Öffnen Sie die Kiro IDE und navigieren Sie zum Powers-Bedienfeld.
2. Suchen Sie AWS Transform in der Liste und installieren Sie es.
3. Öffnen Sie Kiro Chat, klicken Sie auf Power und wählen Sie Try Power.

Wählen Sie alternativ im Bedienfeld „Befugnisse“ die Option „Benutzerdefiniertes Potenzial hinzufügen“ > „Strom importieren“ GitHub und fügen Sie Folgendes ein: <https://github.com/kirodotdev/powers/tree/main/aws-transform>

Agenten-Plugin

Das AWS Transform Agent-Plugin ist unter [awslabs/agent-plugins](#) on GitHub im `plugins/aws-transform` Verzeichnis verfügbar. Das Plugin unterstützt Claude Code, Codex und Cursor.

Das Plugin beinhaltet `.claude-plugin.codex-plugin`, und `.mcp.json` Konfigurationen. Es bietet Zugriff auf alle AWS Transform-Agenten, wie.NET, Mainframe, VMware, SQL Server und benutzerdefinierte Transformationen.

Zur Installation in Claude Code

Führen Sie die folgenden Befehle aus:

```
/plugin marketplace add awslabs/agent-plugins  
/plugin install aws-transform@agent-plugins-for-aws
```

Zur Installation in Codex oder Cursor

Folgen Sie den Anweisungen in der README-Datei des Agent-Plugins-Repositorys.

IDE-Plugin

Das AWS Transform IDE-Plugin ist in VS Code- und Open VSX-kompatiblen Editoren verfügbar. Es stellt benutzerdefinierte AWS Transform-Funktionen zur Verfügung, einschließlich der Erstellung und Ausführung von Transformationsdefinitionen. Es stellt auch Mainframe-Funktionen zur Verfügung, darunter die Rückverfolgbarkeit zwischen Modernisierungsanforderungen, Geschäftsregeln und Quellcode sowie die Möglichkeit, technische Dokumentation auf Abruf zu erstellen. Verwenden Sie zunächst eine der folgenden Methoden zur Installation:

- VS Code: Installieren Sie vom [VS Code Marketplace](#).
- VSX öffnen: Die Installation erfolgt über die [Open VSX-Registrierung](#).

MCP-Server

Verwenden Sie den MCP-Server, um AWS Transform programmgesteuert in einen beliebigen Client zu integrieren. MCP-compatible Sie können den MCP-Server von PyPI aus als installieren. `awslabs.aws-transform-mcp-server` Es bietet 19 Tools für Workspace-Management, Job-Management, Human-in-the-Loop (HITL) -Aufgaben, Umgang mit Artefakten, Connector-Management, Chat und Ressourcensuche.

Voraussetzungen

- Python 3.10 oder höher

Installation

Claude Code

```
claude mcp add awslabs.aws-transform-mcp-server -- uvx awslabs.aws-transform-mcp-server@latest
```

Kiro

Hinzufügen zu ~/.kiro/settings/mcp.json:

```
{
  "mcpServers": {
    "awslabs.aws-transform-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.aws-transform-mcp-server@latest"]
    }
  }
}
```

Konfigurationsdetails für Ihren spezifischen MCP-Client finden Sie in der README-Datei zu [aws-transform-mcp-server](#) unter. GitHub

Authentifizierung

AWS Transform unterstützt die rollenbasierte Authentifizierung mit SSO (Identity Center)AWS Identity and Access Management und IAM.

SSO (IAM Identity Center)

Bitte Sie Ihren KI-Assistenten, „AWS Transform mit SSO zu konfigurieren“. Der Assistent stellt eine Start-URL bereit und öffnet Ihren Browser zur Anmeldung.

IAM role (IAM-Rolle)

Ihre Umgebung stellt AWS Anmeldeinformationen automatisch bereit. Stellen Sie AWS_PROFILE in Ihrem env MCP-Client-Konfigurationsblock ein, um ein bestimmtes Profil auszuwählen.

Informationen zum Einrichten der Authentifizierung für AWS Transform finden Sie unter [Erste Schritte mit AWS Transformieren](#).

Erstellen Sie benutzerdefinierte Agenten für AWS Transformieren

Das [Agent Builder-Toolkit](#) ermöglicht es AWS Partnern und Kunden, Agenten zu erstellen, die auf ihre spezifischen Modernisierungsanforderungen zugeschnitten sind und innerhalb von AWS Transform funktionieren.

Um das Agent Builder-Toolkit zu installieren

1. Öffnen Sie Kiro IDE und navigieren Sie zum Powers-Panel.
2. Suchen Sie in der Liste nach AWS Transform Agent Toolkit und installieren Sie es.

Wählen Sie alternativ im Bedienfeld „Befugnisse“ die Option „Benutzerdefiniertes Potenzial hinzufügen“ > „Strom importieren aus“ GitHub und fügen Sie Folgendes ein: `https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit`

Mit dem Agent Builder-Toolkit können Kompetenzpartner, ISVs oder Kunden für Migration und Modernisierung Transformationslösungen für spezifische Anwendungsfälle erstellen. Sie können spezialisierte Agenten, Tools, Wissensdatenbanken und Workflows mit den KI-Funktionen von AWS Transform Agentic integrieren.

Lebenszyklus der Agenten

Entwicklung

Verwenden Sie Kiro Power, um den Basisagenten und das SDK zu kombinieren und Ihren eigenen maßgeschneiderten Agenten zu schreiben.

Freigeben

Verteilen Sie Agenten in Teams oder über Partnernetzwerke.

Registrieren

Registrieren Sie Agenten bei AWS Transform, damit sie von anderen Benutzern entdeckt werden können.

Bewertungen der Migration

AWS Mithilfe von Transformationsanalysen können Sie die Kosten, die Durchführbarkeit und den geschäftlichen Nutzen einer Migration Ihrer lokalen Infrastruktur zu bewerten. AWS Assessments bieten automatische Empfehlungen zur richtigen Dimensionierung, Vergleiche mehrerer Szenarien und interaktive Verbesserungen im Chat.

Sie können Migrationsbewertungen verwenden, um:

- Holen Sie sich Kostenvoranschläge für Amazon RDS for SQL Server, Amazon EC2, Amazon EBS, Amazon S3 und Amazon FSx
- Erhalten Sie automatisierte Empfehlungen zur richtigen Dimensionierung
- Beurteilen Sie den Geschäftswert und die Auswirkungen auf die Nachhaltigkeit
- Vergleichen Sie mehrere Migrationsszenarien nebeneinander
- Verfeinern Sie Ihre Bewertungen interaktiv per Chat
- Generieren Sie Präsentationen für Führungskräfte und detaillierte Berichte

Voraussetzungen

Bevor Sie eine Migrationsbewertung erstellen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein AWS Transform-Workspace
- Inventardaten in einem unterstützten Format, oder Sie können grobe Schätzungen im Chat verwenden
- Entsprechende Berechtigungen zum Erstellen und Ausführen von Bewertungen

Wie funktionieren Migrationsbewertungen

Migrationsbewertungen folgen einem strukturierten Arbeitsablauf, der Sie vom ersten Datenupload bis zur Erstellung der endgültigen Ergebnisse führt.

Um eine Migrationsbewertung abzuschließen

1. Erstellen Sie in Ihrem AWS Transform-Arbeitsbereich einen Job zur Migrationsbewertung.
2. Laden Sie Ihre Inventardaten vor Ort hoch.

3. Überprüfen Sie die Ermittlungsergebnisse, die AWS Transform aus Ihren Daten generiert.
4. Verwalten Sie den Inventarbereich, indem Sie Server ausschließen oder Gruppierungen anpassen.
5. Konfigurieren Sie Ihr Bewertungsszenario anhand von Preis- und Infrastrukturannahmen.
6. Führen Sie die Bewertung durch.
7. Überprüfen und verfeinern Sie die Ergebnisse im Chat.

Nachdem Sie die Ergebnisse überprüft haben, können Sie weitere Szenarien erstellen, Szenarien vergleichen und Ergebnisse wie Präsentationen und Berichte erstellen.

Inventardaten hochladen

AWS Transform akzeptiert Inventardaten aus mehreren Quellen. In der folgenden Tabelle sind die unterstützten Datenformate aufgeführt.

Datenquelle	Description
AWS Export des Transform Discovery Tools	Automatisiertes Serverinventar, das vom AWS Transform Discovery Tool erkannt wurde
RVTools	Exportiert aus VMware-Umgebungen im ZIP/CSV oder Excel-Format. Sowohl vollständige Exporte als auch Info-only V-Exporte werden unterstützt.
CMDB-Daten	Datenbankexporte für das Konfigurationsmanagement
Tools zur Partnersuche	Daten aus AWS Partner-Discovery-Tools
Evaluator für Migration	Quick Insights-Datei aus der Migration Evaluator-Konsole
MPA-Format	Importdatei für die Bewertung des Migrationsportfolios
AWS Datenvorlage transformieren	Microsoft Excel-Datei, die aus der Vorlage „Assessment Data AWS transformieren“ erstellt wurde

AWS Transform identifiziert das Dateiformat bei der Aufnahme automatisch. Der Aufnahmeprozess validiert Ihre Daten, akzeptiert unvollständige Daten, wenn einige Felder fehlen, und unterstützt

inkrementelle Uploads. Sie können jederzeit zusätzliche Dateien hochladen, um Ihr Inventar zu ergänzen.

Überprüfung der Discovery-Ergebnisse

Nachdem AWS Transform Ihre Inventardaten verarbeitet hat, generiert es eine Zusammenfassung der Ergebnisse. Die Übersichtstabelle enthält die folgenden Informationen:

- Anzahl der Server nach Betriebssystem
- Ausfall physischer und virtueller Server
- Erkennung von SQL Server
- Speicherzusammenfassungen
- Warnungen zur Datenqualität

Überprüfen Sie die Ermittlungsergebnisse, um sicherzustellen, dass AWS Transform Ihre Infrastruktur korrekt identifiziert hat, bevor Sie mit der Bewertung fortfahren.

Verwaltung des Inventarumfangs

Nachdem Sie die Ermittlungsergebnisse überprüft haben, können Sie den Umfang Ihrer Bewertung verfeinern. Verwenden Sie die folgenden Aktionen, um Ihren Inventarumfang zu verwalten:

- Fragen Sie das Inventar für bestimmte Server oder Workloads ab
- Schließen Sie Server aus dem Bewertungsbereich aus
- Überprüfen Sie Servergruppierungen und Anwendungsabhängigkeiten
- Identifizieren Sie SQL Server-Workloads für eine spezielle Bewertung

Konfiguration von Bewertungsszenarien

Bevor Sie eine Bewertung durchführen, konfigurieren Sie die Annahmen, anhand derer AWS Transform Empfehlungen generiert. Sie können diese Annahmen jederzeit ändern und neue Szenarien mit unterschiedlichen Konfigurationen ausführen.

In der folgenden Tabelle sind die verfügbaren Annahmenkategorien aufgeführt.

Annahme	Description
Preismodell	Datenbanksparpläne (für Amazon RDS for SQL Server) oder Reserved Instances On-Demand
Ziel AWS-Region	Der AWS-Region Ort, an dem Sie migrierte Workloads hosten möchten
Ausschlüsse vom Instanztyp	Amazon EC2 EC2-Instance-Familien oder -Typen, die von den Empfehlungen ausgeschlossen werden sollen
Amazon EBS-Konfiguration	Volumetyp und Leistungseinstellungen für den Speicher
SQL Server-Lizenzierung	Bring Your Own Media (BYOM) oder Lizenz inklusive (LI) für Amazon RDS for SQL Server; Lizenz enthalten (LI) oder Bring Your Own License (BYOL) für SQL Server auf EC2

Bewertungsmöglichkeiten

AWS Transform Assessments decken mehrere Dimensionen Ihrer Migration ab. In den folgenden Abschnitten werden die einzelnen Bewertungsfunktionen beschrieben.

Amazon EC2 richtig dimensionieren

AWS Transform analysiert Ihre lokalen Serverspezifikationen und empfiehlt Amazon EC2 EC2-Instances in geeigneter Größe. Die Empfehlungen berücksichtigen die CPU-, Speicher- und Leistungsanforderungen.

Amazon EBS-Speicher

AWS Transform empfiehlt Amazon EBS-Volumetypen und -konfigurationen auf der Grundlage Ihrer aktuellen Speichernutzung und Leistungsanforderungen.

Amazon FSx

AWS Transform bewertet Dateispeicher-Workloads und gibt Empfehlungen für die Amazon FSx-Migration, einschließlich Kostenschätzungen für unterstützte Amazon FSx-Dateisystemtypen.

Amazon RDS für SQL Server

AWS Transform bewertet die Kosten für die Migration von lokalen SQL Server-Datenbanken zu Amazon RDS for SQL Server. Mithilfe von AI-powered Agenten analysiert AWS Transform Ihre lokale SQL Server-Umgebung und liefert innerhalb weniger Minuten ein vollständiges Geschäftsszenario für die Migration mit Rechen- und Speicherempfehlungen, die auf Ihre Workload-Anforderungen abgestimmt sind, sodass Sie eine übermäßige Bereitstellung vermeiden und nur für das bezahlen, was Sie benötigen.

Die Bewertung von RDS for SQL Server umfasst die folgenden Funktionen:

- Bring Your Own Media (BYOM) -Lizenzierung, sodass Sie Ihre vorhandenen SQL Server-Lizenzen verwenden können
- Lizenzoptionen im Lieferumfang enthalten (LI)
- Kostenoptimierung mithilfe von Datenbanksparrplänen, die bis zu 20% Einsparungen im Vergleich zur On-Demand Preisgestaltung bieten
- Prüfung der Eignung für das AWS Migration Acceleration Program (MAP), das Kredite und Unterstützung zur Deckung der Migrationskosten bereitstellt

Sie können Ihre Bewertung von RDS for SQL Server mit jedem unterstützten Datenformat beginnen, einschließlich RVTools-Exporten, Configuration Management Database (CMDDB) -Daten, Exporten aus dem AWS Transform Discovery Tool und anderen Discovery-Tools von Drittanbietern. Erstellen Sie Was-wäre-wenn-Szenarien, um mehrere Kostenmodelle mit benutzerdefinierten Annahmen wie Region, Ressourcennutzung und Preisbedingungen zu vergleichen.

Beispiele für Prompts:

- „Schätzen Sie die Kosten für die Migration meiner SQL Server-Datenbanken zu RDS for SQL Server“
- „Vergleichen Sie die Preise für BYOM mit den Preisen inklusive Lizenz für RDS for SQL Server“
- „Zeigt mir die Optionen für Datenbanksparrpläne für meine RDS-Workloads“

Amazon EC2-SQL-Server

AWS Transform bewertet SQL Server-Workloads und gibt Empfehlungen für die Ausführung von SQL Server auf Amazon EC2, einschließlich Lizenzanalysen und dedizierter Hostzuordnungen.

On-premises Preisgestaltung

AWS Transform schätzt Ihre aktuellen lokalen Kosten, um eine Grundlage für den Vergleich mit der AWS Preisgestaltung zu erhalten. Sie können die Gesamtkosten im Chat anpassen. On-premises Kostenanpassungen spiegeln sich im PDF-Bericht und in den Chat-Antworten wider, nicht jedoch im PPTX-Export.

Beispiele für Prompts:

- „Aktualisieren Sie die Kosten für lokale Server auf 500 USD pro Server und Monat“
- „Fügen Sie die jährlichen Kosten für Rechenzentrumseinrichtungen in Höhe von 50.000 USD hinzu“

Nachhaltigkeit

AWS Transform schätzt die Reduzierung des CO2-Fußabdrucks, die sich aus der Migration zu ergibt. AWS Sie können sich im Chat über Nachhaltigkeitskennzahlen informieren.

Versuche es mit Eingabeaufforderungen wie:

- „Zeigen Sie mir die geschätzte CO2-Reduzierung durch diese Migration“
- „Wie sieht die Verbesserung der Energieeffizienz für meine Workloads aus AWS?“

Bewertung des Geschäftswerts

AWS Transform bewertet den größeren geschäftlichen Nutzen der Migration, der über die Einsparungen bei den Infrastrukturkosten hinausgeht. Die Bewertung umfasst die Produktivität, Belastbarkeit und geschäftliche Flexibilität der Mitarbeiter.

Hier sind einige Beispielaufforderungen:

- „Schätzen Sie die Produktivitätssteigerungen Ihrer Mitarbeiter ab, die sich aus der Migration zu ergeben haben AWS“
- „Mit welchen Verbesserungen der Resilienz kann ich nach der Migration rechnen?“
- „Zeigen Sie mir die Vorteile dieser Migration für die geschäftliche Flexibilität“

Netzwerkkosten

AWS Transform schätzt die netzwerkbezogenen Kosten für Ihre Migration, einschließlich der Anforderungen an Datenübertragung und Konnektivität.

Kosten für den Support

AWS Transform berücksichtigt die Kosten für den AWS Supportplan in der Bewertung auf der Grundlage der von Ihnen ausgewählten Support-Stufe.

Endbenutzer-Datenverarbeitung

AWS Transform bewertet die Rechenlasten der Endbenutzer und gibt Empfehlungen für Computerdienste für AWS Endbenutzer.

Mithilfe von Chat-basierten Bewertungen

Sie können über den Chat mit AWS Transform interagieren, um Bewertungen zu erstellen und zu verfeinern. Chat unterstützt drei Interaktionsmodi.

Sie können Ihre Bewertung iterativ verfeinern, indem Sie das Gespräch fortsetzen. AWS Transform behält den Kontext zwischen den Nachrichten bei und aktualisiert die Bewertungsergebnisse auf der Grundlage Ihrer Eingaben.

Grobe Schätzung mit begrenzten Daten

Sie können eine grobe Kostenschätzung erhalten, indem Sie Ihre Umgebung im Chat beschreiben, ohne detaillierte Inventardateien hochzuladen. Die grobe Schätzung ist eine eigenständige Funktion und kann nicht mit hochgeladenen Inventardaten oder einer Datenanreicherung im Chat kombiniert werden.

Sie können Eingabeaufforderungen wie diese verwenden:

- „Ich habe 200 Windows-Server und 150 Linux-Server, schätze meine AWS Kosten“
- „Geben Sie mir eine grobe Schätzung für die Migration von 500 VMs auf“ AWS
- „Schätzen Sie die Kosten für 50 Server mit durchschnittlich 8 CPUs und 32 GB RAM“

Inventar per Chat hinzufügen

Sie können Inventardetails direkt im Chat angeben, um hochgeladene Dateien zu ergänzen oder zu ersetzen.

Verwenden Sie Eingabeaufforderungen wie die folgenden:

- „Schließen Sie einen Datenbankserver ein, auf dem Oracle auf 4 CPUs mit 128 GB RAM läuft“
- „Fügen Sie 20 Webserver hinzu, auf denen Linux mit 4 CPUs und 16 GB RAM ausgeführt wird“

Kosten ändern und Dienste hinzufügen

Über den Chat können Sie die Kosten vor Ort anpassen und AWS Services zu Ihrer Bewertung hinzufügen.

Beispiel für Eingabeaufforderungen für Anpassungen vor Ort:

- „Erhöhen Sie die lokalen Kosten um 15%, um der bevorstehenden Hardwareaktualisierung Rechnung zu tragen“
- „Fügen Sie die jährlichen Wartungskosten in Höhe von 100.000\$ zu den Basiskosten vor Ort hinzu“

Sie können auch grobe Kostenschätzungen für AWS Services hinzufügen, die von AWS Transform Assessments nicht vollständig unterstützt werden. Dies ermöglicht eine vollständigere Analyse, aber diese Schätzungen sind weniger genau als die automatisierten Empfehlungen.

- „AWS Backup-Kosten für alle migrierten Server hinzufügen“
- „Schließen Sie die CloudWatch Amazon-Überwachungskosten in die Schätzung ein“
- „Fügen Sie AWS Direct Connect-Kosten für eine 10-Gbit/s-Verbindung hinzu“

Szenarien vergleichen

Sie können mehrere Bewertungsszenarien mit unterschiedlichen Annahmen erstellen und diese vergleichen, um die optimale Migrationsstrategie zu ermitteln.

Szenarien erstellen

Probieren Sie Eingabeaufforderungen wie:

- „Erstellen Sie ein BYOM-Szenario für die Migration von SQL Server-Datenbanken zu RDS for SQL Server“
- „Erstellen Sie ein Szenario mit Datenbankparplänen für RDS für SQL Server“
- „Erstellen Sie ein LI-Szenario für alle SQL Server-Workloads auf EC2“
- „Erstellen Sie ein Szenario mit allen Workloads in US-West-2“

Vergleiche werden ausgeführt

Hier sind einige Beispielaufforderungen:

- „Zeig mir einen Kostenvergleich für alle Szenarien“
- „Welches Szenario hat die niedrigsten Gesamtbetriebskosten?“

What-if Analyse

Modellieren Sie die Auswirkungen bestimmter Änderungen, ohne ein völlig neues Szenario zu erstellen.

Beispiele für Prompts:

- „Was passiert, wenn ich meine SQL Server-Workloads auf RDS for SQL Server statt auf EC2 verschiebe?“
- „Was ist der Kostenunterschied zwischen BYOM und License Included for RDS for SQL Server?“
- „Was passiert, wenn ich die 50 kleinsten Server von der Migration ausschließe?“
- „Was ist, wenn ich nur speicheroptimierte Instances verwende?“
- „Welche Auswirkungen hat die Umstellung von GP3- auf IO2-Volumes?“

Generierung von Ergebnissen

Nachdem Sie Ihre Bewertung abgeschlossen haben, können Sie Ergebnisse in verschiedenen Formaten generieren. In der folgenden Tabelle werden die verfügbaren Ausgabeformate beschrieben.

Format	Description	Anpassung
PPTX () PowerPoint	Präsentation für Führungskräfte mit zusammenfassenden Ergebnissen und Empfehlungen	Feste Struktur
XLSX (Excel)	Detaillierter Datenexport mit Empfehlungen auf Serverebene und Kostenaufschlüsselungen	Feste Struktur
PDF	Dokument melden	Per Chat anpassbar

Verwandte Themen

- [Erste Schritte](#)
- [Maßgeschneiderte Jobs](#)
- [Tool zur Entdeckung](#)

Benutzerdefiniert

Was ist AWS Benutzerdefiniert transformieren?

AWS Transform Custom verwendet agentische KI, um Software, Code, Bibliotheken und Frameworks umfassend zu modernisieren und so die technische Verschuldung zu reduzieren. Es behandelt verschiedene Szenarien, darunter Upgrades von Sprachversionen, API- und Servicemigrationen, Framework-Upgrades und -Migrationen, Code-Refactoring und organisationsspezifische Transformationen.

Durch kontinuierliches Lernen verbessert sich der Agent anhand jeder Ausführung und des Feedbacks der Entwickler und liefert qualitativ hochwertige, wiederholbare Transformationen, ohne dass spezielle Automatisierungskenntnisse erforderlich sind.

Die wichtigsten Funktionen

AWS Transform custom bietet die folgenden Funktionen:

- Definition einer auf natürlicher Sprache basierenden Transformation — Erstellen Sie benutzerdefinierte Transformationen mithilfe natürlicher Sprache, Dokumentation und Codebeispielen
- Ausführung der Transformation — Wenden Sie Transformationen konsistent und zuverlässig auf mehrere Codebasen an
- Kontinuierliches Lernen — Verbessern Sie automatisch die Transformationsqualität bei jeder Ausführung
- AWS-verwaltete Transformationen — Verwenden Sie gebrauchsfertige, AWS geprüfte Transformationen für gängige Szenarien

Transformationsmuster

AWS Transform Custom unterstützt verschiedene Transformationsmuster, um Ihren Modernisierungsanforderungen gerecht zu werden. Jedes Muster weist je nach Umfang und Art der erforderlichen Änderungen unterschiedliche Komplexitätsmerkmale auf.

Muster	Description	Komplexität	Beispiele
API- und Servicemigrationen	Migration zwischen API-Versionen oder gleichwertigen Diensten unter Beibehaltung der Funktionalität	Mittel	AWS SDK v1→v2 (Java, Python, JavaScript), Boto2→Boto3, JUnit 4→5, Javax→Jakarta
Aktualisierungen der Sprachversionen	Aktualisierung auf neuere Versionen derselben Programmiersprache, Einführung neuer Funktionen und Ersatz veralteter Funktionen	Low-Medium	Java 8→17, Python 3.9→3.13, 12→22, Versionsupgrades Node.js TypeScript
Framework-Aktualisierungen	Aktualisierung auf neuere Versionen desselben Frameworks, Behebung grundlegender Änderungen	Mittel	Spring Boot 2.x→3.x, React 17→18, Angular-Upgrades, Django-Upgrades
Framework-Migrationen	Migration zu völlig anderen Frameworks, die ähnlichen Zwecken dienen	Hoch	Angular→React, Redux→Zustand, →React Vue.js
Upgrades für Bibliotheken und Abhängigkeiten	Aktualisierung von Bibliotheken von Drittanbietern auf neuere Versionen unter Beibehaltung derselben Sprache und desselben Frameworks	Low-Medium	Pandas 1.x→2.x, NumPy Upgrades, Bibliotheks-Upgrades, Hadoop/HBase/Hive, Lodash-Upgrades

Muster	Description	Komplexität	Beispiele
Code-Refactoring und Modernisierung	Modernisierung von Codemustern und Übernahme von Best Practices, ohne die externe Funktionalität zu ändern	Low-Medium	Drucken→Logging-Frameworks, Verkettung von Zeichenketten→F-Strings, Übernahme von Typhinweisen, Instrumentierung der Beobachtbarkeit
File-by-File Drehbuch und Übersetzungen	Übersetzung unabhängiger Skripte oder Konfigurationsdateien, bei denen die Dateien größtenteils eigenständig sind	Low-Medium	AWS cdk→Terraform, Terraform→, Excel→Python-Notizbücher, CloudFormation Bash→ PowerShell
Architektur-Migrationen	Migration zwischen Hardwarearchitekturen oder Laufzeitumgebungen mit minimalen Codeänderungen	Medium-High	x86 →AWS Graviton (ARM), lokal → Lambda, herkömmlicher Server → Container
Language-to-Language Migrationen	Übersetzung von Codebasen von einer Programmiersprache in eine andere	Sehr hoch	Java→Python, JavaScript →, C→Rust, TypeScript Python→Go

Muster	Description	Komplexität	Beispiele
Benutzerdefiniert Organization-Specific und Transformationen	Einzigartige organisatorische Anforderungen und spezielle Modernisierungsbedürfnisse	Variiert	Benutzerdefinierte interne Bibliotheksmigrationen, unternehmensspezifische Codierungsstandards, Migrationen proprietärer Frameworks

Note

Verwenden Sie für COBOL/mainframe Sprachen Transform for Mainframe. AWS Für Upgrades von .NET Framework auf .NET Core sollten Sie AWS Transform for Windows in Betracht ziehen. Für VMware-Migrationen zu AWS sollten Sie AWS Transform for VMware in Betracht ziehen.

Wie AWS Transformieren Sie benutzerdefinierte Werke

AWS Transform custom wird normalerweise in großen Projekten verwendet, bei denen mehrere Codebasen oder Module transformiert werden. Teams folgen in der Regel einem vierphasigen Arbeitsablauf:

Transformation definieren — Stellen Sie dem Agenten Eingabeaufforderungen, Dokumentation und Codebeispiele in natürlicher Sprache zur Verfügung, der daraufhin eine erste Transformationsdefinition generiert. Diese Definition kann iterativ durch Chat oder direkte Bearbeitung verfeinert werden. Diese Phase kann übersprungen werden, wenn Sie -verwaltete Transformationen verwenden AWS.

Pilotprojekt oder Proof-of-Concept — Testen Sie die Transformation anhand von Beispielcodebasen und verfeinern Sie sie anhand der Ergebnisse. Diese Validierungsphase hilft dabei, die Kosten und den Aufwand der vollständigen Transformation abzuschätzen. Kontinuierliches Lernen verbessert die Qualität in dieser Phase.

Skalierte Ausführung — Richten Sie mithilfe der CLI eine automatisierte Massenausführung ein, bei der Entwickler die Ergebnisse überprüfen und validieren. Überwachen Sie den Fortschritt mithilfe der Webanwendung und verfolgen Sie Transformationen in mehreren Repositorys.

Überwachung und Überprüfung — Kontinuierliches Lernen verbessert automatisch die Qualität der Transformation. Überprüfen Sie die Erkenntnisse, die aus früheren Durchläufen extrahiert wurden, um sicherzustellen, dass sie den Qualitätsstandards entsprechen, und archivieren Sie alle, die nicht nützlich sind.

Wichtige -Konzepte verstehen

In diesem Abschnitt werden die wichtigsten Konzepte für die Arbeit mit AWS Transform custom erklärt.

Transformationsdefinitionen

Eine Transformationsdefinition enthält die Anweisungen und das Wissen, die für die Durchführung einer bestimmten Codetransformation erforderlich sind. Sie wird als Fähigkeit dargestellt und besteht aus:

- `SKILL.md`(erforderlich) — Anweisungen in Markdown mit YAML-Front-Matter (name und description -Feldern), die die Kerntransformationslogik und die Ausführungsanweisungen enthalten
- `references/`Ordner (optional) — Dokumentation, die bei Bedarf während der Transformationsausführung geladen wurde
- `scripts/`Ordner (optional) — Skripten, die die Transformation während der Ausführung herunterlädt und ausführt

AWS Transform CLI lädt Transformationsdefinitionen automatisch in das aktuelle Verzeichnis herunter, wenn sie zur Ausführung, Überprüfung oder Änderung benötigt werden.

Important

Beim Veröffentlichen einer Transformation darf das Verzeichnis nur `SKILL.md` und optional den `references/` Ordner, den `scripts/` Ordner oder beides enthalten. Andere Dateien oder Unterverzeichnisse sind nicht zulässig.

 Note

CLI Version 2.0 und höher verwendet das Skills-Format. Bestehende Transformationsdefinitionen werden automatisch von der CLI verarbeitet.

Transformationsregister

Das Transformationsregister ist das zentrale Repository Ihres AWS Kontos zum Speichern und Verwalten von Transformationsdefinitionen. Folgende Transformationen können in der Registrierung vorgenommen werden:

- Gelistet unter `atx custom def list`
- Wird in mehreren Codebasen ausgeführt
- Mit anderen Benutzern in Ihrem Konto geteilt AWS
- Version-controlled

 Important

Transformationsdefinitionen sind kontospezifisch. Wenn Sie eine Transformation in einem anderen AWS Konto verwenden möchten, müssen Sie sie separat in diesem Konto veröffentlichen.

Entwurf und veröffentlichte Transformationen

AWS Transform Custom unterstützt zwei Status für Transformationen in der Registrierung:

Bei Transformationsentwürfen handelt es sich um in Bearbeitung befindliche oder noch nicht getestete Transformationsdefinitionen. Sie werden als spezifische Versionen gespeichert und können von Benutzern abgerufen, aktualisiert und ausgeführt werden, die auf diese bestimmte Version verweisen. Entwürfe eignen sich für iteratives Entwickeln, Testen und Verfeinern, bevor die Transformation bereit ist, mit Ihrem Team geteilt zu werden. Entwürfe sind auch bestimmten Konversationen zugeordnet. Wenn Sie die CLI neu starten, können Sie `atx --conversation-id {id}` verwenden, um eine vorherige wiederherzustellen.

Veröffentlichte Transformationen stehen in der Transformationsregistrierung Ihres Kontos zur Ausführung durch andere Benutzer mit den erforderlichen IAM-Berechtigungen zur Verfügung. Veröffentlichte Transformationen können mithilfe von gefunden werden. `atx custom def list`

Der typische Arbeitsablauf ist:

1. Transformation lokal erstellen
2. Als Entwurf zum Testen speichern (`atx custom def save-draft`)
3. Verfeinern und validieren
4. Veröffentlichen Sie, um es mit Ihrem Team zu teilen (`atx custom def publish`)

Sie können eine Transformation auch direkt veröffentlichen, ohne sie als Entwurf zu speichern.

Referenzen im Vergleich zu Lektionen

AWS Transform custom verwendet zwei Arten von Wissen, um die Qualität der Transformation zu verbessern:

Referenzen sind vom Benutzer bereitgestellte Dokumentation, die im `references/` Ordner einer Transformationsdefinition gespeichert wird. Verweise unterstützen nur Textdateien (insgesamt maximal 10 MB für alle Dateien) und enthalten in der Regel Dokumentation, API-Spezifikationen, Migrationshandbücher und Codebeispiele. Verweise werden bei der Ausführung der Transformation nach Bedarf geladen. Sie fügen Verweise hinzu, wenn Sie eine Transformationsdefinition im interaktiven Modus erstellen oder aktualisieren.

Lektionen werden automatisch aus früheren Durchläufen einer Transformation extrahiert. Das System für kontinuierliches Lernen generiert sie anhand von Ausführungsverläufen, Feedback von Entwicklern und Codekorrekturen, auf die es bei Transformationen stößt. Es gruppiert verwandte Lektionen in Kategorien, sodass Sie sie gemeinsam überprüfen können. Im Gegensatz zu Referenzen, die Sie im Voraus angeben, sammeln sich die Lektionen im Laufe der Zeit an, wenn Sie die Transformation über verschiedene Codebasen hinweg ausführen, und das System wendet sie automatisch an, um future Läufe zu verbessern. Sie überprüfen und verwalten Lektionen interaktiv mit `atx custom def learnings`

Befehle zum Erstellen und Überprüfen

Der Build- oder Validierungsbefehl ist ein optionaler Parameter, der angibt, wie Ihr Code während des Transformationsprozesses validiert werden soll. Dieser Befehl wird an verschiedenen Stellen während der Transformation ausgeführt, um die Codeintegrität sicherzustellen.

Die Bereitstellung eines Befehls, der die Ergebnisse validiert und Probleme zurückgibt, wenn die Validierung fehlschlägt, ist sehr wichtig, um die Transformationsqualität durch kontinuierliches Lernen zu verbessern. Wenn kein Build oder keine Validierung erforderlich ist, lassen Sie dies in Ihrer Eingabe weg.

Beispiele und ausführliche Anleitungen finden Sie unter Befehle zum Erstellen und Überprüfen im Abschnitt Workflows.

Kontinuierliches Lernen

Kontinuierliches Lernen ist ein System, das automatisch Feedback aus jeder Transformationsausführung erfasst und die Transformationsqualität im Laufe der Zeit verbessert. Das System sammelt Informationen durch:

- Explizites Feedback — Kommentare und Codekorrekturen werden im interaktiven Modus bereitgestellt
- Implizite Beobachtungen — Probleme, auf die der Agent beim Transformieren und Debuggen von Code stößt

Das System des kontinuierlichen Lernens verarbeitet diese Informationen, um Lektionen zu erstellen, die es der Transformationsdefinition hinzufügt, um future Transformationen zu verbessern. Das System führt den Lernprozess nach Abschluss der Transformationen automatisch durch, sodass keine zusätzlichen Eingaben von Ihnen erforderlich sind.

Important

Die Lektionen sind transformationsspezifisch und werden nicht von verschiedenen Transformationen oder Kundenkonten gemeinsam genutzt.

Lektionen verwalten

Das System generiert automatisch Lektionen, aber Sie behalten die Kontrolle darüber, welche Lektionen es für future Läufe verwendet. `atx custom def learnings` Mit dem Befehl wird eine interaktive Terminalsitzung geöffnet, in der die Lektionen, die sich im Zuge einer Transformation angesammelt haben, überprüft und kuratiert werden können.

In dieser Sitzung können Sie:

- Durchsuchen Sie Lektionen, die in Kategorien gruppiert sind, und sehen Sie, wie viele aktive Lektionen jede Kategorie enthält.
- Öffnen Sie eine Lektion, um alle Einzelheiten zu lesen, einschließlich des Hauptteils der Lektion, ihrer Auswirkungen und der Anzahl früherer Läufe, in denen sie konsultiert wurde.
- Archivieren Sie eine Lektion, um zu verhindern, dass das System sie bei future Läufen anwendet, und stellen Sie sie bei Bedarf später wieder her.
- Löschen Sie eine archivierte Lektion, die nicht mehr nützlich ist, dauerhaft.

Schrittweise Anleitungen hierzu finden Sie unter [the section called “Kontinuierliches Lernen”](#).

Client-Side Fähigkeiten

Client-side Fähigkeiten sind zusätzliche Fähigkeiten, die den Agenten bei Transformationsausführungen erweitern. Im Gegensatz zu Transformationsdefinitionen, die definieren, welche Transformation durchgeführt werden soll, bieten Fähigkeiten auf Kundenseite zusätzliche Tools, Skripte und Anweisungen, die der Agent bei jeder Transformation zusätzlich zu seinen integrierten Funktionen verwenden kann.

Client-side Fähigkeiten werden anhand von Verzeichnissen auf Projekt- und Benutzerebene ermittelt. Platzieren Sie Fähigkeiten auf Projektebene, wenn sie für ein Repository spezifische Standards durchsetzen, und auf Benutzerebene, wenn sie für all Ihre Projekte gelten. Project-level Fähigkeiten sind nur verfügbar, wenn ein Code-Repository-Pfad angegeben wird. Eine ausführliche Konfiguration und Verwendung finden Sie unter [the section called “Client-Side Fähigkeiten”](#).

Erste Schritte

In diesem Abschnitt wird beschrieben, wie Sie AWS Transform custom einrichten und Ihre erste Transformation ausführen.

Voraussetzungen

Stellen Sie vor der Installation von AWS Transform custom sicher, dass Sie über Folgendes verfügen:

Unterstützte Plattformen

AWS Transform custom unterstützt die folgenden Betriebssysteme:

- Linux — Vollständige Unterstützung für alle Linux-Distributionen
- macOS — Vollständige Unterstützung für macOS-Systeme
- Windows — Vollständige Unterstützung für systemeigenes Windows mit Windows Terminal und PowerShell (Die `atx ct` Befehle werden unter Windows noch nicht unterstützt)
- Windows-Subsystem für Linux (WSL) — Wird unterstützt, wenn es unter WSL ausgeführt wird

Erforderliche Software

- Node.js 22 oder höher — Herunterladen von <https://nodejs.org/en/download>
- Git — Muss installiert sein und das Arbeitsverzeichnis muss ein gültiges Git-Repo sein, um eine Transformation ausführen zu können. Führen Sie `git init`; `git add .`; `git commit -m "Initial commit"`, um ein Git-Repo in Ihrem Arbeitsverzeichnis zu initialisieren.

Netzwerkanforderungen

Eine Internetverbindung mit Zugriff auf die folgenden Endpunkte ist erforderlich:

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

Wenn Sie in einer Umgebung mit eingeschränktem Internetzugriff arbeiten, aktualisieren Sie die Firewallregeln, um diese URLs auf die Zulassungsliste zu setzen.

Installieren von AWS CLI transformieren

Die empfohlene Installationsmethode ist die Verwendung des Installationsskripts. Wählen Sie die Registerkarte für Ihr Betriebssystem.

So installieren Sie die AWS Transform CLI

1. Führen Sie das Installationsskript aus:

Linux and macOS

```
curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
```

Windows (PowerShell)

Führen Sie unter systemeigenem Windows das Installationsskript vom Windows Terminal aus mit PowerShell.

```
irm https://transform-cli.awsstatic.com/install.ps1 | iex
```

2. Überprüfen Sie die Installation:

```
atx --version
```

Der Befehl sollte die installierte Version der AWS Transform CLI anzeigen.

Konfigurieren der Authentifizierung

AWS Für die benutzerdefinierte Transformation sind AWS Anmeldeinformationen erforderlich, um sich beim Dienst zu authentifizieren. Konfigurieren Sie die Authentifizierung mit einer der folgenden Methoden.

Umgebungsvariablen

Legen Sie die folgenden Umgebungsvariablen fest.

Linux and macOS

```
export AWS_ACCESS_KEY_ID=your_access_key  
export AWS_SECRET_ACCESS_KEY=your_secret_key  
export AWS_SESSION_TOKEN=your_session_token
```

Windows (PowerShell)

```
$env:AWS_ACCESS_KEY_ID="your_access_key"
```



```
$env:AWS_SECRET_ACCESS_KEY="your_secret_key"  
$env:AWS_SESSION_TOKEN="your_session_token"
```

Sie können ein Profil auch mithilfe der `AWS_PROFILE` Umgebungsvariablen angeben.

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
$env:AWS_PROFILE="your_profile_name"
```

Note

Umgebungsvariablen, die mit `$env:` in gesetzt sind, PowerShell gelten nur für die aktuelle Sitzung. Um sie sitzungsübergreifend beizubehalten, legen Sie sie über Systemeigenschaften > Umgebungsvariablen fest oder verwenden `[System.Environment]::SetEnvironmentVariable()`.

AWS Datei mit den Anmeldeinformationen

Konfigurieren Sie die Anmeldeinformationen in der AWS Anmeldeinformationsdatei, die sich `~/.aws/credentials` unter Linux und macOS oder `%USERPROFILE%\.aws\credentials` unter Windows befindet:

```
[default]  
aws_access_key_id = your_access_key  
aws_secret_access_key = your_secret_key
```

IAM-Berechtigungen

Ihre AWS Anmeldeinformationen müssen über Berechtigungen zum Aufrufen des benutzerdefinierten AWS Transform-Dienstes verfügen. Wir empfehlen, die [AWSTransformCustomFullAccess](#) AWS verwaltete Richtlinie Ihrem IAM-Benutzer oder Ihrer IAM-Rolle zuzuordnen. Diese Richtlinie gewährt

vollen Zugriff auf AWS Transform custom, einschließlich der Erlaubnis, die [serviceverknüpfte Rolle](#) zu erstellen, die für die Übertragung von CloudWatch Metriken an Ihr Konto erforderlich ist.

Für eine detailliertere Kontrolle bietet AWS Transform custom auch die folgenden AWS verwalteten Richtlinien:

- [AWSTransformCustomExecuteTransformations](#)— Ermöglicht den Zugriff auf die Ausführung von Transformationen.
- [AWSTransformCustomManageTransformations](#)— Ermöglicht den Zugriff auf das Erstellen, Aktualisieren, Lesen und Löschen von Transformationsressourcen sowie das Ausführen von Transformationen.

Weitere Informationen zu diesen Richtlinien finden Sie unter [AWS Verwaltete Richtlinien für AWS Transform](#). Benutzerdefinierte IAM-Richtlinien mit Berechtigungen auf Ressourcenebene finden Sie im Referenzhandbuch zur [AWS Transform Custom IAM Service](#) Authorization.

Note

- Transformationsdefinitionen sind AWS Ressourcen mit ARNs (Amazon Resource Names). Sie können IAM-Richtlinien verwenden, um den Zugriff auf bestimmte Transformationen oder Gruppen von Transformationen zu steuern, indem Sie den Transformations-ARN in Ihren IAM-Richtlinienressourcenanweisungen angeben. Tags können für die gruppierte Zugriffskontrolle verwendet werden.
- AWS IAM Identity Center ist für den Zugriff auf die AWS Transformation erforderlich, für die Verwendung der CLI jedoch nicht.

Konfigurieren AWS Region

AWS Transform Custom ist in bestimmten AWS Regionen verfügbar und erkennt Ihre Regionskonfiguration automatisch unter Verwendung der AWS Standard-CLI-Priorität.

Unterstützte Regionen

AWS Transform Custom ist in den folgenden AWS Regionen verfügbar:

- `us-east-1`(USA Ost — Nord-Virginia)
- `eu-central-1`(Europa — Frankfurt)

- eu-west-2(Europa - London)
- ca-central-1(Kanada — Zentral)
- ap-northeast-1(Asien-Pazifik — Tokio)
- ap-northeast-2(Asien-Pazifik — Seoul)
- ap-southeast-2(Asien-Pazifik — Sydney)
- ap-south-1(Asien-Pazifik — Mumbai)

Wie wird die Region bestimmt

Die CLI überprüft diese Quellen in der Reihenfolge ihrer Priorität, um zu bestimmen, welche Region verwendet werden soll:

1. AWS_REGION Umgebungsvariable (höchste Priorität)
2. AWS_DEFAULT_REGION Umgebungsvariable
3. Ausgewähltes Profil in der AWS Konfigurationsdatei (über die AWS_PROFILE Umgebungsvariable)
4. Standardprofil in der AWS Konfigurationsdatei
5. Standard-Fallback auf, us-east-1 wenn keine Konfiguration gefunden wurde

Note

Die AWS Konfigurationsdatei befindet sich `~/.aws/config` unter Linux und macOS oder `%USERPROFILE%\aws\config` unter Windows.

Note

Wenn gesetzt, `ATX_CUSTOM_ENDPOINT` wird die Region aus der Endpunkt-URL extrahiert und überschreibt alle anderen Einstellungen.

Deine Region festlegen

Wählen Sie eine der folgenden Methoden, um Ihre Region zu konfigurieren:

Option 1: Umgebungsvariable (für den temporären Gebrauch empfohlen):

Linux and macOS

```
export AWS_REGION=<your-region>
```

Windows (PowerShell)

```
$env:AWS_REGION="<your-region>"
```

Option 2: AWS CLI-Konfiguration (empfohlen für eine permanente Einrichtung):

```
aws configure set region <your-region>
```

Option 3: Profile-specific Konfiguration:

Linux and macOS

```
aws configure set region <your-region> --profile your_profile_name  
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
aws configure set region <your-region> --profile your_profile_name  
$env:AWS_PROFILE="your_profile_name"
```

Option 4: Direkte Dateibearbeitung:

Bearbeiten Sie die AWS Konfigurationsdatei direkt (`~/.aws/config` unter Linux und macOS oder `%USERPROFILE%\\.aws\config` unter Windows):

```
[default]  
region = <your-region>  
  
[profile your_profile_name]  
region = <your-region>
```

Überprüfen Sie Ihre Regionskonfiguration

Um zu überprüfen, welche Region AWS Transform Custom verwenden wird:

Überprüfen Sie die aktuelle Regionseinstellung:

```
aws configure get region
```

Überprüfen Sie die Umgebungsvariablen:

Linux and macOS

```
echo "AWS_REGION: $AWS_REGION"
echo "AWS_DEFAULT_REGION: $AWS_DEFAULT_REGION"
echo "AWS_PROFILE: $AWS_PROFILE"
```

Windows (PowerShell)

```
echo "AWS_REGION: $env:AWS_REGION"
echo "AWS_DEFAULT_REGION: $env:AWS_DEFAULT_REGION"
echo "AWS_PROFILE: $env:AWS_PROFILE"
```

Detaillierte Regionsauflösung in Debug-Protokollen anzeigen:

Linux and macOS

```
tail -f ~/.aws/atx/logs/debug.log
```

Windows (PowerShell)

```
Get-Content "$env:USERPROFILE\.aws\atx\logs\debug.log" -Wait -Tail 10
```

Beispiel für eine Protokollausgabe, die die Quelle der Region zeigt:

```
2026-01-07 22:34:28 [DEBUG]: Initializing FrontendServiceClient with config:
{
  "endpoint": "https://transform-custom.us-east-1.api.aws",
  "region": "us-east-1",
  "regionSource": "AWS_REGION"
}
```

Das `regionSource` Feld zeigt, woher die Region abgeleitet wurde (z. B. „aws-config (profile: default)“, „AWS_REGION“, „default“).

 Important

Wenn Ihre Regionskonfiguration auf eine nicht unterstützte Region verweist, zeigt die CLI eine klare Fehlermeldung mit Anweisungen zur Aktualisierung Ihrer Konfiguration auf eine unterstützte Region an.

Führen Sie Ihre erste Transformation durch

Der schnellste Weg, um loszulegen, ist die Verwendung einer AWS-verwalteten Transformation. AWS-verwaltete Transformationen sind vorgefertigte, AWS geprüfte Transformationen, die ohne jegliche Einrichtung sofort verwendet werden können.

So führen Sie eine -verwaltete Transformation interaktiv aus: AWS

```
atx
```

Bitte Sie dann den Agenten, eine Transformation auszuführen:

```
Execute the AWS/java-aws-sdk-v1-to-v2 transformation on the codebase at ./my-java-project
```

Um eine Transformation nicht interaktiv auszuführen:

```
atx custom def exec -n AWS/java-aws-sdk-v1-to-v2 -p ./my-java-project -c "mvn clean install" -x -t
```

Ausführliche Informationen zu Ausführungsmodi, Konfigurationsoptionen und Befehlsflags finden Sie unter. [the section called "Befehlsreferenz"](#)

Transformationsergebnisse verstehen

Wenn eine Transformation abgeschlossen ist, stellt AWS Transform custom einen Bericht zur Verfügung, in dem die Ergebnisse beschrieben werden. Wenn die Transformation nicht validiert wurde (z. B. erfolgreicher Build für eine Java-Anwendung), enthält der Bericht Empfehlungen für weitere Maßnahmen.

Die meisten Transformationen werden in mehreren Schritten durchgeführt, wobei Git verwendet wird, um Zwischenschritte zu übertragen. Sie können die durch die Transformation vorgenommenen Änderungen mit Standard-Git-Befehlen überprüfen:

```
git status
git log
git diff <original commit-id>
```

Eine benutzerdefinierte Transformation erstellen

Wenn AWS-verwaltete Transformationen Ihren Anforderungen nicht entsprechen, können Sie benutzerdefinierte Transformationen erstellen, die auf Ihre spezifischen Anforderungen zugeschnitten sind.

Um eine benutzerdefinierte Transformation zu erstellen

1. Starten Sie die AWS Transform-CLI im interaktiven Modus:

```
atx
```

2. Teilen Sie dem Agenten mit, dass Sie eine neue Transformation erstellen möchten, und beschreiben Sie Ihre Anforderungen.
3. Stellen Sie Referenzmaterial wie Dokumentation und Codebeispiele bereit, um die Qualität zu verbessern.
4. Testen und verfeinern Sie die Transformation iterativ.
5. Veröffentlichen Sie es im Transformationsregister Ihrer Organisation.

Ausführliche Anweisungen zum Erstellen benutzerdefinierter Transformationen finden Sie unter [the section called “Arbeitsabläufe”](#).

AWS Webanwendung transformieren (optional)

Die AWS Transform-Webanwendung ist eine optionale Schnittstelle für die Überwachung umfangreicher Transformationskampagnen in mehreren Repositorys. Bevor Sie die AWS Transform-Webanwendung verwenden können, müssen Sie eine Benutzeridentität aktiviert haben, um in Ihrer Organisation auf AWS Transform zugreifen zu können. Informationen zur Aktivierung von AWS Transform finden Sie unter [AWS Transform einrichten](#).

So verwenden Sie die AWS Transform-Webanwendung:

1. Besuchen Sie das AWS IAM Identity Center <https://aws.amazon.com/transform/> und melden Sie sich mit Ihren Anmeldeinformationen an.
2. Wählen Sie in der AWS Transform-Webanwendung den Auftragstyp „Benutzerdefiniert /code“ aus.
3. Teilen Sie dem Agenten den Namen der Transformationsdefinition mit, die Sie verwenden möchten.
4. Die Webanwendung bietet einen AWS Transform-CLI-Befehl, der mit Ihrem Team geteilt werden kann. Dieser Befehl ruft die Transformationsdefinition auf und protokolliert die Ausführungsergebnisse in der Webanwendung.
5. Nachdem die Transformationsergebnisse erfasst wurden, können Sie sich im Dashboard Statistiken und Messungen zur Zeitersparnis ansehen und Fragen zum Fortschritt Ihres Jobs stellen.

Die Webanwendung wurde für Unternehmensabläufe konzipiert, bei denen Sie eine zentrale Überwachung der Transformationen über mehrere Codebasen hinweg benötigen.

Note

AWS Für den Zugriff auf die Transform-Webanwendung ist IAM Identity Center erforderlich. AWS Die CLI benötigt kein IAM Identity Center — es werden nur AWS Standardanmeldedaten benötigt.

Einführung in benutzerdefinierte Transformationsbefehle

Hier sind einige der Befehle, die Sie mit benutzerdefinierten Transformationen verwenden können. Die vollständige Liste der Befehle finden Sie in der [Befehlsreferenz für benutzerdefinierte Transformationen AWS transformieren](#).

- `atx custom`
 - Führt eine interaktive Benutzererfahrung für benutzerdefinierte Transformationen aus und ermöglicht die Erstellung, Erkennung, Ausführung und Verfeinerung von Transformationen.
 - Dies ist der Standardbefehl für `atx`
 - `--trust-all-tools(-t)` ist optional und lässt implizit alle vom Agenten angeforderten Werkzeuganforderungen zu. Verwenden Sie es mit Vorsicht, insbesondere in

Produktionsumgebungen. Sie können die Vertrauensstellung von Tools für bestimmte Tools und Befehle mithilfe der [Datei mit den Vertrauenseinstellungen](#) konfigurieren.

- `atx custom --help` | `atx custom -h`
 - Zeigt das Hilfemenü an.
 - Jeder Befehl enthält auch ein Hilfemenü, zum Beispiel `atx custom def exec --help`.
- `atx --version` | `atx -v`
 - Zeigt die Version an.
 - Die Versionsnummer ändert sich mit jeder Version.
- `atx custom def list`
 - Druckt eine Liste der Transformationen aus, die in der Transformationsregistrierung verfügbar sind.
- `atx custom def exec`
 - Führt eine Transformation aus
- `atx custom def learnings`
 - Öffnet eine interaktive Sitzung, in der die Erkenntnisse angezeigt und verwaltet werden können, die eine Transformation aus früheren Durchläufen gezogen hat
- `atx mcp`
 - Wird zur Verwaltung von MCP-Serverkonfigurationen verwendet

Arbeitsabläufe

Transformationen ausführen

In diesem Abschnitt werden die verschiedenen Methoden zur Ausführung von Transformationen und Optionen zur Steuerung des Ausführungsverhaltens beschrieben.

Ausführungsmodi

AWS Transform custom unterstützt drei Ausführungsmodi für unterschiedliche Workflows.

Interaktiver Konversationsmodus

Starten Sie die CLI mit `atx` und bitten Sie den Agenten, eine Transformation in natürlicher Sprache auszuführen. In diesem Modus können Sie eine vollständige Konversation mit dem Agenten führen, die Ausführung jederzeit unterbrechen und während des Transformationsprozesses Feedback geben.

Verwenden Sie diesen Modus, wenn Sie maximale Kontrolle und die Möglichkeit haben möchten, den Agenten durch komplexe Szenarien zu führen.

Direkte interaktive Ausführung

Wird verwendet `atx custom def exec -n <transformation-name> -p <path>`, um eine bestimmte Transformation interaktiv zu starten. In diesem Modus können Sie den Agenten zu Beginn, während oder am Ende der Ausführung überprüfen und mit ihm interagieren. Der Agent wird an wichtigen Entscheidungspunkten eine Pause einlegen und Sie um Ihr Feedback bitten.

Dies ist ideal, um Transformationen zu testen und zu verfeinern, bevor sie autonom ausgeführt werden.

Sie können Transformationen im nicht interaktiven Modus oder im Headless-Modus ausführen. Non-interactive Der Modus unterdrückt Eingabeaufforderungen während einer benannten Transformation. Im Headless-Modus können Sie den Agenten mit einer Klartext-Aufforderung ausführen, wodurch die interaktive Oberfläche vollständig umgangen wird.

Non-interactive Modus

`atx custom def exec -n <transformation-name> -p <path> -x -t` Für die vollständige Automatisierung verwenden. Fügen Sie `-x` diese Option hinzu, um sie im nicht interaktiven Modus auszuführen und `-t` alle Tools automatisch und ohne Aufforderung als vertrauenswürdig einzustufen.

Dieser Modus ist für die CI/CD Pipeline-Integration und die Massenausführung konzipiert, wenn kein menschliches Eingreifen möglich oder gewünscht ist.

Kopfloser Modus

Um Aufgaben zu erledigen, ohne mit dem Agenten zu interagieren, führen Sie die Anweisungen aus `atx -x "<prompt>" -t` und geben Sie sie im Klartext ein.

Ausführung der Transformation ohne Kopf

Verwenden Sie diesen Modus, um eine bestehende Transformationsdefinition auf Ihre Codebasis anzuwenden. Die Transformation führt jeden Schritt automatisch aus, ohne dass Ihre Zustimmung erforderlich ist.

```
atx -x "apply transformation definition <transformation_definition_name> to  
<codebase_path>" -t
```

Transformationsentwicklung ohne Kopf

Transformationsdefinitionen erstellen oder ändern.

Führen Sie den folgenden Befehl aus, um eine ältere Transformationsdefinition in das neue Skillformat (SKILL.md + References/) zu konvertieren:

```
atx -x "convert <legacy_transformation_definition_name> transformation definition to skill and save as draft" -t
```

Führen Sie den folgenden Befehl aus, um eine neue Transformationsdefinition zu erstellen:

```
atx -x "create a transformation definition to <description> with references docs <reference_docs_path>" -t
```

Allgemeine Befehls-Flags

Bei der Ausführung von Transformationen mit `atx custom def exec` werden häufig die folgenden Flags verwendet:

- `-noder --transformation-name` — Gibt den Namen der auszuführenden Transformation an
- `-poder --code-repository-path` — Gibt den Pfad zu Ihrer Codebasis an (verwenden Sie „.“ für das aktuelle Verzeichnis)
- `-coder --build-command` — Gibt den auszuführenden Build- oder Validierungsbefehl an
- `-xoder --non-interactive` — Aktiviert den nicht interaktiven Modus (keine Benutzeraufforderungen)
- `-toder --trust-all-tools` — vertraut automatisch allen Tools, ohne dass Sie dazu aufgefordert werden
- `-doder --do-not-learn` — Verhindert das Extrahieren von Lektionen aus dieser Ausführung
- `--tvoder --transformation-version` — Gibt eine bestimmte Version der Transformation an
- `-goder --configuration` — Stellt eine Konfigurationsdatei oder eine Inline-Konfiguration bereit

Important

Das `--trust-all-tools` Kennzeichen `-t` oder genehmigt automatisch alle Toolausführungen ohne Aufforderung und umgeht die meisten Sicherheitsvorkehrungen (Befehle, die Ihrer `alwaysPromptCommands` Liste entsprechen, erfordern weiterhin

eine ausdrückliche Genehmigung, sofern sie nicht von überschrieben werden).
`trustedShellCommands` Die Weitergabe `--trust-all-tools` ist für eine vollständig autonome Nutzung erforderlich, für die Ausführung der Transformation jedoch nicht erforderlich. `--non-interactive` In Produktionsumgebungen mit Vorsicht verwenden.

Verwendung von Konfigurationsdateien

AWS Transform custom unterstützt optionale Konfigurationsdateien im YAML- oder JSON-Format. Mit Konfigurationsdateien können Sie Ausführungsparameter angeben und dem Agenten zusätzlichen Kontext zur Verfügung stellen.

Um eine Konfigurationsdatei zu verwenden:

```
atx custom def exec --configuration file://config.yaml
```

Sie können die Konfiguration auch als Inline-Schlüssel-Wert-Paare bereitstellen:

```
atx custom def exec --configuration "key=value,key2=value2"
```

Beispiel für eine Konfigurationsdatei (config.yaml):

```
codeRepositoryPath: ./my-project
transformationName: my-transformation
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Ensure compatibility with our internal logging framework version 2.3.
validationCommands: |
  mvn test
  mvn verify
```

Der `additionalPlanContext` Parameter bietet zusätzlichen Kontext für den Ausführungsplan des Agenten. Dies ist besonders nützlich bei AWS-verwalteten Transformationen, um ihr Verhalten an Ihre spezifischen Bedürfnisse anzupassen.

Befehle zum Erstellen und Überprüfen

Der Build- oder Validierungsbefehl ist ein optionaler Parameter, der angibt, wie Ihr Code während des Transformationsprozesses validiert werden soll. AWS Transform custom versucht, auf der Grundlage

der Transformation den besten Build-Befehl abzuleiten, falls dieser nicht angegeben wurde. Es wird jedoch empfohlen, aus Qualitätsgründen spezifisch zu sein.

Beispiele für Build- und Validierungsbefehle:

- Java: `mvn clean install` oder `gradle build`
- Python: `pytest` oder `python -m py_compile`
- Node.js: `npm run build` oder `npm test`
- Linters: oder `eslint` `.pylint` `.`

Selbst für Sprachen oder Transformationen, die nicht erstellt werden müssen, ist es sehr wichtig, einen Befehl bereitzustellen, der die Ergebnisse validiert und Probleme zurückgibt, wenn die Überprüfung fehlschlägt, um die Transformationsqualität zu verbessern.

Wenn kein Build oder keine Validierung erforderlich ist, lassen Sie ihn in Ihrer Eingabe weg.

Steuerung des Lernverhaltens

Standardmäßig extrahiert AWS Transform custom Lektionen aus jeder Transformationsausführung. Sie können das Lernen für bestimmte Ausführungen verhindern.

Um zu verhindern, dass aus einer Ausführung gelernt wird:

```
atx custom def exec -n my-transformation -p ./my-project -d
```

Das `--do-not-learn` Kennzeichen `-d` oder verhindert das Extrahieren von Lektionen aus der aktuellen Ausführung.

Konversationen werden wieder aufgenommen

AWS Mit „Benutzerdefiniert transformieren“ können Sie frühere Konversationen innerhalb von 30 Tagen nach der Erstellung wieder aufnehmen.

So setzen Sie die letzte Konversation fort:

```
atx --resume
```

Um eine bestimmte Konversation wieder aufzunehmen:

```
atx --conversation-id <conversation-id>
```

Important

Konversationen können nur innerhalb von 30 Tagen nach der Erstellung wieder aufgenommen werden. Nach 30 Tagen kann die Konversation nicht mehr fortgesetzt werden.

Verfolgen von Agentenminuten

AWS Mit Transform Custom werden die während einer Transformationssitzung verbrauchten [Agentenminuten](#) nachverfolgt. Die Minuten der Agenten sammeln sich während des gesamten Konversationszyklus an und werden angezeigt, wenn die Konversation beendet ist:

```
Agent minutes used: 12.50
```

Die Minuten der Agenten bleiben auch nach Unterbrechungen bestehen. Wenn Sie eine Sitzung mit Strg+C unterbrechen und später wieder aufnehmen, werden die zuvor gesammelten Minuten übernommen und sammeln sich weiterhin in der wiederaufgenommenen Sitzung an.

Gehen Sie wie folgt vor, um die Agentenminuten während einer interaktiven Sitzung zu überprüfen:

Geben Sie `/usage` an der Eingabeaufforderung ein, um die aktuell gesammelten Agentenminuten anzuzeigen, ohne die Konversation zu beenden.

So legen Sie ein Budgetlimit für Agentenminuten fest:

```
atx custom def exec -n my-transformation -p ./my-project --limit 30
```

Die `--limit` Option legt ein maximales Budget für [Agentenminuten](#) für die Sitzung fest. Die Agentenminuten spiegeln die aktive Arbeitszeit der Agenten wider, nicht die Uhrzeit rund um die Uhr. Wenn das Limit erreicht ist, zeigt die CLI eine Meldung an und wird mit Anweisungen zum Fortfahren beendet:

```
## Budget limit reached: 30.00 / 30.00 Agent Minutes. Exiting.
```

Sie können die Konversation später mit einem erhöhten Limit fortsetzen:

```
atx --conversation-id <conversation_id> -t --limit <increased_limit>
```

Kontinuierliches Lernen

In diesem Abschnitt wird beschrieben, wie Sie die durch kontinuierliches Lernen entstandenen Lektionen überprüfen und verwalten können.

Lektionen verstehen

Das System für kontinuierliches Lernen extrahiert automatisch Lektionen aus früheren Durchläufen einer Transformation. Das System erstellt sie asynchron auf der Grundlage von:

- Feedback der Entwickler wird im interaktiven Modus bereitgestellt
- Bei Transformationen sind Codeprobleme aufgetreten

Die Lektionen häufen sich im Laufe der Zeit an, wenn Sie die Transformation über verschiedene Codebasen hinweg ausführen. Das System wendet sie automatisch an, um future Läufe zu verbessern. Jede Lektion gehört zu einer Kategorie, die alle Lektionen eines ähnlichen Bereichs enthält, sodass Sie verwandte Lektionen gemeinsam überprüfen können. Lektionen, die Sie nicht verwenden möchten, können Sie archivieren oder vollständig löschen.

Lektionen anzeigen und verwalten

Verwenden Sie den `learnings` Befehl, um eine interaktive Sitzung zum Durchsuchen und Verwalten der Lektionen einer Transformationsdefinition zu öffnen.

Um den Lektionen-Viewer zu öffnen:

```
atx custom def learnings -n my-transformation
```

Der Viewer öffnet sich mit einer Liste von Lektionskategorien, von denen jede zeigt, wie viele aktive Lektionen sie enthält. Wählen Sie eine Kategorie aus, um die zugehörigen Lektionen zu sehen, und wählen Sie dann eine Lektion aus, um alle Einzelheiten zu sehen, einschließlich des Hauptteils der Lektion, ihrer Auswirkungen und der Anzahl früherer Lektionen, in denen sie konsultiert wurde.

Lektionen archivieren und wiederherstellen

Das System wendet die Lektionen automatisch an. Wenn Sie nicht möchten, dass das System eine Lektion anwendet, können Sie sie archivieren. Das System behält archivierte Lektionen bei,

wendet sie jedoch nicht auf future Läufe an. Alle archivierten Lektionen sind gruppiert, sodass Sie sie überprüfen und alle wieder aktiv verwenden können.

Lektionen löschen

Eine Lektion, die nicht nützlich ist, dauerhaft entfernen. Das Löschen kann nicht rückgängig gemacht werden, und das System kann eine gelöschte Lektion aus zukünftigen Läufen erneut lernen.

Eine Lektion muss archiviert werden, bevor sie gelöscht werden kann.

Erweiterte Konfiguration

In diesem Abschnitt werden erweiterte Funktionen und Konfigurationsoptionen für AWS Transform custom beschrieben.

Umgebungsvariablen

Sie können das CLI-Verhalten mithilfe von Umgebungsvariablen anpassen.

Note

Die folgenden Beispiele zeigen die Linux- und macOS-Syntax (export). Legen Sie unter Windows Umgebungsvariablen in PowerShell using fest\$env:NAME="value". Die entsprechenden Befehle finden Sie auf den Windows (PowerShell) -Tabs.

ATX_SHELL_TIMEOUT

Überschreibt das Standard-Timeout für Shell-Befehle (900 Minuten). seconds/15

Linux and macOS

```
export ATX_SHELL_TIMEOUT=1800 # 30 minutes
```

Windows (PowerShell)

```
$env:ATX_SHELL_TIMEOUT=1800 # 30 minutes
```

Dies ist nützlich für große Codebasen oder lang andauernde Build-Prozesse.

ATX_DISABLE_UPDATE_CHECK

Deaktivieren Sie automatische Versionsprüfungen und Aktualisierungsbenachrichtigungen während der Befehlsausführung.

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

```
$env:ATX_DISABLE_UPDATE_CHECK="true"
```

ATX_GIT_COMMITTER_NAME und ATX_GIT_COMMITTER_EMAIL

Konfigurieren Sie die Autorenidentität, die für die Checkpoint-Commits verwendet wird, die Transform custom in Ihrem Repository erstellt, wenn Änderungen während einer Transformation angewendet werden. AWS Wenn diese Variablen nicht gesetzt sind, werden Checkpoint-Commits einer Standardidentität () zugeordnet. ATX Bot <checkpoint@atx.bot> Legen Sie beide Variablen fest, um Checkpoints einem bestimmten Autor zuzuordnen.

Linux and macOS

```
export ATX_GIT_COMMITTER_NAME="Jane Developer"
export ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

Windows (PowerShell)

```
$env:ATX_GIT_COMMITTER_NAME="Jane Developer"
$env:ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

Vertraue den Einstellungen

Mit den Vertrauenseinstellungen können Sie bestimmte Tools und Befehle vorab genehmigen, sodass sie ohne Aufforderung ausgeführt werden können. Sie können unabhängig von der Vertrauensstufe auch explizite Berechtigungen für bestimmte Shell-Befehle verlangen. Diese Einstellungen sind in der ~/.aws/atx/trust-settings.yaml Datei konfiguriert.

Die Datei enthält drei Listen:

- `trustedTools`- Tools, die ohne Aufforderung ausgeführt werden können
- `trustedShellCommands`- Shell-Befehle, die ohne Aufforderung ausgeführt werden können
- `alwaysPromptCommands`- Shell-Befehlsmuster, für die eine ausdrückliche Genehmigung erforderlich ist, sofern sie nicht von ihnen überschrieben wird `trustedShellCommands`, unabhängig von der `-t` Flagge oder der Sitzungsvertrauensstellung. Diese Muster werden im nicht interaktiven Modus (`()`) nicht erzwungen. `-x`

Vertrauenswürdige Standardtools:

- `file_read`
- `get_transformation_from_registry`
- `list_available_transformations_from_registry`

Vertrauenseinstellungen bearbeiten:

Sie können die Datei `trust-settings.yaml` manuell bearbeiten, um vertrauenswürdige Tools und Befehle hinzuzufügen oder zu entfernen. Beide `trustedShellCommands` und unterstützen Glob-Platzhaltermuster unter Verwendung von `alwaysPromptCommands` *

 Note

Wenn ein Befehl beiden Listen entspricht, `trustedShellCommands` hat er Priorität.

Im Folgenden werden die einzelnen Befehlslisten beschrieben und es werden Beispiele bereitgestellt:

- `trustedShellCommands`- Befehle, die diesen Mustern entsprechen, werden ohne Aufforderung ausgeführt und umgehen alle anderen Leitplanken. Muster werden mit der vollständigen Befehlszeichenfolge abgeglichen.

Beispiele:

- `cd *`- Entspricht zusammengesetzten Befehlen, die mit `cd` beginnen
- `*&&*`- Vertraut allen Befehlen mit dem Operator `&&`
- `alwaysPromptCommands`- Befehle, die diesen Mustern entsprechen, erfordern eine ausdrückliche Genehmigung, sofern sie nicht von ihnen überschrieben werden `trustedShellCommands`,

unabhängig von der `-t` Markierung oder der Sitzungsvertrauensstellung. Diese Muster werden im nicht interaktiven Modus `()` nicht erzwungen. `-x` In zusammengesetzten Ausdrücken (`&&`, Befehlsersetzungen) werden die Muster den einzelnen Unterbefehlen zugeordnet. `| |`

Beispiele:

- `rm -rf *` - Fordert immer zu rekursiven Force-Delete-Befehlen auf
- `sudo *` - Fordert immer nach Befehlen auf, die mit Sudo ausgeführt werden
- `find * -exec *` - Fordert immer nach Suchbefehlen mit `-exec`

Session-level vertraue:

Bei interaktiven Eingabeaufforderungen können Sie wählen:

- `(y)es` - Einmal ausführen
- `(n)o` - Ablehnen
- `(t)rust` - Nur für die aktuelle Sitzung vertrauen

Session-level Die Vertrauenseinstellungen sind temporär und werden beim Neustart der CLI zurückgesetzt. Sie bieten eine temporäre Genehmigung, ohne `trust-settings.yaml` dauerhaft zu ändern.

Note

Session Trust ist für Befehle, die Ihrer Liste entsprechen, nicht verfügbar.
`alwaysPromptCommands`

Modellieren Sie Context Protocol (MCP) -Server

Die AWS Transform CLI unterstützt Model Context Protocol (MCP) -Server, die ihre Funktionalität um zusätzliche Tools erweitern.

Konfiguration:

Konfigurieren Sie MCP-Server in der `~/.aws/atx/mcp.json` Datei. Die AWS Transform CLI unterstützt zwei Arten von MCP-Servern: lokale befehlsbasierte Server und Remote-HTTP-Server.

Lokale befehlsbasierte Server:

Lokale Server werden als untergeordnete Prozesse auf Ihrem Computer ausgeführt. Konfigurieren Sie sie mit der folgenden `command` Eigenschaft:

```
{
  "mcpServers": {
    "my-local-server": {
      "command": "npx",
      "args": ["-y", "@example/mcp-server"]
    }
  }
}
```

Remote-HTTP-Server:

Remoteserver stellen eine Verbindung zu MCP-Servern her, die unter einer HTTP- oder HTTPS-URL gehostet werden. Konfigurieren Sie sie mit der folgenden `url` Eigenschaft:

```
{
  "mcpServers": {
    "my-remote-server": {
      "url": "https://api.example.com/mcp",
      "headers": {
        "Authorization": "Bearer ${MCP_API_TOKEN}"
      }
    }
  }
}
```

Die `headers` Eigenschaft ist optional und unterstützt die Erweiterung von Umgebungsvariablen mithilfe von `${VAR_NAME}` Syntax. Auf diese Weise können Sie sensible Werte wie API-Token in Umgebungsvariablen und nicht in der Konfigurationsdatei speichern.

Eigenschaften der Konfiguration:

Lokale befehlsbasierte Server unterstützen die folgenden Eigenschaften:

- `command`(erforderlich) — Der Befehl zum Ausführen des Servers
- `args`(optional) — Array von Befehlszeilenargumenten
- `env`(optional) — Umgebungsvariablen, die an den Serverprozess übergeben werden

Remote-HTTP-Server unterstützen die folgenden Eigenschaften:

- `url`(erforderlich) — Die HTTP- oder HTTPS-URL des Remote-MCP-Servers
- `headers`(optional) — HTTP-Header, die in Anfragen aufgenommen werden sollen, mit Unterstützung für die Erweiterung von `${VAR_NAME}` Umgebungsvariablen

Verwaltung von MCP-Servern:

Liste der konfigurierten MCP-Server anzeigen:

```
atx mcp tools
```

Liste der verfügbaren Tools, die von einem bestimmten MCP-Server angeboten werden:

```
atx mcp tools --server <server-name>
```

Nachverfolgung der Nutzung:

Die CLI verfolgt automatisch die Nutzung des MCP-Tools während der Transformationsausführungen. Die Nutzungsstatistiken werden wie `mcp_usage.json` im Konversationsverzeichnis nebenstehend gespeichert. `metadata.json` In der Datei werden Metriken pro Tool für jede Ausführung aufgezeichnet, darunter:

- Anzahl der Aufrufe pro Tool
- Anzahl der Fehler pro Tool
- Gesamtausführungszeit pro Tool
- Details zum letzten Fehler (falls vorhanden)

Client-Side Fähigkeiten

Client-side Fähigkeiten sind zusätzliche Fähigkeiten, die den Agenten bei Transformationsausführungen erweitern. Sie ermöglichen es Ihnen, benutzerdefinierte Tools, Skripts und Anweisungen bereitzustellen, die der Agent zusätzlich zu seinen integrierten Funktionen verwenden kann.

Verzeichnisse zur Erkennung von Fähigkeiten:

Fähigkeiten werden in vier Verzeichnissen in der Reihenfolge ihrer Priorität erkannt. Wenn ein Skill mit demselben Namen in mehreren Verzeichnissen existiert, hat das erste Verzeichnis in der Liste Priorität:

1. <project>/aws/atx/skills/- Project-level, AWS Transformieren CLI-specific
2. <project>/agents/skills/- Project-level, mandantenübergreifend (für alle kompatiblen Agent-Tools verfügbar)
3. ~/.aws/atx/skills/- User-level, Transformieren AWS CLI-specific
4. ~/.agents/skills/- User-level, mandantenübergreifend (für alle kompatiblen Agent-Tools verfügbar)

Die .aws/atx/skills/ Verzeichnisse sind spezifisch für die AWS Transform-CLI. Die .agents/skills/ Verzeichnisse sind mandantenübergreifend, was bedeutet, dass die dort platzierten Fähigkeiten für alle kompatiblen Agent-Tools außerhalb der AWS Transform-CLI verfügbar sind.

Struktur des Skill-Verzeichnisses:

Jeder Skill ist ein Verzeichnis, das eine SKILL.md Datei mit YAML-Frontmatter enthält:

```
~/.aws/atx/skills/
### my-skill/
  ### SKILL.md          # Required: frontmatter + instructions
  ### references/       # Optional: reference docs the agent can read
  #   ### guide.md
  ### scripts/         # Optional: scripts the agent can execute
  ### validate.py
```

SKILL.md Format:

```
---
name: my-skill
description: When to use this skill
---
# Skill Title

Instructions for the agent...
```

Das name Feld muss mit dem Namen des übergeordneten Verzeichnisses übereinstimmen.

Einen Skill deaktivieren:

Um zu verhindern, dass ein Skill geladen wird, ohne die zugehörigen Dateien disable-model-invocation: true zu entfernen, fügen Sie der Titelseite Folgendes hinzu:

```
---  
name: my-skill  
description: When to use this skill  
disable-model-invocation: true  
---
```

Wenn diese Eigenschaft festgelegt ist, überspringt die CLI den Skill bei der Erkennung. Der Agent kann den Skill nur sehen oder verwenden, wenn er in einer Transformationsdefinition ausdrücklich angewiesen wird, die Skill-Datei zu lesen. Verwenden Sie diese Option, um einen Skill vorübergehend zu deaktivieren, ihn als in Bearbeitung zu markieren oder Referenzmaterial aufzubewahren, das nur für menschliche Leser bestimmt ist.

Note

Die Dateien eines deaktivierten Skills verbleiben auf der Festplatte. Wenn eine Transformationsdefinition den Agenten anweist, einen bestimmten Dateipfad zu lesen, kann der Agent trotzdem auf den Inhalt zugreifen. Die `disable-model-invocation` Eigenschaft verhindert die automatische Erkennung und Kontext-Injection, nicht aber den Dateisystemzugriff.

Verfügbarkeit von Fähigkeiten nach Ausführungsmodus:

- Exec-Modus (`atx custom def execmit--code-repository-path`) — Findet Fähigkeiten sowohl aus Verzeichnissen auf Benutzer- als auch auf Projektebene.
- Interaktiver Modus (`atx`) — Anfänglich werden nur Fähigkeiten auf Benutzerebene erkannt. Wenn Sie während der Sitzung einen Code-Repository-Pfad angeben, werden auch Skills auf Projektebene geladen.

Überprüfung der Erkennung von Fähigkeiten:

Überprüfe nach einem Lauf das Debug-Protokoll der CLI, um zu überprüfen, welche Skills entdeckt wurden:

Linux and macOS

```
grep -i "skill" ~/.aws/atx/logs/debug.log | tail -20
```

Windows (PowerShell)

```
Select-String -Pattern "skill" "$env:USERPROFILE\.aws\atx\logs\debug.log" | Select-Object -Last 20
```

Fähigkeiten, bei denen die Validierung fehlschlägt, werden mit einer Warnung in den Debug-Protokollen übersprungen.

Note

Client-side Fähigkeiten erfordern CLI Version 2.0 oder höher.

Wahl zwischen Project-Level und User-Level Fähigkeiten

Wo du eine Fähigkeit platzierst, bestimmt, wem sie zugute kommt und wann sie aktiviert wird.

Project-level Fähigkeiten (<project>/`.aws/atx/skills/`):

Übergeben Sie diese der Versionskontrolle, sodass jedes Teammitglied, das Transformationen gegen das Repository durchführt, sie automatisch erkennt. Nutzen Sie Fähigkeiten auf Projektebene für:

- Repository-specific Konformitätsprüfungen (Dockerfile-Regeln, Terraform-Richtlinien, Validatoren für die Migrationssicherheit)
- Kodierungsstandards der Organisation, die für diese Codebasis gelten (Beobachtbarkeitsmuster, Fehlerbehandlung, Namenskonventionen)
- Erstellen oder testen Sie Skripte, die für das Projekt spezifisch sind (benutzerdefinierte Linter, Architektur-Fitnessfunktionen)
- API-Migrationsleitfäden für interne Bibliotheken, die in diesem Repository verwendet werden

User-level Fähigkeiten (~/`.aws/atx/skills/`):

Diese verbleiben auf Ihrem Computer und werden bei allen Transformationen aktiviert, unabhängig davon, auf welches Repository Sie abzielen. Nutzen Sie Fähigkeiten auf Benutzerebene für:

- Tools für persönliche Workflows (Changelog-Generatoren, Commit-Nachrichtenformatierer)
- Cross-project Präferenzen (bevorzugte Testmuster, Erinnerungen im Stil der Dokumentation)

- Prüfungen zur Einhaltung der Lizenzbestimmungen, die Ihr Unternehmen für alle Repositories benötigt
- Deckungsschwellen oder Quality Gates, die Sie für jede Codebasis, mit der Sie arbeiten, durchsetzen

Tipps für effektive Fähigkeiten:

- Schreiben Sie klare `description` Felder in Ihre `SKILL.md` Titelseite. Der Agent verwendet dieses Feld, um zu entscheiden, wann eine Fähigkeit relevant ist.
- Beendet die Validierungsskripte bei Erfolg mit dem Code 0 und bei einem Fehler ungleich Null. Der Agent interpretiert Exit-Codes, um festzustellen, ob die Vorschriften eingehalten werden.
- Druckt klare, umsetzbare Fehlermeldungen in Skripten. Der Agent liest die Ausgabe, um zu verstehen, was behoben werden muss.
- Platzieren Sie Fähigkeiten auf beiden Ebenen im mandantenübergreifenden Verzeichnis (`.agents/skills/`), um sie mit anderen KI-Entwicklungstools außerhalb der AWS Transform-CLI zu teilen.

Client-Side Beispiele für Fähigkeiten

Diese Beispiele zeigen zwei gängige Muster: eine skriptbasierte Validierungsfähigkeit und eine Fähigkeit, die nur als Referenz dient.

Beispiel: Dockerfile Compliance Checker () Script-Based

Dieser Skill validiert Dockerfiles anhand von bewährten Sicherheits- und Betriebspraktiken. Es verwendet ein Überprüfungsskript, das der Agent vor und nach Änderungen ausführt.

Verzeichnisstruktur:

```
.aws/atx/skills/  
### dockerfile-compliance/  
    ### SKILL.md  
    ### scripts/  
    #   ### lint_dockerfile.sh  
    ### references/  
        ### dockerfile-best-practices.md
```

SKILL.md:

```

---
name: dockerfile-compliance
description: Validates Dockerfiles against security and operational best practices
---
# Dockerfile Compliance Checker

When a transformation creates or modifies Dockerfiles, run the compliance checker.

## When to use

- After creating a new Dockerfile
- After modifying FROM, RUN, USER, or EXPOSE directives
- When containerizing an application as part of a transformation

## How to use

Run: `bash scripts/lint_dockerfile.sh <path-to-Dockerfile>`

If violations are found, consult `references/dockerfile-best-practices.md`
for compliant patterns.

```

Das Validierungsskript sucht nach unverankerten Basis-Image-Tags, die als Root-Benutzer ausgeführt werden, nach fest codierten Geheimnissen in ENV Direktiven und nach fehlenden Definitionen. HEALTHCHECK Der Agent führt das Skript aus, behebt Verstöße anhand von Mustern aus der Referenzdatei und führt das Skript erneut aus, um die Einhaltung der Vorschriften zu bestätigen.

Beispiel: API Deprecation Helper () Reference-Only

Dieser Skill führt den Agenten durch das Ersetzen veralteter API-Aufrufe bei Upgrade-Transformationen. Es werden nur Referenzdateien ohne Skripte verwendet.

Verzeichnisstruktur:

```

.aws/atx/skills/
### api-deprecation-helper/
    ### SKILL.md
    ### references/
        ### aws-sdk-v2-to-v3.md
        ### react-class-to-hooks.md

```

SKILL.md:

```

---
name: api-deprecation-helper
description: Guides the agent through replacing deprecated API calls with modern
  equivalents
---
# API Deprecation Helper

When performing upgrade transformations, use this skill to identify and replace
deprecated API calls with their modern equivalents.

## When to use

- During any version upgrade transformation
- When build warnings mention deprecated APIs
- When transforming code that uses legacy patterns

## Process

1. Identify deprecated API calls in the codebase
2. For each deprecated call, find the replacement in `references/`
3. Apply the replacement, preserving the original behavior
4. Verify the replacement compiles and tests pass

```

Die Referenzdateien enthalten Vorher-Nachher-Codebeispiele. Ordnet beispielsweise `aws-sdk-v2-to-v3.md` Muster wie das modulare V3-Äquivalent mit `s3.putObject(params).promise()` zu `S3Client.PutObjectCommand`.

Schlagworte und Organisation

Sie können Transformationen mit Tags für die Zugriffskontrolle und Kategorisierung organisieren.

Note

Einige dieser Befehle erfordern die Angabe des Amazon-Ressourcennamens (ARN) für eine Transformationsdefinition. Die ARN-Struktur ist: `arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

Um Tags für eine Transformation aufzulisten:

```
atx custom def list-tags --arn <transformation-arn>
```

Um Tags zu einer Transformation hinzuzufügen:

```
atx custom def tag --arn <transformation-arn> --tags '{"env":"prod","team":"backend"}'
```

Um Tags aus einer Transformation zu entfernen:

```
atx custom def untag --arn <transformation-arn> --tag-keys "env,team"
```

Tags können für die gruppierte Zugriffskontrolle in IAM-Richtlinien verwendet werden. Sie können Richtlinien erstellen, die allen Transformationen mit bestimmten Tags (z. B. allen Transformationen, die mit `team:frontend` oder gekennzeichnet sind) Berechtigungen gewähren.

`environment:production`

Protokolle

AWS Transform CLI verwaltet drei Arten von Protokollen zur Fehlerbehebung und zum Debuggen.

Konversationsprotokolle:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

Diese Protokolle enthalten den vollständigen Konversationsverlauf für eine bestimmte Sitzung.

Subagent-Protokolle:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

Diese Protokolle enthalten Ausgaben von Subagenten, die der Haupt-Agent bei Transformationen erzeugt. Sie müssen Subagenten nicht direkt verwalten.

Debug-Protokolle für Entwickler:

Linux and macOS

```
~/.aws/atx/logs/debug*.log  
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\aws\atx\logs\debug*.log  
%USERPROFILE%\aws\atx\logs\error.log
```

Diese Protokolle enthalten erweiterte Informationen zur Fehlerbehebung für die CLI selbst.

Note

Im Protokollverzeichnis befinden sich möglicherweise mehrere Debug-Protokolldateien (d. h. debug1.log, debug2.log). Überprüfen Sie alle relevanten Protokolle und stellen Sie sie bereit, z. B. `~/.aws/atx/custom/` /* und `<conversation-id>~/.aws/atx/logs/` *, wenn Support-Tickets geöffnet werden, um die Problemlösung zu beschleunigen.

CLI-Aktualisierungen

Halten Sie Ihre CLI auf dem neuesten Stand, um auf neue Funktionen und Verbesserungen zugreifen zu können.

Um nach Updates zu suchen:

```
atx update --check
```

Um auf die neueste Version zu aktualisieren:

```
atx update
```

Um auf eine bestimmte Version zu aktualisieren:

```
atx update --target-version <version>
```

Erstellen Sie benutzerdefinierte Transformationen

In diesem Abschnitt wird beschrieben, wie Sie benutzerdefinierte Transformationsdefinitionen erstellen, ändern und verwalten.

Eine neue Transformation erstellen

Verwenden Sie die interaktive CLI, um eine neue Transformationsdefinition zu erstellen.

Um eine Transformationsdefinition zu erstellen

1. Starten Sie die AWS Transform-CLI:

```
atx
```

2. Teilen Sie dem Agenten mit, dass Sie eine neue Transformation erstellen möchten.
3. Geben Sie eine klare, detaillierte Beschreibung des Transformationsziels an. Beinhaltet:
 - Der Quell- und Zielstatus (z. B. „Upgrade von Version X auf Version Y“)
 - Spezifische Änderungen erforderlich (z. B. „Importanweisungen aktualisieren, veraltete Methoden ersetzen“)
 - Irgendwelche besonderen Überlegungen oder Einschränkungen
4. Wenn der Mitarbeiter um Erläuterungen oder zusätzliche Informationen bittet, geben Sie konkrete Beispiele und Referenzmaterialien an.
5. Überprüfen Sie die ursprüngliche Transformationsdefinition, die vom Agenten erstellt wurde.
6. Testen Sie die Transformation an einer Beispielcodebasis.
7. Iterieren Sie, indem Sie Feedback, Codekorrekturen oder zusätzliche Beispiele bereitstellen.
8. Speichern Sie die Transformation lokal oder veröffentlichen Sie sie in der Registrierung.

Bewährte Methoden für die Erstellung von Transformationen:

- Beginnen Sie mit einfachen, klar definierten Transformationen, bevor Sie komplexe versuchen
- Stellen Sie umfassende Referenzmaterialien bereit, einschließlich Migrationsleitfäden und Codebeispielen
- Testen Sie vor der Veröffentlichung an mehreren Beispielcodebasen

- Verwenden Sie deterministische Build- oder Validierungsbefehle, um kontinuierliches Lernen zu ermöglichen
- Erwägen Sie, komplexe Transformationen in mehrere kleinere Schritte zu unterteilen
- Markieren Sie wichtige Informationen in Ihren Transformationsdefinitionen mit „KRITISCH:“ oder „WICHTIG:“, um sicherzustellen, dass der Agent diese Anforderungen priorisiert
- Wenn Sie genaue Anforderungen erfüllen müssen (z. B. die Verwendung eines bestimmten Befehls oder Zeichenfolgenwerts), geben Sie die vollständige Zeichenfolge explizit in Ihren Transformationsdefinitionen an. Sie können diese in Bash-Anführungszeichen setzen, um deutlich darauf hinzuweisen, dass es sich um Terminalbefehle oder buchstäbliche Zeichenketten handelt, wodurch die Variabilität reduziert und eine konsistente Ausführung gewährleistet wird

Bereitstellung von Referenzmaterial

Sie können Referenzdateien für AWS Transform custom bereitstellen, indem Sie während der Konversation Dateipfade angeben. Diese Dateien werden im `references/` Ordner der Transformationsdefinition gespeichert.

Empfohlene Typen von Referenzdateien:

- Before/after Beispielcode
- Dokumentation für die beteiligten APIs, Bibliotheken oder Funktionen
- Human-readable Anleitungen zur Migration

Um eine Referenzdatei bereitzustellen:

```
Take a look at the documentation here: /path/to/migration-guide.md
```

Sie können auch ein Verzeichnis angeben, das mehrere Referenzdateien enthält:

```
Take a look at the docs we have here: /path/to/docs/
```

Note

Nur textbasierte Dateien (.md, .html, .txt, Codedateien) werden unterstützt. Binärdateien, Bilder und Rich-Text-Dateien (z. B. .pdf, .png, .docx) werden derzeit nicht unterstützt. Es ist oft möglich, den Textinhalt zu extrahieren und ihn als Referenz zu verwenden. Wenn Sie viele

kleine Textdateien haben, sollten Sie erwägen, sie zu wenigen Dateien mit beschreibendem Namen zu verketteten. Es gibt ein Limit von insgesamt 10 MB für alle Dateien.

Ändern einer vorhandenen Transformation

Sie können benutzerdefinierte Transformationen sowohl vor als auch nach dem Speichern als Entwürfe oder nach dem Veröffentlichen ändern. Sie können AWS-verwaltete Transformationen nicht ändern. Wenn Sie sie anpassen müssen, können Sie mithilfe der Konfigurationsdatei zusätzlichen Kontext bereitstellen.

Um eine bestehende Transformation zu ändern

1. Starten Sie die AWS Transform-CLI:

```
atx
```

2. Teilen Sie dem Agenten mit, dass Sie eine bestehende Transformation ändern möchten.
3. Wählen Sie, ob Sie:
 - Geben Sie einen Dateipfad zu einer lokal gespeicherten Transformation an (d. h. nicht zu einem gespeicherten oder veröffentlichten Entwurf)
 - Fordern Sie die Liste der Transformationen von der Registrierung an
4. Wenn Sie aus der Registrierung wählen, wählen Sie die Transformation aus, die Sie ändern möchten.
5. Beschreiben Sie gemeinsam mit dem Agenten die Änderungen, die Sie vornehmen möchten.
6. Testen Sie die aktualisierte Transformation an einer Beispielpcodebasis.
7. Veröffentlichen Sie Ihre Aktualisierungen bei Bedarf in der Registrierung.

Transformationen veröffentlichen und verwalten

Sie können Ihre Transformationen mithilfe der interaktiven Benutzeroberfläche oder mit den folgenden Befehlen veröffentlichen und verwalten.

Um eine Transformation als Entwurf zu speichern:

```
atx custom def save-draft -n my-transformation --description "Description of the transformation" --sd ./transformation-directory
```


Um eine Transformation zu veröffentlichen:

```
atx custom def publish -n my-transformation --description "Description of the transformation" --sd ./transformation-directory
```

Um verfügbare Transformationen aufzulisten:

```
atx custom def list
```

Um eine Transformationsdefinition herunterzuladen:

```
atx custom def get -n my-transformation
```

Dadurch wird die Transformationsdefinition in Ihr aktuelles Arbeitsverzeichnis heruntergeladen. Sie können ein Zielverzeichnis mit dem `--td` Flag und eine Version mit dem `--tv` Flag angeben.

Um eine Transformationsdefinition zu löschen:

```
atx custom def delete -n my-transformation
```

Important

Dadurch wird die angegebene Transformationsdefinition dauerhaft aus Ihrem Konto gelöscht.

Transformationsversionen verwalten

AWS Transform Custom verwaltet Versionen Ihrer Transformationsdefinitionen. Sie können eine Version angeben, wenn Sie eine Transformation ausführen oder herunterladen.

Um eine bestimmte Version auszuführen:

```
atx custom def exec -n my-transformation --tv v1 -p ./my-project
```

Um eine bestimmte Version herunterzuladen:

```
atx custom def get -n my-transformation --tv v1
```

Wenn keine Version angegeben ist, wird die neueste Version verwendet.

Befehlsreferenz

Dieser Abschnitt enthält eine umfassende Referenz zu allen benutzerdefinierten AWS Transform-CLI-Befehlen.

Interaktive Befehle

atx

Starten Sie eine interaktive Konversation mit der AWS Transform CLI.

```
atx                # Start new conversation
atx --resume       # Resume most recent conversation
atx --conversation-id <id> # Resume specific conversation
atx -t            # Start with all tools trusted
```

Interaktive Sitzungsbefehle

Die folgenden Befehle können während einer interaktiven Sitzung an der Eingabeaufforderung eingegeben werden:

- /usage- Zeigt die gesammelten [Agentenminuten](#) für die aktuelle Sitzung an

Befehle zur Transformationsdefinition

ATX Benutzerdefinierter Def Exec

Führen Sie eine Transformationsdefinition in einem Code-Repository aus.

Option	Langform	Parameter	Description
-p	--code-repository-path	<path>	Pfad zum Code-Repository, das transformiert werden soll. Verwenden Sie für das aktuelle Verzeichnis „.“

Option	Langform	Parameter	Description
-c	--build-command	<command>	Befehl, der beim Erstellen des Repositorys ausgeführt werden soll
-n	--transformation-name	<name>	Name der Transformationsdefinition in der Registrierung
-x	--non-interactive	-	Führt die Transformation ohne Benutzerunterstützung aus
-t	--trust-all-tools	-	Vertraut allen Tools (keine Tool-Eingabeaufforderungen)
-d	--do-not-learn	-	Deaktivieren Sie das Extrahieren von Lektionen aus dieser Ausführung
-g	--configuration	<config>	Pfad zur Konfigurationsdatei (JSON oder YAML) oder zu Schlüssel=Wert-Paaren
--tv	--transformation-version	<version>	Version der zu verwendenden Transformationsdefinition

Option	Langform	Parameter	Description
<code>--limit</code>	<code>--limit</code>	<code><limit></code>	Legen Sie das Budgetlimit für Agentenminuten fest. Die Transformation wird beendet, wenn das Limit erreicht ist, und kann mit einem erhöhten Limit wieder aufgenommen werden
<code>-h</code>	<code>--help</code>	-	Hilfe für den Befehl anzeigen

benutzerdefinierte ATX-Definitionsliste

Listet die verfügbaren Transformationsdefinitionen auf.

```
atx custom def list
atx custom def list --json    # Output in JSON format
```

atx benutzerdefinierte Definition abrufen

Ruft Details zu einer bestimmten Transformationsdefinition ab.

Option	Langform	Parameter	Description
<code>-n</code>	<code>--transformation-name</code>	<code><name></code>	Der Name der abzurufenden Transformationsdefinition
<code>--tv</code>	<code>--transformation-version</code>	<code><version></code>	Die Version der Transformationsdefinition, die abgerufen werden soll

Option	Langform	Parameter	Description
--td	--target-directory	<directory>	Das Zielverzeichnis, in dem die Transformationsdefinition gespeichert werden soll (Standard: „.“)
--json	--json	-	Antwort im JSON-Format ausgeben
-h	--help	-	Hilfe für den Befehl anzeigen

atx benutzerdefinierte Definition löschen

Löscht eine Transformationsdefinition dauerhaft.

```
atx custom def delete -n <transformation-name>
```

ATX Custom Def veröffentlichen

Veröffentlichen Sie eine Transformationsdefinition in der Registrierung.

Option	Langform	Parameter	Description
-n	--transformation-name	<name>	Der Name der zu veröffentlichenden Transformationsdefinition
--tv	--transformation-version	<version>	Die Version der Transformationsdefinition, die verwendet werden soll (gilt nicht für --description oder --source-directory)

Option	Langform	Parameter	Description
--sd	--source-directory	<directory>	Das Quellverzeichnis, aus dem die lokalen Transformationsdefinitionsdateien gelesen werden sollen (gilt nicht für --transformation-version)
--description	--description	<description>	Eine Beschreibung für die Transformationsdefinition (gilt nicht für --transformation-version)
--json	--json	-	Antwort im JSON-Format ausgeben
-h	--help	-	Hilfe für den Befehl anzeigen

ATX Custom Def Save-Draft

Speichern Sie eine Transformationsdefinition als Entwurf in der Registrierung. Entwürfe laufen nach 30 Tagen ab und werden nicht in der Registrierung angezeigt. Dieser Befehl gibt die Versionsnummer des Entwurfs zurück. Sie müssen Entwürfe explizit unter Verwendung des Transformationsnamens und der Versionsnummer ausführen und abrufen.

```
atx custom def save-draft -n <transformation-name> --description "Description" --sd <directory>
```

Befehle der Lektion

Lernen im Bereich ATX Custom Def

Öffnen Sie eine interaktive Sitzung, um sich die Lektionen anzusehen und zu verwalten, die eine Transformationsdefinition aus früheren Durchläufen gezogen hat. Sie können Lektionen nach

Kategorien durchsuchen, Unterrichtsdetails anzeigen und Lektionen archivieren, wiederherstellen oder löschen.

```
atx custom def learnings -n <transformation-name>
```

Befehle taggen

ATX-Listen-Tags mit benutzerdefinierten Definitionen

Listet Tags für eine Transformationsdefinition auf.

```
atx custom def list-tags --arn <transformation-arn>
```

Benutzerdefiniertes ATX-Tag

Fügen Sie einer Transformationsdefinition Tags hinzu.

```
atx custom def tag --arn <arn> --tags '{"env":"prod","team":"backend"}'
```

ATX Custom Def Untag

Entfernen Sie Tags aus einer Transformationsdefinition.

```
atx custom def untag --arn <arn> --tag-keys "env,team"
```

Befehle aktualisieren

atx-Update

Aktualisieren Sie die AWS Transform-CLI.

```
atx update                # Update to latest version
atx update --check        # Check for updates only
atx update --target-version <version> # Update to specific version
```

MCP-Befehle

ATX-MCP-Werkzeuge

Ermöglicht Kunden die Konfiguration view/confirm ihrer MCP-Tools. Aktualisierungen der Konfigurationen müssen direkt über die Datei ~/ verwaltet werden. aws/atx/mcp.json

```
atx mcp tools      # View list of MCP servers
atx mcp tools -s   # List tools for the specified server
```

AWS-Verwaltete Transformationen

AWS-verwaltete Transformationen sind vorgefertigte, AWS geprüfte Transformationen für allgemeine Anwendungsfälle, die ohne zusätzliche Einrichtung sofort einsatzbereit sind.

-Übersicht

AWS-verwaltete Transformationen weisen die folgenden Merkmale auf:

- Validiert von AWS — Diese Transformationen wurden auf ihre hohe Qualität geprüft AWS
- Sofort einsatzbereit — Keine zusätzliche Einrichtung erforderlich
- Kontinuierlich wachsend — Weitere Transformationen werden kontinuierlich hinzugefügt
- Anpassbar — Pre-built Transformationen können individuell angepasst werden, indem mithilfe des Konfigurationsparameters zusätzliche Hinweise oder Anforderungen bereitgestellt werden, die auf die `additionalPlanContext` Bedürfnisse Ihres Unternehmens zugeschnitten sind
- Early-Access-Support — Einige Transformationen können als Early-Access gekennzeichnet werden, wenn sie weiter getestet und verfeinert werden

Available (Verfügbar) AWS-Verwaltete Transformationen

Im folgenden Katalog sind die derzeit verfügbaren AWS-verwalteten Transformationen nach Anwendungsfällen gruppiert aufgeführt. Jede Tabelle zeigt den Namen der Transformation, die Sprache oder den Stack, für die sie gilt, und ihren Status. Um eine Transformation schnell zu finden, verwenden Sie das Suchfeld oben auf dieser Seite, um nach Namen, Sprache oder Anwendungsfall zu suchen.

Dieser Katalog ist die kanonische Liste der AWS-verwalteten Transformationen. Kiro Power, das Agent-Plugin, das VS Code-Plugin und die CLI führen alle dieselben Transformationen aus. Führen Sie den Befehl aus, um die in Ihrer Registrierung verfügbaren Transformationen aufzulisten. `atx custom def list`

Note

Transformationen, die mit Early Access gekennzeichnet sind, sind funktionsfähig, können aber aufgrund von Kundenfeedback häufig aktualisiert werden.

Laufzeit-Upgrades

Führen Sie ein Upgrade einer Sprache oder Runtime auf eine neuere Version durch oder ändern Sie die Runtime-Distribution.

Transformation	Sprache//Stack	Status	Description
AWS/java-version-upgrade	Java	Allgemein verfügbar	Aktualisieren Sie Java-Anwendungen, die ein beliebiges Build-System verwenden, von einer beliebigen Quell-JDK-Version auf eine beliebige Ziel-JDK-Version, mit der Modernisierung der Abhängigkeiten, einschließlich Jakarta EE-Migration, Datenbanktreibern, ORM-Frameworks und Updates des Spring-Ökosystems. Geben Sie die Ziel-JDK-Version im Chat oder mit dem Parameter <code>additionalPlanContext</code>

Transformation	Sprache//Stack	Status	Description
AWS/python-version-upgrade	Python	Allgemein verfügbar	Migrieren Sie Python-Projekte von Python 3.8 oder 3.9 auf Python 3.11, 3.12 oder 3.13 unter Beibehaltung von Funktionalität und Leistung. Geben Sie die Python-Zielversion im Chat oder mit dem additionalPlanContext Parameter an.
AWS/nodejs-version-upgrade	Node.js	Allgemein verfügbar	Aktualisieren Sie Node.js Anwendungen von einer beliebigen Node.js Quellversion auf eine beliebige Node.js Zielversion. Geben Sie die Zielversion im Chat oder mit dem additionalPlanContext Parameter an.

Transformation	Sprache//Stack	Status	Description
AWS/lambda-nodejs-runtime-upgrade	Node.js (Lambda)	Früher Zugriff	Führen Sie ein Upgrade von AWS Lambda-Funktionen von älteren Node.js Laufzeiten (nodejs4.3 bis nodejs22.x) auf nodejs24.x durch und beheben Sie wichtige Änderungen im Lambda Runtime Interface Client (RIC) und in der 24-Sprach-Runtime. Node.js
AWS/oracle-java-to-corretto	Java (JDK-Distribution)	Frühzeitiger Zugriff	Migrieren Sie Java-Projekte von Oracle JDK zu Amazon Corretto. Ersetzt Oracle-specific interne APIs durch standardmäßige Java-Äquivalente, aktualisiert Build-Konfigurationen (Maven und Gradle) und Container-Basis-Images, entfernt kommerzielle JVM-Flags und generiert einen Lizenzbericht.

Transformation	Sprache//Stack	Status	Description
AWS/ruby-upgrade	Ruby	Frühzeitiger Zugriff	Aktualisieren Sie Ruby-Anwendungen von Ruby 2.x auf Ruby 4.0 und ihre Frameworks auf Rails 8.0 oder Sinatra 4.1. Sie können diese Transformation mit Rails und ActiveRecord Apps, Sinatra-Apps und eigenständigen Edelsteinen verwenden. Bei der Transformation wird jede Ruby-Version mit dem passenden Framework-Upgrade verknüpft und die Testsuite ausgeführt. Anschließend werden Fehler isoliert, bevor zur nächsten Version übergegangen wird.

SDK-Migrationen

Migrieren Sie zwischen Hauptversionen eines AWS SDK.

Transformation	Sprache//Stack	Status	Description
AWS/java-aws-sdk-v1-to-v2	Java	Allgemein verfügbar	Aktualisieren Sie das AWS SDK von Version 1 auf Version 2 für Java-Projekte

Transformation	Sprache//Stack	Status	Description
			mit Maven oder Gradle.
AWS/python-boto2-to-boto3	Python	Allgemein verfügbar	Migrieren Sie Python-Anwendungen von boto2 zu boto3, basierend auf der offiziellen Migration sdokumentation. AWS
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	Allgemein verfügbar	Aktualisieren Sie Node.js Anwendung en vom AWS SDK für JavaScript Version 2 auf Version 3 und profitieren Sie von modularer Architektur, erstklassigem TypeScript Support und verbesserter Leistung, ohne die Version zu ändern. Node.js

Framework-Upgrades und -Migrationen

Aktualisieren Sie ein Framework auf eine neuere Version oder migrieren Sie zu einem anderen Framework.

Transformation	Sprache//Stack	Status	Description
AWS/spring-boot-version-upgrade	Java//Spring Boot	Allgemein verfügbar	Aktualisieren Sie eine ältere Spring Boot-Anwendung auf eine Spring Boot-Ziel

Transformation	Sprache//Stack	Status	Description
			version, einschließlich Build-Dateien und Startern, Eigenschaften, Jackson 3-Paketen, Spring Security 7 DSL, Testinfrastruktur und Observability-Abhängigkeiten.
AWS/JBoss-to-Spring-Boot	Java (JBoss oder WildFly auf Spring Boot)	Früher Zugriff	Migrieren Sie Java EE- oder Jakarta EE-Unternehmensanwendungen, die auf JBoss EAP oder Spring Boot laufen, und vermeiden WildFly Sie so die Abhängigkeiten von Anwendungsservern für ein cloudnatives, containerisiertes Bereitstellungsmodell.
AWS/early-access-angular-to-react-migration	Von Angular zu React	Frühzeitiger Zugriff	Transformieren Sie eine Angular-Anwendung in React.

Transformation	Sprache//Stack	Status	Description
AWS/angular-version-upgrade	Winkel	Frühzeitiger Zugriff	Führen Sie ein Upgrade einer älteren Angular-A nwendung auf eine Angular-Zielversio n durch, einschlie ßlich Komponenten, Services, Vorlagen und Routing.
AWS/vue.js-version-upgrade	Vue.js	Frühzeitiger Zugriff	Führen Sie ein Upgrade der Hauptversion von Vue.js 2 auf Vue.js 3 durch und modernisi eren Sie dabei Komponenten, Statusverwaltung, Routing und globale APIs. Kleinere Updates und Patch-Updates fallen nicht in den Geltungsbereich.

GenAI und Modellmigrationen

Migrieren Sie generative KI-Workloads zu.

Transformation	Sprache/Stack	Status	Description
AWS/GenAI-to-Bedrock-Migrat ion-Assessment	Generative KI-Worklo ads	Frühzeitiger Zugriff	Beurteilen Sie generative KI-Worklo ads für die Migration von Drittanbietern (OpenAI, Google

Transformation	Sprache/Stack	Status	Description
			Gemini, Anthropic Direct und Open-Source-Modelle) zu. Erkennt die Nutzung und Modelle des SDK, klärt die Anforderungen, entwirft ein Modell-Mapping, schätzt Kosten und Risiken ab und generiert Bewertungsartefakte. Assessment-only; ändert den Quellcode nicht. Deckt auch agentische Frameworks wie CrewAI und Strands LangGraph ab.

Language-to-language Migrationen

Translate Sie eine Codebasis von einer Programmiersprache in eine andere.

Transformation	Sprache//Stack	Status	Description
AWS/vba-to-python-migration	VBA zu Python	Früher Zugriff	Migrieren Sie Excel-VBA-Makros, -Module und eingebettete Logik mithilfe von openpyxl, pandas, tkinter oder PyQt 6 und Standardbibliotheken zu entsprechenden

Transformation	Sprache//Stack	Status	Description
			Python-Skripten und -Modulen. UserForms Die Zielsprache ist Python 3.8 oder höher. Wird bei der Konvertierung von eingebettetem VBA-Code in die Formate .bas, .cls, .frm oder .xlsm verwendet.

Datenbankmigrationen

Derzeit sind keine AWS datenbankspezifischen, verwalteten Transformationen verfügbar.

Informationen zur Modernisierung von Microsoft SQL Server-Datenbanken und den zugehörigen .NET-Anwendungen für Amazon Aurora PostgreSQL finden Sie unter [the section called “Modernisierung von SQL Server”](#)

Beobachtbarkeit

Modernisieren Sie die Protokollierung und Überwachung auf native Dienste. AWS

Transformation	Sprache//Stack	Status	Description
AWS/early-access-log4j-to-slf4j-migration	Java (Protokollierung)	Früher Zugriff	Migrieren Sie Java-Anwendungen mit einem Logback-Backend von Log4j (1.x oder 2.x) auf SLF4J. Verwaltet den Quellcode, das Abhängigkeitsmanagement (Maven und Gradle) und die Protokollierung von

Transformation	Sprache//Stack	Status	Description
			Konfigurationsdateien und validiert sie durch Kompilieren, Testen und Restimport-Scan.
AWS/datadog-monitors-to-cloudwatch-alarms	Infrastruktur als Code/Überwachung	Frühzeitiger Zugriff	Migrieren Sie DataDog Metrik-Monitore, die AWS Servicemetriken und benutzerdefinierte Metriken verfolgen, auf native CloudWatch Alarme als Infrastructure-as-Code. Generiert CloudFormation YAML, CDK und TypeScript Terraform HCL.

Architektur

Re-architect, plattformübergreifend oder optimiert Anwendungen für. AWS

Transformation	Sprache/Stack	Status	Description
AWS/java-performance-optimization	Java (Leistung)	Allgemein verfügbar	Optimieren Sie die Leistung von Java-Anwendungen, indem Sie JFR-Profilierungsdaten analysieren, um CPU- und Speicher-Hotspots und Anti-Pattern zu erkennen und anschließend

Transformation	Sprache/Stack	Status	Description
			gezielte Code-Fixes anzuwenden. Anweisungen zum Sammeln von JFR-Daten finden Sie im JFR-Laufzeitleitfaden.
AWS/early-access-java-x86-to-graviton	Java (Arm64/Graviton)	Früher Zugriff	Überprüfen Sie die Kompatibilität von Java-Anwendungen mit der Arm64-Architektur für AWS Graviton-Prozessoren und beheben Sie Inkompatibilitäten, indem Sie Abhängigkeiten aktualisieren, architekturspezifische Codemuster erkennen und native Bibliotheken neu kompilieren, sobald Quellcode verfügbar ist. Arm64-compatible Viele moderne Java-Anwendungen sind es bereits.

Transformation	Sprache/Stack	Status	Description
AWS/oracle-service-bus-to-aws	Java//Integration zu Serverless	Frühzeitiger Zugriff	Migrieren Sie Oracle Service Bus (OSB) - und AWS BPEL-Prozesskonfigurationen auf eine native serverlose Architektur und generieren Sie so ein bereitstellbares TypeScript CDK-Projekt mit Amazon API Gateway, AWS Lambda und Step Functions. AWS

Transformation	Sprache/Stack	Status	Description
AWS/mulesoft-to-aws-native	MuleSoft Java//zu serverlos	Früher Zugriff	Transformieren Sie MuleSoft Mule 3.x- und 4.x-Anwendungen in AWS serverlose Architekturen (Amazon API Gateway, AWS Lambda und AWS Step Functions) für Java 17 auf Lambda mit. AWS SnapStart Die Transformation ordnet Flow-Trigger AWS Ereignisquellen zu, konvertiert DataWeave und MEL-Ausdrücke (MuleSoft Expression Language) in AWS Äquivalente und ersetzt Konnektoren durch AWS SDK for Java v2-Aufrufe. Es produziert SAM-Vorlagen, AWS Lambda-Handler und JUnit 5-Tests.

Transformation	Sprache/Stack	Status	Description
AWS/payshield-hsm-to-aws-payment-cryptography	Java (HSM für Zahlungskryptografie) AWS	Allgemein verfügbar	Migrieren Sie Java-Anwendungen vom Thales PayShield Hardware Security Module (HSM) - Protokoll zum AWS Payment Cryptography SDK v2. Die Migration umfasst die Befehlszuweisung, die Schlüsselmigration, die Einrichtung von Abhängigkeiten und Paritätstests.

Codebase-Analyse

Analysieren Sie Codebasen und Portfolios, um die Modernisierung zu planen. Durch diese Transformationen werden Berichte erstellt, ohne dass Ihr Code geändert wird.

Transformation	Sprache//Stack	Status	Description
AWS/comprehensive-codebase-analysis	Mehrere Sprachen	Allgemein verfügbar	Führen Sie eine gründliche statische Analyse einer Codebasis durch, um eine hierarchische Dokumentation mit Querverweisen zu erstellen, die Verhalten analysiert, Architektur dokumentiert und Business Intelligence

Transformation	Sprache//Stack	Status	Description
			nce kombiniert, wobei der Schwerpunkt auf Erkenntnissen über technische Schulden liegt.
AWS/agentic-readiness-analysis	Mehrere Sprachen	Frühzeitiger Zugriff	Beurteilen Sie, ob Systeme bereit sind, sicher von KI-Agenten aufgerufen zu werden. Dabei geht es um APIs, Identität, Statusmanagement, menschliches Eingreifen und Beobachtbarkeit.
AWS/modernization-readiness-analysis	Mehrere Sprachen	Frühzeitiger Zugriff	Scannen Sie Portfolios auf Cloud-native Reifeglücken und ordnen Sie die Ergebnisse den AWS Modernisierungspfaden zu.

Transformation	Sprache//Stack	Status	Description
AWS/portfolio-agentic-readiness-analysis	Portfolio	Frühzeitiger Zugriff	Sammeln Sie Berichte zur individuellen Eignungsanalyse für ein Anwendungsportfolio, um übergreifende Hindernisse, gemeinsame Behebungsmuster und priorisierte Empfehlungen zu identifizieren.
AWS/portfolio-modernization-readiness-analysis	Portfolio	Frühzeitiger Zugriff	Fassen Sie einzelne Berichte zur Modernisierungsanalyse für ein Portfolio zusammen und erstellen Sie eine konsolidierte Roadmap mit priorisierten Migrationswellen und empfohlenen Modernisierungspfaden.

Transformation	Sprache//Stack	Status	Description
AWS/business-rules-extraction	Mehrere Sprachen	Frühzeitiger Zugriff	Bei dieser Transformation wird eine monolithische Codebasis statisch analysiert, um eine Dokumentation zu erstellen, die erneut geschrieben werden kann, ohne dass ein Build, ein Run oder Änderungen am Quellcode erforderlich sind. Dabei wird das System in begrenzte Domänen zerlegt und die Geschäftsregeln, Workflows, bereichsübergreifende Anliegen und die Datenbankstruktur für jede Domäne extrahiert. Das Ergebnis umfasst ein maschinenlesbares Manifest, ein interaktives Dashboard und sprachneutrale Implementierungsspezifikationen pro Domain, die als Leitfaden für Modernisierungen oder vollständige

Transformation	Sprache//Stack	Status	Description
			Neufassungen dienen.

Anpassen AWS-Verwaltete Transformationen

Sie können AWS-verwaltete Transformationen an die spezifischen Anforderungen Ihres Unternehmens anpassen, indem Sie über den Konfigurationsparameter zusätzlichen Kontext bereitstellen. `additionalPlanContext`

Beispiel: Anpassen des Java-Versionsupgrades

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-version-upgrade
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Update all internal library dependencies to versions compatible with Java 17.
  Ensure compatibility with our custom authentication framework.
```

Beispiel: Anpassen AWS der SDK-Migration

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-aws-sdk-v1-to-v2
buildCommand: gradle build
additionalPlanContext: |
  Maintain our existing error handling patterns.
  Use our organization's standard credential provider chain.
  Update logging to use our internal logging framework.
```

Häufige Anwendungsfälle

Dieser Abschnitt enthält schrittweise Anleitungen für gängige Transformationsszenarien mit der AWS Transform CLI.

Lambda-Runtime-Upgrades

Lambda verbietet regelmäßig ältere Sprachlaufzeiten, sodass Teams ihre Lambda-Funktionen auf unterstützte Versionen aktualisieren müssen. AWS Transform custom kann diese Upgrades

mithilfe der von -verwalteten Sprachversions-Upgrade-Transformationen automatisieren. AWS Um beispielsweise eine in Python 3.9 geschriebene Lambda-Funktion auf Python 3.13 zu aktualisieren, würden Sie die `AWS/python-version-upgrade` Transformation verwenden. Ähnliche Transformationen sind für Java (`AWS/java-version-upgrade`) und Node.js (`AWS/nodejs-version-upgrade`) verfügbar und decken die gängigsten Lambda-Laufzeitsprachen ab.

Um eine einzelne Lambda-Funktion interaktiv zu aktualisieren, navigieren Sie zum Stammverzeichnis des Quell-Repositorys Ihrer Funktion und starten Sie die AWS Transform-CLI mit. `atx` Beschreiben Sie in der interaktiven Sitzung das Upgrade, das Sie benötigen — zum Beispiel „Aktualisieren Sie diese Lambda-Funktion von Python 3.9 auf Python 3.13“. Der Agent wählt die entsprechende AWS verwaltete Transformation aus, analysiert Ihren Code, aktualisiert die Sprachsyntax, passt Abhängigkeiten an und modernisiert veraltete API-Aufrufe. Sie können einen Build- oder Validierungsbefehl wie `pytest` oder angeben, `python -m py_compile *.py` damit der Agent überprüfen kann, ob der transformierte Code kompiliert und Tests bestanden hat. Während der gesamten interaktiven Sitzung können Sie die vom Agenten vorgeschlagenen Änderungen überprüfen, Feedback geben und Anpassungen anfordern, bevor Sie das Endergebnis akzeptieren.

Wenn Sie Lambda-Laufzeiten für viele Repositorys aktualisieren müssen, verwenden Sie den nicht-interaktiven Modus, um Transformationen in großem Umfang auszuführen. Rufen Sie für jedes Repository die CLI mit den entsprechenden Flags auf, um sie ohne Benutzereingabe auszuführen. Um beispielsweise eine Node.js 16-Lambda-Funktion auf Node.js 22 zu aktualisieren:

```
atx custom def exec \  
  -n AWS/nodejs-version-upgrade \  
  -p ./my-lambda-repo \  
  -c "npm test" \  
  -g "additionalPlanContext='Upgrade from Node.js 16 to Node.js 22'" \  
  -x -t
```

Das `-x` Flag führt die Transformation nicht interaktiv aus und `-t` vertraut allen Werkzeugausführungen, sodass keine Eingabeaufforderungen erforderlich sind. Sie können diesen Befehl mithilfe einer einfachen Shell-Schleife in Dutzenden oder Hunderten von Repositorys skriptweise ausführen. Überprüfen Sie nach Abschluss jeder Transformation den Git-Diff, um die Änderungen zu überprüfen, und führen Sie Ihre Testsuite aus, um sicherzustellen, dass die aktualisierte Funktion ordnungsgemäß funktioniert. Sie können AWS Transform Custom auch in Ihre CI/CD Pipeline integrieren, um veraltete Lambda-Funktionen kontinuierlich zu identifizieren. Mit diesem Ansatz wird nicht nur das unmittelbare Problem veralteter Laufzeiten behoben, sondern es

wird auch ein kontinuierlicher Prozess zur Erkennung und Aktualisierung von Funktionen eingerichtet, bevor sie den Support-Status erreichen.

Teams auf zentralen Plattformen können über die [AWS Transform-Webanwendung](#) Kampagnen erstellen, um die Transformation zu definieren, Lambda-Ziel-Repositorys festzulegen und den Fortschritt im gesamten Unternehmen zu verfolgen. Eine ausführliche Anleitung zum Aufbau einer skalierbaren Bereitstellungslösung in Produktionsqualität mithilfe von AWS Batch finden Sie unter [Erstellen einer skalierbaren Code-Modernisierungslösung](#) mit Transform custom. AWS

AWS Transform benutzerdefinierte Endpunkte und Schnittstellenendpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und einer AWS Transform benutzerdefinierten Verbindung herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellen-Endpunkte basieren auf einer Technologie [AWS PrivateLink](#), die es Ihnen ermöglicht, privat auf AWS Transform benutzerdefinierte Dienste zuzugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung zu benötigen. Direct Connect Der Datenverkehr zwischen Ihrer VPC und AWS Transform Custom verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere [Elastic-Netzwerk-Schnittstellen](#) in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter [Schnittstellen-VPC-Endpunkte \(AWS PrivateLink\)](#) im Amazon-VPC-Benutzerhandbuch.

Note

- Sie müssen die AWS PrivateLink Integration für Amazon S3 aktivieren, da AWS Transform Custom S3-API-Aufrufe durchführt. Eine ausführliche Anleitung finden Sie in der [AWS PrivateLink Amazon S3 S3-Dokumentation](#). Wenn Sie bei der Verwendung von AWS Transform Custom auf Probleme mit dem S3-Zugriff stoßen, lesen Sie unsere [Anleitung zur Fehlerbehebung](#).
- Wenn Sie die Funktion AWS PrivateLink Private DNS nicht verwenden (siehe [Privates DNS](#)), müssen Sie:
 - Routing zu VPC-Schnittstellenendpunkten konfigurieren (siehe Dokumentation [Routing zu VPC-Schnittstellenendpunkten](#))

- Legen Sie die `ATX_CUSTOM_ENDPOINT` Umgebungsvariable fest, um Ihre benutzerdefinierte Domäne anzugeben, zum Beispiel:

```
ATX_CUSTOM_ENDPOINT=https://transform-custom.<region>.api.aws atx
```

Überlegungen zu AWS Transform benutzerdefinierte VPC-Endpunkte

Bevor Sie einen VPC-Endpunkt für eine AWS Transform benutzerdefinierte Schnittstelle einrichten, sollten Sie die [Eigenschaften und Einschränkungen der Schnittstellen-Endpunkte](#) im Amazon VPC-Benutzerhandbuch lesen.

AWS Transform custom unterstützt das Aufrufen all seiner API-Aktionen über den Schnittstellenendpunkt.

Voraussetzungen

Beginnen Sie mit den nachstehenden Schritten erst, wenn Folgendes vorliegt:

- Ein AWS Konto mit entsprechenden Berechtigungen zum Erstellen und Konfigurieren von Ressourcen.
- Eine VPC wurde bereits in Ihrem AWS Konto erstellt.
- Vertrautheit mit AWS Services, insbesondere Amazon VPC und AWS Transform Custom.

Erstellen eines Schnittstellen-VPC-Endpunkts für AWS Transform benutzerdefiniert

Sie können einen VPC-Endpunkt für den AWS Transform benutzerdefinierten Service entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter [Erstellung eines Schnittstellenendpunkts](#) im Benutzerhandbuch für Amazon VPC.

Erstellen Sie mit diesem Dienstenamen die folgenden VPC-Endpoints für AWS Transform benutzerdefinierte Zwecke:

- `com.amazonaws. region.transform-benutzerdefiniert`

region Ersetzen Sie es durch AWS Region, in der Sie die AWS Transform benutzerdefinierte CLI verwenden möchten, z. B. com.amazonaws.us-east-1.transform-custom.

Weitere Informationen finden Sie unter [Zugriff auf einen Service über einen Schnittstellenendpunkt](#) im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für AWS Transform benutzerdefiniert

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf AWS Transform benutzerdefinierte Endpunkte steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für AWS Transform Benutzerdefinierte Aktionen

Im Folgenden finden Sie ein Beispiel für eine AWS Transform benutzerdefinierte Endpunktrichtlinie. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten AWS Transform benutzerdefinierten Aktionen.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "transform-custom:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Verwenden eines lokalen Computers zum Herstellen einer Verbindung zu einem AWS Transform Benutzerdefinierter Endpunkt

In diesem Abschnitt wird beschrieben, wie Sie einen lokalen Computer verwenden, um über einen AWS PrivateLink Endpunkt in Ihrer AWS VPC eine Verbindung zu einem AWS Transform benutzerdefinierten Computer herzustellen.

1. [Stellen Sie eine VPN-Verbindung zwischen Ihrem lokalen Gerät und Ihrer VPC her.](#)
2. [Erstellen Sie einen VPC-Endpunkt für eine AWS Transform benutzerdefinierte Schnittstelle.](#)
3. [Richten Sie einen eingehenden Endpunkt von Amazon Route 53 ein.](#) Auf diese Weise können Sie den DNS-Namen Ihres AWS Transform benutzerdefinierten Endpunkts von Ihrem lokalen Gerät aus verwenden.

Fehlerbehebung

Dieser Abschnitt enthält Anleitungen zur Behebung häufiger Probleme mit Transform custom. AWS

Speicherorte protokollieren

AWS Transform CLI verwaltet Protokolle an den folgenden Orten:

Konversationsprotokolle:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

Diese Protokolle enthalten den vollständigen Konversationsverlauf zum Debuggen bestimmter Transformationsausführungen.

Subagent-Protokolle:

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

Diese Protokolle enthalten Ausgaben von Subagenten, die der Haupt-Agent bei Transformationen erzeugt. Sie müssen Subagenten nicht direkt verwalten.

Debug-Protokolle für Entwickler:

Linux and macOS

```
~/.aws/atx/logs/debug*.log  
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\aws\atx\logs\debug*.log  
%USERPROFILE%\aws\atx\logs\error.log
```

Diese Protokolle enthalten detaillierte Informationen zu CLI-Vorgängen und Fehlern. Jede Protokolldatei hat ein Limit von 5 MB, bevor sie übertragen wird. In diesem Verzeichnis befinden sich möglicherweise mehrere Debug-Protokolle, z. B. debug1.log und debug2.log.

Häufige Fehler

Probleme bei der Installation:

Falls die Installation fehlschlägt, stellen Sie sicher, dass Node.js 22 oder höher installiert sind:

```
node --version
```

Laden Sie bei <https://nodejs.org/en/download> Bedarf Node.js von herunter.

Probleme mit der Authentifizierung:

Stellen Sie sicher, dass Ihre AWS Anmeldeinformationen korrekt konfiguriert sind:


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

Stellen Sie sicher, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle über die erforderlichen `transform-custom:*` Berechtigungen verfügt.

Probleme mit der Netzwerkverbindung:

Wenn Verbindungsfehler auftreten, überprüfen Sie den Netzwerkzugriff auf die erforderlichen Endpunkte:

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

Wenn Sie in einer Umgebung mit eingeschränktem Internetzugriff arbeiten, aktualisieren Sie die Firewallregeln, um diese URLs auf die Zulassungsliste zu setzen.

Probleme mit der Konfiguration der Region:

Wenn Sie auf regionsbezogene Fehler stoßen:

- Stellen Sie sicher, dass Ihre Region unterstützt wird
- Suchen Sie nach Umgebungsvariablen, die Ihre Konfiguration überschreiben könnten: `echo $AWS_REGION $AWS_DEFAULT_REGION`
- Überprüfen Sie die Konfiguration Ihrer Region: `aws configure get region`
- Aktualisieren Sie bei Bedarf Ihre Region: `aws configure set region <your-region>`
- Einzelheiten zur Auflösung der Region finden Sie in den Debug-Protokollen

Probleme mit Git:

Stelle sicher, dass Git installiert ist und dein Repository unter der Git-Quellcodeverwaltung steht:

```
git --version  
git status
```

AWS Für Transform Custom müssen sich die Repositories unter der Git-Quellcodeverwaltung befinden.

Probleme bei der Ausführung der Transformation:

Wenn eine Transformation fehlschlägt:

1. Überprüfen Sie die Konversationsprotokolle unter `~/.aws/atx/custom/<conversation_id>/logs/`
2. Suchen Sie in der Transformationsausgabe nach Build- oder Testfehlern
3. Stellen Sie sicher, dass der Build-Befehl für Ihr Projekt korrekt ist
4. Versuchen Sie, die Transformation im interaktiven Modus auszuführen, um Feedback zu geben

Probleme bei der Wiederaufnahme der Konversation:

Wenn Sie eine Konversation nicht fortsetzen können:

- Stellen Sie sicher, dass die Konversation weniger als 30 Tage alt ist
- Vergewissern Sie sich, dass die Konversations-ID korrekt ist
- Stellen Sie sicher, dass Sie über eine Netzwerkverbindung verfügen

Supportanfragen

Weitere Unterstützung erhalten Sie über die [AWS Konsole](#) unter AWS Support.

Wenn Sie ein Support-Ticket öffnen, geben Sie Folgendes an:

- Konversationsprotokolle von `~/.aws/atx/custom/<conversation_id>/logs/`
- Der Subagent protokolliert von `~/.aws/atx/custom/<conversation_id>/logs/subagents/`
- Debug-Protokolle von `~/.aws/atx/logs/`
- Schritte, um das Problem zu reproduzieren
- AWS CLI-Version transformieren (`atx --version`)

Probleme mit dem S3-Zugriff

Der benutzerdefinierte AWS Transform-Dienst stellt vorsignierte S3-URLs zur Verfügung, um das Hoch- und Herunterladen der potenziell großen Client-Computer mit Transformationsdateien to/

from zu erleichtern. Das bedeutet, dass die CLI nicht nur mit den AWS Transform-Dienstendpunkten interagiert, sondern auch mit den S3-Dienstendpunkten. Diese Interaktionen verwenden vorsignierte URLs, sodass für die IAM-Anmeldeinformationen Ihres Kunden keine S3-Berechtigungen erforderlich sind. Manchmal können jedoch die Proxy-Serverkonfigurationen Ihres lokalen Computers und die S3-VPC-Endpunktrichtlinien Ihres Netzwerks diesen Datenverkehr einschränken.

Bitte schauen Sie sich die [the section called "Speicherorte protokollieren"](#) detaillierteren Fehlermeldungen an, um die Ursache von Toolfehlern oder verweigerten S3-Zugriffen im Zusammenhang mit dem Herunterladen und Hochladen von Transformationsdateien zu ermitteln.

Wenn Sie einen VPN/Proxy Server verwenden, der die Umgebungsvariablen `https_proxy` und die `no_proxy` Umgebungsvariablen nutzt, sollten Sie erwägen, Ihrem `no_proxy` Umgebungsvariablenwert die folgenden Werte hinzuzufügen, um beispielsweise den Proxy für die benutzerdefinierten Dienstendpunkte S3 und AWS Transform zu umgehen:

Linux and macOS

```
export no_proxy=.s3.amazonaws.com,transform-custom.<region>.api.aws
```

Windows (PowerShell)

```
$env:no_proxy=".s3.amazonaws.com,transform-custom.<region>.api.aws"
```

Wenn Sie eine [AWS PrivateLink für Amazon S3](#) in Ihrer VPC verwenden, ist für diese möglicherweise eine Richtlinie zur Einschränkung des S3-Datenverkehrs definiert. Bitte stellen Sie sicher, dass Ihre S3-VPC-Endpunktrichtlinie die Buckets im Besitz von AWS Transform Custom Service zulässt `GetObject` und `PutObject` für sie funktioniert. Dies kann erreicht werden, indem Sie Ihrer VPC-Endpunktrichtlinie die folgende Anweisung hinzufügen:

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": ["s3:PutObject", "s3:GetObject"],
  "Resource": "arn:aws:s3::aws-transform-custom-*/*"
}
```

Explizite Deny Aussagen in Richtlinien haben Vorrang Allow vor Aussagen. Suchen Sie in den S3 VPC-Endpunktrichtlinien nach Deny Aussagen, die den Zugriff einschränken könnten.

AWS Versionsgeschichte von Transform CLI

In der folgenden Tabelle finden Sie Einzelheiten zu aktuellen und früheren Versionen der AWS Transform CLI. Die Tabelle enthält die Version, das Veröffentlichungsdatum und die Versionshinweise für jede Version.

Version	Datum der Veröffentlichung	Versionshinweise
3.6.0 (aktuell)	17. Juli 2026	- Der <code>atx custom def learnings</code> Unterbefehl wurde hinzugefügt, mit dem eine interaktive TUI-Sitzung geöffnet wird, in der die automatisch für eine Transformationsdefinition auf der Grundlage früherer Läufe generierten Erkenntnisse angezeigt und verwaltet werden können. - Die Erfassung der Nutzungstelemetrie während der Ausführung der Transformation wurde hinzugefügt. Um Telemetrie zu deaktivieren, legen Sie die <code>ATX_DISABLE_TELEMETRY=true</code> Umgebungsvariable fest. Weitere Informationen finden Sie unter Nutzung Telemetrie. - Es wurde ein Problem unter Windows behoben, bei dem Dateioperationen, die Pfade <code>~</code> (Stammverzeichnis) verwendeten, in ein unerwartetes Verzeichnis verschoben wurden. Dies führte zu read/write Dateifehlern während einer Sitzung. - Es wurde ein Problem behoben, bei dem MCP-Server- und Toolnamen, die Sonderzeichen enthielten, zu Verbindungsfehlern führen konnten. Die CLI bereinigt Namen jetzt automatisch, sodass sie nur gültige Zeichen verwenden.
3.5.0	8. Juli 2026	- Native Windows-Unterstützung hinzugefügt. Sie können die AWS Transform Custom-Befehle jetzt direkt unter Windows ausführen. (Die <code>atx ct</code> Befehle werden unter Windows noch nicht unterstützt) - Es wurden Steuerungseingaben hinzugefügt, <code>atx ct analysis run</code> sodass die Analysen zur Bereitschaft von Agenturen und zur Modernisierung Ihre Präferenzen

Version	Datum der Veröffentlichung	Versionshinweise
		widerspiegeln. Verwenden Sie diese <code>--context</code> Option für die strategische Gestaltung, <code>--agent-scope</code> um den Agentenzugriff auf die Bereitschaft der Agenten festzulegen und <code>--prefer/</code>, um Modernisierungsempfehlungen auf bestimmte Technologien auszurichten oder von ihnen <code>--avoid</code> abzuwenden. - Transformationsdefinitionen im Skill-Format können jetzt einen <code>scripts/</code> Ordner enthalten, sodass Sie Hilfsskripte zusammen mit Ihren Referenzen bündeln können. <code>SKILL.md</code> - Hinzugefügt <code>--wait</code> zu <code>atx ct remediation create</code>, der wartet, bis die Behebung abgeschlossen ist. - Headless-Modus für One-Shot-Ausführung hinzugefügt. Führen Sie <code>atx -x "prompt" -t</code> den Befehl aus, um eine Eingabeaufforderung zu übergeben, eine Antwort zu erhalten und den Vorgang ohne interaktive Eingabeaufforderungen zu beenden. Im Headless-Modus müssen Sie allen Tools vertrauen.
3.4.1	2. Juli 2026	Es wurde ein Problem mit interaktiven Sitzungen behoben, das mit Version 3.4.0 eingeführt wurde. Nachdem der Agent nicht mehr reagiert hat, bleibt die CLI möglicherweise bei der Eingabeaufforderung „Denken“ (in der Benutzeroberfläche mit einem Auslassungszeichen gekennzeichnet), anstatt zur Eingabeaufforderung zurückzukehren. Die CLI bringt Sie jetzt nach jeder Antwort zur Eingabeaufforderung zurück.

Version	Datum der Veröffentlichung	Versionshinweise
3.4.0 (nicht empfohlen)	29. Juni 2026	 Bekanntes Problem In interaktiven Sitzungen bleibt die CLI möglicherweise auf der Eingabeaufforderung „Thinking“ (in der Benutzeroberfläche mit einem Auslassungszeichen gekennzeichnet), nachdem der Agent nicht mehr reagiert hat. Dadurch können Sie Ihre nächste Nachricht nicht eingeben. Um dieses Problem zu beheben, führen Sie ein Upgrade auf Version 3.4.1 oder höher durch, indem Sie Folgendes ausführen: <pre>atx update</pre> • Es wurde <code>atx ct schema</code> ein maschinenlesbares Manifest der vollständigen <code>atx ct</code> Befehlsoberfläche für Skripting und Automatisierung hinzugefügt. • Es wurde eine Überprüfung des Token-Gültigkeitsbereichs hinzugefügt, wenn Sie eine Quelle hinzufügen oder aktualisieren, wodurch Probleme mit Anmeldeinformationen oder Berechtigungen sofort auftauchen, anstatt sie später bei der Analyse fehlschlagen zu lassen. • Pull Requests zur automatischen Problembehebung wurden verbessert, sodass nun auch der Kontext gefunden werden kann und der Entwurfsmodus für besser überprüfbare PRs unterstützt wird. • Verbessertes CLI-Fortschrittsfeedback mit Echtzeitkontext über die aktuelle Aktivität, die geschätzten Agentenminuten und die Aktivität der Unteragenten. • Die konfigurierbare Identität des Checkpoint-Commit-Autors wurde über die Umgebungsvariablen <code>ATX_GIT_COMMITTER_NAME</code> und die <code>ATX_GIT_COMMITTER_EMAIL</code> Umgebungsvariablen hinzugefügt.

Version	Datum der Veröffentlichung	Versionshinweise
		• Verschiedene kleine Bugfixes und Verbesserungen.
3.3.0	18. Juni 2026	• Konsistente <code>--json</code> und befehlübergreifende <code>--help</code> Unterstützung hinzugefügt <code>atx ct</code>. • Das Setup des Security Agents wurde behoben, sodass der Agent-Bereich während der Installation erstellt und beim Teardown entfernt wird. • Verschiedene kleine Bugfixes und Verbesserungen.
3.2.0	15. Juni 2026	• Befehle zur kontinuierlichen Modernisierung (<code>atx ct</code>) zur Standard-CLI-Distribution für alle Benutzer hinzugefügt. • Die Ausführung von Sub-Agenten wurde verbessert, sodass beim Warten auf Serverantworten ein Zahlenauswahlfeld mit der Meldung „Denke...“ angezeigt wird, was ein klares visuelles Feedback darüber bietet, dass gerade gearbeitet wird. • Der Spinner wurde dahingehend verbessert, dass er nach 3 Sekunden Pause nach der Agentenausgabe automatisch mit der Meldung „Working on it...“ neu gestartet wird, sodass das Terminal zwischen den einzelnen Verarbeitungsschritten nie eingefroren erscheint. • Verbesserter Denk-Spinner mit einer subtilen Schimmeranimation für ein ausgefeilteres visuelles Erscheinungsbild.

Version	Datum der Veröffentlichung	Versionshinweise
3.1.0	3. Juni 2026	• <code>ATX_MAX_VALIDATION_LOOPS</code> Umgebungsvariable hinzugefügt, um maximale Validierungsschleifen zu konfigurieren. • Problem behoben: Bei der Suche nach Updates werden nun keine falschen Warnungen mehr angezeigt, dass „Update verfügbar“ angezeigt wird, wenn die installierte Version bereits neuer als die Registrierungsversion ist. • Behobendelete <code>--transformation-name ""</code> : Es wird keine unsinnige Bestätigungsaufforderung mehr angezeigt. Leere Werte werden jetzt mit einem eindeutigen Validierungsfehler zurückgewiesen. • Behoben: Unbekannte Unterbefehle zeigen jetzt „unbekannter Befehl“ statt einer verwirrenden internen Fehlermeldung an. • Der Versionsvergleich wurde behoben, sodass bei Aktualisierungsprüfungen ein numerischer Vergleich anstelle von Zeichenkettenungleichheit verwendet wird.

Version	Datum der Veröffentlichung	Versionshinweise
3.0.0	21. Mai 2026	• Es wurde eine Überprüfung von Transformationsnamen vor dem Flug hinzugefügt, die ähnliche Namen aus Ihrer Registrierung vorschlägt, wenn ein Name nicht gefunden wird, sodass Tippfehler erkannt werden können, ohne dass ein separater Listenbefehl erforderlich ist. • Es wurden optionale Erklärungen für Shell-Befehle hinzugefügt, die zeigen, was sie tun und warum. • Das Banner mit den Vertrauenseinstellungen wurde verbessert und enthält nun mehr Informationen zu Toolberechtigungen. • Es wurde ein Banner mit der Option „Lernen deaktiviert“ hinzugefügt, wenn die Flagge „Nicht lernen“ verwendet wird. Dadurch wird die Lernfunktion besser sichtbar gemacht und erklärt, wie sie aktiviert werden kann. • Breaking Change: Node.js 22 oder später ist jetzt erforderlich. Führen Sie ein Upgrade von durch, https://nodejs.org/ wenn Sie eine ältere Version verwenden.

Version	Datum der Veröffentlichung	Versionshinweise
2.0.0	14. Mai 2026	• Unterstützung für Remote-MCP-Server hinzugefügt — Verbindung zu HTTP- und HTTPS-MCP-Servern mit automatischem SSE-Fallback, Bearer-Token-Authentifizierung mit Erweiterung der Umgebungsvariablen in Headern und Proxyunterstützung (). HTTP_PROXY/HTTPS_PROXY • Unterbefehl als Alias für hinzugefügt <code>atx resume. atx -- resume</code> • <code>grepTool</code> für die Textsuche in mehreren Dateien mit Ausgabesteuerung hinzugefügt — unterstützt Regex-Muster, Filter-Glob-Filterung, Suche ohne Berücksichtigung von Groß- und Kleinschreibung, konfigurierbare Grenzwerte und Kürzung der Ausgabe. <code>depth/result</code> • Verbesserte MCP-Implementierung zur Verwendung des Standard-MCP-SDK für konsistenteres Verhalten und einfachere Unterstützung future MCP-Funktionen. • Verbesserte Handhabung von Shell-Ausgaben — Die Ausgabe wird jetzt elegant auf 30.000 Zeichen pro Stream gekürzt, anstatt einen schwerwiegenden Fehler zu verursachen, wobei der Anfang und das Ende der Ausgabe für den Kontext beibehalten werden. • Es wurde ein Problem behoben, bei dem Strg+C während einer interaktiven Sitzung die CLI vorzeitig beenden konnte, Linux/macOS anstatt den aktuellen Vorgang abzubrechen und zur Eingabeaufforderung zurückzukehren. • Die Meldung „Vertrauensabweisung“ wurde behoben und zeigt nun einen speziellen Grund an, warum Vertrauen nicht verfügbar ist, unabhängig davon, warum für den Befehl eine Autorisierung erforderlich war. • Die Warnung vor gefährlichen Befehlen wurde behoben, in <code>alwaysPromptCommands</code> der nicht mehr erwähnt wurde, dass der Befehl als vertrauenswürdig eingestuft wurde.

Version	Datum der Veröffentlichung	Versionshinweise
1.10.0	29. April 2026	• Verbesserte Werkzeugbeschreibungen mit toolübergreifender Anleitung, sodass der Agent für jede Aufgabe das beste Tool auswählen kann und die unnötige Nutzung von Shells reduziert wird. • Hinzugefügt <code>alwaysPromptCommands</code> in <code>trust-settings.yaml</code> — Konfiguration von Shell-Befehlsmustern, für die unabhängig von den Vertrauenseinstellungen immer eine ausdrückliche Genehmigung erforderlich ist. Unterstützt Glob-Platzhalter und passt jeden Unterbefehl in zusammengesetzten Ausdrücken an. <code>trustedShellCommands</code> kann diese Muster überschreiben. Wird im nicht interaktiven Modus nicht erzwungen, um zu verhindern, dass automatische Pipelines beschädigt werden. • Problem behoben, bei dem relative Pfade nicht in absolute Pfade aufgelöst wurden.
1.9.0	23. April 2026	• Verbesserte Aufforderungen zur Genehmigung von Tools — für jede Option wird nun direkt angezeigt, was sie bewirkt, eine „Warum“-Meldung erklärt, warum eine Genehmigung erforderlich ist, und die Vertrauensbestätigung enthält einen Hinweis <code>trust-settings.yaml</code> darauf, dass Sie dauerhaft vertrauen können.
1.8.0	16. April 2026	• Das Präfix <code>ATX:</code> für die Agentenausgabe wurde von <code>></code> bis geändert, um eine klarere visuelle Unterscheidung zwischen Benutzereingaben und Agentenausgaben zu ermöglichen. • Die Anzeige des Resume-Befehls, wenn die CLI-Wiederholungsversuche erschöpft sind, wurde behoben. • Fehler beim Wiederaufnehmen aus einem anderen Arbeitsverzeichnis behoben. Fordert im interaktiven Modus zur Eingabe eines korrigierten Pfads auf, schlägt im nicht interaktiven Modus schnell mit einem beschreibenden Fehler fehl.

Version	Datum der Veröffentlichung	Versionshinweise
1.7.1	9. April 2026	• Ein SSO-Anmeldefehler („Sitzungstoken wurde nicht gefunden oder ist ungültig“) behoben, wenn sich die Region des Anmeldeinformationsanbieters von der Region des Profils unterscheidet. <code>sso_region</code> • Das Zwischenspeichern von Anmeldeinformationen wurde behoben, sodass Sitzungen mit langer Laufzeit nicht mehr fehlschlagen, wenn die Anmeldeinformationen auf der Festplatte rotiert werden.
1.7.0	2. April 2026	• Der <code>exec</code> Befehl, bei Eingabevalidierungsfehlern mit Code 1 zu beenden, wurde behoben, sodass die CLI in Skripten und CI/CD Pipelines zuverlässig ist. • Anzeige von Warnmeldungen des Dienstes hinzugefügt. • Unterstützung für MFA-Eingabeaufforderungen für AWS Anmeldeinformationsprofile hinzugefügt. • Fehler behoben, bei denen STS-Anmeldeinformationen aufgerufen wurden, um die HTTP (S) -Proxyeinstellungen zu respektieren.
1.6.0	18. März 2026	• <code>--limit <minutes></code> Option hinzugefügt, um ein Budget für Agentenminuten <code>exec</code> und <code>interactive</code> Befehle festzulegen. Wenn das Limit erreicht ist, zeigt die CLI die Nutzung an und beendet das Programm mit Anweisungen zur Wiederaufnahme. • Die Protokollierung der ersten Benutzernachricht in Konversationsprotokollen wurde behoben.

Version	Datum der Veröffentlichung	Versionshinweise
1.5.0	11. März 2026	• Unterstützung für die gleichzeitige Ausführung von Aufgaben hinzugefügt, was schnellere Transformationen ermöglicht. • Es wurden am Ende jeder Konversation eine Anzeige für die Nutzung von Agentenminuten und ein <code>/usage</code> Befehl im interaktiven Modus hinzugefügt, mit dem die Nutzung jederzeit überprüft werden kann.
1.4.0	2. März 2026	• Verbesserte Fehlermeldungen beim Speichern von Transformationsdefinitionen mit nicht unterstützten Dateien. • Es wurde ein Timeout für Serviceaufrufen hinzugefügt, um zu verhindern, dass die CLI hängen bleibt, wenn die Verbindung unterbrochen wird. • Fehler behoben, bei dem der CLI-Prozess nach erfolgreichem Abschluss hängen blieb. • Die Regionsüberprüfung bei der Wiederaufnahme von Konversationen wurde behoben.
1.3.0	19. Februar 2026	• Die Beschränkung für MCP-Serverpfade wurde aufgehoben — Benutzer können jetzt einen beliebigen Pfad für die <code>command</code> Eigenschaft in der MCP-Konfiguration angeben. • Verbesserte Stabilität der MCP-Serververbindungen.
1.2.0	9. Februar 2026	• Unterstützung für die Proxykonfiguration über Umgebungsvariablen (<code>https_proxy</code> <code>no_proxy</code>, usw.) wurde hinzugefügt. • Allgemeine Stabilitätsverbesserungen und Fehlerkorrekturen.
1.1.1	16. Januar 2026	Fehlerbehebungen und Stabilitätsverbesserungen.

Version	Datum der Veröffentlichung	Versionshinweise
1.1.0	13. Januar 2026	Unterstützung für die AWS CLI-Regionskonfiguration, frühzeitige Überprüfung der Anmeldeinformationen und verbesserte Funktionalität zur Wiederaufnahme von Kampagnen hinzugefügt.
1.0.1	18. Dezember 2025	Reibungsloses Herunterfahren, übersichtlichere Fehlerprotokolle und allgemeine Verbesserungen.
1.0.0	1. Dezember 2025	Erste Version der AWS Transform CLI.

AWS Transformieren Sie die kontinuierliche Modernisierung

Was ist AWS Kontinuierliche Modernisierung transformieren?

AWS Transform Continuous Modernization bietet Analysen und Problembehebungen für Ihre Quellcode-Repositorys. Du kannst GitHub Organisationen, GitLab Gruppen, Bitbucket-Workspaces und lokale Repositorys miteinander verbinden und dann automatisierte Analysen durchführen, um technische Probleme, Sicherheitslücken, Modernisierungsmöglichkeiten und die Bereitschaft der Agenten in deiner gesamten Codebasis zu identifizieren.

Sämtliche Analysen und Problembehebungen werden von dir aus mit deinen Zugangsdaten ausgeführt. AWS-Konto Ihr Quellcode bleibt unter Ihrer Kontrolle.

Note

Wir empfehlen, mit dem Kiro Power- oder Agent-Plugin zu beginnen. Die Agentenkompetenz koordiniert die Einrichtung, das Onboarding und die kontinuierliche Nutzung der kontinuierlichen Modernisierung, einschließlich der Bereitstellung der Infrastruktur, der Konfiguration der Quellen, der Ausführung von Analysen, der Prüfung der Ergebnisse und der Problembehebung. Installationsanweisungen finden Sie unter [Entwicklertools](#).

Die wichtigsten Funktionen

AWS Die kontinuierliche Modernisierung von Transform bietet die folgenden Funktionen:

- **Tech Debt Analysis** — Durchsucht Repositorys nach veralteten Abhängigkeiten, Sicherheitslücken, Problemen mit der Codequalität und Modernisierungsmöglichkeiten. Führen Sie schnelle Metadatenscans für alle Paketmanifeste oder eine umfassende Analyse auf Codeebene durch. Definieren Sie benutzerdefinierte Analyse Kriterien mithilfe von Transformationsdefinitionen, die auf Ihre Umgebung zugeschnitten sind.
- **Autonome Problembehebung** — Generieren Sie validierte Pull-Requests in großem Umfang. Jeder Befund kann mithilfe der zugehörigen Transformationsdefinition automatisch korrigiert werden. Bei der Korrektur werden Verzweigungen erstellt und PRs/MRs automatisch in GitHub, GitLab, und Bitbucket geöffnet.

- **Berichterstattung** — Generieren Sie HTML-Berichte, in denen die Ergebnisse nach Schweregrad, Repository und Analysetyp aufgeführt sind. Verfolgen Sie den Fortschritt der Problembehebung und die Suche nach einer Lösung im Laufe der Zeit.
- **Kontinuierliche Überwachung** — Planen Sie wiederkehrende Analysen mit Amazon EventBridge Scheduler. Konfigurieren Sie tägliche, wöchentliche oder benutzerdefinierte Cron-Zeitpläne, um Ihr Portfolio kontinuierlich auf neue Probleme zu überwachen.

Arten von Analysen

AWS Transform Continuous Modernization unterstützt die folgenden Analysetypen, um Ihren Modernisierungsanforderungen gerecht zu werden.

Typ	Description
rapid-techdebt-analysis	Schnelles Scannen von Paketmanifesten (pom.xml, requirements.txt) ausschließlich auf Metadaten beschränkt package.json, um veraltete Versionen und veraltete Abhängigkeiten zu identifizieren. Analysiert den Quellcode nicht.
tech-debt-comprehensive	Umfassende technische Schuldenanalyse auf Codeebene mithilfe des AWS Transform -Agenten. Untersucht den Quellcode, um Schuldenmuster, Probleme mit der Codequalität, Architekturprobleme und Verbesserungsmöglichkeiten zu identifizieren.
security	Sicherheitslücken und CVE-Erkennung mithilfe des AWS Security Agents. Durchsucht Quellcode und Abhängigkeiten nach bekannten Sicherheitslücken, unsicheren Codierungsmustern und ausnutzbaren Schwachstellen. Erfordert eine einmalige Einrichtung der Infrastruktur.

Typ	Description
agentic-readiness	Bewertung der Eignung für KI- und Agentenintegration Es werden 56 Kriterien in fünf Kategorien bewertet: Infrastruktur und Plattform , Anwendungsarchitektur, Datengrundlagen sowie Betrieb und Beobachtbarkeit. Identity/ Security/Governance
modernization-readiness	Bewertung der Möglichkeiten zur Modernisierung der Cloud. Bewertet die Einsatzbereitschaft in allen Bereichen Infrastruktur, Anwendung, Daten, Sicherheit und Betrieb. Identifiziert Kandidaten für Containerisierung, serverlose Migration und Plattform-Upgrades.
custom	Führen Sie eine beliebige Transformationsdefinition (TD) als Analyse aus. Verwenden Sie diesen Typ, um Ihre eigenen Analysekriterien zu definieren oder AWS verwaltete Transformationen auszuführen, die nicht von den integrierten Typen abgedeckt werden.

Verständnis wichtiger Konzepte

Quellen

Aus einer Quelle geht hervor, wo sich Ihre Repositories im Rahmen der kontinuierlichen Modernisierung befinden. Unterstützte Quelltypen:

- GitHub— Organizations mit persönlichen Zugriffstoken (klassisch)
- GitLab— Gruppen oder Benutzer, einschließlich selbst gehosteter Instanzen
- Bitbucket — Workspaces (Cloud) oder Projekte (Rechenzentrum)
- Lokal — Übergeordnete Verzeichnisse, die Git-Repositories enthalten

Repositorien

Repositorien werden durch das Scannen von Quellen entdeckt. Nach der Erkennung können Sie nach Quelle, Labels oder anderen Kriterien filtern, Labels für die Organisation (Team, Priorität, Migrationswelle) anwenden und spezifische Repositorys zur Analyse oder Behebung gezielt auswählen.

Analysen

Eine Analyse ist ein Scan eines oder mehrerer Repositorys unter Verwendung eines bestimmten Analysetyps. Jede Analyse liefert Ergebnisse, die Probleme in Ihrem Code identifizieren. Sie können Analysen bei Bedarf ausführen oder sie so planen, dass sie automatisch ausgeführt werden. Zu den Analysetypen gehören Rapid-Tech-Debt-Analysis, Tech-Debt-Comprehensive, Security, Agentic-Readiness, Modernization-Readiness und Custom. Jede Analyse verfolgt ihren Status (ausstehend, läuft, abgeschlossen, storniert oder fehlgeschlagen) und die gescannten Repositorys.

Ergebnisse

Die Ergebnisse sind die Ergebnisse der Analyse. Jedes Ergebnis umfasst den Schweregrad (hoch, mittel oder niedrig), den Status (offen, verworfen oder veraltet) und die Korrekturtransformation, mit der das Problem behoben werden kann (sofern automatisch behoben werden kann). Neue Ergebnisse beginnen mit „offen“. Benutzer können Ergebnisse mit einem Grund verwerfen. Re-analysis markiert gelöste Ergebnisse automatisch als veraltet.

Abhilfemaßnahmen

Bei Abhilfemaßnahmen werden Transformationsdefinitionen angewendet, um die Ergebnisse zu korrigieren. Drei Modi: ergebnisbasiert (jedes Ergebnis verwendet seine eigene Korrekturtransformation), TD-Override (überschreibt die Transformationsdefinition für bestimmte Ergebnisse) und direktes TD (führt eine Transformation für ein Repository ohne Ergebnisse durch). Die Ausgabe hängt vom Quellanbieter ab (GitHub PR, GitLab MR, Bitbucket PR oder Local Branch).

Definitionen der Transformation

Eine Transformationsdefinition enthält die Anweisungen und das Wissen, die für die Durchführung einer bestimmten Codetransformation erforderlich sind. Bei der kontinuierlichen Modernisierung werden Transformationsdefinitionen für benutzerdefinierte Analysen (`--type custom --transformation-name name`) und Problembehebungen (`--transformation-name name`) verwendet. Listet die verfügbaren Transformationsdefinitionen mit `atx custom def list` auf.

Wie AWS Transformation: Kontinuierliche Modernisierung funktioniert

AWS Transform Continuous Modernization wird in der Regel bei Großprojekten eingesetzt, bei denen mehrere Codebasen kontinuierlich analysiert und behoben werden müssen. Teams folgen in der Regel diesem Arbeitsablauf:

1. Quellen Connect — Füge GitHub Organisationen, GitLab Gruppen, Bitbucket-Workspaces oder lokale Verzeichnisse als Quellen hinzu. Stelle Authentifizierungstoken mit entsprechenden Gültigkeitsbereichen bereit.
2. Repositorys entdecken — Führen Sie Discovery-Scans durch, um alle Repositorys in Ihren Quellen aufzulisten. Verwenden Sie Labels, um Repositorys nach Team, Priorität oder Migrationswelle zu organisieren.
3. Analyse ausführen — Führen Sie Analysen in Ihrem gesamten Portfolio durch. Wählen Sie schnelle Scans für schnelle Ergebnisse oder umfassende Analysen für detaillierte Ergebnisse. Die Sicherheitsanalyse erfordert eine einmalige Einrichtung der Infrastruktur.
4. Ergebnisse der Triage — Überprüfen Sie die Ergebnisse nach Schweregrad, Repository oder Analysetyp. Falsch positive Ergebnisse mit dokumentierten Gründen zurückweisen. Re-run Analyse, um gelöste Probleme als veraltet zu kennzeichnen.
5. Korrigieren — Erstellen Sie Abhilfemaßnahmen, um die Ergebnisse zu korrigieren. Durch die kontinuierliche Modernisierung werden automatisch Filialen erstellt und pull/merge Anfragen mit den Problembehebungen geöffnet. Verfolgen Sie den Status der Problembehebung und versuchen Sie, Fehler erneut zu versuchen.
6. Kontinuierliche Analyse einrichten — Planen Sie wiederkehrende Analysen mit Amazon EventBridge Scheduler. Konfigurieren Sie den Analyserhythmus (täglich, wöchentlich oder benutzerdefinierter Cron), um Ihr Portfolio kontinuierlich auf neue Probleme zu überprüfen. Kombinieren Sie es mit automatisierter Problembehebung, um die Integrität des Codes im Laufe der Zeit aufrechtzuerhalten.

Rechenoptionen

Die kontinuierliche Modernisierung unterstützt drei Rechenoptionen für die Durchführung von Analysen und Problembehebungen. Die Agentenfähigkeiten von Kiro Power und das Agenten-Plugin helfen Ihnen dabei, die Infrastruktur für jede Option einzurichten.

 Note

Unabhängig von der Rechenoption finden alle Analysen und Problembehebungen AWS-Konto unter Verwendung Ihrer Anmeldeinformationen statt. Ihr Quellcode bleibt unter Ihrer Kontrolle.

Lokal (Standard)

Standardmäßig werden Analysen auf Ihrem lokalen Computer ausgeführt. Für diese Option ist keine zusätzliche Infrastruktur erforderlich. Der Server wird lokal ausgeführt und führt Analysen mithilfe lokaler Rechenressourcen aus. Gut zum Ausprobieren des Tools, für kleine Repositorien oder für den individuellen Gebrauch.

Amazon Amazon EC2

Führen Sie Analysen auf einer persistenten Amazon EC2 EC2-Instance in Ihrem AWS-Konto aus. Diese Option entlastet Ihren lokalen Computer, unterstützt größere Analysen und ermöglicht wiederkehrende geplante Analysen. Die Instanz läuft auch zwischen den Einsendungen weiter.

Der Agenten-Skill stellt einen AWS CloudFormation Stack bereit, der Folgendes umfasst:

- Eine Amazon EC2 EC2-Instance (Amazon Linux 2023) mit Docker und dem Container für kontinuierliche Modernisierung
- Eine IAM-Rolle mit Berechtigungen für AWS Transform, Amazon S3, AWS KMS, Secrets Manager und den Security Agent
- AmazonSSMManagedInstanceCore für Shell-Zugriff über SSM (kein SSH-Schlüsselpaar oder eingehende Ports erforderlich)
- Eine Sicherheitsgruppe ohne Regeln für eingehenden Datenverkehr

Ihr IAM-Benutzer oder Ihre IAM-Rolle benötigt Berechtigungen für Amazon EC2 EC2-Lebenszyklusmanagement, AWS CloudFormation Stack-Operationen, IAM-Rollenerstellung, Amazon S3 S3-Bucket-Operationen, Secrets Manager Secret Management und SSM-Befehle.

Um die EC2-Ausführung einzurichten, installieren Sie das Kiro Power- oder Agent-Plugin (siehe [Entwicklertools](#)) und fragen Sie dann den Agenten: „Richten Sie eine EC2-Instance für die kontinuierliche Modernisierungsanalyse ein“. Der Agent stellt die Infrastruktur bereit, überprüft, ob der Container fehlerfrei ist, und übermittelt Ihre Analysen über SSM — SSH ist nicht erforderlich.

AWS Batch (Fargate)

Führen Sie Analysen als isolierte Jobs auf AWS Batch mit Fargate für serverloses Computing aus. Jede Analyse wird in einem eigenen Container ausgeführt, ohne dass eine persistente Infrastruktur verwaltet werden muss. Gut für die parallel Analyse mehrerer Quellen oder Analysetypen.

Bei dieser Option wird der AWS Transform-CDK-Infrastrukturstapel wiederverwendet. Der Agent-Skill stellt die erforderliche Infrastruktur bereit, einschließlich:

- AWS Batch-Job-Warteschlange und Rechenumgebung
- Jobdefinition mit dem Container-Image für kontinuierliche Modernisierung
- IAM-Rollen für die Ausführung von Batch-Jobs
- Eine Lambda-Funktion für die Einreichung von Jobs

Um die Batch-Ausführung einzurichten, installieren Sie das Kiro Power- oder Agent-Plugin (siehe [Entwicklertools](#)) und fragen Sie dann den Agenten: „Meine Analyse auf Fargate ausführen“ oder „Batch-Ausführung für kontinuierliche Modernisierung einrichten“. Der Agent stellt den CDK-Stack bereit, speichert Ihre Quellanmeldedaten in Secrets Manager und sendet Analyseaufträge an Batch. AWS

Einrichtung des Security Agents

Der `security` Analysetyp verwendet den AWS Security Agent-Dienst zur Erkennung von Sicherheitslücken und CVE. Im Gegensatz zu anderen Analysetypen erfordert er eine einmalige Einrichtung der Infrastruktur in Ihrem AWS-Konto.

Der Befehl `setup` stellt einen AWS CloudFormation Stapel bereit, der Folgendes umfasst:

- Ein Amazon S3 S3-Bucket für den Quellcode-Upload
- Eine IAM-Rolle, die übernommen wird von `securityagent.amazonaws.com`
- Eine verwaltete Richtlinie für die Rolle des Sicherheitsagenten

Ihr IAM-Benutzer oder Ihre IAM-Rolle muss über die folgenden zusätzlichen Berechtigungen verfügen, um das Setup ausführen zu können:

- `cloudformation:CreateStack`, `cloudformation:UpdateStack`,
`cloudformation:DescribeStacks`

- `iam:CreateRole`, `iam:PutRolePolicy`, `iam:AttachRolePolicy`, `iam:CreatePolicy`
- `s3:CreateBucket`, `s3:PutBucketEncryption`, `s3:PutBucketPublicAccessBlock`

Verwenden Sie die folgenden Befehle, um die Security Agent-Infrastruktur zu verwalten:

```
# Provision the security agent infrastructure
atx ct setup security-agent

# Check the status
atx ct setup security-agent --status

# Delete the infrastructure
atx ct setup security-agent --delete
```

Nach Abschluss der Installation können Sie Sicherheitsanalysen auf die gleiche Weise wie andere Analysetypen ausführen.

Erste Schritte

Voraussetzungen

Um die kontinuierliche Modernisierung effektiv nutzen zu können, solltest du über grundlegende Kenntnisse der Git-Versionskontrolle verfügen, mit deiner Quellcodeplattform (, oder Bitbucket) vertraut sein GitHub GitLab, über Grundkenntnisse in Bezug auf AWS IAM-Berechtigungen verfügen und Erfahrung mit Befehlszeilentools haben.

Bevor du Continuous Modernization verwendest, vergewissere dich, dass du über Folgendes verfügst:

- AWS Transform CLI ist installiert:

```
curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
```

- Node.js 2.2 oder später
- Gültige AWS Anmeldeinformationen (`AWS_PROFILE` oder Umgebungsvariablen)
- Die AWS verwaltete Richtlinie, die Ihrem IAM-Benutzer oder Ihrer IAM-Rolle `AWSTransformCustomFullAccess` zugeordnet ist

Schnellstart

1. Starten Sie den Server für kontinuierliche Modernisierung:

```
atx ct server &
```

2. Fügen Sie eine Quelle hinzu:

```
atx ct source add --name name --provider provider --org org-or-group --token token
```

Wo *name* ist eine beschreibende Kennung für Ihre Quelle, *provider* ist die Plattform (github,,gitlab, oderlocal)bitbucket, *org-or-group* ist Ihr Organisations- oder Gruppenname und *token* ist Ihr Authentifizierungstoken.

3. Entdecken Sie Repositorien:

```
atx ct discovery scan --source name
```

4. Führen Sie eine Analyse durch:

```
atx ct analysis run --type type --source name --wait
```

5. Erkunden Sie die Ergebnisse:

```
atx ct findings list --json
```

6. Ergebnisse korrigieren:

```
atx ct remediation create --ids id1,id2 --name "remediation-name"
```

Arbeiten mit kontinuierlicher Modernisierung

Quellenverwaltung

Verwenden Sie `atx ct source` Befehle, um Repositorys zu verbinden. Unterstützte Anbieter: GitHub, GitLab, Bitbucket, local.

GitHub Organisationen

Token: persönliches Zugriffstoken (klassisch) mit repo Gültigkeitsbereich. Read-only zur Analyse, vollständiges Repo zur Behebung.

```
atx ct source add --name name --provider github --org org --token pat
```

GitLab Gruppen und Benutzer

Token: persönliches Zugriffstoken mit api Gültigkeitsbereich.

```
atx ct source add --name name --provider gitlab --org group-or-user --token pat  
# Self-hosted:  
atx ct source add --name name --provider gitlab --org group-or-user --token pat --url  
https://gitlab.example.com
```

Bitbucket-Workspaces und -Projekte

Bitbucket Cloud — Bereiche:read:repository:bitbucket,,,. write:repository:bitbucket
read:pullrequest:bitbucket write:pullrequest:bitbucket --email Benötigt auch und.
--username

```
atx ct source add --name name --provider bitbucket --org workspace --token api-token --  
email email --username username
```

Bitbucket-Rechenzentrum:

```
atx ct source add --name name --provider bitbucket --org project-key --token http-  
access-token --url https://bitbucket.example.com
```

Lokale Repositorys

```
atx ct source add --name name --provider local --path parent-directory
```

Important

--path muss auf ein übergeordnetes Verzeichnis verweisen, das Git-Repos als Unterverzeichnisse enthält, nicht auf ein einzelnes Repo.

Quellen verwalten

```
atx ct source list
atx ct source remove --name name
```

Entdeckung und Verwaltung von Repositorien

```
atx ct discovery scan --source name
atx ct discovery status --source name
atx ct discovery scan --source name --path new-directory
```

Nach der Entdeckung:

```
atx ct repository list
atx ct repository list --source name
atx ct repository list --labels "team:frontend,priority:high"
atx ct repository update --source name --repo "source::slug" --labels
"team:frontend,priority:high"
atx ct repository update --source name --labels "migration:wave-1"
```

Analyse wird ausgeführt

Das `--type` Kennzeichen gibt an, welche Art von Analyse ausgeführt werden soll:

- `rapid-techdebt-analysis`— Veraltete Abhängigkeiten und einfache Erfolge.
- `tech-debt-comprehensive`— Eingehendere AI-powered Analysen zu Abhängigkeiten, Sicherheit, Mustern, Leistung, Wartbarkeit, Architektur, Codequalität und Infrastrukturergebnissen.
- `security`— Sicherheitslücken und Sicherheitslücken.
- `agentic-readiness`— Bereitschaft Ihrer Repositorien für KI-Agenten (Frameworks, APIs, Dokumentation).
- `modernization-readiness`— Modernisierungsmöglichkeiten in allen Bereichen Ihrer Infrastruktur, Anwendung, Daten, Sicherheit und Betriebsabläufe.

```
atx ct analysis run --type type --source name [--repo source::slug] [--wait]
atx ct analysis get --id id --json
atx ct analysis list --json
atx ct analysis list --status pending/running/complete/cancelled/failed --json
atx ct analysis list --type type --json
```

```
atx ct analysis cancel --id id  
atx ct analysis delete --id id [--cascade-findings]
```

Maßgeschneiderte Analyse

```
atx ct analysis run --type custom --transformation-name name --source source --  
repo source::slug --wait
```

Konfiguration mit -g Flag: Schlüsselwert, JSON oder Dateipfad.

TDs auflisten: `atx custom def list`

Verwaltung der Erkenntnisse

```
atx ct findings list --json  
atx ct findings list --repo source::slug --source name --severity high/medium/low  
--type analysis-type --status open/dismissed/obsolete --analysis-id id --fix-  
transform transform-name --json
```

Status finden

- open— Aktiv
- dismissed— Manuell abgewiesen (erfordert einen Grund)
- obsolete— System-set wenn die erneute Analyse das Ergebnis nicht mehr ergibt

```
atx ct findings update --id id --status dismissed --reason "reason"  
atx ct findings update --id id --status open  
atx ct findings batch-update --ids id1,id2 --status dismissed --reason "reason"  
atx ct findings get --id id  
atx ct findings delete --id id
```

Feststellung von Obsoleszenz

Re-analysis kennzeichnet behobene Ergebnisse als veraltet. Kann nicht erneut geöffnet werden. Zur Prüfung aufbewahrt.

Erstellung von Abhilfemaßnahmen

Drei Modi: ergebnisbasiert, TD Override, Direct TD.

```
atx ct remediation create --ids id1,id2 --name "name"  
atx ct remediation create --ids id1,id2 --transformation-name TD  
atx ct remediation create --transformation-name TD --repo source::slug
```

Ausgabe nach Anbieter: GitHub PR, GitLab MR, Bitbucket PR, Lokaler Zweig.

Note

Das Token muss Schreibzugriff für die PR/MR Erstellung haben.

Lokale Ausführung mit `--local` Flagge.

```
atx ct remediation create --transformation-name TD --repo source::slug -g  
  "additionalPlanContext=Upgrade to Node.js 22"  
atx ct remediation list  
atx ct remediation status --id id  
atx ct remediation retry --id id  
atx ct remediation delete --id id
```

AWS Webanwendung transformieren (optional)

Die AWS Transform-Webanwendung ist eine optionale Schnittstelle zur Überwachung kontinuierlicher Modernisierungsanalysen, Ergebnisse und Abhilfemaßnahmen in Ihrem gesamten Codequellenportfolio.

Bevor Sie die AWS Transform-Webanwendung verwenden können, müssen Sie eine Benutzeridentität für den Zugriff auf AWS Transform in Ihrer Organisation aktiviert haben. Informationen zur Aktivierung von AWS Transform finden Sie unter [AWS Transform einrichten](#).

So verwenden Sie die AWS Transform-Webanwendung:

1. Besuchen Sie das AWS IAM Identity Center <https://aws.amazon.com/transform/> und melden Sie sich mit Ihren Anmeldeinformationen an.
2. Wenn nach der Anmeldung keine kontinuierliche Modernisierung angezeigt wird, melden Sie sich stattdessen mit IAM-Anmeldeinformationen an. Um die Anmeldung mit IAM-Anmeldeinformationen zu aktivieren:
 - a. Öffnen Sie in der AWS Management Console AWS Transform und wählen Sie Einstellungen.

- b. Aktivieren Sie im Abschnitt AWS Zugriffstransformation mit IAM-Anmeldeinformationen den Zugriff auf IAM-Anmeldeinformationen.
 - c. Kopieren Sie auf derselben Einstellungsseite den Anmeldelink, der unter URL der Webanwendung (mit IAM) angezeigt wird.
 - d. Fügen Sie die Anmelde-URL in dasselbe Browserfenster ein, in dem die AWS Management Console geöffnet ist. Dadurch wird sichergestellt, dass die Webanwendung die AWS Anmeldeinformationen dieses Kontos verwendet.
3. Öffnen Sie das linke Navigationsmenü und wählen Sie Continuous Modernization. Das Dashboard zeigt zusammenfassende Statistiken an, darunter Quellen, Repositorien, Gesamtzahl der Ergebnisse nach Schweregrad und Analysetypen.
 4. Verwenden Sie die Registerkarten Analysen, Ergebnisse und Abhilfemaßnahmen, um detaillierte Ergebnisse anzuzeigen.
 5. Chatten Sie direkt von der Webanwendung aus mit AWS Transform, um Fragen zu Ihren Analysen, Ergebnissen oder Abhilfemaßnahmen zu stellen.

Die Webanwendung wurde für den Betrieb auf Unternehmensebene konzipiert, bei dem Sie einen zentralen Überblick über kontinuierliche Modernisierungsanalysen und Problembehebungen für mehrere Codebasen benötigen.

Entwicklertools

Mit dem AWS Transform Power- und Agent-Plugin können Sie von agentischen IDEs aus auf die kontinuierliche Modernisierung zugreifen. Der Agent orchestriert die Einrichtung, das Onboarding und die kontinuierliche Nutzung der kontinuierlichen Modernisierung durch Konversation.

- Kiro IDE — [Installieren Sie Transform Kiro Power.AWS](#) Öffnen Sie Kiro Chat und bitten Sie den Agenten, Ihnen bei der kontinuierlichen Modernisierung der Workflows zu helfen.
- Claude Code, Codex, Cursor — Installiere die [awslabs/agent-plugins \(Verzeichnis\)](#)plugins/aws-transform. Das Agent-Plugin bietet dieselben Funktionen wie das Kiro Power.

Agenten-Skills

Das Kiro Power- und Agent-Plug-In verfügen über Fähigkeiten, mit denen Workflows zur kontinuierlichen Modernisierung mithilfe von Konversationsinteraktionen orchestriert werden können:

Fähigkeit	Description
Richtlinie	Interaktives Onboarding, das Sie Schritt für Schritt durch den gesamten Workflow führt
Quelle	Quellverbindungen hinzufügen, auflisten und entfernen
Erkennung	Scannen Sie Quellen, um Repositorys zu finden
Analyse	Führen Sie Analysen aller Typen durch und verwalten Sie sie
Ergebnisse	Analyseergebnisse abfragen, filtern und verwalten
Abhilfe	Erstellen und verwalten Sie Abhilfemaßnahmen, um die Ergebnisse zu korrigieren
EC2-Ausführung	Bereitstellung und Verwaltung einer Amazon EC2 EC2-Instance für Remote-Analysen
Batch-Ausführung	Senden Sie Analyseaufträge mit AWS Fargate an Batch
Plan	Richten Sie mit Amazon EventBridge Scheduler wiederkehrende Analysen nach einem Cron-Zeitplan ein
Berichterstellung	Generieren Sie eigenständige HTML-Berichte mit Diagrammen, in denen die Ergebnisse, die Verteilung des Schweregrads und der Fortschritt der Problembehebung dargestellt werden

CLI-Referenz

In der folgenden Tabelle sind alle Unterbefehle zusammengefasst. `atx` `ct`

Unterbefehl	Description
<code>atx ct server</code>	Starten Sie den Continuous Modernization Server
<code>atx ct status</code>	Zeigen Sie den Systemstatus an, einschließlich Quellen, Repositorys, Analysen, Ergebnissen und Abhilfemaßnahmen
<code>atx ct source add</code>	Füge eine Quelle hinzu (GitHub, GitLab, Bitbucket oder lokal)
<code>atx ct source list</code>	Listet die konfigurierten Quellen auf
<code>atx ct source remove</code>	Eine Quelle entfernen
<code>atx ct discovery scan</code>	Entdecken Sie Repositorys aus einer Quelle
<code>atx ct discovery status</code>	Überprüfen Sie den Discovery-Scan-Status
<code>atx ct repository list</code>	Listet Repositorys mit optionalen Filtern auf
<code>atx ct repository get</code>	Holen Sie sich ein einzelnes Repository
<code>atx ct repository update</code>	Repository-Labels aktualisieren
<code>atx ct repository delete</code>	Löschen Sie ein Repository
<code>atx ct analysis run</code>	Führen Sie eine Analyse für Repositorys durch
<code>atx ct analysis get</code>	Holen Sie sich Analysedetails
<code>atx ct analysis list</code>	Listen Sie Analysen mit optionalen Status- und Typfiltern auf
<code>atx ct analysis cancel</code>	Brechen Sie eine laufende Analyse ab
<code>atx ct analysis delete</code>	Löschen Sie eine Analyse
<code>atx ct findings list</code>	Listet Ergebnisse mit Filtern für Repo, Quelle, Schweregrad, Typ, Status und Analyse auf

Unterbefehl	Description
<code>atx ct findings get</code>	Holen Sie sich einen einzigen Befund
<code>atx ct findings update</code>	Aktualisiere den Befundstatus (offen oder abgelehnt)
<code>atx ct findings batch-update</code>	Mehrere Ergebnisse Batch aktualisieren
<code>atx ct findings delete</code>	Löschen Sie ein verworfenes oder veraltetes Ergebnis
<code>atx ct remediation create</code>	Erstellen Sie eine Korrektur anhand von Ergebnissen oder einer Transformationsdefinition
<code>atx ct remediation list</code>	Alle Abhilfemaßnahmen auflisten
<code>atx ct remediation status</code>	Überprüfen Sie den Behebungsstatus und sehen Sie sich die Links an PR/MR
<code>atx ct remediation retry</code>	Versuchen Sie erneut, eine fehlgeschlagene Behebung durchzuführen
<code>atx ct remediation delete</code>	Löschen Sie eine Korrektur
<code>atx ct setup security-agent</code>	Stellen Sie die Infrastruktur von Security Agents bereit oder verwalten Sie sie
<code>atx ct schema</code>	Druckt ein maschinenlesbares JSON-Manifest der vollständigen <code>atx ct</code> Befehlsoberfläche — alle Befehle, Optionen und Argumente —, sodass Agenten und die Automatisierung die CLI erkennen können, ohne den Hilfetext zu analysieren

Fehlerbehebung

Verbindung verweigert oder Server läuft nicht

Die CLI für die kontinuierliche Modernisierung erfordert einen laufenden Server. Starten Sie es mit `atx ct server &` und überprüfen Sie mit `atx ct status --health`.

Der Discovery-Scan gibt keine Repositorys zurück

Stellen Sie bei lokalen Quellen sicher, dass das Verzeichnis auf ein übergeordnetes Verzeichnis `--path` verweist, das Repositorys als Unterverzeichnisse enthält (z. B. `/home/user/repos`), und nicht direkt auf ein Repository (z. B.). `/home/user/repos/my-app` Der Scanner sucht nach untergeordneten Verzeichnissen, die einen `.git` Ordner enthalten.

SETUP_REQUIRED Fehler

Die Quelle ist in Ihrem Konto vorhanden, aber die Anmeldeinformationen sind auf diesem Computer nicht konfiguriert. Führen Sie `atx ct source add --name name` das Programm aus, um die Anmeldeinformationen lokal zu konfigurieren.

AUTH_REQUIRED Fehler

Für die Quelle wurde kein gültiges Token gefunden. Stellen Sie sicher, dass Ihr Token korrekt ist und die erforderlichen Gültigkeitsbereiche hat. Stellen Sie sicher GitHub, dass das Token einen `repo` Gültigkeitsbereich hat. Für GitLab, stellen Sie den `api` Umfang sicher.

INVALID_INPUT-Fehler

Stellen Sie sicher, dass Sie den richtigen Namen für den Analysetyp verwenden. Folgende Werte sind zulässig: `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`.

Berechtigungsfehler bei der Problembehebung

Bei der Behebung werden Verzweigungen und pull/merge Anfragen erstellt, für die Schreibzugriff auf das Repository erforderlich ist. Aktualisieren Sie Ihr Token mit Schreibberechtigungen. Stellen Sie GitHub nämlich den vollen `repo` Umfang sicher. Für GitLab, stellen Sie den `api` Umfang sicher. Für Bitbucket: Ensure `write:repository:bitbucket` und `write:pullrequest:bitbucket` Scopes.

Das Setup des Security Agents schlägt fehl

Stellen Sie sicher, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle über die erforderlichen AWS CloudFormation, IAM- und Amazon S3 S3-Berechtigungen verfügt, die im Abschnitt Security

Agent Setup von aufgeführt sind. [Wie AWS Transformation: Kontinuierliche Modernisierung funktioniert](#) Überprüfen Sie den Status mit. `atx ct setup security-agent --status`
Kontinuierliche Modernisierung ist in der Webanwendung nicht sichtbar

Wenn die kontinuierliche Modernisierung nicht angezeigt wird, nachdem Sie sich bei der AWS Transform-Webanwendung angemeldet haben, melden Sie sich mit den IAM-Anmeldedaten von dort an, AWS-Konto wo AWS Transform aktiviert ist, und nicht mit AWS IAM Identity Center. Informationen zu den erforderlichen Schritten finden Sie unter [AWS Webanwendung transformieren \(optional\)](#).

Discovery-Tool

Das AWS Transform Discovery-Tool hilft Ihnen dabei, das Serverinventar in Ihrer Organisation automatisch zu ermitteln, um sich auf die Migration vorzubereiten. Das Tool unterstützt VMware vCenter Hyper-V, Microsoft und importierte Server. Um das Discovery-Tool zu verwenden, konfigurieren Sie eine oder mehrere Discovery-Quellen, lassen das Tool laufen und überprüfen dann die Ergebnisse im Bereich Ermittelter Inventar.

Nachdem Sie eine Discovery-Quelle konfiguriert haben, beginnt das Discovery-Tool mit der Erfassung von Informationen. Die Zeit, die das Discovery-Tool benötigt, um Ihr Netzwerk vollständig zu analysieren, hängt von der Größe Ihrer Umgebung ab. Für ein Geschäftsszenario zur direktionalen Migration können Sie die MPA-Dateien (Migration Portfolio Assessment) verwenden, die das Tool nach Abschluss der Servererfassung generiert.

Arbeitsablauf des Discovery-Tools

Der Workflow für das Discovery-Tool besteht aus zwei Arten von Aktivitäten:

- Konfigurationsaktivitäten
- Überprüfung und Verwendung von Daten

In den folgenden Schritten wird beschrieben, wie Sie das Discovery-Tool installieren und verwenden und mit den gesammelten Daten arbeiten:

1. Installieren Sie das Discovery-Tool.
2. Konfigurieren Sie die Discovery-Quellen. Sie können eine oder mehrere der folgenden Optionen konfigurieren: VMware vCenter, Hyper-V Microsoft-Hosts oder Server über einen CSV-Dateiimport. Die Datenermittlung beginnt, nachdem Sie eine Quelle konfiguriert haben.
3. Richten Sie den Betriebssystemzugriff ein und überprüfen Sie dann den Erfassungsstatus von Servern, Datenbanken und Netzwerkverbindungen.
 - Passen Sie die Betriebssystemanmeldedaten nach Bedarf an.
4. (Optional) Konfigurieren Sie Oracle-Anmeldeinformationen, um die direkte SQL-Erfassung zu aktivieren, oder verwenden Sie die OS-level Fallback-Erkennung über SSH oder WinRM.
5. Um einen Business Case für die Migration zu generieren, laden Sie die ZIP-Datei in die [Migrationsbewertung](#) hoch oder entpacken Sie sie und laden Sie die MPA-Dateien aus dem

Verzeichnis `mpa_exports` hoch. Der Export umfasst Daten aus allen konfigurierten Quellen und enthält MPA-Dateien für VMware sowie Hyper-V importierte Server.

Das Discovery-Tool unterstützt die folgenden Ermittlungspfade:

- Automatische Erkennung von VMware vCenter — Automatische Erkennung von Servern, die von VMware vCenter verwaltet werden.
- Hyper-V automatische Erkennung — Automatische Erkennung von Servern, die von Hyper-V Microsoft-Hosts verwaltet werden.
- Serverimport — Importieren Sie das Serverinventar manuell über eine CSV-Datei.

Das Discovery-Tool einrichten

Voraussetzungen

Im Folgenden sind die Voraussetzungen für die Verwendung des AWS Transform Discovery-Tools aufgeführt:

Allgemeine Voraussetzungen

- Das Tool benötigt 4 vCPUs, 16 GB RAM und eine 35-GB-Festplatte.
- DHCP muss im Netzwerk für die Discovery-Tool-VM verfügbar sein.
- Das Tool sammelt Daten mithilfe eines zentralisierten Ansatzes. Server im Geltungsbereich müssen eingehende Konnektivität von der Discovery-Tool-VM zulassen (Standardports, benutzerdefinierte Portkonfiguration wird unterstützt):
 - Linux — SSH TCP/22
 - Windows — TCP/5985 für HTTP, TCP/5986 für HTTPS
 - SNMP — UDP/161 (wird nur für die Netzwerkerfassung verwendet, nicht für Betriebssystemmetriken)
- Für Linux Benutzerkonten, die SSH verwenden können, um eine Verbindung zum Server herzustellen. Das Discovery-Tool führt Befehle über SSH für Netzwerkerfassung und Betriebssystemmetriken aus. Die meisten Befehle werden als normaler Benutzer ausgeführt. Eine kleine Anzahl von Befehlen versucht `sudo` und greift automatisch zurück, wenn `sudo` nicht verfügbar ist: `dmidecode` (Server-UUID und Hersteller), `lvs` (LVM-Erkennung) und/oder `ss` oder `netstat` (Netzwerkverbindungen mit Prozessinformationen). Ohne `sudo` sammelt das

Discovery-Tool immer noch den Großteil der Daten, aber UUID-, LVM- und Netzwerkdetails auf Prozessebene fehlen. Wir empfehlen, sudo ohne Passwort für den SSH-Benutzer zu konfigurieren, um eine vollständige Datenerfassung zu gewährleisten. Eine vollständige Aufschlüsselung finden Sie unter [the section called “Erforderliche Berechtigungen”](#)

Voraussetzungen für VMware

- VMware vCenter Server Version 6.5, 6.7, 7.0 oder 8.0.
- Berechtigungen zur Bereitstellung einer OVA in Ihrem VMware vCenter.
- Für das VMware vCenter Server-Setup ein vCenter-Benutzer, dem die Read-Only Rolle auf der Ebene des Root-Rechenzentrums zugewiesen wurde. Details hierzu finden Sie unter [the section called “Erforderliche Berechtigungen”](#).

Hyper-V Voraussetzungen

- Windows Server mit aktivierter Hyper-V Rolle.
- WinRM ist auf Hyper-V Hosts aktiviert.
- Ein Benutzerkonto, das Mitglied der Gruppen Fernverwaltungsbenutzer, Hyper-V Administratoren und Systemmonitor-Benutzer auf jedem Hyper-V Host ist und über WMI-Lesezugriff auf den root \cimv2 Namespace verfügt. Details hierzu finden Sie unter [the section called “Erforderliche Berechtigungen”](#).
- Unterstützte Authentifizierung: NTLM (nur HTTPS) und Kerberos (HTTP oder HTTPS).

Voraussetzungen für den Serverimport

- Eine CSV-Datei mit Server-Hostnamen oder IP-Adressen und den Namen der Anmeldeinformationen (optional), die den benutzerfreundlichen Namen der Betriebssystemanmeldeinformationen zugeordnet sind, die im Discovery-Tool konfiguriert wurden oder konfiguriert werden sollen. Die CSV-Datei muss die folgenden Header verwenden:

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- Server müssen von der Discovery-Tool-VM aus erreichbar sein. Standardports: SSH-Port 22 für Linux, WinRM-Port 5985/5986 für Windows. Benutzerdefinierte Ports werden unterstützt.

Voraussetzungen für das Linux-Installationsprogramm

- Eine unterstützte Linux-Distribution: Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, AlmaLinux Debian 10—12 oder SLES 15 SP5.
- Mindestens 4 vCPU, 16 GB RAM, 35 GB verfügbarer Festplattenspeicher.
- Port 5000 muss verfügbar sein (wird nicht von einem anderen Dienst verwendet).
- systemd ist für die Dienstverwaltung erforderlich.
- Die Discovery-Tool-VM muss Netzwerkzugriff auf Ihre Zielinfrastruktur haben. Standardports: vCenter auf Port 443, Hyper-V Hosts auf Port 5985/5986, Server auf Port 22. Benutzerdefinierte Ports werden für SSH, WinRM und SNMP unterstützt.

Voraussetzungen für die Oracle-Datenbank

- Netzwerkzugriff vom Discovery-Tool auf Oracle-Hosts auf Port 1521 (oder benutzerdefiniertem Port).
- Unterstützte Oracle-Versionen: Sie können Oracle Database 12c Release 1 (12.1) und höher über direkte SQL-Verbindungen abrufen. OS-level Die Fallback-Erkennung funktioniert mit allen Oracle-Versionen.
- Ein schreibgeschütztes Oracle-Dienstkonto mit SELECT_CATALOG_ROLE-Zuweisung. Details hierzu finden Sie unter [the section called “Oracle-Datenbank \(SQL\)”](#).
- Für die OS-level Fallback-Erkennung: SSH- oder WinRM-Zugriff auf den Oracle-Host (verwendet vorhandene Betriebssystemanmeldeinformationen).

Auf VMware bereitstellen

Spezifikationen für virtuelle Maschinen von VMware

- Betriebssystem — Amazon Linux 2023
- Arbeitsspeicher — 16 GB
- CPU — 4 Kerne
- Festplatten — 35 GB
- VMware-Anforderungen — Weitere Informationen finden Sie unter [VMware-Hostanforderungen für die Ausführung von AL2023 auf VMware](#)

Stellen Sie die VMware OVA bereit

1. Laden Sie die OVA-Datei von dieser URL herunter: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova>
2. Melden Sie sich bei vCenter als VMware-Administrator an.
3. Verwenden Sie eine der folgenden Methoden, um die OVA-Datei zu installieren:
 - a. Verwenden Sie die Benutzeroberfläche: Wählen Sie „Datei“, wählen Sie „OVF-Vorlage bereitstellen“, wählen Sie die in Schritt 1 heruntergeladene OVA-Datei des Erkennungstools aus, und schließen Sie dann den Assistenten ab. Stellen Sie sicher, dass die Proxyeinstellungen im Servermanagement-Dashboard korrekt konfiguriert sind.
 - b. Verwenden Sie die Befehlszeile: Um die OVA-Datei des Discovery-Tools von der Befehlszeile aus zu installieren, laden Sie das VMware Open Virtualization Format Tool (ovftool) herunter und verwenden Sie es. Um ovftool herunterzuladen, wählen Sie auf der Seite mit der [OVF-Tool-Dokumentation](#) eine Version aus. Dies ist ein Beispiel für die Verwendung des Befehlszeilentools ovftool zur Installation der OVA-Datei des Discovery-Tools.

```
ovftool --acceptAllEulas --name='discovery tool' --datastore=datastore1 -  
dm=thin AWS-Transform-discovery-tool.ova 'vi://username:password@vcenterurl/  
Datacenter/host/esxi/'
```

Beschreibungen der ersetzbaren Werte im Beispiel:

- Der Name ist der Name, den Sie für Ihre Discoverytool-VM verwenden möchten.
 - Der Datenspeicher ist der Name des Datenspeichers in Ihrem vCenter.
 - Der OVA-Dateiname ist der Name der heruntergeladenen OVA-Datei des Discovery-Tools.
 - Das username/password sind Ihre vCenter-Anmeldeinformationen.
 - Die vcenterurl ist die URL Ihres vCenter.
 - Der vi-Pfad ist der Pfad zu Ihrem VMware ESXi-Host.
4. Suchen Sie das bereitgestellte Discovery-Tool in Ihrem vCenter. Right-click die VM und wählen Sie dann Power, Power On.
 5. Nach einigen Minuten wird die IP-Adresse des Discovery-Tools in vCenter angezeigt. Sie verwenden diese IP-Adresse, um eine Verbindung zum Discovery-Tool herzustellen.

Bereitstellen auf Hyper-V

Hyper-V Spezifikationen der virtuellen Maschine

- Betriebssystem — Amazon Linux 2023
- RAM — Wir empfehlen, mindestens 16 GB zuzuweisen
- CPU — Wir empfehlen, mindestens 4 Kerne zuzuweisen
- Festplatten — 35 GB (in der virtuellen Festplatte enthalten)
- Hyper-V Anforderungen — siehe [Hyper-V Hostanforderungen für den Betrieb von AL2023](#) auf Hyper-V

Stellen Sie die virtuelle Festplatte Hyper-V bereit

1. Laden Sie die VHD-Datei von dieser URL herunter: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd>
2. Kopieren Sie die VHD-Datei auf den Windows Server-Computer, auf dem die Hyper-V Rolle aktiviert ist.
3. Öffnen Sie den Hyper-V Manager.
4. Wählen Sie „Neu“ und anschließend „Virtuelle Maschine“.
5. Schließen Sie den Einrichtungsassistenten ab. Wählen Sie auf der Seite „Generation angeben“ Generation 1 aus. Virtuelle Maschinen der Generation 2 unterstützen das VHD-Format nicht. Weisen Sie auf der Seite „Arbeitsspeicher zuweisen“ mindestens 16384 MB zu. Wählen Sie auf der Seite Virtuelle Festplatte Connect die Option Vorhandene virtuelle Festplatte verwenden und wählen Sie die kopierte VHD-Datei aus.
6. Starten Sie die VM. Suchen Sie nach einigen Minuten auf der Registerkarte Netzwerk der VM im Hyper-V Manager nach der IP-Adresse, oder stellen Sie eine Verbindung zur VM-Konsole her und starten Sie den Vorgang `ip addr`. Sie verwenden diese IP-Adresse, um eine Verbindung zum Discovery-Tool herzustellen.

Auf Linux bereitstellen

Das Discovery-Tool ist als eigenständiges Linux-Installationsprogramm für die Bereitstellung auf unterstützten Linux-Distributionen verfügbar. Verwenden Sie diese Option, wenn Sie das Discovery-Tool direkt auf einem vorhandenen Linux-Server installieren möchten, anstatt eine virtuelle Maschine bereitzustellen.

Spezifikationen für Linux-Server

- RAM — Wir empfehlen, mindestens 16 GB zuzuweisen
- CPU — Wir empfehlen, mindestens 4 Kerne zuzuweisen
- Festplatten — 35 GB

Unterstützte Distributionen

- Amazon Linux — Amazon Linux 2, Amazon Linux 2023
- Red Hat Enterprise Linux und Derivate — RHEL 8—9, Rocky Linux 8—9, 9 AlmaLinux
- Ubuntu — 20.04, 22.04, 24.04
- Debian — 10, 11, 12
- SUSE — SLES 15 SP5

Installieren Sie das Discovery-Tool

Laden Sie das Installationsskript von dieser URL herunter: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh>

Um das Discovery-Tool unter Linux zu installieren

1. Laden Sie das Installationsskript auf Ihren Linux-Server herunter.

```
curl -O https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh
chmod +x AWS-Transform-discovery-tool.sh
```

2. (Optional) Führen Sie die Kompatibilitätsprüfung durch, um sicherzustellen, dass Ihr System die Anforderungen erfüllt.

```
sudo ./AWS-Transform-discovery-tool.sh check
```

3. Installieren Sie das Discovery-Tool. Wählen Sie eine der folgenden Optionen:

Option 1: Installation mit automatischer Installation von Abhängigkeiten (empfohlen)

Diese Option installiert automatisch alle fehlenden Systemabhängigkeiten, bevor der Dienst installiert wird.


```
sudo ./AWS-Transform-discovery-tool.sh install --install-deps
```

Option 2: Installation ohne automatische Installation von Abhängigkeiten

Diese Option sucht nach fehlenden Abhängigkeiten und zeigt Fehler mit manuellen Installationsanweisungen an, falls wichtige Abhängigkeiten fehlen. Verwenden Sie diese Option, wenn Ihre Organisation die automatische Paketinstallation einschränkt und Sie es vorziehen, Systempakete manuell zu verwalten.

```
sudo ./AWS-Transform-discovery-tool.sh install
```

4. Starten Sie den Discovery Tool-Dienst.

```
sudo ./AWS-Transform-discovery-tool.sh start
```

5. Greifen Sie auf das Discovery-Tool unter `https://ip_address:5000`.

Führen Sie den Befehl aus, um das Discovery-Tool zu deinstallieren `sudo ./AWS-Transform-discovery-tool.sh uninstall`.

Sie können den Dienst auch mit den folgenden Befehlen verwalten:

- `sudo ./AWS-Transform-discovery-tool.sh status`— Prüfen Sie, ob der Dienst läuft.
- `sudo ./AWS-Transform-discovery-tool.sh stop`— Stoppen Sie den Dienst.
- `sudo ./AWS-Transform-discovery-tool.sh logs`— Serviceprotokolle anzeigen.

Systemabhängigkeiten

Das Installationsprogramm sucht nach den folgenden Systemabhängigkeiten:

-Abhängigkeit	Schweregrad	Zweck
OpenSSL	Kritisch	Generiert den Datenbank-Verschlüsselungsschlüssel
libcrypt	Kritisch	Von der Python-Laufzeit erforderlich

-Abhängigkeit	Schweregrad	Zweck
Kerberos-Bibliotheken	Warning	Erforderlich für die Kerberos-Authentifizierung bei Windows-Servern. Ohne dies funktionieren NTLM und Standardauthentifizierung weiterhin.

Damit das Discovery-Tool gestartet werden kann, sind kritische Abhängigkeiten erforderlich. Wenn sie fehlen und Sie Option 2 (ohne `--install-deps`) gewählt haben, zeigt das Installationsprogramm eine Fehlermeldung mit Anweisungen zur manuellen Installation an. Warning-level Abhängigkeiten sind optional — das Installationsprogramm warnt Sie, fährt aber mit der Installation fort.

Note

Das Installationsprogramm überprüft die Systemkompatibilität, einschließlich der Glibc-Version und der Systemd-Verfügbarkeit. Auf Systemen mit systemd 250 oder höher (Amazon Linux 2023, RHEL 9, Rocky 9, 9, Ubuntu 24.04+, Debian 12+) wird der Datenbankverschlüsselungsschlüssel im Ruhezustand mit `systemd-creds` verschlüsselt. AlmaLinux Auf älteren Systemen wird der Verschlüsselungsschlüssel als berechtigungsgeschützte Datei gespeichert.

Konfigurieren Sie das Discovery-Tool

Rufen Sie die Discovery-Tool-Konsole auf

1. Rufen Sie in einem Webbrowser auf: `https://ip_address:5000`, wobei *ip_address* sich die IP-Adresse des Discovery-Tools aus Deploy Discovery Tool befindet. Das Discovery-Tool verwendet ein selbstsigniertes Zertifikat für die HTTPS-Verbindung, was zu einer Sicherheitswarnung führt. Wählen Sie Das Risiko akzeptieren und fahren Sie mit der Discovery-Tool-Konsole fort.
2. Wenn Sie zum ersten Mal auf die Discovery Tool Console zugreifen, erstellen Sie ein Anmeldekennwort für das Discovery Tool. Erstellen Sie ein Passwort, das Sie für future Anmeldungen verwenden werden.

 Important

Merken Sie sich dieses Passwort - es gibt keinen Mechanismus zur Passwortwiederherstellung.

Zugreifen auf das Discovery-Tool (VM)

- Die Discovery-Tool-VM verfügt standardmäßig über einen Benutzernamen und ein Passwort („Discovery“, „Passwort“). Aus Sicherheitsgründen empfehlen wir, dass Sie das Passwort aktualisieren, indem Sie es verwenden, `sudo passwd discovery` nachdem Sie sich über die Konsole Ihres Hypervisors bei der VM angemeldet haben (z. B. vSphere Client for VMware oder Hyper-V Manager for Hyper-V).
- Der SSH-Zugriff ist standardmäßig deaktiviert. Benutzer können vorkonfigurierte Dateien `enablessh` und `disablessh` Aliase für den enable/disable SSH-Zugriff auf die Discovery-Tool-VM verwenden. Benutzer können über SSH auf die VM zugreifen, `ssh discovery@<VM-IP>` nachdem sie den SSH-Zugriff aktiviert haben. Benutzern wird empfohlen, den SSH-Zugriff in den meisten Fällen deaktiviert zu lassen und ihn nur zu aktivieren, wenn er aktiv benötigt wird. Die Kennwortänderung wird bei der Ausführung erzwungen. `enablessh`
- Um auf das Datenverzeichnis des Discovery-Tools unter `zuzugreifen/home/ec2-user/.local/share/DiscoveryTool`, empfehlen wir, `ec2-user` durch Ausführen `sudo su ec2-user` zu wechseln.

Konfiguration der Kerberos-Authentifizierung

Die Kerberos-Authentifizierung ist die empfohlene Methode, um über das Discovery-Tool eine Verbindung zu Windows-Servern herzustellen. Das Discovery-Tool VM verwendet native Amazon Linux 2023 Kerberos-Bibliotheken, um sich gegenüber Ihrer Active Directory-Domain zu authentifizieren.

Im Folgenden sind die wichtigsten Punkte zur Kerberos-Authentifizierung auf dem Discovery-Tool VM aufgeführt:

- Verwenden Sie den `kinit` Befehl, um ein Kerberos-Ticket zu erhalten und das Ticket `klist` zu verifizieren.
- Die Kerberos-Konfigurationsdatei befindet sich unter `/etc/krb5.conf`

- Bevor Sie das Discovery-Tool konfigurieren, stellen Sie sicher, dass es über die CLI auf der Discovery-Tool-VM kinit erfolgreich ist.

Voraussetzungen für Kerberos

Bevor Sie die Kerberos-Authentifizierung konfigurieren, stellen Sie sicher, dass Sie über die folgenden Informationen und die Netzwerkkonnektivität verfügen.

1. Erkundigen Sie sich bei Ihrem Active Directory-Administrator nach den folgenden Informationen:
 - Der Kerberos-Bereichsname (normalerweise Ihr Domänenname in Großbuchstaben, z. B.).
EXAMPLE.COM
 - Der Hostname oder die IP-Adresse des Key Distribution Center (KDC), bei dem es sich in der Regel um einen Domänencontroller handelt (z. B.). dc01.example.com
 - Ein Dienstkonto mit Berechtigungen zur Authentifizierung bei den Windows-Zielservern.
2. Stellen Sie sicher, dass die Discoverytool-VM über Netzwerkkonnektivität mit den folgenden Geräten verfügt:
 - Das KDC auf Port 88 (TCP und UDP) für die Kerberos-Authentifizierung.
 - Die Windows-Zielserver auf WinRM-Ports (5985 für HTTP, 5986 für HTTPS).

Konfigurieren von Kerberos

Führen Sie die folgenden Schritte aus, um die Kerberos-Authentifizierung auf der Discoverytool-VM zu konfigurieren.

1. Stellen Sie eine SSH-Verbindung zur Discoverytool-VM her.

```
ssh discovery@<discovery-tool-vm-ip>
```

2. Bearbeiten Sie die Kerberos-Konfigurationsdatei unter. /etc/krb5.conf

```
sudo nano /etc/krb5.conf
```

Fügen Sie die folgende Konfiguration hinzu und ersetzen Sie die Platzhalterwerte durch Ihre Umgebungsdetails.

```
[libdefaults]
    default_realm = EXAMPLE.COM
```

```
dns_lookup_realm = false
dns_lookup_kdc = true

[realms]
EXAMPLE.COM = {
    kdc = dc01.example.com
}

[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

Important

Kerberos unterscheidet zwischen Groß- und Kleinschreibung. Der Bereichsname muss in Großbuchstaben geschrieben werden (z. B. EXAMPLE.COM nicht). example.com Der Domainname in dem [domain_realm] Abschnitt muss in Kleinbuchstaben geschrieben werden.

Mehrere Active Directory-Domänen

Das Discovery-Tool unterstützt mehrere Kerberos-Anmeldeinformationen für verschiedene Active Directory-Domänen. Alle Anmeldeinformationen werden unabhängig authentifiziert, sodass Sie mehrere Anmeldeinformationen normal konfigurieren können und die Isolierung automatisch erfolgt.

Wenn Sie Server in mehreren Domänen haben, fügen Sie Einträge für jeden Bereich in Ihrer /etc/krb5.conf Datei hinzu:

```
[libdefaults]
    default_realm = DEV.COMPANY.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
DEV.COMPANY.COM = {
    kdc = dc01.dev.company.com
}
PROD.COMPANY.COM = {
    kdc = dc01.prod.company.com
```

```
}
```

```
[domain_realm]  
  .dev.company.com = DEV.COMPANY.COM  
  dev.company.com = DEV.COMPANY.COM  
  .prod.company.com = PROD.COMPANY.COM  
  prod.company.com = PROD.COMPANY.COM
```

3. Stellen Sie sicher, dass Sie ein Kerberos-Ticket erhalten können, indem Sie den `kinit` Befehl ausführen.

```
kinit username@REALM.COM
```

Geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden. Wenn der Befehl ohne Fehler abgeschlossen wurde, war die Authentifizierung erfolgreich.

4. Überprüfen Sie das Ticket, indem Sie den `klist` Befehl ausführen.

```
klist
```

Die erwartete Ausgabe ähnelt der folgenden.

```
Ticket cache: FILE:/tmp/krb5cc_1000  
Default principal: username@REALM.COM  
  
Valid starting      Expires            Service principal  
01/01/2025 12:00:00  01/01/2025 22:00:00  krbtgt/REALM.COM@REALM.COM
```

5. Konfigurieren Sie das Discovery-Tool mit demselben Prinzipal, bei dem Groß- und Kleinschreibung beachtet wird, wie Sie es mit verwendet haben `kinit` (z. B. `username@REALM.COM`).

Eine explizite `krb5.conf` Konfiguration ist möglicherweise nicht erforderlich, wenn in Ihrer Umgebung DNS-SRV-Einträge für die Kerberos-Serviceerkennung konfiguriert sind. [Weitere Informationen zu den Kerberos-Konfigurationsoptionen finden Sie in der MIT-Kerberos-Dokumentation `krb5.conf` und in der Beispieldatei `krb5.conf`.](#)

Suchen Sie nach der Kerberos-Konfiguration auf Computern, die in eine Domäne eingebunden sind

Wenn Sie nicht über die Kerberos-Konfigurationsdetails verfügen, können Sie sie von einem Windows-Computer abrufen, der der Domäne angehört. Führen Sie die folgenden Befehle über eine Befehlszeile auf dem Computer aus, der mit der Domäne verbunden ist.

Führen Sie den folgenden Befehl aus, um den Domänennamen zu finden.

```
echo %USERDNSDOMAIN%
```

Beispielausgabe:

```
EXAMPLE.COM
```

Führen Sie den folgenden Befehl aus, um den Hostnamen des Domänencontrollers zu ermitteln.

```
nltest /dsgetdc:EXAMPLE.COM
```

Beispielausgabe:

```
DC: \\dc01.example.com
Address: \\10.0.1.100
Dom Guid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Dom Name: EXAMPLE.COM
Forest Name: example.com
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: 0xe00033fd
The command completed successfully
```

Ordnen Sie die Ausgabe wie folgt Ihrer `krb5.conf` Konfiguration zu:

- **Realm** — Verwenden Sie den Wert von `%USERDNSDOMAIN%` in Großbuchstaben (z. B. `EXAMPLE.COM`).
- **KDC** — Verwendet den DC-Hostnamen aus der `nltest` Ausgabe (z. B.). `dc01.example.com`

vCenter-Zugriff konfigurieren

1. Auf der Discovery-Tool-Seite unter Schritt 1. Konfigurieren Sie Discovery-Quellen und wählen Sie **Configure sources** aus.

2. Geben Sie auf der Seite „Discovery-Quellen konfigurieren“ den Friendly Name, vCenter FQDN/IP, den Benutzernamen und das Passwort ein.
3. Wählen Sie Save configuration (Konfiguration speichern) aus.

Das Discovery-Tool beginnt mit der Erfassung von vCenter-Informationen, wie unter [Entdecktes Inventar](#) beschrieben.

Wählen Sie nach der Erstkonfiguration im Statusfenster des Discovery-Tools die Option vCenter-Zugriff bearbeiten aus, um Ihre vCenter-Zugriffseinstellungen zu ändern.

Das Discovery-Tool sammelt Daten von allen konfigurierten vCenter-Servern parallel. Wenn ein vCenter Server während der Erfassung nicht erreichbar ist, meldet das Tool einen teilweisen Erfolg und setzt die Erfassung von den verbleibenden vCenter Servern fort.

Wenn eine VM auf mehreren vCenter-Servern erscheint (z. B. aufgrund gemeinsam genutzter ESXi-Hosts oder Cross-vCenter vMotion), dedupliziert das Discovery-Tool automatisch VMs. Jede einzelne virtuelle Maschine erscheint nur einmal in der Bestandsliste.

Konfigurieren Sie Hyper-V den Zugriff

1. Auf der Discovery-Tool-Seite unter Schritt 1. Konfigurieren Sie Discovery-Quellen und wählen Sie Configure sources aus.
2. Geben Sie auf der Seite Discovery-Quellen konfigurieren einen benutzerfreundlichen Namen, den Host-FQDN oder die IP-Adresse, den Authentifizierungstyp (NTLM oder Kerberos), den WinRM-Benutzernamen und das WinRM-Passwort ein.
3. Wählen Sie Save configuration (Konfiguration speichern) aus.

[Das Discovery-Tool beginnt, Hyper-V Informationen zu sammeln, wie unter Entdecktes Inventar beschrieben.](#)

Die Erfassung beginnt automatisch, nachdem Sie die Anmeldeinformationen gespeichert haben.

Bei Hyper-V Failoverclustern können Sie mehrere Hosts im selben Cluster hinzufügen. Das Tool dedupliziert automatisch VMs, die auf mehr als einem Host erscheinen.

Server importieren

1. Navigieren Sie auf der Startseite des Discovery-Tools zur Seite Server importieren.

2. Bereiten Sie eine CSV-Datei mit den folgenden Spalten vor: `hostname_or_ip` (erforderlich), `os_credential_name` (optional) und `oracle_credential_name` (optional).
 - Der `hostname_or_ip` Wert muss eine gültige IPv4-Adresse oder ein vollqualifizierter Domänenname (FQDN) sein.
 - Der `os_credential_name` Wert muss, falls angegeben, dem Anzeigenamen einer Betriebssystemanmeldeinformationen entsprechen, die Sie bereits konfiguriert haben (SSH, WinRM oder SNMP). Lassen Sie das Feld leer für Server, für die Sie noch keine Betriebssystemanmeldeinformationen konfiguriert haben.
 - Der `oracle_credential_name` Wert muss, falls angegeben, mit dem Anzeigenamen eines Oracle-Anmeldedatums übereinstimmen, das Sie bereits konfiguriert haben.
3. Laden Sie die CSV-Datei hoch. Das Tool validiert alle Zeilen und lehnt die Datei ab, wenn eine Zeile ungültig ist.

Nach einem erfolgreichen Import beginnt das Tool automatisch mit der Erfassung von Datenbank-, Netzwerk- und Betriebssystemmetriken für die importierten Server, sofern die Betriebssystemanmeldedaten konfiguriert sind. Wenn Sie eine weitere CSV-Datei hochladen, werden bestehende Datensätze aktualisiert, ohne dass Duplikate erstellt werden, und neue Datensätze werden mit dem Inventar zusammengeführt.

Importieren Sie eine selbstsignierte Zertifizierungsstelle in das Discovery-Tool (optional)

Dies ist erforderlich, wenn Sie WinRM über HTTPS und Zielservers WinRM-HTTPS-Zertifikate verwenden, die von einer selbstsignierten Zertifizierungsstelle (CA) signiert wurden, und Sie „Server-SSL-Zertifikat validieren“ im Discovery-Tool aktivieren möchten.

Voraussetzungen

1. Self-signed CA-Zertifikat, das zum Signieren der WinRM-HTTPS-Zertifikate auf Zielservers verwendet wurde
2. Zertifikat im PEM-Format (Erweiterung PEM oder .CRT)

So importieren Sie eine selbstsignierte Zertifizierungsstelle in die Discoverytool-VM:

1. SSH zur Discoverytool-VM

2. Platzieren Sie die CA-Zertifikate, die die WinRM-Zertifikate Ihrer Zielsever signiert haben, im Trust Store-Verzeichnis `/etc/pki/ca-trust/source/anchors/` auf der Discovery-Tool-VM. Beispiel: `sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`. Hinweis: Wenn Ihre Zielsever Zertifikate verwenden, die von verschiedenen Zertifizierungsstellen signiert wurden, kopieren Sie alle relevanten CA-Zertifikate in dieses Verzeichnis.
3. Aktualisieren Sie den Vertrauensspeicher für Zertifikate: `sudo update-ca-trust`
4. Starten Sie die VM neu
5. (Optional) Um zu überprüfen, ob Zertifikate erfolgreich importiert wurden, können Sie den folgenden Befehl ausführen. `sudo trust list --filter=ca-anchors | grep -A 5 "<certificate_name>"`

Siehe [Installation und Konfiguration für Windows Remote Management](#)

Konfigurieren Sie das Discovery-Tool für den Betriebssystemzugriff

Konfigurieren Sie den Betriebssystemzugriff so, dass das Discovery-Tool:

- Entdecken Sie Datenbanken, um eine Datenbankbewertung durchzuführen und die VM-Migration zu unterstützen,
- Verfolgen Sie die Netzwerkverbindungen zwischen Servern in Ihrem Inventar, einschließlich des mit jeder Verbindung verbundenen Prozesses, um die Zuordnung von Anwendungsabhängigkeiten und die Wellenplanung zu unterstützen. Es werden nur Verbindungen berücksichtigt, bei denen sich beide Endpunkte im Inventar des Discovery-Tools befinden.

Aktivieren Sie das Discovery-Tool OS Access

1. Rufen Sie die Seite „OS Access einrichten“ auf, um Windows- und Linux-Anmeldeinformationen einzugeben.
2. Wählen Sie ein Protokoll aus, für das Sie Anmeldeinformationen hinzufügen möchten.
3. Geben Sie die erforderlichen Anmeldeinformationen für das ausgewählte Protokoll ein.
4. Wählen Auto-connect Sie diese Option, damit das Discovery-Tool alle angegebenen Anmeldeinformationen auf den erkannten Servern durchsucht, bis für jeden Server passende Anmeldeinformationen gefunden wurden.

Wichtige Sicherheitsempfehlungen zur automatischen Verbindungsfunktion finden [the section called “ Auto-Connect Funktion mit Vorsicht verwenden”](#) Sie unter.

5. Wählen Sie „Einrichten und verbinden“.

Nach Abschluss des Betriebssystemabgleichs wird eine Meldung angezeigt, dass die Datenerfassung im Gange ist, und es wird ein Fehler bezüglich Servern angezeigt, für die keine Übereinstimmung mit den Anmeldeinformationen gefunden wurde.

Einrichtung unterstützter Protokolle

Sie müssen WinRM-, SSH- und SNMP-Protokolle auf Zielserversn einrichten, damit das Discovery-Tool mit ihnen kommunizieren kann.

WinRM und WMI einrichten

WinRM wird automatisch mit allen derzeit unterstützten Versionen des Windows-Betriebssystems installiert.

Verwenden Sie das `winrm` Befehlszeilentool, um die WinRM-Konfiguration zu überprüfen oder zu bearbeiten:

- Überprüfen Sie die installierten WinRM-Listener: `winrm enumerate winrm/config/listener`
- Überprüfen Sie die WinRM-Konfigurationen: `winrm get winrm/config`
- Beispielbefehl zum Einrichten von WinRM: `winrm quickconfig -transport:https`

Listener-Ports

Der Standard-HTTP-Port ist 5985; HTTPS ist 5986. Sie können bei Bedarf andere Ports verwenden. Die Ports zwischen dem Discovery Tool und den Zielserversn müssen geöffnet sein.

Verschlüsselung

Das Discovery-Tool verwendet verschlüsselte WinRM-Kommunikation. Wir empfehlen, dass WinRM-Listener auf Zielserversn ebenfalls Verschlüsselung verwenden: `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM im Vergleich zu Kerberos

Die WinRM-Authentifizierungsprotokolle Kerberos und NTLM werden vom Discovery-Tool unterstützt. NTLM kann nur mit HTTPS verwendet werden, und Kerberos kann sowohl mit HTTP als auch mit HTTPS verwendet werden.

WMI-Anforderungen

Das Discovery-Tool fragt die folgenden WMI-Namespace ab. Das WinRM-Konto benötigt Lesezugriff auf jeden Namespace, der für Ihre Sammlungsmodule relevant ist:

WMI-Namespace	Verwendet von
root\cimv2	Betriebssystem-Metriken, Hyper-V Host-Metadaten, SQL Server-Sammlung
root\virtualization\v2	Hyper-V VM-Inventar
root\StandardCIMV2	Netzwerksammlung
root\Microsoft\SqlServer\ComputerManagement*	SQL Server-Sammlung
root\Microsoft\SqlServer\ReportServer*	SQL Server-Sammlung (SSRS)

Stellen Sie bei der Netzwerkerfassung sicher, dass die folgenden Bedingungen erfüllt sind:

- Netzwerkkonnektivität über ICMP zulassen
- Netzwerkkonnektivität über TCP-Port 135 und kurzlebigen TCP-Portbereich (49152 — 65535) zulassen
- Deaktivieren Sie UAC
- Remote-DCOM-Berechtigungen sind eingerichtet
- Erstellen Sie ein spezielles Dienstkonto mit den erforderlichen Mindestberechtigungen
- WMI-Namespace-Berechtigungen werden für Windows-Konten mit folgenden Namespaces eingerichtet:, Klasse \\root\\standardcimv2 MSFT_NetTCPConnection

Für die SQL Server-Sammlung ist aufgrund der komplexen Berechtigungsanforderungen für WMI-Objekte ein Windows-Konto (lokal oder domänengebunden) erforderlich, das zur lokalen Administratorgruppe gehört.

SSH einrichten

- Der Standardport ist 22. Benutzerdefinierte Ports werden unterstützt. Der konfigurierte Port muss zwischen dem Discovery-Tool und den Zielsevern geöffnet sein.
- Damit die SSH-Netzwerkerfassung ordnungsgemäß funktioniert, geben Sie einen Benutzer an, der für passwortloses Sudo konfiguriert ist.
- Stellen Sie sicher, dass die folgenden Befehle auf den Linux-Zielservern verfügbar sind (standardmäßig auf den meisten Distributionen installiert): `ss` oder `netstat` für die Netzwerkerfassung und `lsblk`, `iostat`, `dmidecode`, `smartctl`, `top`, `ps`, `freeip`, und `df` für die Erfassung von Betriebssystemmetriken.

Das Discovery-Tool unterstützt zwei Authentifizierungsmethoden für SSH:

Option 1: Nutzernamen und Passwort

Geben Sie den SSH-Benutzernamen und das Passwort ein. Dies ist die Standardauthentifizierungsmethode.

Option 2: Privater SSH-Schlüssel

Geben Sie den SSH-Benutzernamen und einen privaten Schlüssel im PEM-Format an. Um diese Option zu verwenden, wählen Sie bei der Konfiguration der SSH-Anmeldeinformationen in der Dropdownliste Authentifizierungstyp die Option SSH-Schlüssel aus. Wenn der private Schlüssel mit einer Passphrase verschlüsselt ist, geben Sie die Passphrase in das optionale Feld Schlüssel-Passphrase ein.

Die folgenden Schlüsselformate werden unterstützt:

- RSA
- ECDSA
- Ed25519
- OpenSSH-Format
- PKCS #8 -Format

Beide Authentifizierungsmethoden unterstützen die automatische Verbindung. Anmeldeinformationen werden im Ruhezustand verschlüsselt gespeichert.

Richten Sie SNMP ein

- Der Standardport ist 161/UDP. Benutzerdefinierte Ports werden unterstützt. Der konfigurierte Port muss zwischen dem Discovery-Tool und den Zielsevern geöffnet sein.
- Für SNMP v2: Geben Sie eine schreibgeschützte Community-Zeichenfolge an, die auf TCP-Verbindungs-oids zugreifen kann.
- Für SNMP v3: Geben Sie username/password auth/privacy Informationen mit Lesezugriff an, die auf TCP-Verbindungs-oids zugreifen können

Das Discovery-Tool benötigt Zugriff auf:

- "1.3.6.1.2.1.6.13.1.1." (tcpConnState)
- "1.3.6.1.2.1.6.19.1.8." (tcpConnectionProcess)
- "1.3.6.1.2.1.25.4.2.1.2." (hrSWRunName)

Konfigurieren Sie den Oracle-Datenbankzugriff

Konfigurieren Sie den Oracle-Datenbankzugriff so, dass detaillierte Oracle-Datenbankmetadaten direkt über SQL-Verbindungen erfasst werden. Zu den gesammelten Metadaten gehören die CDB- und PDB-Topologie, die Verwendung von Funktionen und die installierten Optionen. Diese Daten helfen Ihnen, Oracle-Datenbankmigrationen genauer zu planen. Sie können Oracle Database 12c, Version 1 (12.1) und höher, über direkte SQL-Verbindungen abrufen. OS-level Die Fallback-Erkennung funktioniert mit allen Oracle-Versionen.

Konfigurieren Sie die Oracle-Anmeldeinformationen im Discovery-Tool

1. Wählen Sie auf der Seite mit dem Discovery-Tool in der Seitenleiste die Option Datenbankzugriff aus.
2. Wählen Sie „Oracle-Anmeldeinformationen hinzufügen“.
3. Geben Sie die folgenden Informationen ein:
 - Benutzerdefinierter Name — Ein beschreibender Name für diesen Berechtigungsnachweis (z. B.). `Oracle Production`
 - Port — Der Oracle-Listener-Port (Standard 1521).

- **Dienstname** — Der Oracle-Dienstname für die Zieldatenbank.
 - **Benutzername** — Der Benutzername des Oracle-Dienstkontos.
 - **Passwort** — Das Passwort für das Oracle-Dienstkonto.
 - **Auto-connect**— Aktivieren Sie diese Option, um die Anmeldeinformationen für alle Server in Ihrem Inventar zu testen. Deaktivieren Sie diese Option, um die Anmeldeinformationen manuell bestimmten Servern zuzuweisen.
4. Um weitere Anmeldeinformationen hinzuzufügen (z. B. für verschiedene Oracle-Umgebungen), wählen Sie erneut Oracle-Anmeldeinformationen hinzuzufügen.
 5. Wählen Sie Speichern.

Modi für Anmeldeinformationen

Wenn Sie Oracle-Anmeldeinformationen konfigurieren, können Sie zwischen zwei Modi wählen:

- **Manuell** — Pinnen Sie Anmeldeinformationen an einen bestimmten Server an. Das Discovery-Tool verwendet diese Anmeldeinformationen ausschließlich für diesen Server. Wenn die Verbindung fehlschlägt, erfolgt kein Fallback. Korrigieren Sie die Konfiguration der Anmeldeinformationen, um das Problem zu beheben.
- **Auto-connect**— Das Erkennungstool versucht, alle Anmeldeinformationen für die automatische Verbindung mit jedem Server in Ihrem Inventar zu vergleichen. Wenn die Anmeldeinformationen für einen Server erfolgreich sind, verwendet das Discovery-Tool diese Anmeldeinformationen für alle nachfolgenden Sammelrunden.

Ablauf der Erkennung

Wenn Sie Oracle-Anmeldeinformationen konfigurieren, versucht das Discovery-Tool zunächst, eine direkte SQL-Verbindung herzustellen. Wenn alle Datenbankanmeldedaten fehlschlagen, greift das Tool auf die OS-level Erkennung über SSH oder WinRM zurück, sodass Sie Oracle-Installationen ohne Datenbankzugriff weiterhin erkennen können.

Das Discovery-Tool wird aktualisiert

Das Discovery-Tool verfügt nicht über eine automatische Aktualisierungsfunktion. Sie erhalten jedoch nach 30 Tagen nach der Installation eine Erinnerungsbenachrichtigung zur Aktualisierung. Es wird empfohlen, die Anwendung auf dem neuesten Stand zu halten, um die neuesten Funktionen und Sicherheitspatches zu erhalten.

Um das Tool manuell zu aktualisieren

1. Laden Sie die neueste Image-Datei des Discovery-Tools (OVA für VMware oder VHD für Hyper-V) über den bereitgestellten Link herunter.
2. (Optional) Wir empfehlen, die Image-Datei des vorherigen Discovery Tools zu löschen, bevor Sie die neueste bereitstellen.
3. Folgen Sie den Schritten im Abschnitt Das Discovery-Tool bereitstellen, um die aktualisierte Version bereitzustellen.

Aufheben des Zugriffs

Sie können den Zugriff für jede Discovery-Quelle unabhängig voneinander widerrufen. Wenn Sie den Zugriff für eine Quelle widerrufen, sind Daten aus anderen Quellen nicht betroffen.

- **Widerrufen des vCenter-Zugriffs** — Löscht vCenter-Anmeldeinformationen und -Daten. VMware-collected Löscht keine Hyper-V Daten, importierten Serverdaten oder Betriebssystemanmeldedaten.
- **Hyper-V Zugriff widerrufen** — Löscht nur Hyper-V Anmeldeinformationen und Hyper-V-collected Daten.
- **Importierte Server löschen** — Entfernt importierte Server aus dem Inventar. Downstream-Erfassungsdaten (Netzwerk, Datenbank), die von diesen Servern gesammelt wurden, werden beibehalten.

Erforderliche Berechtigungen für das Discovery-Tool

Das Discovery-Tool stellt über mehrere Protokolle eine Verbindung zu Ihrer Infrastruktur her. Für jedes Protokoll und Erfassungsmodul sind spezifische Kontoberechtigungen erforderlich. In diesem Abschnitt werden die Mindestberechtigungen beschrieben, die für die vollständige Datenerfassung erforderlich sind, und welche Daten Sie verlieren, wenn bestimmte Berechtigungen nicht verfügbar sind.

VMware vCenter

Das Discovery-Tool stellt über Port 443 (HTTPS) eine Verbindung zu VMware vCenter Server her und führt schreibgeschützte Operationen durch. An Ihrer vCenter-Umgebung werden keine Änderungen vorgenommen.

Erforderliche Mindestrolle: Read-Only, auf der vCenter-Root-Ebene zugewiesen.

Die Read-Only Rolle bietet den gesamten Zugriff, den das Discovery-Tool benötigt, um das VM-Inventar (Name, UUID, CPU, Arbeitsspeicher, Festplatte, Netzwerk, Betriebsstatus, Gastbetriebssystem) und Leistungskennzahlen (CPU-Auslastung, Speicherauslastung, Festplatten-IOPS und Durchsatz) zu erfassen.

Empfehlung: Erstellen Sie einen dedizierten vCenter-Benutzer mit der integrierten Read-Only Rolle auf der Ebene des Root-Rechenzentrums.

Hyper-V Hosts (Windows)

Das Discovery-Tool stellt über WinRM (Port 5985 für HTTP, Port 5986 für HTTPS) eine Verbindung zu Hyper-V Hosts her und führt PowerShell Befehle zum Sammeln von VM-Inventar, Host-Metadaten und Speicherleistung aus.

Erforderliche Mindestanzahl an Gruppenmitgliedschaften auf jedem Host: Hyper-V

Windows-Gruppe	Warum wird es benötigt
Benutzer der Fernverwaltung	Basisversion des WinRM-Fernzugriffs
Hyper-V Administratoren	Erfassung des VM-Inventars (VM-Liste, Festplatte, Netzwerk, Arbeitsspeicher, Gastbetriebssystem)
Benutzer von Performance Monitor	I/O Leistungsindikatoren für Speicher (read/write IOPS und Durchsatz pro VM)

Das Konto benötigt außerdem WMI-Lesezugriff auf den `root\cimv2` Namespace für die Host-Betriebssystemversion und die Hardware-UUID. Dieser Zugriff wird standardmäßig für lokale Administratoren gewährt, muss jedoch für Konten, die keine Administratoren sind, explizit konfiguriert werden.

Empfehlung: Erstellen Sie ein dediziertes Domänendienstkonto und fügen Sie es den Gruppen Remote Management Users, Hyper-V Administrators und Performance Monitor-Benutzer auf jedem Hyper-V Host hinzu. Vermeiden Sie die Verwendung von Domänenadministratorkonten.

Linux-Server (SSH)

Das Discovery-Tool stellt über SSH (Port 22) eine Verbindung zu Linux-Servern her, um Betriebssystemmetriken, Netzwerkverbindungen und Serverinventar zu erfassen. Die meisten Datenerfassungen werden von einem normalen Benutzer ausgeführt. Bei einer kleinen Anzahl von Befehlen wird versucht, sudo automatisch auf Sudo zurückzugreifen, wenn sudo nicht verfügbar ist.

Erforderlicher Mindestzugriff: Ein SSH-Benutzerkonto, mit dem Sie sich am Zielsystem anmelden können.

Empfohlener Zugriff: Derselbe SSH-Benutzer, der mit passwortlosem Sudo für die vollständige Datenerfassung konfiguriert wurde.

Was benötigt Sudo und was passiert ohne Sudo:

Gesammelte Daten	Sudo benötigt?	Was verlierst du ohne Sudo
Servername, Betriebssystem, CPU, Arbeitsspeicher, IP, Festplattenanzahl	Nein	Nichts — als normaler Benutzer gesammelt
CPU-, Arbeitsspeicher- und Netzwerkauslastung	Nein	Nichts — als normaler Benutzer gesammelt
Festplatten-IOPS, Durchsatz und Speicherplatz	Nein	Nichts — als normaler Benutzer gesammelt
Konfiguration der Netzwerkschnittstelle	Nein	Nichts — als normaler Benutzer gesammelt
Laufende Prozesse (Name, PID, Befehl)	Nein	Nichts — als normaler Benutzer gesammelt
Server-UUID und SMBIOS-UUID	Ja	UUID-Felder sind im Export leer
Hardwarehersteller (physische oder virtuelle Erkennung)	Ja	Die Erkennung des Ressourcentyps ist bei älteren Distributionen weniger genau

Gesammelte Daten	Sudo benötigt?	Was verlierst du ohne Sudo
Erkennung logischer LVM-Volumen	Ja	LVM-Volumes wurden nicht erkannt; der Volumetyp wird möglicherweise als „Unbekannt“ angezeigt
Netzwerkverbindungen mit Prozessname und PID	Ja	Verbindungen werden weiterhin gesammelt, jedoch ohne Prozesszuweisung (die Spalten PID und Prozessname sind leer)
OS-level Oracle-Datenbank-Erkennung (Fallback, wenn Oracle-Anmeldeinformationen nicht konfiguriert sind)	Ja	Die grundlegende Oracle-Präsenzerkennung (Oratab, Process Monitor) funktioniert auch ohne Sudo. Für die detaillierte Erfassung (opatch, lsnrctl, ASM, Grid Infrastructure) ist ein <code>sudo -u oracle</code> passwortloser Zugriff auf die Oracle-Home-Binärdateien erforderlich.

Note

Das Discovery-Tool versagt nie vollständig, weil Sudo fehlt. Es sammelt, was es kann, und meldet Teilergebnisse. Für die vollständigsten Daten — insbesondere die Zuordnung von Netzwerkabhängigkeiten mit Prozessnamen — empfehlen wir jedoch `sudo` ohne Passwort.

Erforderliche Dienstprogramme auf den Zielsevern: Die folgenden Befehle sollten verfügbar sein (standardmäßig auf den meisten Linux-Distributionen installiert): `ss` oder `netstat`, `lsblk`, `top`, `ps`, `free`, `ip`, `df`, `hostname`, `cat` und `nproc`. `grep` Optional für zusätzliche Daten: `iostat` (I/O Festplattendetail), `dmidecode` (Hardware-UUID), `smartctl` (Festplattenschnittstellentyp), `lvdisplay` (LVM-Erkennung).

Windows-Server (WinRM) — Betriebssystemmetriken

Das Erkennungstool stellt über WinRM eine Verbindung zu Windows-Servern her, um Betriebssystemmetriken (Serverinventar, Leistung, Speicher, Netzwerkschnittstellen und laufende Prozesse) zu sammeln.

Erforderlicher Mindestzugriff: Ein WinRM-enabled Benutzerkonto mit Remotezugriff auf den Zielservers.

Empfohlener Zugriff: Ein Benutzer in der lokalen Administratorgruppe für die vollständige Datenerfassung.

Berechtigungsstufe	Was es ermöglicht	Was verlierst du ohne es
Fernverwaltungsbenutzer (WinRM-Zugriff)	Erfassung aller Windows-Daten	Es wurden keine Daten vom Server gesammelt
WMI-Lesezugriff auf <code>root\cimv2</code>	Servename, Betriebssystemversion, Speicher, UUID, BIOS-Seriennummer, Festplattenspeicher	Die Felder für das Serverinventar sind leer
Benutzer des Systemmonitors	CPU-Auslastung, Netzwerkdurchsatz, Festplatten-IOPS und Durchsatz	Leistungskennzahlen wurden nicht erfasst
Lokaler Administrator	Namen der Eigentümer des laufenden Prozesses	Die Prozessliste wurde gesammelt, aber die user/owner Spalte ist leer

Note

Die Mitgliedschaft als lokaler Administrator gewährt Systemmonitor-Benutzern implizit Zugriff und WMI-Lesezugriff, sodass alle oben genannten Anforderungen erfüllt werden.

Note

Die OS-level Oracle-Datenbank-Fallback-Erkennung unter Windows verwendet Registrierungsabfragen `Get-Service` und `Get-Process` -befehle, wenn die Oracle-Anmeldeinformationen nicht konfiguriert sind. Für diese Befehle ist nur der Standardzugriff von Remote Management-Benutzern erforderlich. Es sind keine zusätzlichen Berechtigungen erforderlich, die über die Anforderungen an die Betriebssystemmetriken hinausgehen.

Windows-Server (WinRM) — SQL Server-Sammlung

Die SQL Server-Sammlung erkennt SQL Server-Instanzen, Reporting Services (SSRS) und Integration Services (SSIS) auf Windows-Servern.

Empfohlener Zugriff: Ein Benutzer in der lokalen Administratorgruppe auf jedem Windows-Zielserver.

Ein lokaler Administrator wird empfohlen, da die SQL Server-Discovery mehrere WMI-Namespaces abfragt und für einige Operationen erweiterte Zugriffsrechte erfordert:

Was wurde entdeckt	Genehmigung erforderlich	Was verlierst du ohne sie
SQL Server Database Engine-Instanzen (Version, Edition, Status)	WMI-Lesezugriff auf Namespaces <code>root\Microsoft\SqlServer\ComputerManagement*</code>	SQL Server-Instanzen wurden nicht erkannt
SQL Server Reporting Services (SSRS)	WMI-Lesezugriff auf Namespaces <code>root\Microsoft\SqlServer\ReportServer</code>	SSRS-Komponenten wurden nicht erkannt
SSRS-URL und Port-Konfiguration	Erhöhte Rechte (Lokaler Administrator)	SSRS-URL-Reservierungsdetails fehlen
SQL Server Integration Services (SSIS)	Lesezugriff auf die Registrierung (HKLM)	SSIS-Version und -Edition fehlen
Port-to-service Assoziation	Zugriff auf die TCP-Listener-Aufzählung	Die Abhörports können den SQL Server-Diensten nicht zugeordnet werden

Note

Die SQL Server-Sammlung ist Windows-only. Das Discovery-Tool überspringt Linux-Server bei der SQL Server-Erkennung.

Oracle-Datenbank (SQL)

Die Oracle-Datenbanksammlung stellt eine direkte Verbindung zu Oracle-Instanzen auf Port 1521 (oder einem benutzerdefinierten Port) her, um Datenbank-Metadaten zu sammeln. Für das Discovery-Tool sind keine DBA- oder SYSDBA-Rechte erforderlich.

Erforderlicher Mindestzugriff: Ein schreibgeschütztes Oracle-Dienstkonto mit der Gewährung `SELECT_CATALOG_ROLE`.

Das Discovery-Tool greift nicht auf die Ansichten von Diagnostics Pack oder Tuning Pack zu, sodass keine zusätzliche Oracle-Lizenz für die Datenerfassung erforderlich ist.

SQL, um das Konto zu erstellen:

```
CREATE USER discovery_user IDENTIFIED BY <password>;
GRANT CREATE SESSION TO discovery_user;
GRANT SELECT_CATALOG_ROLE TO discovery_user;
```

OS-level Fallback: Wenn Datenbankanmeldedaten nicht konfiguriert sind oder die Verbindung fehlschlägt, verwendet das Discovery-Tool vorhandene SSH- oder WinRM-Betriebssystemanmeldeinformationen, um Oracle-Installationen zu erkennen. Es sind keine zusätzlichen Oracle-specific Betriebssystemberechtigungen erforderlich, die über das Betriebssystem-Metrikmodul hinausgehen.

Erfassung im Netzwerk

Für die Netzwerkerfassung werden je nach Betriebssystem des Servers unterschiedliche Protokolle verwendet:

Betriebssystem des Servers	Protocol (Protokoll)	Berechtigungen erforderlich
Linux	SSH	Normaler Benutzer für Verbindungsdaten. Für Details auf Prozessebene (PID und Prozessname) wird sudo ohne Passwort empfohlen.

Betriebssystem des Servers	Protocol (Protokoll)	Berechtigungen erforderlich
Linux	SNMPv2	Eine nur lesbare Community-Zeichenfolge mit Zugriff auf die TCP-MIB (tcpConnState, tcpConnectionProcess) und die Host-Ressourcen-MIB (hr). SWRunName
Linux	SNMPv3	Ein USM-Benutzer mit Lesezugriff auf dieselben MIBs wie SNMPv2. Unterstützt die Sicherheitsstufen noAuthNoPriv, auth und NoPriv authPriv.
Windows	WinRM	WMI-Lesezugriff auf den root\StandardCIMV2 Namespace (MSFT_NetTCPConnection-Klasse).

Kurzreferenz: Mindestberechtigungen nach Anwendungsfall

Anwendungsfall	Account type (Art des Kontos)	Mindestberechtigungen
VMware-VM-Erkennung	vCenter-Benutzer	Read-Only Rolle auf der Ebene des Root-Rechenzentrums
Hyper-V VM-Erkennung	Windows-Domäne oder lokales Konto	Fernverwaltungsbenutzer + Hyper-V Administratoren + Performance Monitor-Benutzer auf jedem Host
Linux-Betriebssystem-Metriken — vollständige Daten	SSH-Benutzer	Passwortloses Sudo
Linux-Betriebssystem-Metriken — unvollständige Daten	SSH-Benutzer	Normaler Benutzer (kein Sudo). UUID, Hersteller, LVM und Netzwerkprozessinformationen werden fehlen.

Anwendungsfall	Account type (Art des Kontos)	Mindestberechtigungen
Windows-Betriebssystem-Metriken — vollständige Daten	WinRM-Benutzer	Lokaler Administrator
Windows-Betriebssystem-Metriken — Basisdaten	WinRM-Benutzer	Fernverwaltungsbenutzer + WMI-Lesezugriff auf root\cimv2
Erkennung der SQL Server-Datenbank	WinRM-Benutzer	Lokaler Administrator
Oracle-Datenbankerkennung (SQL)	Oracle-Dienstkonto	SELECT_CATALOG_ROLE (schreibgeschützt, kein DBA oder SYSDBA)
Netzwerksammlung — Linux (SSH)	SSH-Benutzer	Passwortloses Sudo für Daten auf Prozessebene; regulärer Benutzer nur für Verbindungsdaten
Netzwerksammlung — Linux (SNMP)	SNMP-Community-Zeichenfolge oder USM-Benutzer	Lesezugriff auf TCP- und Host-Ressourcen-MIBs
Netzwerksammlung — Windows	WinRM-Benutzer	WMI-Lesezugriff auf root\StandardCIMV2

Datenerfassung

Zeitplan für die Erfassung des Discovery-Tools

Nach Ihrer ersten Erfassung wird das Discovery-Tool nach einem gestaffelten Zeitplan weiter ausgeführt, um Ressourcenkonflikte zu vermeiden:

- VMware-Erkennung — jede Stunde (um :00 Uhr UTC)
- Hyper-V Entdeckung — jede Stunde (um 20 Uhr UTC)

Das Discovery-Tool erfasst außerdem Betriebssystem-Metriken über die folgenden unabhängigen Module, von denen jedes seinen eigenen gestaffelten Zeitplan hat:

- Netzwerkmetriken — alle 15 Sekunden, bei großen Umgebungen möglicherweise seltener
- Metriken zur Serverleistung — alle 10 Minuten (at:03, :13, :23, :33, :43, :53 UTC)
- Messdaten zur Speicherleistung — alle 10 Minuten (um :07, :17, :27, :37, :47, :57 UTC)
- Laufende Prozesse — stündlich (um :40 UTC)
- Daten zur Serverbereitstellung — täglich (um 00:05 Uhr UTC)
- Daten zur Speicherbereitstellung — täglich (um 00:35 UTC)
- Netzwerkschnittstellen — täglich (um 01:05 UTC)
- SQL Server-Erkennung — täglich (um 03:05 Uhr UTC)
- Oracle-Datenbankerkennung — täglich (um 05:05 Uhr UTC)

Sie können jedes Modul für Betriebssystemmetriken unabhängig starten, stoppen oder auslösen, indem Sie die Option Jetzt Daten sammeln verwenden.

Um eine Erfassung manuell auszuführen, wählen Sie im Menü Aktionen:

- Start — Aktiviert das Discovery-Modul.
- Stopp — Deaktiviert das Discovery-Modul.
- Jetzt Daten sammeln — Startet sofort die Erkennung. Verwenden Sie diese Option beispielsweise, nachdem Sie eine Änderung in Ihrem Netzwerk vorgenommen haben.

Diese Aktionen gelten pro Modul. Sie können die Module für Betriebssystem-Metriken einzeln steuern.

Versuche zur Erfassung von Betriebssystemdaten

Wenn ein neuer Server erkannt wird, versucht das Discovery-Tool, alle konfigurierten Anmeldeinformationen für jede IP-Adresse und den Hostnamen zu verwenden. Nachdem das Discovery-Tool gültige Anmeldeinformationen gefunden hat, verwendet es diese Anmeldeinformationen weiter, sofern Sie keine neuen Anmeldeinformationen hinzufügen.

Nach einem Erfassungsfehler versucht das Discovery-Tool nach 3 Minuten, 30 Minuten, 2 Stunden und dann 6 Stunden, Netzwerkdaten für einen Server zu sammeln. Nach 4 fehlgeschlagenen

Versuchen versucht das Discovery-Tool weiterhin, alle konfigurierten Anmeldeinformationen einmal alle 6 Stunden zu testen.

Inventar wurde entdeckt

Nachdem Sie eine Discovery-Quelle konfiguriert haben, beginnt der Wert Anzahl der erkannten Server im Statusfenster des Discovery-Tools zu steigen. Der Erkennungsstatus für die konfigurierte Quelle ändert sich im Bereich des Sammlungsmoduls auf Aktiviert. Auf der Inventarseite werden Server aus allen konfigurierten Quellen angezeigt: VMware-VMs, Hyper-V VMs und importierte Server. Jeder Server zeigt seine Quelle und seinen Erfassungsstatus pro Modul an.

Rufen Sie die Seite Entdecktes Inventar auf, um die Server zu sehen, die das Discovery-Tool gefunden hat. Wählen Sie auf dieser Seite die Option Inventar herunterladen aus, um eine ZIP-Datei (`discovery_tool_export.zip`) herunterzuladen, die bis zu 30 Tage gesammelte Daten enthält, einschließlich MPA-Dateien für alle konfigurierten Quellen, Daten zur Leistungsauslastung, Datenbankinformationen und Informationen zur Server-zu-Server-Kommunikation.

Sie können die ZIP-Datei herunterladen, während das Discovery-Tool weiterhin funktioniert, und Teilergebnisse erhalten. Laden Sie diese Datei zu [Migration Assessment](#) hoch, um ein Geschäftsszenario für die Migration zu erhalten.

Optionen für den Export

Beim Exportieren von Daten können Sie den Export mit den folgenden Optionen anpassen:

Datumsbereich

Wählen Sie ein Start- und Enddatum aus, um nur Daten zu exportieren, die innerhalb dieses Zeitraums gesammelt wurden. Beide Daten sind inklusive. Der maximale Datumsbereich beträgt 30 Tage.

Note

Das Discovery-Tool speichert gesammelte Daten für bis zu 30 Tage. Wenn Sie Daten benötigen, die sich über mehr als 30 Tage erstrecken, führen Sie alle 30 Tage inkrementelle Exporte durch, um alle Daten zu erfassen.

Auswahl des Moduls

Wählen Sie aus, welche Datenmodule in den Export aufgenommen werden sollen. Sie können alle Module exportieren oder bestimmte auswählen:

Modul	Description
VMware-Daten	Inventar virtueller Maschinen von vCenter Servern
Hyper-V Daten	Inventar virtueller Maschinen von Hyper-V Hosts
Netzwerkdaten	Netzwerkverbindungen zwischen Servern
Serverinventar	Informationen zur Serverhardware und zum Betriebssystem
Metriken zur Serverleistung	CPU-, Arbeitsspeicher- und Netzwerkauslastung
Leistung des Serverspeichers	Festplatten-IOPS und Durchsatz
Speicherkonfiguration	Konfiguration von Festplatte und Volume
Netzwerkschnittstellen	Einzelheiten zum Netzwerkadapter
Metriken verarbeiten	Ausgeführte Prozesse
SQL Server-Daten	Inventar der SQL Server-Datenbank
Oracle-Datenbankdaten	Oracle-Datenbankinventar — CDBs, PDBs, Funktionen, Optionen und Komponenten

Wenn Sie keine Module auswählen, exportiert das Discovery-Tool alle verfügbaren Daten.

Gesammelte Datenpunkte

Das Discovery-Tool sammelt umfassende Daten zu VMware- Hyper-V, Betriebssystemmetriken, Datenbank- und Netzwerkkomponenten. In den folgenden Abschnitten werden die spezifischen Datenpunkte beschrieben, die für jede Komponente gesammelt wurden.

VMware-Datenerfassung

In dieser Tabelle werden die vom Discovery-Tool gesammelten Informationen zu virtuellen VMware-Maschinen beschrieben:

Name	Typ	Kategorie	Beispielwert
vm_name	Zeichenfolge	Informationen zur virtuellen Maschine	„w2k22-snmpd-v2-de-de-mssql-2022-testcase4-1“
VM_ID	Zeichenfolge	Informationen zur virtuellen Maschine	„vm-30920“
vm_uuid	Zeichenfolge	Informationen zur virtuellen Maschine	„4201ecf8-cc44-ee7e-01da-34dfb2acf6c0“
Energiezustand	Zeichenfolge	Informationen zur virtuellen Maschine	„Eingeschaltet“
Host	Zeichenfolge	Informationen zur virtuellen Maschine	„esxi-70-node1.testlab.local“
primäre_IP-Adresse	Zeichenfolge	Informationen zur virtuellen Maschine	„192.168.0.52“
CPUs	Ganzzahl	Informationen zur virtuellen Maschine	2
memory	Ganzzahl	Informationen zur virtuellen Maschine	4096
total_disk_capacity_mib	Ganzzahl	Informationen zur virtuellen Maschine	32768

Name	Typ	Kategorie	Beispielwert
os_gemäss_der_konfiguration_sdatei	Zeichenfolge	Informationen zur virtuellen Maschine	„Microsoft Windows Server 2016 oder höher (64-Bit)“
max_cpu_usage_pct_dec	Gleitkommazahl	VM-Leistung	79,33
avg_cpu_usage_pct_dec	Gleitkommazahl	Leistung virtueller Rechner	45,06
max_ram_usage_pct_dec	Gleitkommazahl	VM-Leistung	63,99
avg_ram_utl_pct_dec	Gleitkommazahl	Leistung virtueller Rechner	29,27

Hyper-V Datenerhebung

In dieser Tabelle werden die vom Discovery-Tool gesammelten Informationen zur Hyper-V virtuellen Maschine beschrieben:

Name	Typ	Kategorie	Beispielwert
vm_name	Zeichenfolge	Informationen zur virtuellen Maschine	„win2022-hyperv-test-01“
VM_ID	Zeichenfolge	Informationen zur virtuellen Maschine	„a1b2c3d4-e5f6-7890-abcd-ef1234567890“
Energiezustand	Zeichenfolge	Informationen zur virtuellen Maschine	„Läuft“

Name	Typ	Kategorie	Beispielwert
CPUs	Ganzzahl	Informationen zur virtuellen Maschine	4
Speicher_MB	Ganzzahl	Informationen zur virtuellen Maschine	8192
Festplattenpfade	Zeichenfolge	Festplatte	„C:\\ VMs\\ disk1.vhdx“
Festplattengröße_GB	Gleitkommazahl	Festplatte	127,0
Netzwerkadapter	Zeichenfolge	Netzwerk	„00:15:5“ D:01:02:03
ip_adressen	Zeichenfolge	Netzwerk	„10.0.1.50“
host_name	Zeichenfolge	Host	„hyperv-host-01.example.com“
host_os_version	Zeichenfolge	Host	„Windows Server 2022-Rechenzentrum“
Clustername	Zeichenfolge	Host	„01“ FailoverCluster
hypervisor	Zeichenfolge	Informationen zur virtuellen Maschine	"Hyper-V"

Importierte Serverdaten

Importierte Server werden nicht automatisch erkannt. Sie werden über eine CSV-Datei importiert. Das Discovery-Tool sammelt keine Daten auf Hypervisor-Ebene für importierte Server. Stattdessen sammelt es Datenbank-, Netzwerk- und Betriebssystem-Metrikdaten, indem es beim Import die Betriebssystemanmeldedaten verwendet, die jedem Server zugeordnet sind.

Die OS-related Daten des Discovery-Tools

Das Discovery-Tool erfasst Serverinventar-, Leistungs-, Speicher-, Netzwerkschnittstellen- und Prozessdaten über SSH (Linux) und WinRM (Windows). In den folgenden Tabellen werden die gesammelten Datenpunkte beschrieben.

Serverinventar (server_inventory.csv)

Kombiniert Serverbereitstellung (Hardware- und Betriebssystemkonfiguration) mit aggregierter Speicherleistung. Wird alle 24 Stunden gesammelt.

Name	Typ	Kategorie	Beispielwert
server_id	Zeichenfolge	Server-Info	„vm-webserver-01“
Servername	Zeichenfolge	Server-Info	„Webserver-01“
resource_type	Zeichenfolge	Server-Info	„virtuelle_Maschine“
Energiestatus	Zeichenfolge	Server-Info	„Läuft“
os_type	Zeichenfolge	Server-Info	„Linux“
Betriebssystemname	Zeichenfolge	Server-Info	„Amazon Linux“
os_version	Zeichenfolge	Server-Info	„2023“
primärer_Hostname	Zeichenfolge	Server-Info	„webserver-01.example.com“
primäre_IP-Adresse	Zeichenfolge	Server-Info	„10.0.2.101“
Netzmaske	Zeichenfolge	Server-Info	„255.255.255.0“
Gesamtzahl der Netzwerkkarten	Ganzzahl	Server-Info	2
Gesamtzahl der Festplatten	Ganzzahl	Server-Info	1
CPU-Anzahl	Ganzzahl	Server-Info	4

Name	Typ	Kategorie	Beispielwert
Gesamtspeicher_GB	Gleitkommazahl	Server-Info	15,88
server_uuid	Zeichenfolge	Server-Info	„4201ecf8-cc44-ee7e-01da-34dfb2acf6c0“
smbios_uuid	Zeichenfolge	Server-Info	„4201ecf8-cc44-ee7e-01da-34dfb2acf6c0“
Clustername	Zeichenfolge	Server-Info	„Produktionscluster-01“
Hypervisor-Objekt-ID	Zeichenfolge	Server-Info	„vm-30920“
Hypervisor-Typ	Zeichenfolge	Server-Info	„VMware“
Hypervisor-Version	Zeichenfolge	Server-Info	„8.0.0“
Hypervisor-Hostname	Zeichenfolge	Server-Info	„esxi-node1.example.com“
Hypervisor-Host-ID	Zeichenfolge	Server-Info	„Host-1234“
Hypervisor-ID	Zeichenfolge	Server-Info	„4201ecf8-cc44-ee7e-01da-34dfb2acf6c0“
disk_read_iops_avg	Gleitkommazahl	Leistung des Speichers	12,5
disk_read_iops_peak	Gleitkommazahl	Speicherleistung	245,0
disk_write_iops_avg	Gleitkommazahl	Leistung des Speichers	8.3
disk_write_iops_peak	Gleitkommazahl	Speicherleistung	180,0
festplatte_total_iops_avg	Gleitkommazahl	Leistung des Speichers	20,8

Name	Typ	Kategorie	Beispielwert
festplatte_total_iops_peak	Gleitkommazahl	Speicherleistung	425,0
disk_readthroughput_avg_mbps	Gleitkommazahl	Leistung des Speichers	1.2
disk_read_throughput_peak_mbps	Gleitkommazahl	Leistung des Speichers	24,5
disk_write_throughput_avg_mbps	Gleitkommazahl	Leistung des Speichers	0.8
disk_write_throughput_peak_mbps	Gleitkommazahl	Leistung des Speichers	18,0
Festplattengesamtdurchsatz_avg_mbps	Gleitkommazahl	Leistung des Speichers	2.0
disk_total_throughput_peak_mbps	Gleitkommazahl	Leistung des Speichers	42,5

Metriken zur Serverleistung (server_performance_metrics.csv)

Auslastung des CPU-, Arbeitsspeicher- und Netzwerkdurchsatzes. Alle 10 Minuten entnommen und über einen Zeitraum von 30 Tagen aggregiert.

Name	Typ	Kategorie	Wert der Stichprobe
server_id	Zeichenfolge	Server-Info	„vm-webserver-01“
data_source	Zeichenfolge	Server-Info	„BETRIEBSSYSTEM“
CPU_Auslastung_AVG_PCT	Gleitkommazahl	CPU	45,06
CPU-Auslastung_Peak_Pct	Gleitkommazahl	CPU	79,33

Name	Typ	Kategorie	Wert der Stichprobe
CPU-Anzahl	Ganzzahl	CPU	4
Speicher_insgesamt_GB	Gleitkommazahl	Arbeitsspeicher	15,88
Speicherauslastung_avg_pct	Gleitkommazahl	Arbeitsspeicher	29,27
Speicherauslastung_Peak_Pct	Gleitkommazahl	Arbeitsspeicher	63,99
Netzwerk_in_AVG_Mbit/s	Gleitkommazahl	Netzwerk	0,52
Network_in_Peak_Mbit/s	Gleitkommazahl	Netzwerk	12.3
network_out_avg_mbps	Gleitkommazahl	Netzwerk	0,31
network_out_peak_mbps	Gleitkommazahl	Netzwerk	8.7
Netzwerk_insgesamt_avg_mbps	Gleitkommazahl	Netzwerk	0,83
netzwerk_total_peak_mbps	Gleitkommazahl	Netzwerk	21,0

Speicherleistung (server_storage_performance.csv)

Per-volume Festplatten I/O - und Speicherauslastung. Alle 10 Minuten entnommen und über einen Zeitraum von 30 Tagen aggregiert.

Name	Typ	Kategorie	Wert der Stichprobe
server_id	Zeichenfolge	Server-Info	„vm-webserver-01“

Name	Typ	Kategorie	Wert der Stichprobe
data_source	Zeichenfolge	Server-Info	„BETRIEBSSYSTEM“
datenträger_volume_id	Zeichenfolge	Informationen zum Volumen	"/dev/nvme0n1p1"
disk_mount_point	Zeichenfolge	Informationen zum Volumen	"/"
Dateisystem	Zeichenfolge	Informationen zum Volumen	„xfs“
festplatte_total_gb	Gleitkommazahl	Festplatte enkapazität	30.0
festplatte_benutzte_GB	Gleitkommazahl	Festplatte enkapazität	12,5
disk_free_gb	Gleitkommazahl	Festplatte enkapazität	17,5
disk_read_iops_avg	Gleitkommazahl	Festplatte I/O	12,5
disk_read_iops_peak	Gleitkommazahl	Festplatte I/O	245,0
disk_write_iops_avg	Gleitkommazahl	Festplatte I/O	8.3
disk_write_iops_peak	Gleitkommazahl	Festplatte I/O	180,0
festplatte_total_iops_avg	Gleitkommazahl	Festplatte I/O	20,8
festplatte_total_iops_peak	Gleitkommazahl	Festplatte I/O	425,0

Name	Typ	Kategorie	Wert der Stichprobe
disk_readthroughput_avg_mbps	Gleitkommazahl	Festplattendurchsatz	1.2
disk_read_throughput_peak_mbps	Gleitkommazahl	Festplatten-Durchsatz	24,5
disk_write_throughput_avg_mbps	Gleitkommazahl	Festplatten-Durchsatz	0.8
disk_write_throughput_peak_mbps	Gleitkommazahl	Festplatten-Durchsatz	18,0
Festplattengesamtdurchsatz_avg_mbps	Gleitkommazahl	Festplatten-Durchsatz	2.0
disk_total_throughput_peak_mbps	Gleitkommazahl	Festplatten-Durchsatz	42,5

Speicherkonfiguration (storage_config.csv)

Hardwaredetails zur physischen Festplatte. Wird alle 24 Stunden gesammelt.

Name	Typ	Kategorie	Beispielwert
server_id	Zeichenfolge	Server-Info	„vm-webserver-01“
Festplatten-Controller-ID	Zeichenfolge	Festplatten-Informationen	"/dev/sda"
vmdk_vhd_dateiname	Zeichenfolge	Festplatten-Informationen	„webserver-01.vmdk“
Datenträger_Volumetyp	Zeichenfolge	Festplatten-Informationen	„Virtuell“
disk_provisioned_gb	Gleitkommazahl	Festplatten-Informationen	30.0

Name	Typ	Kategorie	Beispielwert
Festplattengerätetyp	Zeichenfolge	Festplatten-Informationen	„SCSI-FESTPLATTE“
Festplattenschnittstellentyp	Zeichenfolge	Festplatten-Informationen	„SCSI“
disk_protocol	Zeichenfolge	Festplatten-Informationen	„LSI Logic SAS“

Netzwerkschnittstellen (network_interfaces.csv)

Konfiguration des Netzwerkadapters. Wird alle 24 Stunden gesammelt.

Name	Typ	Kategorie	Beispielwert
server_id	Zeichenfolge	Server-Info	„vm-webserver-01“
Schnittstellename	Zeichenfolge	Informationen zur Schnittstelle	„eth0“
Schnittstellenindex	Ganzzahl	Informationen zur Schnittstelle	2
mac_address	Zeichenfolge	Informationen zur Schnittstelle	„0A:1B:2C:3D:4E:5F“
Adaptertyp	Zeichenfolge	Informationen zur Schnittstelle	„vmxnet3“
Name des virtuellen_Netzwerks	Zeichenfolge	Informationen zur Schnittstelle	„VM-Netzwerk“

Name	Typ	Kategorie	Beispielwert
virtual_network_id	Zeichenfolge	Informationen zur Schnittstelle	„dvportgroup-1234“
virtueller_Schalter	Zeichenfolge	Informationen zur Schnittstelle	„vSwitch0“
ipv4_Adresse	Zeichenfolge	IP-Konfiguration	„10.0.2.101“
ipv4_subnetzmaske	Zeichenfolge	IP-Konfiguration	„255.255.255.0“
ipv4_gateway	Zeichenfolge	IP-Konfiguration	„10.0.2.1“
ipv6_adresse	Zeichenfolge	IP-Konfiguration	„fe80: :a1b:2cff:fe3d:4e5f“
Länge des IPV6-Präfixs	Ganzzahl	IP-Konfiguration	64
ipv6_gateway	Zeichenfolge	IP-Konfiguration	„fe80: :1“
DNS-Server	Zeichenfolge	IP-Konfiguration	„10.0.0.2“
dhcp_aktiviert	Boolesch	IP-Konfiguration	false
Schnittstellenstatus	Zeichenfolge	Informationen zur Schnittstelle	„Hoch“

Name	Typ	Kategorie	Beispielwert
vlan_id	Ganzzahl	Informationen zur Schnittstelle	100
is_primary	Boolesch	Informationen zur Schnittstelle	true

Laufende Prozesse (process_metrics.csv)

Snapshot der laufenden Prozesse. Jede Stunde erfasst und über 30 Tage dedupliziert.

Name	Typ	Kategorie	Beispielwert
server_id	Zeichenfolge	Server-Info	„vm-webserver-01“
Prozessname	Zeichenfolge	Informationen zum Prozess	„sshd“
process_id	Ganzzahl	Informationen zum Prozess	1234
Befehlszeile verarbeiten	Zeichenfolge	Informationen zum Prozess	„/usr/sbin/sshd -D“
Prozessbenutzer	Zeichenfolge	Informationen zum Prozess	„Wurzel“

Netzwerk-Sammlung

Das Modul Netzwerksammlung hilft Ihnen dabei, Abhängigkeiten zwischen Servern in Ihrem lokalen Rechenzentrum zu ermitteln. Diese Netzwerkdaten beschleunigen Ihre Migrationsplanung, indem sie einen Überblick darüber bieten, wie Anwendungen zwischen Servern kommunizieren.

Dieses Modul sammelt Netzwerkdaten für Server aus allen konfigurierten Quellen, einschließlich VMware Hyper-V, und importierten Servern. Es verwendet WinRM, um Daten von Windows-Servern zu sammeln, und verwendet SSH, SNMPv2 und SNMPv3, um Daten von Linux-Servern zu sammeln.

Erfassung von Netzwerkdaten

Das Netzwerkerfassungsmodul erfasst TCP-IPv4-Verbindungen im Status ESTABLISHED oder TIME_WAIT zwischen Servern in Ihrem ermittelten Inventar. Eine Verbindung wird in der Ausgabe nur angezeigt, wenn sowohl die Quell- als auch die Ziel-IP-Adresse zu Servern gehören, die das Discovery-Tool erkannt oder die Sie importiert haben. Verbindungen zu oder von IP-Adressen außerhalb Ihres Inventars — wie externe Dienste, Cloud-Endpunkte oder Server, die dem Discovery-Tool noch nicht hinzugefügt wurden — sind nicht enthalten.

Bei diesem Design konzentrieren sich die Netzwerkdaten auf Server-zu-Server-Abhängigkeiten innerhalb Ihrer Umgebung. Dies sind die Informationen, die für die Zuordnung von Anwendungsabhängigkeiten und die Planung von Migrationswellen benötigt werden.

Diese Datenpunkte werden für jede Verbindung gesammelt:

Name	Typ	Kategorie	Beispielwert
Quell-IP	Zeichenfolge	Connection (Verbindung)	„192.168.1.10“
Quell-Port	Ganzzahl	Connection (Verbindung)	49152
Prozess-ID der Quelle	Ganzzahl	Prozess	1234
Name des Quellprozesses	Zeichenfolge	Prozess	"java"
Ziel-IP	Zeichenfolge	Connection (Verbindung)	„192.168.1.20“
Zielport	Ganzzahl	Connection (Verbindung)	5432
Zielprozess-ID	Ganzzahl	Prozess	5678

Name	Typ	Kategorie	Beispielwert
Name des Zielprozesses	Zeichenfolge	Prozess	„Postgres“
Status	Zeichenfolge	Connection (Verbindung)	„ETABLIERT“
Transportprotokoll	Zeichenfolge	Connection (Verbindung)	„TCP“
IP-Version	Zeichenfolge	Connection (Verbindung)	„IPv4“
Anzahl	Ganzzahl	Connection (Verbindung)	42

Tip

Um die Vollständigkeit Ihrer Netzwerkabhängigkeitsübersicht zu maximieren, konfigurieren Sie alle Erkennungsquellen (VMware und Server-CSV-Import) und fügen Sie Betriebssystemanmeldedaten hinzu Hyper-V, bevor Sie die Netzwerkdaten überprüfen. Je mehr Server sich in Ihrem Inventar befinden, desto mehr Verbindungen kann das Netzwerkmodul erfassen.

Erfassung von privaten Adressen im Netzwerk

Standardmäßig erfasst das Netzwerkerfassungsmodul nur Verbindungen, bei denen es sich bei beiden Endpunkten um Server in Ihrem ermittelten Inventar handelt. Sie können die Erfassung privater Adressen aktivieren, um auch Verbindungen zu und von privaten IP-Adressen nach RFC 1918 (10.0.0) zu erfassen. 0/8, 172.16.0. 0/12, 192,168,0. 0/16), die nicht in Ihrem Inventar sind.

Um mit der Erfassung privater Adressen zu beginnen

1. Suchen Sie auf der Collector-Konfigurationsseite nach dem Abschnitt Sammlungsmodule.
2. Suchen Sie unter Anwendungserkennung nach Netzwerkverbindungen.
3. Öffnen Sie das Drop-down-Menü Aktionen.

4. Wählen Sie Erfassung privater Adressen starten aus.
5. Wenn der Modulstatus Aktiviert war, können Sie sehen, wie er sich in Aktiviert · Privatadresse ändert.

Um die Erfassung privater Adressen zu beenden, öffnen Sie das Drop-down-Menü Aktionen und wählen Sie Erfassung privater Adressen beenden aus. Zuvor gesammelte private Adressdaten werden auch nach dem Stoppen beibehalten.

Verbindungen mit privaten Adressen erscheinen nur im vollständigen CSV-Export (in der ZIP-Datei), nicht in den MPA-CSV-Dateien. Wenn eine IP-Adresse zu einem Server gehört, der sich bereits in Ihrem Inventar befindet, wird sie unabhängig von dieser Einstellung immer anhand der erkannten Server-ID identifiziert.

Diese Einstellung bleibt auch nach Neustarts bestehen. Sie können die Erfassung privater Adressen jederzeit starten oder beenden. Zuvor gesammelte private Adressdaten werden unabhängig von der aktuellen Einstellung exportiert.

SQL Server-Sammlung

Das SQL Server-Sammlungsmodul sammelt SQL Server-Informationen von Windows-Servern aus allen konfigurierten Quellen, einschließlich VMware Hyper-V, und importierten Servern. Das Modul verwendet WinRM, um eine Remoteverbindung zu jedem Windows-Server herzustellen und PowerShell Abfragen auszuführen. Es sammelt Informationen über alle installierten SQL Server-Dienste (Komponenten) mithilfe von WMI-Namespace, Registrierungs- und Dateieigenschaften.

Eine SQL Server-Komponente ist eine bestimmte Dienst- oder Feature-Instanz, die als Teil einer SQL Server-Bereitstellung auf einem Windows-Server installiert wird. Das Discovery-Tool sammelt Database Engine, Analysis Services, Reporting Services und Integration Services.

SQL Server-Datenerfassung

Das SQL Server-Sammlungsmodul sammelt Informationen zu SQL Server-Komponenten. In dieser Tabelle werden die wichtigsten gesammelten Datenpunkte beschrieben:

Name	Typ	Kategorie	Wert der Stichprobe
Engine-Typ	Zeichenfolge	Komponente	sql_server

Name	Typ	Kategorie	Wert der Stichprobe
Ist eine Engine-Komponente	Boolesch	Komponente	Y
Status	Zeichenfolge	Service	Läuft, gestoppt, StartPending
Version	Zeichenfolge	Service	2015.131.5026.0
Edition	Zeichenfolge	Service	Entwickler-Edition (64-Bit)
Name des SQL-Dienstes	Zeichenfolge	Service	MsDtsServer130, Mssql
Typ des SQL-Dienstes	Zeichenfolge	Service	SQL Server-Dienst, Integration Services-Dienst
Instance-Name	Zeichenfolge	Instance	MSSQLSERVER
Anzeigenname	Zeichenfolge	Service	SQL Server (MSSQLSERVER 2017)
Startmodus	Zeichenfolge	Service	Automatisch, Manuell, Deaktiviert
Servicekonto-Name	Zeichenfolge	Service	NT Service/MsDtsServer130
Ist geclustert	Boolesch	Konfiguration	N

Note

Das vollständige Format umfasst alle Diensttypen. Das MPA-Format umfasst nur Komponenten der Datenbank-Engine. Je nach Typ und Konfiguration des SQL-Dienstes sind nicht alle Felder verfügbar.

Oracle-Datenbanksammlung

Mit der Erfassung von Oracle-Datenbanken können Sie Oracle-Datenbankinstanzen in allen konfigurierten Quellen, einschließlich VMware Hyper-V, und importierten Servern ermitteln. Das Modul sammelt die folgenden Daten:

- Aufzählung der Container-Datenbank (CDB) und der Pluggable Database (PDB)
- Version und Ausgabe
- Installierte Optionen
- Statistiken zur Nutzung von Funktionen
- Komponenteninventar (DBA_REGISTRY)
- Dimensionierung von Datendateien
- Topologie-Flags (RAC, Data Guard und Multitenant-Architektur)

Database-connected (SQL)

Wenn Sie Oracle-Anmeldeinformationen konfigurieren, stellt das Discovery-Tool mithilfe des schreibgeschützten Dienstkontos eine direkte Verbindung zur Oracle-Datenbank her. Dies bietet eine vollständige SQL-level Erfassung, einschließlich PDB-Details, Funktionsnutzung und installierter Optionen. Alle CSV-Dateien enthalten vollständige Daten.

OS-level Fallback

Wenn Sie keine Datenbankanmeldedaten konfiguriert haben oder wenn die Verbindung fehlschlägt, verwendet das Discovery-Tool SSH oder WinRM, um Oracle-Installationen zu erkennen. Es erkennt Oracle-Homes, -Listener, -Patches, -Versionen und -Editionen ohne Datenbankzugriff. Für OS-detected Hosts enthält die exportierte CDB-CSV den Instanznamen, den Hostnamen, die Version und die Edition. Die CSV-Dateien für PDB, Funktionen, Optionen und Komponenten enthalten keine Zeilen.

Die Oracle-Sammlung erzeugt die folgenden CSV-Dateien in der Export-ZIP-Datei. Jede Tabelle beschreibt die pro Datei gesammelten Datenpunkte.

CDB-Daten (oracle_data_cdb_full.csv)

Eine Zeile pro CDB-Instance. In dieser Tabelle werden die gesammelten CDB-Datenpunkte beschrieben:

Name	Typ	Kategorie	Beispielwert	Quelle
Instance-Name	Zeichenfolge	Identität	„ORCL“	SQL, OS

Name	Typ	Kategorie	Beispielwert	Quelle
Host Name (Hostname)	Zeichenfolge	Identität	„oracledb01.example.com“	SQL, OS
DB-Name	Zeichenfolge	Identität	„ORKL“	Nur SQL
Eindeutiger Datenbankname	Zeichenfolge	Identität	„ORCL_PRIMARY“	Nur SQL
DBID	Ganzzahl	Identität	1234567890	Nur SQL
Version	Zeichenfolge	Version	„19.0.0.0“	SQL, OS
Vollversion	Zeichenfolge	Version	„19.21.0.0.0“	Nur SQL
Edition	Zeichenfolge	Version	„Enterprise Edition“	SQL, OS
Datenbank-Typ	Zeichenfolge	Konfiguration	„SINGLE“	Nur SQL
Datenbankrolle	Zeichenfolge	Konfiguration	„PRIMÄR“	Nur SQL
Modus öffnen	Zeichenfolge	Konfiguration	„LESEN, SCHREIBEN“	Nur SQL
Protokollmodus	Zeichenfolge	Konfiguration	„ARCHIVELOG“	Nur SQL
Plattform	Zeichenfolge	Konfiguration	„Linux x86 64-Bit“	Nur SQL
CDB-Flagge	Zeichenfolge	Konfiguration	„JA“	Nur SQL

Name	Typ	Kategorie	Beispielwert	Quelle
Ist RAC	Zeichenfolge	Topologie	„JA“ oder „NEIN“	Nur SQL
Ist Data Guard Standby	Zeichenfolge	Topologie	„JA“ oder „NEIN“	Nur SQL
Schutzmodus	Zeichenfolge	Topologie	„MAXIMALE LEISTUNG“	Nur SQL
Data Guard Broker	Zeichenfolge	Topologie	„AKTIVIERT“	Nur SQL
NLS-Zeichensatz	Zeichenfolge	Konfiguration	„AL32UTF8“	Nur SQL
PDB-Anzahl	Ganzzahl	Dimensionierung	3	Nur SQL
Flashback aktiviert	Zeichenfolge	Konfiguration	„JA“	Nur SQL
Erkennungspfad	Zeichenfolge	Metadaten	„Phase2“ oder „Phase1b“	SQL, OS

PDB-Daten (oracle_data_pdb_full.csv)

Eine Zeile pro PDB (austauschbare Datenbank). In dieser Tabelle werden die gesammelten PDB-Datenpunkte beschrieben:

Note

PDB-Daten erfordern Anmeldeinformationen für die Oracle-Datenbank (SQL-Verbindung). OS-level Fallback füllt diese CSV-Datei nicht auf.

Name	Typ	Kategorie	Beispielwert	Quelle
Name der CDB-Instanz	Zeichenfolge	Identität	„ORCL“	Nur SQL
PDB-Name	Zeichenfolge	Identität	„APPPDB1“	Nur SQL
Modus öffnen	Zeichenfolge	Status	„LESEN, SCHREIBEN“	Nur SQL
Lebenszyklus-Status	Zeichenfolge	Status	„NORMAL“	Nur SQL
Anzahl Tablespaces	Ganzzahl	Dimensionierung	5	Nur SQL
Anzahl der Datendateien	Ganzzahl	Dimensionierung	12	Nur SQL
Gesamtgröße in Byte	Ganzzahl	Dimensionierung	5368709120	Nur SQL
Anzahl der Benutzerschemas	Ganzzahl	Dimensionierung	8	Nur SQL
Anzahl der DB-Links	Ganzzahl	Konnektivität	2	Nur SQL
Installierte Komponenten	Zeichenfolge	Konfiguration	„APEX; JVM; XML“	Nur SQL
Anzahl verschlüsselter Tablespaces	Ganzzahl	Sicherheit	1	Nur SQL

Daten zur Nutzung von Funktionen (oracle_data_features_full.csv)

Eine Zeile pro Eintrag zur Feature-Nutzung aus DBA_FEATURE_USAGE_STATISTICS. In dieser Tabelle werden die gesammelten Datenpunkte zur Feature-Nutzung beschrieben:

Note

Für Daten zur Funktionsnutzung sind Anmeldeinformationen für die Oracle-Datenbank erforderlich (SQL-Verbindung). OS-level Fallback füllt diese CSV-Datei nicht auf.

Name	Typ	Kategorie	Beispielwert	Quelle
Name der CDB-Instanz	Zeichenfolge	Identität	„ORCL“	Nur SQL
Name	Zeichenfolge	Feature	„Partitionierung (Benutzer)“	Nur SQL
Entdeckte Verwendungen	Ganzzahl	Usage	42	Nur SQL
Wird derzeit verwendet	Zeichenfolge	Usage	„WAHR“	Nur SQL
Erstes Nutzungsdatum	DateTime	Usage	„2024-01-15T00:00:00“	Nur SQL
Datum der letzten Verwendung	DateTime	Usage	„2026-06-01T00:00:00“	Nur SQL

Optionsdaten (oracle_data_options_full.csv)

Eine Zeile pro V\$OPTION-Eintrag pro CDB. In dieser Tabelle werden die gesammelten Datenpunkte für installierte Optionen beschrieben:

Note

Für Optionsdaten sind Anmeldeinformationen für die Oracle-Datenbank erforderlich (SQL-Verbindung). OS-level Fallback füllt diese CSV-Datei nicht auf.

Name	Typ	Kategorie	Beispielwert	Quelle
Name der CDB-Instanz	Zeichenfolge	Identität	„ORCL“	Nur SQL
Optionsname	Zeichenfolge	Option	„Fortgeschrittene Analytik“	Nur SQL
Ist installiert	Zeichenfolge	Option	„WAHR“	Nur SQL
Container-ID	Ganzzahl	Option	0	Nur SQL

Komponentendaten (oracle_data_components_full.csv)

Eine Zeile pro DBA_REGISTRY-Komponente. In dieser Tabelle werden die gesammelten Datenpunkte der Komponenten beschrieben:

Note

Für Komponentendaten sind Anmeldeinformationen für die Oracle-Datenbank erforderlich (SQL-Verbindung). OS-level Fallback füllt diese CSV-Datei nicht auf.

Name	Typ	Kategorie	Beispielwert	Quelle
Name der CDB-Instanz	Zeichenfolge	Identität	„ORCL“	Nur SQL
PDB-Name	Zeichenfolge	Identität	„APPPDB1“	Nur SQL
Komponenten-ID	Zeichenfolge	Komponente	„APEX“	Nur SQL
Name der Komponente	Zeichenfolge	Komponente	„Oracle Application Express“	Nur SQL

Name	Typ	Kategorie	Beispielwert	Quelle
Version	Zeichenfolge	Komponente	„22.1.0.15.0“	Nur SQL
Status	Zeichenfolge	Komponente	„GÜLTIG“	Nur SQL
Schema	Zeichenfolge	Komponente	„APEX_220100“	Nur SQL

Sicherheitsüberlegungen

Sicherung der Discovery-Tool-VM

Die VM-Sicherheit des Discovery-Tools ist von entscheidender Bedeutung, da das Discovery-Tool alle Anmeldeinformationen, Protokolle und Kundendaten auf der Discovery-Tool-VM speichert.

Der SSH-Zugriff auf die Discoverytool-VM ist standardmäßig deaktiviert und der Zugriff ist nur vom Client vCenter UI -> "Launch Web Console" aus möglich.

Das Discovery-Tool VM verfügt über ein Standard-Anmeldekennwort „Passwort“ für den Benutzer „Discovery“.

- Wir empfehlen, dieses Passwort unmittelbar nach der Bereitstellung zu aktualisieren.
- Sie müssen das Passwort aktualisieren, wenn Sie SSH mit `enablessh` dem Befehl aktivieren möchten, nachdem Sie sich mit Launch Web Console vCenter angemeldet haben. Bitte beachten Sie, dass Sie diesen Befehl jedes Mal, wenn er aufgerufen wird, zurücksetzen müssen.

Anmeldeinformationen sichern

Allgemeine bewährte Methoden für die Verwaltung von Anmeldeinformationen

- Speichern Sie Anmeldeinformationen sicher
- Wechseln Sie regelmäßig alle Anmeldeinformationen
- Verwenden Sie Passwort-Manager oder sichere Tresore
- Überwachen Sie die Verwendung von Anmeldeinformationen

- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie nur die erforderlichen Mindestberechtigungen

SNMP v2-Anmeldeinformationen

- Verwenden Sie komplexe, nicht standardmäßige Community-Strings
- Vermeiden Sie häufig verwendete Zeichenketten wie „öffentlich“ oder „privat“
- Behandeln Sie Community-Zeichenketten wie Passwörter

SNMP v3-Anmeldeinformationen

- Aktivieren Sie sowohl Authentifizierung als auch Datenschutz
- Verwenden Sie starke Authentifizierungsprotokolle (SHA wird MD5 vorgezogen)
- Verwenden Sie starke Verschlüsselungsprotokolle (AES wird dem vorgezogen)
- Verwenden Sie komplexe Passwörter sowohl für die Authentifizierung als auch für den Datenschutz
- Verwenden Sie eindeutige Benutzernamen (vermeiden Sie gebräuchliche Namen)

WinRM-Anmeldeinformationen

- Vermeiden Sie es, die WinRM-Zertifikatsprüfung zu deaktivieren.
- Es wird empfohlen, ein dediziertes Dienstkonto mit den erforderlichen Mindestberechtigungen zu erstellen.
- Vermeiden Sie die Verwendung von Domänenadministrator- oder lokalen Administratorkonten, es sei denn, Sie benötigen die SQL Server-Sammlung. Für die SQL Server-Sammlung ist lokaler Administratorzugriff erforderlich, da sie mehrere WMI-Namespaces abfragt und Befehle mit erhöhten Rechten verwendet. Für Betriebssystemmetriken ohne SQL Server-Erkennung ist ein Konto ohne Administratorrechte mit Fernverwaltungsbenutzern, Systemmonitor-Benutzern und WMI-Lesezugriff ausreichend. root\cimv2 Einzelheiten zu den einzelnen [the section called „Erforderliche Berechtigungen“](#) Modulen finden Sie unter.

Hyper-V Anmeldedaten

- Verwenden Sie spezielle Dienstkonto mit minimalen Hyper-V Verwaltungsberechtigungen.
- Vermeiden Sie die Verwendung von Domänenadministratorkonten.

- Hyper-V Anmeldeinformationen unterstützen NTLM (nur HTTPS) und Kerberos-Authentifizierung.
- Das Discovery-Tool speichert Anmeldeinformationen, die im Ruhezustand mithilfe von SQLCipher verschlüsselt sind.

Oracle-Anmeldeinformationen

- Verwenden Sie ein dediziertes, schreibgeschütztes Dienstkonto mit nur `SELECT_CATALOG_ROLE`. Verwenden Sie keine DBA-, SYSDBA- oder SYSOPER-Rechte.
- Das Discovery-Tool führt nur Lesevorgänge aus und schreibt niemals in die Oracle-Datenbank.
- Das Discovery-Tool greift nicht auf die Ansichten von Diagnostics Pack oder Tuning Pack zu, sodass keine zusätzliche Oracle-Lizenz erforderlich ist.
- Wechseln Sie das Passwort für das Oracle-Dienstkonto regelmäßig und aktualisieren Sie die Anmeldeinformationen im Discovery-Tool.

Speicherung von Anmeldeinformationen

Das Discovery-Tool verschlüsselt gespeicherte Anmeldeinformationen im Ruhezustand mithilfe eines Datenbank-Verschlüsselungsschlüssels. Auf Systemen mit Systemd 250 oder höher wird dieser Schlüssel mit `systemd-creds` verschlüsselt. Auf älteren Systemen wird der Schlüssel als berechtigungsgeschützte Datei gespeichert. In beiden Fällen könnte ein Angreifer mit Root-Zugriff auf den Host des Discovery Tools auf den Verschlüsselungsschlüssel zugreifen und die gespeicherten Anmeldeinformationen entschlüsseln. Beschränken Sie den Zugriff auf den Discovery Tool-Host und behandeln Sie ihn in Ihrer Umgebung als privilegiertes System.

Verwenden Sie die Auto-Connect Funktion mit Vorsicht

Das Discovery-Tool verwendet zwei Mechanismen, um Servern während der OS-level Erfassung Anmeldeinformationen zuzuweisen: automatische Verbindung und manuell. OS-level Die Sammlung umfasst die Module Netzwerk, SQL Server, Oracle-Datenbank und Betriebssystem-Metriken. Diese Module stellen Verbindungen zu einzelnen Servern aus allen Quellen her, einschließlich VMware-VMs, Hyper-V VMs und importierten Servern.

Manuell: Ein Server kann manuell mit bestimmten Anmeldeinformationen verknüpft werden. In diesem Fall verwendet das Discovery-Tool nur diese Anmeldeinformationen, unabhängig von Erfolg oder Misserfolg. Sie müssen den Erfassungsstatus für diesen Server manuell überwachen und Anpassungen vornehmen.

Auto-connect: Wenn dem Server keine Anmeldeinformationen manuell zugeordnet wurden, verwendet das Discovery-Tool den automatischen Verbindungsmechanismus für diesen Server. Das bedeutet:

- Zu Beginn jeder Sammelrunde erhält das Discovery-Tool eine Liste der Anmeldeinformationen, die für diesen Server verfügbar sind (basierend auf den Betriebssystemtypen) und die auch so konfiguriert sind, dass sie „automatisch verbunden“ werden können.
- Das Discovery-Tool testet dann alle Anmeldeinformationen in einer Schleife mit dem Server.
 - Wenn funktionierende Anmeldeinformationen gefunden werden, ist die Sammelrunde für den Server erfolgreich. Das Discovery-Tool erinnert sich daran und versucht es beim nächsten Mal zuerst.
 - Wenn keine funktionierenden Anmeldeinformationen gefunden werden, ist die Sammelrunde für den Server fehlgeschlagen.
 - Netzwerkmodul: Der Server verwendet einen Backoff-Zeitplan und startet die nächste Sammelrunde in 3 Minuten, 30 Minuten, 2 Stunden und 6 Stunden nach jedem Ausfall (ähnlich einem exponentiellen Backoff).
 - SQL Server-Sammlung: Das Discovery-Tool versucht es nicht erneut. Es unternimmt jeden Tag einen Versuch pro Server.

Impacts/Risks:

Verwenden Sie die automatische Verbindung nur, wenn Sie sicher sind, dass die Risiken in Ihrem System gemindert sind:

Risiko 1: Wenn die automatische Verbindung für mehrere falsche Anmeldeinformationen konfiguriert ist, kann der automatische Versuch, sie gegen Server auszuführen, zu Kontosperrungen in Produktionsumgebungen führen, in denen Sperrrichtlinien konfiguriert sind. Beispielsweise kann ein Rechenzentrum seine VMs so einrichten, dass sie nach drei fehlgeschlagenen SSH-Anmeldeversuchen gesperrt werden. In diesem Fall würde es zu legitimen Kontosperrungen kommen, wenn die automatische Verbindung für 3 falsche SSH-Anmeldeinformationen konfiguriert ist. Wenn Sperrungen in mehreren Systemen auftreten, könnten kritische Geschäftsprozesse beeinträchtigt werden, was möglicherweise zu kaskadierenden Ausfällen in abhängigen Systemen führen könnte. Darüber hinaus kann es in Security Operations Centers zu Warnmeldungen aufgrund von Massenauthentifizierungsfehlern kommen, was zu falsch positiven Sicherheitsvorfällen führen kann, die Ressourcen belasten und echte Angriffe verschleiern können.

Risiko 2: Ein Akteur mit Zugriff auf das Discovery-Tool (kennt das Erkennungstool-Passwort) kann Betriebssystemanmeldedaten auf allen Servern mit Brute-Force-Angriffen erzwingen, indem er eine große Anzahl von Testanmeldedaten konfiguriert und automatische Verbindungen verwendet, um die erfolgreichen Anmeldeinformationen zu finden.

Abhilfemaßnahmen:

Befolgen Sie diese Richtlinien:

- Stellen Sie sicher, dass das Passwort des Discovery-Tools ordnungsgemäß gesichert ist und nur autorisierten Akteuren bekannt ist
- Stellen Sie sicher, dass die richtigen Anmeldeinformationen für die Umgebung eingegeben werden, falls Sperrrichtlinien gelten. Wir empfehlen, nur bekannte, funktionierende Anmeldeinformationen zu konfigurieren, auch wenn keine Richtlinien zur Kontosperrung vorhanden sind, um eine minimale Betriebsbelastung einzelner VMs sicherzustellen.
- "Auto-connect" ist eine Opt-in-Funktion. Wählen Sie diese Option nicht aus und verwenden Sie die manuelle Zuweisung von Anmeldeinformationen nicht, wenn Kontosperrungen umweltschädlich sind.

Sicherheit beim CSV-Import

Wenn Sie Server mithilfe einer CSV-Datei importieren, sollten Sie die folgenden Auswirkungen auf die Sicherheit berücksichtigen:

- Die CSV-Datei kann Hostnamen oder IP-Adressen interner Server enthalten. Behandeln Sie sie wie sensible Daten.
- Die `oracle_credential_name` Spalten `os_credential_name` und verweisen anhand eines benutzerfreundlichen Namens auf vorkonfigurierte Anmeldeinformationen. Die CSV-Datei enthält keine Geheimnisse.
- All-or-nothing Validierung: Wenn eine Zeile in der CSV ungültig ist, wird der gesamte Upload abgelehnt. Dies verhindert Teilimporte, die zu einem verwirrenden Zustand führen könnten.
- Importierte Server sind sofort im Inventar sichtbar und können abgeholt werden. Stellen Sie vor dem Import sicher, dass das Betriebssystem und die Oracle-Anmeldeinformationen den richtigen Gültigkeitsbereich haben.

Überlegungen zum Widerrufen des Zugriffs

Wenn Sie den Zugriff widerrufen, wird der Löschvorgang auf die jeweilige Quelle beschränkt:

- Durch das Widerrufen vCenter vCenter-Zugriffs werden nur vCenter-Daten gelöscht. Serverdaten werden nicht beeinträchtigt Hyper-V oder importiert.
- Durch das Widerrufen des Hyper-V Zugriffs werden nur Hyper-V Daten gelöscht. VMware oder importierte Serverdaten sind davon nicht betroffen.
- Durch das Löschen importierter Server werden sie aus dem Inventar entfernt, aber die nachgelagerten Erfassungsdaten (Netzwerk-, Datenbank-, Betriebssystemmetriken) bleiben erhalten.
- Um alle quellspezifischen Inventardaten zu entfernen, müssen Sie jede Quelle unabhängig voneinander sperren oder löschen. Downstream-Erfassungsdaten (Netzwerk-, Datenbank-, Betriebssystemmetriken) bleiben auch dann erhalten, wenn alle Quellen gesperrt wurden.

Fehlerbehebung

Überprüfen der Konnektivität des Discovery-Tools mit vCenter

Wenn bei der Konfiguration des VMware-Moduls Fehler auftreten, gehen Sie wie folgt vor, um die Konnektivität zu überprüfen:

Greifen Sie auf das Discovery-Tool VM zu

- Log-in zum Discovery-Tool VM, öffnen Sie Remote Console in vCenter
 - Benutzername: discovery
 - Passwort: Passwort

Testen Sie die vCenter-Konnektivität

1. Testen Sie den vCenter-API-Zugriff:

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/  
mob
```

2. Ergebnis des erwarteten Erfolgs:

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/
mob > tmp.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
  0     0    0     0    0     0      0      0  --:--:-- --:--:-- --:--:--    0*
Trying 192.168.2.125:443...
* Connected to vcsa (192.168.2.125) port 443 (#0)
...
</xml>
* Connection #0 to host vcsa left intact
```

Testen Sie das SSL-Zertifikat

1. Führen Sie diesen Befehl aus:

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. Ausgabe mit erwartetem Erfolg:

- Sollte vSphere-Zertifikatsdetails anzeigen
- Überprüft die SSL/TLS Konnektivität auf Port 443

```
[ec2-user@discoverytool ~]$ openssl s_client -showcerts -servername vcsa -connect
vcsa:443
CONNECTED(00000003)
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/CN=vcsa.onpremsim.env/C=US
  i:/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
  Engineering
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```



```
---
Server certificate
subject=/CN=vcsa.onpremsim.env/C=US
issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
Engineering
---
```

WinRM-Problembehandlung

Wenn Sie Verbindungsprobleme mit WinRM haben, gehen Sie wie folgt vor, um die Verbindung zu testen. Diese Schritte gelten auch für Hyper-V Verbindungsprobleme, da das Discovery-Tool WinRM für die Kommunikation mit Hyper-V Hosts verwendet.

Testen Sie die grundlegende WinRM-Konnektivität mithilfe der Ports 5985 (HTTP) und 5986 (HTTPS). Wir müssen sicherstellen, dass die Konnektivität auf Port 5986 (HTTPS) funktioniert

```
# Check WinRM listener configuration
winrm enumerate winrm/config/listener

# Note: Replace <HOST> with the target computer's hostname or IP address. Adjust the
# username and password as needed.
# Test WinRM connection on port 5985 (HTTP)
$cred = Get-Credential
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5985

# Test WinRM connection on port 5986 (HTTPS)
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5986
```

Wenn die obigen Tests fehlschlagen, versuchen Sie, eine PowerShell Sitzung mit deaktivierter Zertifikatsvalidierung einzurichten:

```
$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSsession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Kerberos-Fehlerbehebung

Wenn bei der Erfassung von Daten von Windows-Servern Fehler bei der Kerberos-Authentifizierung auftreten, können Sie anhand der folgenden Abschnitte häufig auftretende Probleme diagnostizieren und beheben.

Überprüfen Sie die Netzwerkanforderungen

Bevor Sie Probleme mit der Kerberos-Authentifizierung beheben, stellen Sie sicher, dass das Discovery-Tool die erforderlichen Netzwerkendpunkte erreichen kann.

Um die Netzwerkanforderungen für Kerberos zu überprüfen

1. Überprüfen Sie die DNS-Auflösung für den Domänencontroller. Führen Sie den folgenden Befehl von der Discoverytool-VM aus:

```
nslookup dc01.example.com
```

Sie können jedoch auch `dig` verwenden.

```
dig dc01.example.com
```

Wenn die DNS-Auflösung fehlschlägt, stellen Sie sicher, dass die Discoverytool-VM so konfiguriert ist, dass sie einen DNS-Server verwendet, der Ihre Active Directory-Domäne auflösen kann. Überprüfen `/etc/resolv.conf` und bestätigen Sie, dass die Nameservereinträge auf Ihre Domänen-DNS-Server verweisen.

2. Überprüfen Sie die Konnektivität zum Key Distribution Center (KDC) an Port 88. Führen Sie den folgenden Befehl aus:

```
nc -zv dc01.example.com 88
```

Erwartete Ausgabe:

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```

Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass keine Firewallregeln den Verkehr von der Discoverytool-VM zum Domänencontroller an Port 88 blockieren.

3. Überprüfen Sie die Konnektivität zu den Windows-Zielservers an WinRM-Ports. Führen Sie die folgenden Befehle aus:

```
nc -zv <windows-server> 5985  
nc -zv <windows-server> 5986
```

Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass WinRM auf dem Zielsystem aktiviert ist und dass Firewallregeln eingehenden Verkehr an den Ports 5985 und 5986 zulassen.

Allgemeine Kerberos-Probleme

Im Folgenden werden häufig auftretende Kerberos-Probleme und deren Lösungen beschrieben.

Fehler bei der Berücksichtigung von Groß-

Symptom: Bei der Authentifizierung wird die Fehlermeldung „Server nicht in der Kerberos-Datenbank gefunden“ angezeigt.

Dieser Fehler tritt normalerweise auf, wenn der Kerberos-Bereichsname nicht in Großbuchstaben geschrieben ist. Kerberos-Bereiche müssen in Ihrer Datei in Großbuchstaben angegeben werden. `krb5.conf` Verwenden Sie z. B. `EXAMPLE.COM` statt `example.com`.

Verhinderung der Kontosperrung

Das Discovery-Tool verwendet einen Backoff-Mechanismus, um zu verhindern, dass Konten aufgrund wiederholter fehlgeschlagener Authentifizierungsversuche gesperrt werden. Wenn Ihr Dienstkonto gesperrt wird, können Sie den Erfassungsvorgang zurücksetzen, indem Sie das Erfassungsmodul über die Weboberfläche des Discovery-Tools unter beenden und erneut starten. `https://<discovery-tool-vm-ip>:5000`

Kinit schlägt über die CLI fehl

In der folgenden Tabelle sind häufig auftretende kinit Fehler und deren Lösungen aufgeführt.

Fehler	Ursache	Lösung
KDC für Realm kann nicht gefunden werden	Der KDC-Hostname oder die IP-Adresse ist nicht erreichbar, oder der Bereich ist nicht konfiguriert. <code>krb5.conf</code>	Stellen Sie sicher, dass die <code>krb5.conf</code> Datei den richtigen KDC-Hostnamen und den richtigen Bereich enthält. Bestätigen Sie die DNS-Auflösung und die Netzwerkkonnektivität zum KDC auf Port 88.
Die Vorauthentifizierung ist fehlgeschlagen	Das Passwort für das Dienstkonto ist falsch.	Überprüfen Sie das Passwort und versuchen Sie es erneut. Wenn das

Fehler	Ursache	Lösung
		Konto gesperrt ist, entsperren Sie es in Active Directory, bevor Sie es erneut versuchen.
Der Client wurde nicht in der Kerberos-Datenbank gefunden	Der Prinzipalname stimmt mit keinem Konto in Active Directory überein.	Stellen Sie sicher, dass der Prinzipalname genau mit dem Kontonamen übereinstimmt, einschließlich Groß- und Kleinschreibung. Verwenden Sie das Format <code>username@REALM</code> mit dem Bereich in Großbuchstaben.
Die Netzwerkadresse für KDC kann nicht aufgelöst werden	DNS kann den KDC-Hostnamen nicht auflösen.	Überprüfen Sie die DNS-Konfiguration in <code>/etc/resolv.conf</code> . Vergewissern Sie sich, dass der DNS-Server den KDC-Hostnamen auflösen kann. Testen Sie mit <code>odernslookup. dig</code>

Die Erfassung schlägt trotz erfolgreicher Initiierung fehl

Wenn die Datenerfassung `kinit` erfolgreich ist, die Datenerfassung aber immer noch fehlschlägt, überprüfen Sie Folgendes:

1. Stellen Sie sicher, dass der für die Erfassung verwendete Prinzipalname `kinit` genau der Groß- und Kleinschreibung entspricht, die während der Erfassung verwendet wurde.
2. Stellen Sie sicher, dass das Dienstkonto über die erforderlichen Berechtigungen auf den Zielsevern verfügt.
3. Stellen Sie sicher, dass WinRM auf den Zielsevern aktiviert ist.
4. Stellen Sie sicher, dass der für die Erfassung verwendete Hostname mit dem in Active Directory registrierten Hostnamen übereinstimmt.

Kerberos funktioniert auf einigen Servern, auf anderen jedoch nicht

Wenn die Kerberos-Authentifizierung für einige Server erfolgreich ist, für andere jedoch fehlschlägt, untersuchen Sie die folgenden Bereiche:

Wenn sich Ihre Server über mehrere Active Directory-Domänen erstrecken, konfigurieren Sie für jede Domäne separate Kerberos-Anmeldeinformationen. Stellen Sie sicher, dass Ihre `/etc/krb5.conf` Datei Einträge für alle Bereiche enthält. Für jede Domain sind eigene Anmeldeinformationen mit dem richtigen `username@REALM` Principal erforderlich.

Vergleichen Sie die WinRM-Konfiguration auf einem funktionierenden Server mit einem ausgefallenen Server. Führen Sie auf jedem Server den folgenden Befehl aus:

```
winrm get winrm/config
```

Testen Sie die Konnektivität mit Remote Desktop, um das Problem zu isolieren. Das Discovery-Tool verwendet das Format `username@DOMAIN`, während Remote Desktop das Format `DOMAIN\username` verwendet.

Stellen Sie sicher, dass das Dienstkonto Mitglied der lokalen Administratorgruppe auf dem ausgefallenen Server ist. Führen Sie den folgenden Befehl auf dem Zielsystem aus:

```
net localgroup Administrators
```

WMI benötigt lokale Administratorrechte, um auf Betriebssysteminformationen zugreifen zu können. Für die SQL Server-Sammlung ist außerdem erforderlich, dass das Dienstkonto über lokalen Administratorzugriff auf dem Zielsystem verfügt.

Checkliste für die Kerberos-Konfiguration

Verwenden Sie die folgende Checkliste, um Ihre Kerberos-Konfiguration zu überprüfen, bevor Sie mit der Datenerfassung beginnen.

- Die `krb5.conf` Datei ist auf der Discovery-Tool-VM vorhanden.
- Der Bereichsname ist in Großbuchstaben geschrieben. `krb5.conf`
- Die Ausführung `kinit` mit dem Dienstkonto ist ohne Fehler erfolgreich.
- Beim Ausführen wird ein gültiges, nicht abgelaufenes Ticket `klist` angezeigt.
- Der Prinzipalname entspricht exakt dem Active Directory-Kontonamen.
- Die DNS-Auflösung funktioniert für den KDC-Hostnamen.
- Die Netzwerkkonnektivität zum KDC an Port 88 wurde bestätigt.
- Die Netzwerkkonnektivität zu Windows-Zielsystemen an den Ports 5985 und 5986 wurde bestätigt.

- (Multi-domain) Jede Active Directory-Domäne hat ihre eigenen Anmeldeinformationen, die im Discovery-Tool konfiguriert sind, [realms] und krb5.conf enthält [domain_realm] Einträge für alle Domänen.

Fehlerbehebung bei der Oracle-Datenbank

Um Probleme mit der Erfassung von Oracle-Datenbanken zu diagnostizieren, wie z. B. fehlende Daten oder Fehler, überprüfen Sie Folgendes.

Verbindung verweigert oder Timeout

Symptom: Der Oracle-Sammlungsstatus zeigt einen Verbindungsfehler für einen Server an.

Um dieses Problem zu beheben, überprüfen Sie Folgendes:

- Stellen Sie sicher, dass der Oracle-Listener auf dem Zielhost läuft: `lsnrctl status`
- Überprüfen Sie die Netzwerkkonnektivität vom Discovery-Tool zum Oracle-Host auf Port 1521 (oder Ihrem benutzerdefinierten Port): `nc -zv <oracle-host> 1521`
- Stellen Sie sicher, dass die Firewallregeln eingehende Verbindungen auf dem Oracle-Listener-Port zulassen.
- Überprüfen Sie den Dienstnamen, indem Sie ihn `lsnrctl services` auf dem Oracle-Host ausführen. Wenn der Dienstname falsch ist, lehnt der Oracle-Listener die Verbindung ab.

Fehler bei der Authentifizierung () ORA-01017

Symptom: Die Erfassung schlägt aufgrund eines ungültigen Benutzernamens oder Passworts fehl.

Überprüfen Sie Folgendes, um dieses Problem zu beheben:

- Stellen Sie sicher, dass das Oracle-Dienstkonto existiert und nicht gesperrt ist: `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- Stellen Sie sicher, dass das Passwort korrekt ist, indem Sie die Verbindung manuell herstellen: `sqlplus discovery_user/<password>@<host>:1521/<service_name>`
- Wenn das Konto gesperrt ist, entsperren Sie es: `ALTER USER discovery_user ACCOUNT UNLOCK;`

Unzureichende Rechte (ORA-01031)

Symptom: Die Verbindung ist erfolgreich, aber die Erfassung gibt unvollständige Daten zurück.

Überprüfen Sie Folgendes, um dieses Problem zu beheben:

- Stellen Sie sicher, dass `SELECT_CATALOG_ROLE` gewährt wurde: `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- Gewähren Sie die erforderliche Rolle, falls sie fehlt: `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

Die manuellen Anmeldeinformationen zeigen einen Fehler an, aber die automatische Verbindung funktioniert

Wenn Sie Anmeldeinformationen manuell an einen Server anheften, greift das Erkennungstool nicht zurück, falls die Verbindung fehlschlägt. Stellen Sie sicher, dass der Port und der Dienstname, die Sie für die Anmeldeinformationen konfiguriert haben, mit dem Oracle-Listener auf dem jeweiligen Server übereinstimmen. Wenn der Server über einen nicht standardmäßigen Port- oder Dienstnamen verfügt, aktualisieren Sie die Konfiguration der Anmeldeinformationen entsprechend.

OS-level Fallback erkennt Oracle nicht

Wenn keine Datenbankanmeldedaten konfiguriert sind und das OS-level Fallback Oracle nicht erkennt:

- Stellen Sie sicher, dass die SSH- oder WinRM-Betriebssystemanmeldeinformationen konfiguriert sind und für den Server funktionieren (überprüfen Sie den Status der Erfassung von Betriebssystemmetriken).
- Stellen Sie bei Linux-Hosts sicher, dass die Prozesse des Oracle Process Monitor (pmon) /etc/oratab vorhanden sind oder dass sie ausgeführt werden.
- Stellen Sie bei Windows-Hosts sicher, dass Oracle-Registrierungseinträge unter vorhanden sind HKLM\SOFTWARE\Oracle oder dass `oracle.exe` Prozesse ausgeführt werden.

SNMP-Fehlerbehebung

Greifen Sie auf das Discovery-Tool VM zu

- Log-in zum Discovery-Tool VM, öffnen Sie Remote Console in vCenter
 - Benutzername: discovery

- Passwort: Passwort

Installieren Sie die SNMP-Tools (falls erforderlich)

- `sudo yum install net-snmp-utils -y`

Testen Sie die SNMP-Verbindung zu Linux-Servern

1. `snmptable -v 2c -c <COMMUNITY_STRING>
<REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. Beispiel:

```
#SNMPv2c:
snmptable -v 2c -c public 192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with authentication):
snmptable -v 3 -u <username> -a MD5 -A <auth_password>
192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with privacy):
snmptable -v 3 -u <username> -a MD5 -A <auth_password> -x DES -X <priv_password>
192.168.1.100 .1.3.6.1.2.1.6.13.1
```

Fehler bei der Netzwerkerfassung

Zum Lesen des Passworts ist ein Terminal erforderlich

Fehler:

```
ss command failed on <host>: sudo: a terminal is required to read the password; either
use the -S option to read from standard input or configure an askpass helper sudo: a
password is required
```

Der Befehl `ss` fordert zur Eingabe des Benutzerpassworts auf. Der konfigurierte SSH-Benutzer muss sich in der Gruppe `sudoers` befinden und mit passwortlosem Sudo für den Befehl konfiguriert sein. `ss/netstat` Um passwortloses Sudo zu konfigurieren:

1. Erstellen Sie eine neue Sudoers-Datei:


```
sudo vi -f /etc/sudoers.d/<username>
```

2. Füge die Zeile hinzu:

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. Nach dieser Änderung `sudo netstat -tnap` sollte es ausgeführt `sudo ss -tnap` werden, ohne nach einem Passwort zu fragen

Die Netzwerksammlung lief ohne Sudo

Wenn auf der Seite Entdecktes Inventar die folgende Warnung angezeigt wird:

```
Network collection ran without sudo. Process-level connection data may be missing.
```

Diese Warnung weist darauf hin, dass das SSH-Benutzerkonto keinen Sudo-Zugriff auf dem Zielsystem hat. Ohne Sudo kann das Discovery-Tool immer noch Netzwerkverbindungsdaten sammeln, aber es kann nicht feststellen, welchem Prozess die einzelnen Verbindungen gehören. Um vollständige Verbindungsdaten auf Prozessebene zu sammeln, stellen Sie sicher, dass der SSH-Benutzer über Sudo-Zugriff auf dem Zielsystem verfügt.

Fehler beim Sammeln von Betriebssystem-Metriken

Fehlende Server-UUID für Linux-Server

Wenn das Discovery-Tool nicht in der Lage ist, die Server-UUID für Linux-Server zu ermitteln (wird als leer angezeigt oder fehlt), überprüfen Sie, ob die für diese Server konfigurierten SSH-Anmeldeinformationen über Sudo-Rechte verfügen. Das Tool verwendet, um die `dmidecode` Server-UUID zu lesen. Wenn `dmidecode` es nicht installiert ist, greift das Tool auf Lesen zurück `/sys/class/dmi/id/product_uuid`, wofür ebenfalls Sudo-Zugriff erforderlich ist. Ohne `sudo` kann keine Methode die UUID abrufen.

Lösung: Stellen Sie sicher, dass das SSH-Benutzerkonto, das dem Discovery-Tool zur Verfügung gestellt wurde, Sudo-Zugriff auf den Linux-Zielsystemen hat.

Probleme beim Zugriff auf das Inventar „Ermittelt“

Wenn Sie im Status „Serversammlung“ eine Meldung wie Fehlende Anmeldeinformationen oder Zugriff verweigert sehen, gehen Sie wie folgt vor:

1. Wählen Sie den Server in der Tabelle der erkannten Server aus.
2. Wählen Sie Zugangsdaten verwalten. Sie haben folgende Möglichkeiten:
 - a. Wählen Sie alternative Anmeldeinformationen aus der Dropdownliste Anmeldeinformationen auswählen aus.
 - b. Wählen Sie Neue Anmeldeinformationen verwenden und geben Sie neue Anmeldeinformationen ein.
3. Speichern.

Das Discovery-Tool versucht erneut, die Verbindung herzustellen, nachdem Sie Ihre Änderungen gespeichert haben.

Fehlerbehebung bei der SSH-Schlüsselauthentifizierung

Testen der SSH-Schlüsselkonnektivität über das Discovery-Tool

Wenn die SSH-Schlüsselauthentifizierung fehlschlägt, überprüfen Sie die Konnektivität zwischen dem Discovery-Tool und dem Zielservers:

1. Melden Sie sich beim Discovery-Tool an (über die vSphere-Konsole oder SSH beim Linux-Host).
2. Testen Sie die SSH-Konnektivität mit Ihrem privaten Schlüssel:

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. Wenn die Verbindung erfolgreich ist, liegt das Problem darin, wie der Schlüssel in das Discovery-Tool hochgeladen wurde. Re-upload Geben Sie den Schlüssel ein und überprüfen Sie, ob der Benutzername übereinstimmt.
4. Wenn die Verbindung fehlschlägt, überprüfen Sie die Fehlermeldung in der folgenden Tabelle.

Fehlermeldung	Ursache	Auflösung
Permission denied (publickey)	Der öffentliche Schlüssel befindet sich nicht in der <code>authorized_keys</code> Datei des Zielservers,	Fügen Sie den öffentlichen Schlüssel <code>~/.ssh/authorized_keys</code> auf dem Zielserver für den richtigen Benutzer hinzu. Überprüfen Sie die Dateiberechtigungen: <code>chmod 700 ~/.ssh</code>

Fehlermeldung	Ursache	Auflösung
	oder der Benutzername ist falsch.	<code>&& chmod 600 ~/.ssh/authorized_keys</code> .
Connection timed out after 20s	Port 22 ist vom Discovery-Tool aus nicht erreichbar.	Stellen Sie sicher, dass Port 22 zwischen dem Discovery-Tool und dem Zielsystem geöffnet ist. Überprüfen Sie Firewalls und Sicherheitsgruppen.
Connection refused	Der SSH-Dienst läuft nicht auf dem Zielsystem.	Starten Sie den SSH-Dienst: <code>sudo systemctl start sshd</code>
Invalid SSH key for credential ' <i>name</i> '	Das Schlüsselformat wird nicht unterstützt, die Schlüsseldaten sind beschädigt oder die Passphrase fehlt oder ist falsch.	Stellen Sie sicher, dass das Schlüsselformat RSA, ECDSA oder Ed25519 im PEM-, OpenSSH- oder PKCS #8 -Format ist. Wenn der Schlüssel verschlüsselt ist, stellen Sie sicher, dass die Passphrase korrekt ist.

Fehlerbehebung beim Linux-Installationsprogramm

Port 5000 wird bereits verwendet

Symptom: Der Discovery Tool-Dienst kann nach der Installation nicht gestartet werden.

Lösung: Identifizieren und beenden Sie den Prozess über Port 5000:

```
sudo ss -tlnp | grep :5000
```

Beenden Sie den Konflikt verursachenden Prozess und starten Sie dann das Discovery-Tool neu:

```
sudo ./AWS-Transform-discovery-tool.sh start
```

Häufige Fehlermeldungen

In dieser Tabelle werden häufig auftretende Fehlermeldungen und ihre Erklärungen beschrieben:

Fehlermeldung	Speicherort	Erklärung
Ein Passwort wurde bereits erstellt	Passwortseite erstellen	Race Condition, wenn zwei Benutzer gleichzeitig Passwörter erstellen; aktualisiere
Der Export ist fehlgeschlagen	Seite „Inventar“	Versuchen Sie es erneut oder senden Sie Protokolle
Eine Erfassung auf Abruf ist bereits im Gange	Seite „Inventar“	Rennbedingung, wenn zwei Benutzer gleichzeitig mit der manuellen Erfassung beginnen. Versuchen Sie es erneut, nachdem die aktuelle manuelle Erfassung abgeschlossen ist
Command timed out after 60s	Status der Servererfassung	Ein Befehl auf dem Zielsystem wurde nicht innerhalb von 60 Sekunden abgeschlossen. Dies kann auf stark ausgelasteten Servern auftreten. Versuchen Sie erneut, die Erfassung durchzuführen, oder untersuchen Sie die Auslastung des Zielservers.
Ein oder mehrere Anmeldeinformationen enthalten unbekannte UUIDs	Seite für den Zugriff auf das Betriebssystem	Race Condition, wenn zwei Benutzer die Anmeldeinformationen für das Betriebssystem gleichzeitig bearbeiten. Versuchen Sie es erneut
Ungültiges Passwort	Sign-in Seite	Falsches Passwort für die Anmeldung. Wenden Sie sich an den Administrator oder wenden Sie sich an
Ihre Sitzung ist abgelaufen. Bitte melden Sie sich erneut an.	Sign-in Seite	Die Sitzung ist abgelaufen. Sie müssen sich erneut anmelden
Ein interner Fehler ist aufgetreten	Verschiedene Seiten	Versuchen Sie es erneut oder senden Sie Protokolle

Versionshinweise

In diesem Abschnitt werden die Funktionen, Verbesserungen und Fehlerkorrekturen für das AWS Transform Discovery-Tool nach Veröffentlichungsdatum geordnet beschrieben.

Date	Version	Versionshinweise
30. Juni 2026	1.0.1646	Neue Features • Oracle-Datenbankerkennung hinzugefügt. Das Tool erfasst CDB- und PDB-Topologie, Version, Edition, installierte Optionen, Funktionsnutzung und Komponenteninventar. Das Discovery-Tool unterstützt direkte SQL-Verbindungen (mithilfe von SELECT_CATALOG_ROLE) und die OS-level Fallback-Erkennung über SSH oder WinRM. • Unterstützung für mehrere Kerberos-Anmeldeinformationen in verschiedenen Active Directory-Domänen hinzugefügt. Alle Anmeldeinformationen werden unabhängig authentifiziert, sodass die Erfassung von Windows-Servern in mehreren Domänen ohne Authentifizierungskonflikte ermöglicht wird. Verbesserungen • Verbesserte Erfassung von Betriebssystem-Metriken für ältere Hosts. Es wurde eine Fallback-Datenerfassung für ältere Betriebssysteme (RHEL 5, SLES 11, Windows Server 2008 R2) hinzugefügt, bei denen moderne Befehle nicht verfügbar sind. Speicher-, Leistungs- und Netzwerkschnittstellendaten werden jetzt über alternative Systemschnittstellen gesammelt. Fehlerbehebungen • Es wurden Fehler bei der Kerberos-Authentifizierung für Server behoben, die über entdeckt wurden. Hyper-V Das Discovery-Tool löst den Server-Hostnamen (FQDN) jetzt

Date	Version	Versionshinweise
		korrekt aus Hyper-V Gast-Metadaten auf, was für den Kerberos-SPN-Abgleich erforderlich ist.

Date	Version	Versionshinweise
14. Mai 2026	1.0.1363	Neue Features • Es wurde ein Linux-Installationsprogramm für die Bereitstellung des Discovery-Tools auf unterstützten Linux-Distributionen hinzugefügt (Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, 9, Ubuntu 20.04—24.04, Debian AlmaLinux 10—12, SLES 15 SP5). • Unterstützung für die Konfiguration mehrerer VMware vCenter Server mit automatischer VM-Deduplizierung über vCenter hinweg hinzugefügt. • SSH-Authentifizierung mit privatem Schlüssel als Alternative zu Benutzername und Passwort für den Zugriff auf das Linux-Betriebssystem hinzugefügt. Zu den unterstützten Schlüsselformaten gehören RSA, ECDSA, Ed25519, OpenSSH und PKCS #8. • Netzwerksammlung für private Adressen hinzugefügt, um Verbindungen zu und von privaten IP-Adressen nach RFC 1918 zu erfassen, die sich nicht in Ihrem erkannten Inventar befinden. • Es wurden Exportoptionen hinzugefügt, um einen benutzerdefinierten Datumsbereich auszuwählen und auszuwählen, welche Datenmodule in den Export aufgenommen werden sollen. Verbesserungen • Verbesserte Zuverlässigkeit bei der planmäßigen Erfassung durch Staffelung der Sammelpläne. • Verbesserte Leistung bei der Erfassung von Betriebssystem-Metriken durch Batching von SSH-Befehlen. • Bei Änderungen der Anmeldeinformationen wird jetzt sofort versucht, zuvor ausgefallene Server erneut auszuführen.

Date	Version	Versionshinweise
		• Bei der Erfassung von Betriebssystem-Metriken wird jetzt ein teilweiser Status gemeldet, wenn einige Befehle leere Ergebnisse zurückgeben. • Verbesserte Fehlersichtbarkeit bei vCenter-Verbindungsproblemen im Dashboard.
7. April 2026	1.0.1074	Neue Features • Unterstützung für Microsoft Hyper-V Discovery hinzugefügt, einschließlich der automatischen Erkennung von VMs von Hyper-V Hosts mit Failovercluster-Deduplizierung. • Unterstützung für den Serverimport per CSV-Datei-Upload hinzugefügt. • Erfassung von Betriebssystem-Metriken mit sechs unabhängigen Modulen hinzugefügt: Serverleistung, Speicherleistung, Serverbereitstellung, Speicherbereitstellung, Netzwerkschnittstellen und laufende Prozesse. • Hyper-V Bereitstellungsoption mit einer VHD-Imagedatei hinzugefügt. • Die Stärkung der lokalen Sicherheit wurde verbessert, indem EC2-specific Dienste entfernt und der Zugriff auf den Endpunkt der Instanzmetadaten blockiert wurde.

Date	Version	Versionshinweise
26. März 2026	1.0.1014	Fehlerkorrekturen und Verbesserungen • Die Überprüfung der Groß- und Kleinschreibung von Kerberos-Domänen wurde vom Backend ins Frontend verschoben. • Wechselte von Python-kerberos zu Python-pykerberos und machte den dateibasierten Cache zum Standard. • Die Überprüfung der Server-ID bei der Massенbearbeitung ohne Berücksichtigung von Groß- und Kleinschreibung wurde behoben. • Der ZIP-Exportdateiname wurde korrigiert (jetzt <code>discovery_tool_export.zip</code>). • Der Dienst, der die Prüfung ausführt, wurde behoben und es wurden Debug-Logs für Systemanmeldedaten hinzugefügt. • Es wurde ein Netzwerkconfigurationsskript hinzugefügt, um Artefakte zu erstellen.
16. Dezember 2025	1.0.718	Neue Features und Verbesserungen • SMBIOS-UUID-Unterstützung hinzugefügt, um die Duplizierung von virtuellen Rechnern in Downstream-Diensten zu verhindern. • Einführung von Min/Max/Avg Tracking und erweiterten Speichermetriken für eine verbesserte Ressourcenüberwachung. • Es wurden Verbesserungen bei der API-Validierung hinzugefügt. • Es wurden Funktionen im Hilfebereich mit kontextbezogener Anleitung hinzugefügt. • Die Terminologie wurde in der gesamten Benutzeroberfläche von „Collector“ auf „Tool“ aktualisiert.

Date	Version	Versionshinweise
31. Oktober 2025	1.0.0	Erstversion Erster Start des AWS Transform Discovery-Tools. Diese Version beinhaltet: • Offline-Erfassung (keine Abhängigkeit von einem AWS Konto oder Application Discovery Service). • Erkennung und Überwachung durch VMware. • Erkennung von SQL Server-Datenbanken. • Server-to-server Erfassung von Kommunikation über SSH, WMI und SNMP.

AWS Steckverbinder transformieren

AWS Transform Connectors ermöglichen Ihnen den sicheren Zugriff auf Ressourcen über Kontogrenzen hinweg für Migrations- und Modernisierungsworkflows. Auf diese Weise können Sie über Kontogrenzen hinweg auf Ressourcen zugreifen und diese verwalten und gleichzeitig Sicherheitskontrollen und Berechtigungen beibehalten. Ein Konnektor stellt eine Verbindung zwischen Ihrem AWS Transform-enabled Quellkonto und externen Ressourcen in AWS Zielkonten oder in Systemen von Drittanbietern dar.

Connectors erfordern Zugriffsanfragen vom Quell-Connector und die Genehmigung durch den Eigentümer des Zielkontos. Sie stellen diese Anfrage, wenn Sie einen Quell-Connector einrichten. In ähnlicher Weise erhalten Sie möglicherweise Anfragen zur Genehmigung von Ziel-Connectors, um anderen Konten den Zugriff auf Ihr Konto zu ermöglichen.

- **Connector-Erstellung:** Erstellen Sie Connectors in Ihrem AWS Transform-enabled Quellkonto und geben Sie dabei das Zielkonto und die erforderlichen Berechtigungen an
- **Einrichtung von Berechtigungen:** AWS Transform erfordert bestimmte IAM-Rollen und -Berechtigungen im Zielkonto, um Migrationsaktionen durchzuführen, darunter:
 - Verwaltung von Migrationsdaten mit AWS KMS
 - Regionsübergreifende API-Aufrufe tätigen
 - Installation von Replikationsagenten auf VMware-Servern
 - Erstellung einer Netzwerkinfrastruktur (VPCs, Subnetze, Routing)
 - Amazon EC2 EC2-Instances starten und Stacks bereitstellen CloudFormation
 - Ausführung von Migrationsworkflows über Migration Hub
- **Genehmigungsprozess:** Sie müssen Ziel-Connector-Anfragen genehmigen, bevor AWS Transform auf Ihre Ressourcen zugreifen kann.
- **Aktive Verbindung:** Sobald Sie einen Connector genehmigt haben, können AWS Transform-Jobs sicher auf Ressourcen im Zielkonto zugreifen und diese verwalten.

Rückverfolgbarkeit durch Benutzer für behördliche Abläufe

AWS CloudTrail zeichnet standardmäßig Agentenaktionen auf Ihren AWS Ressourcen unter der AWS Transform-Dienstidentität auf. Bei der Rückverfolgbarkeit durch Benutzer werden diese Aktionen dem jeweiligen AWS IAM Identity Center-Benutzer zugeordnet, der den Job initiiert oder

mit ihm interagiert hat, sodass Sicherheitsüberprüfungen und Vorfälle auf Benutzerebene untersucht werden können.

 Note

Die Rückverfolgbarkeit von Benutzern wird nur für Benutzer von IAM Identity Center (IDC) unterstützt.

Um die Rückverfolgbarkeit von Benutzern zu aktivieren, aktivieren Sie in Ihren AWS Transform-Profileinstellungen die Option **Hintergrundsitzung**. Wenn diese Option aktiviert ist, erstellt AWS Transform automatisch eine IAM Identity [Center-Hintergrundsitzung](#), wenn Sie mit einem Job interagieren, und verwendet sie, um identitätserweiterte IAM-Rollensitzungen für Connector-Operationen zu erstellen. In diesen Sitzungen wird Ihre Benutzeridentität in nachgelagerte AWS Serviceanrufe und Ereignisse eingebettet. AWS CloudTrail Wenn Hintergrundsitzungen deaktiviert sind, greift AWS Transform auf Standardsitzungen mit übernommenen Rollen ohne Benutzeridentitätskontext zurück.

Neue Konnektoren werden automatisch konfiguriert, um die Rückverfolgbarkeit der Benutzer zu unterstützen. Bei vorhandenen Konnektoren müssen Sie Folgendes manuell `sts:SetContext` zur Vertrauensrichtlinie der Konnektorrolle hinzufügen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": ["transform.amazonaws.com"] },
      "Action": ["sts:AssumeRole", "sts:SetContext"],
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "your-account-id" }
      }
    }
  ]
}
```

Sie können Ihre aktiven Hintergrundsitzungen auf der Jobseite auf der Registerkarte **Hintergrundsitzungen** anzeigen und widerrufen. Wenn Sie eine Sitzung widerrufen, werden sie und alle daraus abgeleiteten Connector-Sitzungen sofort ungültig.

Weitere Informationen finden Sie unter [Übersicht über die Verbreitung vertrauenswürdiger Identitäten](#) im AWS IAM Identity Center-Benutzerhandbuch.

Konnektoren verwalten

Auf der Connectors-Seite können Sie Folgendes sehen:

- Registerkarte „Quell-Connectors“: Listet alle Connectors auf, die Sie für die Verbindung mit anderen Konten erstellt haben, und zeigt die Zielkonten und den Connector-Status an
- Registerkarte „Ziel-Connectors“: Zeigt eingehende Connector-Anfragen von anderen Konten an, die auf Ihre Ressourcen zugreifen möchten und für die Ihre Genehmigung oder Ablehnung erforderlich ist

AWS Transform erfordert eine Bestätigung für kritische Aktionen wie das Genehmigen, Ablehnen oder Löschen von Connectoren, um versehentliche Änderungen zu vermeiden, die Ihre aktiven Migrationsworkflows stören könnten.

Um einen Konnektor zu erstellen

1. Navigieren Sie zur Registerkarte Quellkonnektoren.
2. Geben Sie das Zielkonto und den Ressourcentyp an.
3. Konfigurieren Sie die erforderlichen Berechtigungen und den Zugriffsbereich.

So richten Sie Berechtigungen ein

1. Wählen Sie, ob Sie eine neue IAM-Rolle mit den erforderlichen Berechtigungen erstellen möchten, oder
2. Wählen Sie eine vorhandene Rolle aus, die Sie zuvor für Connectors erstellt haben.
3. Stellen Sie sicher, dass die Rolle über alle erforderlichen Berechtigungen für AWS Transform-Operationen verfügt.

Um eingehende Anfragen zu verwalten

1. Überprüfen Sie Connector-Anfragen auf der Registerkarte Destination Connectors.
2. Genehmigen Sie legitime Anfragen, um den kontoübergreifenden Zugriff zu ermöglichen.
3. Lehnen Sie unbefugte oder unnötige Verbindungsversuche ab.

Um Ihre Konnektoren zu verwalten

1. Überwachen Sie Ihre aktiven Konnektoren auf Sicherheit und Konformität.
2. Löschen Sie Konnektoren, wenn Sie sie nicht mehr benötigen. Beachten Sie, dass dadurch die Ausführung von Jobs, die den Connector verwenden, fehlschlägt.
3. Aktualisieren Sie die Berechtigungen, wenn sich Ihre Anforderungen ändern.

Migrationen (einschließlich VMware)

AWS Transform kann Ihnen helfen, Ihre virtuellen und Bare-Metal-Serverumgebungen zu Amazon EC2 mithilfe generativer KI, einschließlich VMware Hyper-V, und anderer Quellen zu migrieren. Dieses Kapitel bietet einen Überblick über die AWS Transform-Migrationsfunktionen und den Ablauf des Migrationsprozesses.

Funktionen und Hauptmerkmale

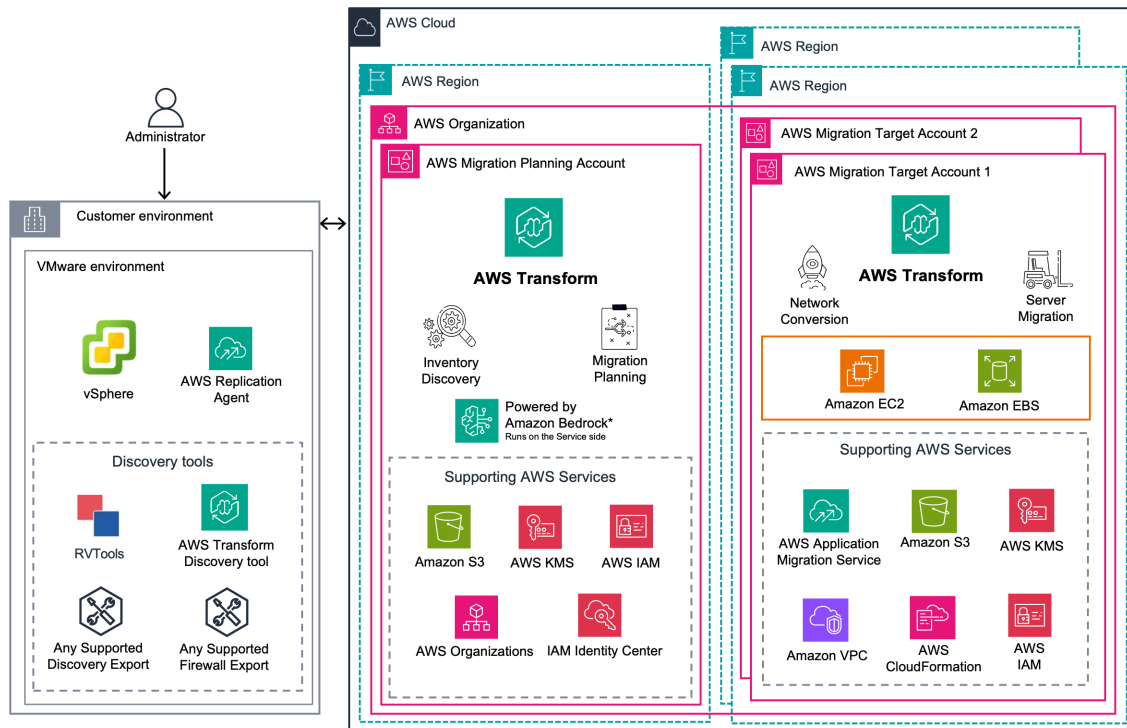
AWS Transform bietet die folgenden Funktionen und Hauptmerkmale für die Migration Ihrer Serverumgebungen zu AWS.

- Mehrere Erkennungsoptionen:
 - Unterstützte Erkennung Ihrer VMware-Umgebung mithilfe von Collectors von AWS Application Discovery Service.
 - Verwenden Sie das Open-Source-Tool [Export for vCenter](#) (VMware-Umgebungen).
 - Import unabhängig gesammelter Discovery-Daten (beliebige Quellumgebung).
- AI-driven Konvertierung Ihrer Quellnetzwerkconfiguration in eine Amazon VPC-Netzwerkarchitektur.
- AI-driven Generierung von Migrationsplänen, einschließlich Gruppierung von Anwendungen und vorgeschlagenen Migrationswellen.
- Rehosten Sie Ihre Server so, dass sie nativ auf Amazon EC2 laufen.
- Lokalisierte Webanwendungsoberfläche, sodass Sie AWS Transform für Migrationen in Ihrer bevorzugten Sprache verwenden können. Weitere Informationen finden Sie unter [Spracheinstellungen](#).

AWS Transform unterstützt die Migration von Windows- und Linux-Servern unterstützter Betriebssysteme. Die vollständige Liste der unterstützten Betriebssysteme finden Sie im AWS Transform MGN Benutzerhandbuch unter [Unterstützte Betriebssysteme](#).

AWS Transformieren Sie die Migrationsarchitektur

Dieses Diagramm zeigt einen Überblick über die AWS Transform-Migrationsarchitektur.



Jobs im Bereich Migration

Um AWS Transform für Migrationen verwenden zu können, benötigen Sie zunächst einen Workspace. Dabei handelt es sich um einen logischen Container, in dem Sie einen oder mehrere Transformationsjobs erstellen können. In den Abschnitten dieses Themas wird beschrieben, wie Sie einen Workspace erstellen und darin einen Migrationsjob erstellen und starten.

Einen Workspace einrichten

Informationen zur Einrichtung eines Workspace finden Sie unter [Erste Schritte](#).

Der Workspace, den Sie verwenden, bestimmt AWS-Region, wo Sie Transformationsjobs erstellen können. AWS-Region Dort werden sich Ihre Jobs befinden. Ihre Discovery-Daten und AWS Transform-Empfehlungen werden ebenfalls darin enthalten sein. AWS-Region Wenn Sie Workspaces und Jobs in einem anderen Workspace erstellen möchten AWS-Region, bitten Sie Ihren Administrator, einen anderen Workspace für Sie zu erstellen. Informationen zur unterstützten Version finden Sie AWS-Regionen unter [Unterstützte Regionen](#).

Auch wenn der AWS-Region Ort, an dem Sie Jobs erstellen und Discovery-Daten und Empfehlungen speichern können, von Ihrem AWS Transform-Administrator festgelegt wird, können Sie ein anderes

AWS-Region als Ziel für die Migration angeben. Mit anderen Worten, Sie können die Erkennung und den Empfang von AWS Transform-Empfehlungen in einem AWS-Region System ausführen, Ihre Zielumgebung dann aber in einer anderen erstellen AWS-Region. Wenn Sie das tun, übertragen Sie Ihre Daten überall hin AWS-Regionen. Weitere Informationen finden Sie unter [the section called “Ziel Connect AWS-Konto s und Regionen”](#).

Arten von Job

AWS Transform bietet die folgenden Arten von Migrationsaufträgen, aus denen Sie je nach Ihren Migrationsanforderungen wählen können. Zusätzlich zu diesen voreingestellten Optionen können Sie jederzeit dynamisch jeden Schritt zu Ihrem Job hinzufügen oder daraus entfernen, um Ihren Migrations-Workflow anzupassen.

End-to-end Migration

1. Discovery durchführen
2. Migrationsplan erstellen
3. Zielkonten Connect
4. landing zone bauen
5. Netzwerk migrieren
6. Server migrieren

Planung von Erkennung und Migration

1. Führen Sie die Entdeckung durch
2. Migrationsplan erstellen

Netzwerk-Migration

1. Zielkonten Connect
2. Netzwerk migrieren

Landezone

1. Zielkonten Connect
2. landing zone bauen

Landezone, Netzwerk und Servermigration

1. Zielkonten Connect
2. landing zone bauen
3. Netzwerk migrieren
4. Server migrieren

Migrationsplanung und Servermigration

Beinhaltet Discovery, Wave Plan und Rehosting.

1. Discovery durchführen
2. Migrationsplan erstellen
3. Zielkonten Connect
4. Server migrieren

Einen Job erstellen und starten

Der erste Schritt eines Migrationsprojekts besteht darin, einen AWS Transform-Job zu erstellen. Für Migrationsprojekte können Sie je nach Ihren Zielen verschiedene Jobtypen wählen. Das folgende Verfahren beschreibt, wie Sie einen neuen Migrationsjob beliebiger Art erstellen und starten. Informationen zu den verschiedenen Auftragsarten finden Sie unter [the section called “Arten von Job”](#).

Um einen neuen Migrationsjob zu erstellen und zu starten

1. Wähle auf deiner Workspace-Landingpage die Option Job erstellen aus.
2. Wähle die Migrationsoption und gib dann die Art des Migrationsauftrags an, den du erstellen möchtest. Informationen zu den Schritten, die in den einzelnen Migrationsauftragstypen enthalten sind, finden Sie unter [the section called “Arten von Job”](#).
3. Nachdem Sie alle Chat-Fragen beantwortet haben, wählen Sie Job erstellen.

Einen Workspace-Übersichtsbericht herunterladen

Du kannst während deiner Migration jederzeit einen Workspace-Übersichtsbericht als herunterladbares PDF erstellen. Der Bericht bietet einen konsolidierten Überblick über alle Migrationsjobs in Ihrem Workspace, einschließlich Jobstatus und aktuellen Workflow-Schritten,

Benutzeraktionen und -genehmigungen, Details zur Wellenplanung, Netzwerkmigrationstopologie, Landezonenkonfiguration, Rehost-Fortschritt, Containerisierungsentscheidungen und wichtige erzeugte Artefakte. Um einen Bericht zu erstellen, bitten Sie den Agenten im Chat um eine Workspace-Zusammenfassung — zum Beispiel: „Geben Sie mir eine Workspace-Zusammenfassung meines Migrationsfortschritts für alle Jobs“. Der Agent stellt Daten aus allen Jobs zusammen und stellt das PDF direkt im Chat als herunterladbare Datei bereit. Sie können diesen Bericht verwenden, um den gesamten Migrationsfortschritt zu verfolgen oder den Status mit Beteiligten zu teilen.

Einschränkungen

AWS Transform hat die folgenden Einschränkungen:

- Wenn Sie einen laufenden Migrationsauftrag beenden und dann den Agenten bitten, ihn neu zu starten, wird der Job wieder von vorne gestartet und Sie verlieren alle Fortschritte, die Sie mit dem Job gemacht haben. Artefakte, die im Job vor dem Neustart erstellt wurden, sind jedoch weiterhin verfügbar.
- Sie können ein Ziel AWS-Region pro Migrationsauftrag angeben. Um Anwendungen in verschiedene Zielregionen zu migrieren, erstellen Sie mehrere Migrationsaufträge.
- Multi-account Migration — Nur eine Region — Sie können innerhalb eines einzigen Kontos zu mehreren Konten migrieren AWS-Region. Bei Migrationen mit mehreren Regionen müssen Sie separate Projekte für jede Zielregion erstellen.
- Multi-account Migration — Ein Konto pro Welle — Jede Migrationswelle kann nur auf ein Konto abzielen. Anträge, für die unterschiedliche Zielkonten erforderlich sind, müssen in separaten Wellen platziert werden.
- Multi-account Migration — AWS Organizations erforderlich — Alle Zielkonten müssen Teil einer AWS Organisation sein.

Entdecken Sie die Quelldaten

Um lokale Daten zu ermitteln und zu sammeln, können Sie das [AWS Transform Discovery Tool](#), den AWS Migration Evaluator Collector verwenden oder Exporte aus RVTools und ModelizeIT sowie Exporte im AWS Migration Portfolio Assessment (MPA) -Format hochladen, die von Tools wie Cloudamize generiert wurden. AWS Transform kann Exporte des AWS Transform-Discovery-Tools als CSV- und JSON-Dateien in einem ZIP-Dateiformat verarbeiten, RVTools-Exporte entweder als Excel-Datei oder als ZIP-Datei mit CSV-Dateien und ModelizeIT CSV-Exporte in einer ZIP-Datei. Für jede Datenquelle akzeptiert AWS Transform die primäre Serverdatei einzeln. Zusätzliche Dateien wie

Verbindungen werden jedoch nur verarbeitet, wenn sie in einer ZIP-Datei mit den Serverdateien oder in einer Excel-Datei mit dem Serverblatt enthalten sind.

Wir empfehlen Ihnen, die detailliertesten verfügbaren Daten hochzuladen und Ihre Exportdateien vor dem Hochladen zu überprüfen, um die Vollständigkeit und Richtigkeit der Daten sicherzustellen. Vergewissern Sie sich, dass alle erforderlichen Dateien in Ihrem Upload enthalten sind, und stellen Sie sicher, dass die Daten Ihren aktuellen Umgebungsstatus widerspiegeln. Diese vorläufige Überprüfung trägt dazu bei, den Bedarf an erneuten Uploads zu minimieren und stellt sicher, dass AWS Transform Ihre lokale Umgebung genauer erfassen und die Migrationsplanung, einschließlich Anwendungsgruppierung und Wellenplanung, besser unterstützen kann. Sie können auch schrittweise Daten hinzufügen, sobald Sie bessere Daten erhalten.

AWS Transform erkennt automatisch das Dateiformat und die Struktur, analysiert und extrahiert strukturierte Entitätsdatensätze, entfernt Duplikate aus mehreren Dateien, überprüft die Datenqualität, meldet Probleme und erstellt dann eine Zusammenfassung, die für die nachgelagerte Migrationsplanung bereit ist.

Nachdem Sie Ihre lokalen Daten freigegeben und bestätigt haben, können Sie die Ermittlungsdaten überprüfen, indem Sie im Jobplan die Option Lokale Daten ermitteln erweitern und Zusammenfassung der Inventarbereitschaft auswählen. Sie können auch Fragen zu den hochgeladenen Daten stellen, um sicherzustellen, dass AWS Transform alles korrekt aufgenommen hat, oder um Fehler bei der Datenverarbeitung zu identifizieren und zu korrigieren. Sie können beispielsweise nach dem Betriebssystem und den Versionen fragen. Wenn Sie Fehler korrigieren müssen, können Sie Ihre Inventardaten mit dem von Ihnen verwendeten Discovery-Tool erneut hochladen. AWS Transform verarbeitet, dedupliziert und führt die aktualisierten Datensätze automatisch zusammen. Sie können auch eine zuvor hochgeladene Datei entfernen, wenn Sie diese Inventardaten nicht mehr verwenden möchten.

Erstellen Sie einen Migrationsplan

Der Arbeitsschritt zur Migrationsplanung in AWS Transform for VMware ist ein kollaboratives, chat-basiertes Erlebnis für die Planung großer Migrationen. AWS Transform-Agenten wenden AWS Prescriptive Guidance an, um Kunden von der Analyse der lokalen Daten bis hin zur endgültigen Planung der Migrationswelle zu begleiten.

Nachdem der Job Discover On-Premises-Daten erfolgreich abgeschlossen wurde, verwendet AWS Transform die Discovery-Daten, um Anwendungen in Migrationswellen zu gruppieren. AWS Transform führt Sie durch die einzelnen Schritte zur Analyse und zum Umfang Ihrer Server, zur

Gruppierung zu Anwendungen, zur Generierung von Verschiebegruppen und zur Erstellung von Migrationswellen. Bei der Analyse Ihrer lokalen Umgebung können Sie Fragen stellen, um besser zu verstehen, wie AWS Transform Ihre installierte Software analysiert hat, beispielsweise Serverabhängigkeiten und Netzwerkarchitektur.

AWS Transform unterstützt Anpassungen des Umfangs innerhalb von Anwendungsgruppen und Wellen. Sie können Discovery-Daten jederzeit erneut hochladen. AWS Transform verarbeitet, dedupliziert und führt neue Datensätze automatisch mit vorhandenen Daten zusammen. Wenn Änderungen erkannt werden, z. B. neu entdeckte Abhängigkeiten oder Infrastrukturerweiterungen, kennzeichnet AWS Transform die betroffenen Abhängigkeitsgruppen und gibt Empfehlungen für Anpassungen des Wave-Plans. Bei der Migrationsplanung können auch unstrukturierte Textdaten verwendet werden, um den Planungsprozess zu bereichern.

Es gibt vier Phasen der Migrationsplanung:

- Unter Umfang und Analyse können Sie Ihre Discovery-Daten überprüfen, Fragen zu Ihrer Software- und Netzwerkumgebung stellen und festlegen, welche Ressourcen für die Migration vorgesehen sind.
- In Gruppen-Apps können Sie eine Kombination aus geschäftlichen und technischen Regeln angeben, z. B. in Bezug auf die Hostnamenanalyse, Netzwerkabhängigkeiten und Geschäftsregeln, sodass Ihre Infrastruktur bei der Migrationsplanung in Anwendungen gruppiert werden kann. Wenn Sie bereits über ein Inventar Ihrer Anwendungen verfügen, kann die Migrationsplanung dieses stattdessen verwenden.
- Unter Verschiebungsgruppen generieren können Sie der Migrationsplanung Ihre technischen und geschäftlichen Anforderungen mitteilen, sodass sie festlegen kann, welche Anwendungen zusammen verschoben werden müssen. Zu den technischen Abhängigkeiten gehören Datenbanken, Nachrichtenwarteschlangen oder andere Ressourcen, die von mehreren Apps gemeinsam genutzt werden. Zu den geschäftlichen und betrieblichen Abhängigkeiten gehören geschäftliche Kritikalität, RPO und RTO, Standort des Rechenzentrums und Anwendungseigentümer.
- Schließlich können Sie in Build Waves der Migrationsplanung einen Kontext zu Ihren Zeitplänen und Prioritäten geben, sodass sie einen Wellenplan erstellen kann, den Sie migrieren können. Sie können Move-Gruppen für die Aufnahme in eine Welle auf der Grundlage von Faktoren wie Prioritätsbewertung, Move-Gruppengröße, Benutzeranzahl und Anwendungskomplexität auswählen.

Terminologie der Migrationsplanung:

- Migrationswellen sind logische Gruppen, die zusammen migriert werden. Migrationswellen bestehen aus einer oder mehreren Bewegungsgruppen.
- Eine Verschiebungsgruppe besteht aus einer Reihe voneinander abhängiger Anwendungen, die zusammen verschoben werden müssen. Sie können technische Abhängigkeiten wie eine gemeinsam genutzte Datenbank oder geschäftliche Abhängigkeiten wie die Unterstützung einer gemeinsamen Geschäftsfunktion haben.
- Eine Abhängigkeit ist eine Beziehung zwischen Systemen. Es gibt verschiedene Arten von Abhängigkeiten, darunter:
 - Kritische oder harte Abhängigkeiten, bei denen Systeme ohne die Abhängigkeit nicht funktionieren können. Typische Beispiele hierfür sind Anwendungen, die von Datenbanken, anderen Anwendungen oder Diensten abhängig sind.
 - Weiche Abhängigkeiten, die für den Betrieb des Systems nicht entscheidend sind. Typische Beispiele hierfür sind latenzunempfindliche Abhängigkeiten, die unabhängig voneinander migriert werden können.
 - Non-technical Zu den Abhängigkeiten gehören geschäftliche, organisatorische, betriebliche und Compliance-Abhängigkeiten. Dies sind Abhängigkeiten, die sich auf Ihre Organisation und ihre Prioritäten beziehen. Beispiele hierfür sind gemeinsame Geschäftsfunktionen und organisatorische Eigenverantwortung.

Workflow

Die Migrationsplanung ist ein interaktiver und iterativer Arbeitsablauf. Sie können jederzeit zurückgehen und Änderungen an den vorherigen Schritten vornehmen. Ein typischer Workflow zur Migrationsplanung ist:

1. Die Migrationsplanung beginnt mit der Zusammenfassung der verfügbaren Discovery-Daten. Überprüfen Sie die verfügbaren Daten und kehren Sie jederzeit zum Ermittlungsschritt zurück, um zusätzliche Daten bereitzustellen.
2. Im Schritt „Umfang und Analyse“ können Sie Fragen zu Ihrer lokalen Umgebung stellen, um die gesammelten Daten zu validieren. Zu den Beispielfragen gehören:
 - a. Meine Server nach Betriebssystem auflisten
 - b. Fassen Sie meine lokale Netzwerktopologie zusammen
 - c. Führen Sie die gängigsten Technologien auf, die in meiner Umgebung ausgeführt werden.
3. Wenn Sie bei der Analyse Ihrer Umgebung Server identifizieren, die nicht migriert werden sollten, können Sie AWS Transform anweisen, diese Ressourcen auszuschließen. Beispiele hierfür sind:

- a. Entfernen Sie alle Server, deren Hostname Legacy enthält
 - b. Entfernen Sie alle Server in Version 10.0.2. 0/24 Subnetz
 - c. Entfernen Sie alle Server, auf denen Versionen von Windows ausgeführt werden, die älter als 2022 sind
4. Sobald Sie Ihre Umgebung ausreichend untersucht und Ihren Migrationsumfang bestimmt haben, können Sie AWS Transform anweisen, mit dem nächsten Schritt der Migrationsplanung fortzufahren.
5. Der nächste Schritt ist die Gruppierung von Anwendungen. Wenn Sie Ihre Server bereits Anwendungen zugeordnet haben, können Sie AWS Transform anweisen, diese Zuordnung zu verwenden, und diesen Schritt überspringen. Wenn Sie Ihre Anwendungen nicht vordefiniert haben, können Sie die technische und geschäftliche Logik angeben, die Ihre Anwendungen definiert. AWS Transform führt Sie durch den Prozess der Anwendungsgruppierung und schlägt Ihnen die Datenpunkte vor, die Sie bereitstellen können, um Ihre Server effektiv zu Anwendungen zusammenzufassen. Je mehr Informationen Sie zu Ihren lokalen Anwendungen bereitstellen können, desto effektiver kann AWS Transform Ihre Server in Apps gruppieren. Sobald Sie genügend Informationen bereitgestellt haben, können Sie AWS Transform anweisen, die Anwendungsgruppierung durchzuführen.
6. Sobald die Anwendungsgruppierung durchgeführt wurde, überprüfen Sie die Anwendungsgruppen. Sie können AWS Transform anweisen, alle erforderlichen Änderungen vorzunehmen, zum Beispiel:
- a. Verschieben Sie Server Example-Server nach Application-5
 - b. Benennen Sie Anwendung-5 in „HR-App-Testumgebung“ um
 - c. Entfernen Sie alle Linux-Server aus der IIS-Entwicklungsfarm
7. Sobald Ihre Apps gruppiert sind, weisen Sie AWS Transform an, mit dem nächsten Schritt fortzufahren
8. Der nächste Schritt ist die Gruppierung von Verschiebungen. Im Schritt Gruppierung verschieben identifizieren Sie Anwendungen, die zusammen verschoben werden müssen. Stellen Sie den Kontext zu Ihren technischen und nichttechnischen Abhängigkeiten bereit. AWS Transform führt Sie durch den Prozess und schlägt Ihnen Datenpunkte vor, die Sie angeben können, um Ihre Apps zu gruppieren. In dieser Phase müssen mehrere Überlegungen angestellt werden, darunter:
- a. Was sollte die Zielgröße der Umzugsgruppe sein?
 - b. Möchten Sie Umgebungen, zum Beispiel Dev, Test und Prod, für jede App kombinieren oder sie aufteilen?

- c. Wie möchten Sie Netzwerkabhängigkeiten berücksichtigen? Sind alle Abhängigkeiten kritisch oder können einige Abhängigkeiten als weiche Abhängigkeiten betrachtet und auf mehrere Verschiebungsgruppen aufgeteilt werden?
9. Sobald Sie Ihre Regeln für die Gruppierung von Zügen angegeben haben, weisen Sie AWS Transform an, Ihre Strategie zur Gruppierung von Zügen auszuführen. Anschließend können Sie Ihre Zuggruppen überprüfen und ändern. Nachdem Sie Ihre Move-Gruppen überprüft haben, können Sie AWS Transform anweisen, mit dem letzten Schritt der Migrationsplanung fortzufahren.
10. Die Wellenplanung ist der letzte Schritt der Migrationsplanung. In diesem Schritt gruppieren Sie Ihre Umzugsgruppen in Migrationswellen und priorisieren diese Wellen. Im Schritt der Wellenplanung führt Sie AWS Transform durch die Bereitstellung der Geschäftsprioritäten, die erforderlich sind, um Ihre Umzugsgruppen in Wellen zu gruppieren und diese Wellen dann zu priorisieren. Zu den Überlegungen bei der Wellenplanung gehören:
- a. Die geschäftliche Bedeutung jeder Ihrer Move-Gruppen
 - b. Die Migrationszeitpläne und die Zeitpläne für jede Move-Gruppe
 - c. Die mit jeder Umzugsgruppe verbundenen Risiken
 - d. Die Anzahl der Server, die pro Welle migriert werden sollen
11. Sobald Sie ausreichend Informationen zur Gruppierung in Wellen gegeben haben, weisen Sie AWS Transform an, die Wellenplanung durchzuführen. Anschließend können Sie Ihre Wellen überprüfen und ändern.
12. Sobald Sie Ihren Wave-Plan fertiggestellt haben, können Sie die Migrationsplanung abschließen und mit der Ausführung fortfahren. Sie können jederzeit zur Migrationsplanung zurückkehren, um Ihren Plan zu verfeinern und zu wiederholen.
13. Für jede Welle können Sie eine Migrationsstrategie zuweisen: rehosten (Server zu Amazon EC2 migrieren) und containerisieren (Quellcode containerisieren und auf Amazon Elastic Container Service oder Amazon Elastic Kubernetes Service bereitstellen). Wenn Sie einer Welle die Strategie containerisieren zuweisen, führt AWS Transform den Workflow zur Containerisierung des Quellcodes für diese Welle während der Ausführung der Migration aus. Weitere Informationen finden Sie unter [Containerisierung des Quellcodes](#). Informationen zu den AWS empfohlenen Strategien für das 7Rs-Framework, bevor Sie sie zuweisen, finden Sie unter [the section called "7R-Empfehlungen"](#)

Empfehlungen zur Migrationsstrategie (7R)

Während der Migrationsplanung kann AWS Transform Ihr entdecktes Inventar analysieren und für jeden Server und jede Anwendung eine Migrationsstrategie — eine der branchenüblichen 7Rs — empfehlen. Jede Empfehlung beinhaltet einen vorgeschlagenen AWS Zielservice, eine Vertrauensbewertung und die Gründe dafür. Dies gibt Ihnen einen soliden Ausgangspunkt für Ihren Wellenplan und zeigt Modernisierungsmöglichkeiten auf, die Sie sonst möglicherweise verpassen würden.

Die sieben Strategien lauten Rehost, Replatform, Refactoring, Repurchase, Restoration, Retention und Relocation. AWS Transform liest Signale in Ihren Daten — wie Betriebssystem, Auslastung und Workload-Typ —, um erklärbare Empfehlungen auszusprechen. Es kann beispielsweise empfehlen, inaktive oder ausgelaufene Server außer Betrieb zu nehmen, SQL Server- oder Open-Source-Datenbanken nach Amazon RDS zu verlagern, E-Mail- und Collaboration-Workloads auf Microsoft 365 zu verlagern, spezialisierte Altsysteme beizubehalten und die verbleibenden Workloads auf Amazon EC2 neu zu hosten. Die Empfehlungen werden von einzelnen Servern bis hin zu Anwendungen und für Ihr gesamtes Portfolio zusammengefasst, mit einer nach Strategie aufgeschlüsselten Kritikalität und Zusammenfassungen auf Wellenebene.

So erstellen Sie einen Bericht zur Migrationsstrategie (7 Rs):

1. Schließen Sie den Schritt Lokale Daten ermitteln ab und gruppieren Sie Ihre Server in Anwendungen. Beide sind erforderlich, damit AWS Transform Empfehlungen pro Server und pro Anwendung geben kann.
2. Bitten Sie AWS Transform im Chat zur Migrationsplanung um einen Bericht zur Migrationsstrategie (7 Rs) — zum Beispiel einen Bericht generieren. R-strategy Nach Abschluss der Anwendungsgruppierung bietet AWS Transform auch an, den Bericht für Sie zu erstellen.
3. AWS Transform analysiert Ihr Inventar, wendet das 7Rs-Framework an und generiert den Bericht. Sie können Details wie den Namen Ihrer Organisation und alle Filter für den Umfang der Analyse angeben.
4. Lesen Sie sich die Empfehlungen durch. Um eine Empfehlung anzupassen, teilen Sie AWS Transform im Chat mit, ob Sie einen einzelnen Server oder eine Anwendung ändern oder eine Änderung in großen Mengen vornehmen möchten (z. B. nach Betriebssystem, Umgebung, Welle oder Priorität). AWS Transform aktualisiert den Bericht mit Ihren Änderungen.

Standardmäßig erstellt AWS Transform ein interaktives HTML-Dashboard, das Sie filtern und erkunden können. Auf Anfrage können Sie auch ein PDF-Dokument erstellen, um es mit

den Beteiligten zu teilen, oder ein Microsoft PowerPoint (PPTX) -Foliendeck zur Präsentation erstellen. Das PDF und die PowerPoint Ausgaben sind Momentaufnahmen derselben Analyse. Der Bericht enthält eine empfohlene Strategie und einen AWS zielgerichteten Service für jeden Server und jede Anwendung, Vertrauensbewertungen und Argumentation, hervorgehobene Modernisierungsmöglichkeiten, eine nach Strategie aufgeschlüsselte Kritikalität, Zusammenfassungen auf Wellenebene und Risikokennzeichnungen.

Die in diesem Bericht empfohlene Strategie ergänzt die Strategie pro Welle, die Sie bei der Planung der Welle festlegen. Informationen zur Containerisierung von Quellcode finden Sie unter.

[Containerisierung des Quellcodes](#)

Diagrammerstellung und Berichterstattung

Während der Migrationsplanung wandelt AWS Transform Ihre entdeckten Bestands- und Planungsergebnisse in visuelle Diagramme und Analyseberichte um. Sie generieren sie in Konversation im Planungsschat — zum Beispiel mit „Zeigen Sie mir ein Netzwerktopologiediagramm“ oder „Erstellen Sie einen Risikobericht“. AWS Transform erstellt sie aus den Daten, die Sie bereits bereitgestellt haben, ohne dass eine Einrichtung erforderlich ist.

Diagramme sind interaktiv und ermöglichen es Ihnen, Ihre Umgebung visuell zu erkunden. Zu den verfügbaren Diagrammen gehören:

- Netzwerktopologie — Eine interaktive Karte Ihrer Server und ihrer Netzwerkbeziehungen, die auf große Umgebungen mit Tausenden von Knoten skaliert werden kann.
- Anwendungsabhängigkeit — Direkte Beziehungen zwischen Anwendungen, abgeleitet von Ihren beobachteten Netzwerkverbindungen.
- Wave-Gantt-Diagramm — Eine Zeitleiste Ihrer Migrationswellen mit Zeitplänen, Abhängigkeiten, Meilensteinen und Fortschritten (verfügbar nach der Wellenplanung).
- Allgemeine Diagramme — Kreisdiagramme, Balkendiagramme, Histogramme, Baumkarten und Übersichtstabellen mit den von Ihnen ausgewählten Datendimensionen.

Berichte bieten ausführliche Analysen und Empfehlungen zu Ihren Migrationsdaten. Zu den verfügbaren Berichten gehören:

- Risikobewertung — Bewertet jede Anwendung im Hinblick auf technische Komplexität, Abhängigkeitsrisiko, Migrationsbereitschaft und betriebliches Risiko mit Zusammenfassungen pro Anwendung, pro Welle und für das gesamte Portfolio.

- Migrationsstrategie (7 Rs) — und Strategieempfehlungen pro Anwendung. Per-server Weitere Informationen finden Sie unter [the section called “7R-Empfehlungen”](#).
- Allgemeine und benutzerdefinierte Berichte — Analyseberichte für Anfragen wie Zusammenfassungen der Bereitschaft von Führungskräften, Abwägungen zwischen Kosten und Risiken und Bewertungen von Kandidaten für die Containerisierung.

Einige Ergebnisse hängen davon ab, wie weit Sie in der Planung sind.

Anwendungsabhängigkeitsdiagramme verwenden beispielsweise Ihre Netzwerkverbindungsdaten. Das Wellen-Gantt-Diagramm und die Zusammenfassungen der Berichte auf Wellenebene sind nach Abschluss der Wellenplanung verfügbar. Wenn eine Voraussetzung fehlt, teilt Ihnen AWS Transform mit, was erforderlich ist, und kann den erforderlichen Schritt zuerst ausführen.

AWS Transform stellt Diagramme als interaktives HTML bereit, das Sie filtern und untersuchen können. Standardmäßig stellt AWS Transform Berichte als eigenständige HTML-Datei bereit. Auf Anfrage kann AWS Transform auch ein PDF-Dokument generieren, das mit Stakeholdern geteilt werden kann, oder ein Microsoft PowerPoint (PPTX) -Foliendeck zur Präsentation. PDF und PowerPoint Ausgaben sind Momentaufnahmen derselben Analyse.

Ziel Connect AWS-Konto s und Regionen

Konfigurieren Sie Ihren AWS-Konto Zielconnector für Netzwerkmigration, landing zone Zone-Build und Servermigration. Dies umfasst drei Schritte: Wählen Sie Ihren Migrationstyp aus, geben Sie Ihre MAP-Vertragsdetails an (falls zutreffend) und richten Sie den Connector ein. Diese Einstellungen gelten für alle Migrationsphasen — Netzwerkmigration, landing zone und Server-Rehost.

Schritt 1: Auswahl des Migrationstyps

Wählen Sie aus, ob Sie eine Migration mit einem oder mehreren Konten durchführen möchten:

- Single-account Migration — Alle Workloads werden auf ein Ziel migriert. AWS-Konto Das Connector-Zielkonto und das Zielkonto sind identisch.
- Multi-account Migration — Workloads werden auf verschiedene Zielkonten migriert. Der Connector muss mit dem Organisationsverwaltungskonto oder einem für beide AWS Transform MGN registrierten Delegierten Administratorkonto (DA) verbunden sein. CloudFormation StackSets

Schritt 2: MAP-Vereinbarung

Wenn Ihre Migration Teil des AWS Migration Acceleration Program (MAP 2.0) ist, geben Sie Ihre Migration Portfolio Experience (MPE) -ID an — einen 10-stelligen Code mit Großbuchstaben und Zahlen (z. B. ABCDE12345). Wenn Sie Ihre MPE-ID angeben, wird das MAP-Tag auf alle Ressourcen angewendet, die in den Phasen Netzwerkmigration, landing zone und Server-Rehost erstellt wurden. Das Tag-Format ist:

- Schlüssel: map-migrated Wert: mig~~MPE_ID~~

Sie müssen MAP-Tags verwenden, um MAP-Guthaben zu erhalten. Weitere Informationen zu MAP finden Sie unter [AWS Migration Acceleration Program](#).

Schritt 3: Konfiguration des Connectors

Sie verwenden den Zielkonto-Connector, um Ihren Migrationsjob mit der AWS Umgebung zu verbinden, in der sich Ihre Workloads nach der Migration befinden werden. Bevor Sie beginnen, stellen Sie sicher, dass Ihr Ziel AWS-Konto über die erforderlichen Berechtigungen, Kontingente und Konfigurationen verfügt, um Ihre migrierte Infrastruktur zu unterstützen.

Wenn Sie die Connector-Anfrage genehmigen, gewähren Sie AWS Transform-Berechtigungen für:

- Verwalten Sie Amazon S3 S3-Bucket-Operationen (read/write) für die VMware-Migration sowie den Zugriff auf AWS Migration Hub und AWS Application Migration Service (MGN). Dazu gehören Berechtigungen für die folgenden Elemente, die alle auf Ressourcen innerhalb des Zielkontos beschränkt sind, die mit CreatedBy:AWSTransform oder CreatedFor:AWSTransform gekennzeichnet sind:
 - Migrationswellen verwalten.
 - Netzwerkkonfigurationen verwalten (Amazon EC2, VPC, Transit Gateway, Direct Connect, Load Balancers, Network Firewall).
 - Stack-Bereitstellungen verwalten CloudFormation .
 - Führen Sie automatisierte Agenteninstallationen über Systems Manager durch.
- Migrieren Sie Ihre lokalen Workloads mithilfe der in der Discovery-Region gespeicherten Informationen auf das Ziel AWS-Konto und die Region.
- Bereitstellung und Verwaltung der Landezoneninfrastruktur im Ziel AWS-Konto und in der Region. Dazu gehören Berechtigungen für die folgenden Elemente, die CreatedBy:AWSTransform gegebenenfalls auf Ressourcen beschränkt sind, die mit gekennzeichnet sind:

- Führen Sie Amazon S3 S3-Bucket-Operationen (Erstellen, Lesen, Schreiben, Löschen) für Buckets durch, die mit `transform-vmware-landing-zone-` beginnen.
- Verwalte CloudFormation Stack-Bereitstellungen und ändere Sets für Landing-Zone-Stacks.
- Führen Sie AWS Control Tower Tower-Operationen durch. Sie können Landezonen verwalten, Baselines aktivieren und Kontrollen aktivieren.
- AWS Organizations verwalten. Sie können Organisationseinheiten erstellen und verwalten, Konten erstellen und Konten verschieben.
- Verwalten Sie Service Control Policies (SCPs) über AWS Control Tower.
- Verwalten Sie die Bereitstellungsartefakte von AWS Service Catalog.

Note

Connectortypen werden möglicherweise aktualisiert, wenn für neue Funktionen eine Änderung der Berechtigungen erforderlich ist. Die aktuelle Version für den Connectortyp für das Zielkonto ist 2.0. Wenn Sie einen neuen Connector erstellen, verwendet er die neueste Version.

Bevor Sie den Connector einrichten, sollten Sie sich mit den Kontrollen vertraut machen, die an Ihrer Migration beteiligt sind:

Account	Description
AWS Konto transformieren	Jedes Mitgliedskonto in Ihrer AWS Organisation, in dem Sie AWS Transform eingerichtet haben. Hier läuft dein AWS Transform-Workspace. Es muss nicht das Verwaltungskonto sein.
Connector-Zielkonto	Das Konto, für das Ihr AWS Transform-Connector konfiguriert ist. Das hängt von Ihrem Migrationstyp ab: • Single-accountMigration — Connect zu dem Konto her, zu dem Sie Workloads migrieren. Das Connector-Zielkonto und das Zielkonto sind identisch. • Multi-accountMigration — Connect dem Organisationsverwaltungskonto oder einem Delegated Administrator (DA) -Konto her. Das DA-Konto muss sowohl für MGN als auch CloudFormation StackSets in

Account	Description
	Ihrer Organisation als delegierter Administrator registriert sein. AWS AWS Transform überprüft, ob es sich bei dem verbundenen Konto um das Verwaltungskonto oder ein DA-Konto handelt, und passt sein Verhalten entsprechend an.
Zielkonto	Das AWS-Konto , wohin Ihre Workloads migriert werden. Bei einer Migration mit einem einzelnen Konto entspricht dies dem Connector -Zielkonto. Bei einer Migration mit mehreren Konten sind dies die einzelnen Mitgliedskonten, die die migrierten Workloads erhalten.

Verwenden eines delegierten Administratorkontos

Für Migrationen mehrerer Konten AWS empfiehlt es sich, ein delegiertes Administratorkonto (DA) anstelle des Organisationsverwaltungskontos direkt zu verwenden. Ein DA-Konto folgt dem Prinzip der geringsten Rechte, indem es den Umfang der für Migrationsvorgänge erforderlichen Berechtigungen einschränkt. Das DA-Konto muss sowohl für MGN als auch CloudFormation StackSets in Ihrer AWS Organisation als delegierter Administrator registriert sein.

Der Hauptunterschied zwischen den beiden Optionen ist:

- Verwaltungskonto — Kann vertrauenswürdigen Zugriff für MGN und CloudFormation StackSets unternehmensweit ermöglichen. AWS CloudFormation StackSets Aufruf-APIs transformieren mit `CallAs: SELF`.
- Delegiertes Administratorkonto — Der vertrauenswürdige Zugriff kann nicht direkt aktiviert werden (dies muss über das Verwaltungskonto erfolgen), kann jedoch MGN-Quellserver verwalten, Instanzen starten und die Bereitstellung für CloudFormation StackSets mehrere Mitgliedskonten durchführen. AWS CloudFormation StackSets APIs für Transform-Aufrufe mit `CallAs: DELEGATED_ADMIN`

Weitere Informationen finden Sie unter [Delegierter Administrator für MGN im MGN-Benutzerhandbuch](#).

IAM-Rollen, die während der Connector-Setup erstellt wurden

Während der Connector-Setup erstellt AWS Transform die folgende IAM-Rolle in Ihrem Zielkonto:

- **AWSTransform-Connector-role**— Wird erstellt, wenn Sie den Zielkonto-Connector im Verwaltungskonto oder im delegierten Administratorkonto Ihrer AWS Organisation einrichten. Diese Rolle ermöglicht es AWS Transform, eine Verbindung zu Ihrem Zielkonto herzustellen und in Ihrem Namen Migrationsvorgänge durchzuführen.

Einrichtung des Zielkonto-Connectors

Important

Während der Connector-Setup wird ein Amazon S3 S3-Bucket in Ihrem Ziel erstellt AWS-Konto. Dieser Bucket erzwingt standardmäßig keinen HTTPS-only Zugriff (SecureTransport). Wenn Sie möchten, dass die Bucket-Richtlinie sicheren Transport beinhaltet, müssen Sie die Richtlinie selbst aktualisieren. Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden für Amazon S3](#).

Um einen vorhandenen Zielkonto-Connector zu verwenden

1. Erweitern Sie im Bereich Jobplan die Option Zielkonto auswählen und wählen Sie dann Connectors erstellen oder auswählen aus.
2. Wählen Sie auf der Registerkarte Zusammenarbeit einen vorhandenen Connector aus und wählen Sie dann Connector verwenden aus. Wenn ein Connector nicht verfügbar ist, ist seine Version nicht mit dem ausgewählten Jobtyp kompatibel.

Important

Wenn Sie einen Connector mit einem Ziel angeben AWS-Region , das sich von der AWS Transformationsregion unterscheidet, überträgt AWS Transform Ihre Daten zwischen diesen AWS-Regionen.

3. Klicken Sie auf Weiter.

Um einen neuen Konnektor zu erstellen

1. Erweitern Sie im Bereich Job Plan die Option Connect-Zielkonto und wählen Sie dann Connectors erstellen oder auswählen aus.
2. Geben Sie das AWS-Konto und AWS-Region für Ihr Ziel an, und wählen Sie dann Weiter.

⚠ Important

Wenn sich das Ziel von der Erkennung AWS-Region unterscheidet AWS-Region, überträgt AWS Transform Ihre Daten AWS-Regionen.

3. Wählen Sie aus, ob Sie verwaltete Amazon S3 S3-Schlüssel für die Verschlüsselung verwenden möchten. Wenn Sie Ihren eigenen KMS-Schlüssel angeben, können Sie die Standardschlüsselrichtlinie oder eine weniger freizügige Richtlinie verwenden. Informationen zum Erstellen eines KMS-Schlüssels finden Sie unter [Erstellen eines KMS-Schlüssels](#) im AWS Key Management Service Entwicklerhandbuch.

AWS Transform verwendet die `kms:DescribeKey` Berechtigung, um zu überprüfen, ob der Schlüssel vorhanden ist, `kms:GenerateDataKey` und `kms:Decrypt` um Auftragsdaten im Amazon S3 S3-Bucket zu verschlüsseln und zu entschlüsseln. Weitere Informationen finden Sie unter [Senkung der Kosten SSE-KMS mit Amazon S3 Bucket Keys](#).

4. Klicken Sie auf Weiter.
5. Kopieren Sie den Bestätigungslink, teilen Sie ihn einem Administrator des Ziels mit und bitten Sie ihn AWS-Konto, die Verbindungsanfrage zu genehmigen.
6. Nachdem der Administrator die Anfrage genehmigt hat, wählen Sie den neu erstellten Connector aus der Liste aus und klicken Sie auf Connector verwenden.
7. Wählen Sie „Zur AWS Transformation senden“.

Wenn Sie die AWS Transform MGN Vorlage ändern möchten, um Aktionen nach dem Start zu ermöglichen, fügen Sie der Ziel-Connector-Rolle die folgende Berechtigung hinzu. Diese JSON-Richtlinienerklärung erteilt die `iam:PassRole` Berechtigung für die Rolle „Aktionen nach dem Start“. Sie finden den Rollennamen auf der Registerkarte Zusammenarbeit, nachdem der Connector erstellt wurde. Informationen zum Hinzufügen von Berechtigungen zu einer Rolle finden Sie unter [Aktualisieren von Berechtigungen für eine Rolle](#) im IAM-Benutzerhandbuch.

```
{
  "Sid": "MGNPostLaunchActions",
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
```



```
}
```

Unterstützte Zielregionen

Eine Migrationszielregion ist die Region, AWS-Region in der migrierte Ressourcen bereitgestellt werden, einschließlich Landing Zones, Netzwerkinfrastruktur und Server-Rehosting. Wenn Sie den Connector erstellen, geben Sie ein Ziel an. AWS-Region Sie können eine der folgenden Optionen verwenden AWS-Regionen:

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Taipeh)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Tokio)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Neuseeland)
- Asien-Pazifik (Thailand)
- Kanada (Zentral)
- Kanada West (Calgary)
- Europa (Frankfurt)
- Europa (Zürich)

- Europa (Irland)
- Europa (London)
- Europe (Paris)
- Europe (Stockholm)
- Europa (Milan)
- Europa (Spain)
- Israel (Tel Aviv)
- Mexiko (Zentral)
- Südamerika (São Paulo)

Important

Wenn Sie ein Ziel angeben AWS-Region , das sich von der AWS Transform unterscheidet AWS-Region, werden einige Ihrer Daten übertragen AWS-Regionen.

Beachten Sie, dass Ihre Serverreplikationsdaten direkt von Ihrer Quellumgebung zu Ihrem Zielkonto und Ihrer Zielregion übertragen werden.

landing zone bauen

AWS Transform führt Sie durch den Entwurf und die Implementierung einer AWS landing zone im Rahmen Ihres Migrationsprojekts. Eine landing zone ist eine AWS Umgebung mit mehreren Konten, die als Grundlage für Ihre Workloads dient. Organisationsgrenzen, Governance-Kontrollen und Kontostrukturen sind vorhanden, bevor Workloads eintreffen. AWS Transform analysiert Ihren Migrationsbestand und Ihre Geschäftsanforderungen, um eine Organisationseinheit (OU) und eine Kontostruktur zu empfehlen, empfohlene Service Control Policies (SCPs) anzuwenden und die Infrastruktur als Code (IaC) and/or bereitzustellen.

Der landing zone Agent führt Sie durch zwei Phasen:

- Aufbau der Foundation — Richten Sie die Struktur der zentralen landing zone ein: AWS Control Tower, grundlegende Organisationseinheiten und Kernkonten.
- Workload-Kontodesign — Entwerfen und erstellen Sie Workload-Organisationseinheiten und Konten auf der Grundlage Ihrer Migrationswellen, Geschäftsbereiche und Anforderungen an die Trennung der Umgebung.

AWS Transform unterstützt sowohl Greenfield-Umgebungen (keine bestehende landing zone) als auch Brownfield-Umgebungen (bestehende Organisationseinheiten und Konten wurden bereits bereitgestellt). In Brownfield-Szenarien erkennt AWS Transform Ihre bestehende Organisationsstruktur und empfiehlt nur die Änderungen, die erforderlich sind, um Lücken im Vergleich zu bewährten Verfahren zu schließen. AWS

Einrichtung des Konnektors

Der landing zone Agent benötigt einen AWS-Konto Ziel-Connector, um Ressourcen in Ihrem Organisationsverwaltungskonto bereitzustellen. Der Connector hat folgende Berechtigungen:

- [AWS Control Tower](#) einrichten
- Erstellen Sie [Organisationseinheiten und Konten](#)
- Konfigurieren Sie [Service Control Policies \(SCPs\)](#)

Wenn Sie die Connector-Anfrage genehmigen, gewähren Sie AWS Transform-Berechtigungen für:

- Bereitstellung und Verwaltung der Landezoneninfrastruktur im Ziel AWS-Konto und in der Region. Dazu gehören Berechtigungen für die folgenden Elemente, die `ATWorkspace:{workspace-id}` gegebenenfalls auf Ressourcen beschränkt sind, die mit `CreatedBy:AWSTransform` und von gekennzeichnet sind:
 - S3-Bucket-Operationen (Erstellen, Lesen, Schreiben, Löschen) für Buckets, die mit `beginnen transform-vmware-landing-zone-`
 - CloudFormation Stack-Bereitstellungen und Change-Set-Management für Landingzone-Stacks
 - AWS Betrieb des Control Tower (Verwaltung von Landezonen, Aktivierung von Basislinien und Kontrollen)
 - AWS Verwaltung von [Organizations](#) (Organisationseinheiten erstellen und verwalten, Konten erstellen und Konten verschieben)
 - Verwaltung von Service Control Policy (SCP) über AWS Control Tower
 - AWS Verwaltung von Artefakten für die Bereitstellung von [Service Catalog](#)

Wenn Sie den Connector erstellen, geben Sie ein Ziel an. AWS-Region Diese Region sollte mit Ihrer Heimat-Control-Tower-Region identisch sein. Weitere Informationen zu Control Tower-Regionen finden Sie unter [So AWS-Regionen arbeiten Sie mit AWS Control Tower](#).

Zu Beginn der Einrichtung der landing zone ruft AWS Transform Ihre Connector-Konfiguration ab und präsentiert die Konto-ID der AWS Organisationsverwaltung und die Zielregion zur Bestätigung. Weitere Informationen finden Sie unter [Konnektoren](#).

⚠ Important

Abhängigkeit von der Region des IAM Identity Center — AWS Transform erfordert AWS IAM Identity Center (IAM Identity Center), was bedeutet, dass Ihre Connector-Region sowohl mit Ihrer AWS Control Tower Tower-Heimatregion als auch mit Ihrer IAM Identity Center-Region übereinstimmen muss. Wenn IAM Identity Center in Ihrer Organisation bereits konfiguriert ist, schlägt die AWS Control Tower Tower-Initialisierung fehl, wenn der Connector auf eine andere Region abzielt. Weitere Informationen finden Sie unter [Überlegungen für IAM Identity Center-Kunden](#) im AWS Control Tower Tower-Benutzerhandbuch.

Einrichtung der Stiftung

In der Phase der Einrichtung des Fundaments wird mithilfe des [AWS Control Tower](#) die Infrastruktur der Kernlandezone eingerichtet. Wenn AWS Control Tower eine landing zone einrichtet, stellt er automatisch eine Reihe von verwalteten Ressourcen in Ihrem Verwaltungskonto bereit, die die Governance-Grundlage für Ihr gesamtes AWS Unternehmen bilden:

- Root — Das übergeordnete Element der obersten Ebene, das alle OUs in Ihrer landing zone enthält.
- Security OU — Automatisch von Control Tower erstellt. Enthält zwei gemeinsame Konten: das Log Archive-Konto (zentrale, unveränderliche Protokollierung aller AWS API-Aktivitäten und Ressourcenänderungen in Ihrem Unternehmen) und das Audit-Konto (schreibgeschützter Zugriff auf alle Konten zur Sicherheits- und Compliance-Überprüfung). Diese Konten können nach der Ersteinrichtung nicht umbenannt oder ersetzt werden.
- Obligatorische Kontrollen (Guardrails) — Control Tower wendet automatisch präventive und detektive Kontrollen in Ihrem gesamten Unternehmen an, um grundlegende Governance-Richtlinien durchzusetzen. Diese können nicht deaktiviert werden.
- IAM Identity Center-Verzeichnis — Control Tower erstellt ein cloudnatives Verzeichnis mit vorkonfigurierten Gruppen und Single Sign-On-Zugriff für Ihre landing zone Zone-Benutzer. [Weitere Informationen finden Sie unter IAM Identity Center AWS](#).

Control Tower verwendet [CloudFormation StackSets](#), um diese Ressourcen konsistent für alle Konten und Regionen in Ihrem Unternehmen bereitzustellen und zu verwalten. Sie dürfen von Control Tower verwaltete Ressourcen nicht außerhalb der unterstützten Methoden ändern oder löschen, da dies dazu führen kann, dass Ihre landing zone in einen unbekannten Zustand übergeht.

Konventionen für Konto-E-Mails

AWS erfordert eine eindeutige E-Mail-Adresse für jedes Konto. Diese E-Mails erhalten wichtige Benachrichtigungen für das Konto. AWS Transform verwendet die Plus-Adressierung, um eindeutige Konto-E-Mails aus einem einzigen Postfach zu generieren.

Format: `prefix+account-name@domain`

Sie geben ein Präfix (zum Beispiel `aws-admin`) und eine Domain (zum Beispiel `acme.com`) an, und AWS Transform leitet alle Konto-E-Mails automatisch ab. Beispiel:

- Konto prüfen: `aws-admin+audit@acme.com`
- Konto protokollieren: `aws-admin+log-archive@acme.com`
- Sandbox-Konto: `aws-admin+sandbox@acme.com`

In Brownfield-Szenarien untersucht AWS Transform bestehende Konto-E-Mails, um auf die bereits verwendete Plus-Adressierungskonvention zu schließen, und bietet an, mit demselben Muster fortzufahren.

Empfohlene Fundamentstruktur

Basierend auf AWS bewährten Methoden empfiehlt AWS Transform die folgende grundlegende Organisationsstruktur. Sie können sie vor der Erstellung anpassen.

Organisationseinheit	Zweck	Konten
Sicherheit	Zentralisierte Protokollierung und Überwachung von Audits. Die Isolierung dieser Dienste in speziellen Konten soll dazu beitragen, dass Ihr Audit-Trail von den Workload-Teams getrennt bleibt.	Prüfung, Protokollarchiv

Organisationseinheit	Zweck	Konten
Infrastruktur	Gemeinsames Netzwerk (Transit Gateway, VPN), DNS und gemeinsame Dienste. Es wird empfohlen, diese zu zentralisieren, um Doppelarbeit zu vermeiden und Ihrem Netzwerkteam einen zentralen Ort für die Verwaltung der Konnektivität zu bieten.	Keine (leer erstellt)
Sandbox	Entwickler experimentieren mit Ausgabenlimits und eingeschränktem Zugriff. Es wird empfohlen, Entwicklern Raum zum Experimentieren zu geben, ohne die Produktionsressourcen zu gefährden.	Sandbox
Workloads	Enthält Produktions- Non-Production und optional regulierte Sub-OUs. Workload-Konten werden in der nächsten Phase auf der Grundlage Ihrer Migrationsanforderungen entworfen.	Keine (leer erstellt)

Note

Die Sicherheits-OU mit den [Konten Audit und Log Archive](#) wird im Rahmen der Control Tower Foundation-Setup erstellt. Die Organisationseinheiten „Infrastruktur“, „Sandbox“ und „Workloads“ werden separat erstellt, nachdem Sie die Struktur bestätigt haben.

In Brownfield-Szenarien vergleicht AWS Transform Ihr vorhandenes Fundament mit dieser empfohlenen Struktur und meldet nur die Lücken. Zum Beispiel: „Ihre Stiftung hat Sicherheits- und Infrastruktur-Organisationseinheiten, aber keine Sandbox-Organisationseinheit.“

Service-Kontrollrichtlinien (Service Control Policies, SCPs)

SCPs sind [Berechtigungsregelungen auf Organisationsebene, mit denen die maximalen Berechtigungen für alle Konten in Ihrer Organisation festgelegt werden](#). AWS Sie gewähren

keinen Zugriff, sondern definieren Grenzen, die niemand im Konto überschreiten darf, nicht einmal Kontoadministratoren.

Im Rahmen der Installation des Control Tower werden automatisch Basisplanken angebracht. AWS Transform empfiehlt außerdem zusätzliche SCPs, die dazu beitragen sollen, die Position Ihres Unternehmens zu stärken. Diese basieren auf AWS bewährten Verfahren für eine möglichst lebensfähige landing zone.

SCPs können auf die Organisationseinheiten Infrastruktur, Sandbox und Workloads angewendet werden. Die Security OU wird vom Control Tower verwaltet und kann mit diesem Tool nicht von SCPs angegriffen werden.

Important

Die Security OU ist eine grundlegende Organisationseinheit, die von Control Tower verwaltet wird. Sie können ihm keine Konten, SCPs oder Ressourcen über den landing zone Agent hinzufügen.

In Brownfield-Szenarien überprüft AWS Transform, welche SCPs bereits angewendet wurden, und empfiehlt nur solche, die Lücken schließen würden.

Bereitstellung von Foundation

Nachdem der Foundation-Entwurf abgeschlossen ist, entscheiden Sie, wie Sie Folgendes bereitstellen möchten:

- Für mich bereitstellen — AWS Transform stellt die grundlegenden Organisationseinheiten, Konten und SCPs in Ihrem AWS Unternehmen bereit.
- Ich führe die Bereitstellung selbst durch — AWS Transform generiert Infrastructure as Code (IaC) -Artefakte zum Herunterladen in Ihrem bevorzugten Format (siehe). [the section called “IaC-Formate”](#)
- Entwerfen Sie zuerst Workload-Konten — Überspringen Sie die Bereitstellung und fahren Sie mit der Entwurfsphase für Workload-Konten fort. Sie können später alles zusammen bereitstellen.

Control Tower Tower-Initialisierung

Wenn AWS Transform feststellt, dass AWS Control Tower in Ihrer Organisation noch nicht initialisiert ist, wird dem Benutzer ein Link zur AWS Transform-Konsolenseite angezeigt. Durch das Generieren

der Operation im Link wird ein CloudFormation Stack für den Bootstrap des Control Tower erstellt. Der Prozess erstellt diesen Stack in der CloudFormation Konsole für Ihre Zielregion. Nachdem die Stack-Erstellung abgeschlossen ist, setzt AWS Transform die Bereitstellung fort.

Entwurf des Workload-Kontos

In der Phase des Workload-Kontodesigns entwirft AWS Transform die Organisationseinheit und die Kontostruktur für Ihre Anwendungs-Workloads auf der Grundlage Ihres Migrationsinventars, Ihrer Geschäftsanforderungen und Ihrer Präferenzen zur Trennung der Umgebung.

Kontext der Migrationsplanung

AWS Transform ruft Daten aus Ihrer Migrationsplanungsphase ab, darunter Wellenpläne, Zuordnungen von Servern zu Anwendungen und gemeinsamen Kontexten. Wenn Daten zur Migrationsplanung verfügbar sind, zeigt AWS Transform eine Zusammenfassung an und fordert Sie auf, diese zu bestätigen oder anzupassen. Wenn keine Daten zur Migrationsplanung verfügbar sind, stellt AWS Transform direkt Ermittlungsfragen.

Erkennung

AWS Transform stellt Fragen, um Ihre Workload-Anforderungen zu verstehen. Sie können jede Frage überspringen. Zu den Themen gehören:

- Anzahl der Geschäftsbereiche oder Teams, die AWS
- Branche und alle anwendbaren Frameworks (HIPAA, SOC2 PCI-DSS, FedRAMP)
- Ob Workloads sensible Daten verarbeiten (PII, PHI, Finanzen)
- Präferenzen für die Trennung von Umgebungen (dev/test/staging/prod als separate Konten oder als gemeinsam genutzte Konten)
- Anforderungen an die Isolierung von Arbeitslasten
- Geschäftsanwendungen und ihre Zwecke
- Gruppierung von Servern in Anwendungen
- Anforderungen an Kostenverfolgung und -zuweisung (nach Geschäftseinheit, Projekt, Umgebung)
- Erwartetes Wachstum in den nächsten 12 bis 24 Monaten
- Bevorzugte Kontostrategie (einzelne App pro Konto, gruppiert oder umgebungsbezogen)

Vorgeschlagene Arbeitslaststruktur

Basierend auf Ihren Antworten und Daten zur Migrationsplanung schlägt AWS Transform eine Organisationseinheit und eine Kontostruktur im Rahmen der Workloads-Organisationseinheit vor. Der Vorschlag enthält die Gründe für jede Entwurfsentscheidung.

AWS Transform folgt diesen Gestaltungsprinzipien:

- Alle Server in einer Migrationswelle werden demselben Konto zugewiesen — Wellen können nicht auf mehrere Konten aufgeteilt werden. Dies ist eine Rehost-Beschränkung während der Wave-Ausführung.
- Wenn Sie isolierte Umgebungen anfordern, erstellt AWS Transform Workloads/Production Workloads/Non-Production Unter-OU.
- Wenn geeignete Frameworks identifiziert werden, erstellt AWS Transform Workloads/Regulated Workloads/Standard Unter-OU.
- Wenn mehrere Geschäftsbereiche unterschiedliche Governance erfordern, erstellt AWS Transform unter Workloads unternehmensbereichsspezifische Organisationseinheiten.
- Anwendungen mit kritischen oder sensiblen Daten erhalten eine einzige App pro Konto. In diesem Fall werden Sie möglicherweise aufgefordert, Ihren Wave-Plan erneut zu bearbeiten.
- Eng verbundene Anwendungen mit gemeinsamen Abhängigkeiten sind in einem Konto zusammengefasst.

Jedes vorgeschlagene Konto umfasst: Name, Zweck, Ziel-OU und Geschäftseinheit. AWS Transform zeigt die verwendete Benennungskonvention (z. B. <business-unit>-<environment>-<workload>).

Sie können die vorgeschlagene Struktur überprüfen und ändern, bevor AWS Transform die Änderungen anwendet. Nach der Anwendung können Sie iterieren und weitere Änderungen vornehmen, bis Sie zufrieden sind.

Workload-SCP-Konfiguration

Nachdem die Workload-Struktur erstellt wurde, präsentiert AWS Transform die verfügbaren SCPs und fragt Sie, ob Sie welche auf Ihre Workload-OU anwenden möchten. Sie wählen aus, welche SCPs und auf welche Organisationseinheiten angewendet werden sollen. AWS Transform wendet die SCPs an und zeigt den aktualisierten Organisationsbaum mit einer SCP-Übersichtstabelle an.

Bereitstellung von Workloads

Nachdem der Workload-Entwurf abgeschlossen ist, entscheiden Sie, wie Sie Folgendes bereitstellen möchten:

- Für mich bereitstellen — AWS Transform stellt die Workload-OU's, Konten und SCPs für Ihr AWS Unternehmen bereit.
- Ich führe die Bereitstellung selbst durch — AWS Transform generiert IaC-Artefakte zum Herunterladen in Ihrem bevorzugten Format (siehe). [the section called “IaC-Formate”](#)

IaC-Formate

Wenn Sie Self-Deployment wählen, generiert AWS Transform Infrastructure-as-Code-Artefakte in den folgenden Formaten:

- [AWS Cloud Development Kit \(AWS CDK\)](#) — TypeScript Projekt für die programmatische Infrastrukturbereitstellung.
- HashiCorp Terraform — Generiert HCL-Vorlagen (HashiCorp Configuration Language) für die Verwaltung von landing zone Zone-Ressourcen.
- Landing Zone Accelerator (LZA) — YAML-Konfigurationsdateien, die auf der LZA Universal Configuration Version 1.1.0 basieren. Diese für Unternehmen geeigneten Vorlagen können zusammen mit dem Landing Zone Accelerator verwendet werden, um Umgebungen mit mehreren Konten einzurichten. AWS Die generierten Dateien enthalten vorkonfigurierte Einstellungen für Unternehmensführung, Organisationsstruktur und Netzwerke, die den Best Practices entsprechen. AWS Weitere Informationen finden Sie unter [LZA Universal Configuration](#).

Note

Bei der Bereitstellung über die Landing Zone Accelerator (LZA) -Pipeline müssen sich Ihr AWS Transform-Konto und die LZA-Installation in derselben Organisation befinden. AWS Die Bereitstellung schlägt fehl, wenn die in AWS Transform und LZA verwendeten Organisations-IDs nicht übereinstimmen. Informationen zum Einrichten Ihrer LZA-Installation mithilfe von [AWS Organizations finden Sie unter Organisationsbasierte Installation](#).

Nachdem Sie ein Format ausgewählt haben, generiert AWS Transform die Artefakte und stellt sie zum Herunterladen zur Verfügung.

Um sicherzustellen, dass die heruntergeladene Datei nicht beschädigt oder manipuliert wurde, generieren Sie eine Prüfsumme, laden Sie sie herunter und vergleichen Sie sie dann mit einem lokal generierten Hash mithilfe von:

```
openssl dgst -sha256 -binary <file.zip> | base64
```

Genehmigungsverfahren für die Bereitstellung

Anfragen zur Bereitstellung von Landezonen müssen vor der Ausführung ausdrücklich genehmigt werden. Wenn Sie eine Bereitstellungsanfrage einreichen, wird sie über die Registerkarte „Genehmigungen AWS umwandeln“ automatisch an autorisierte Genehmiger weitergeleitet.

Genehmigende Personen überprüfen CloudFormation Vorlagen und Landezonenkonfigurationen. Nur Benutzer mit der Administratorrolle in AWS Transform können Bereitstellungsanfragen genehmigen. Jede Einreichung löst einen neuen Überprüfungszyklus aus, und Bereitstellungen werden erst nach Erhalt der Bestätigung fortgesetzt.

Wenn ein Genehmiger Ihre Anfrage ablehnt, wenden Sie sich direkt an ihn, um die erforderlichen Änderungen zu besprechen. Das System verfolgt alle Genehmigungsentscheidungen zu Prüfungszwecken und führt den Verlauf der Bereitstellung.

Tag: Ressourcen für die landing zone

AWS Transform markiert automatisch alle generierten Ressourcen "CreatedBy": "AWSTransform" zusammen mit Definitions- und Ausführungs-IDs zur Nachverfolgung.

Automatische Tags

Alle Landingzone-Ressourcen erhalten die folgenden Tags:

- CreatedBy— AWS-Transform
- ATWorkspace— Workspace-ID

 Note

Wenn Ihre Migration Teil des AWS Migration Acceleration Program (MAP 2.0) ist, können Sie das erforderliche MAP-Tag hinzufügen: Key: map-migrated Value: migMPE_ID (wobei MPE_ID Ihre ID für die Bewertung Ihres Migrationsportfolios ist). Das MAP-Tag wird während der Connector-Setup-Phase angefordert. AWS Transform wendet diese Tags während der Bereitstellung der landing zone an.

Änderungen rückgängig machen

Nur Elemente, die nicht bereitgestellt wurden, können entfernt werden. Sobald eine Organisationseinheit oder ein Konto bereitgestellt wurde, kann es nicht mehr über den landing zone Agent entfernt werden.

Beim Entfernen von Elementen kommt es auf die Reihenfolge an. Sie müssen die Kinder vor den Eltern entfernen:

1. Entfernen Sie zuerst Konten (per E-Mail).
2. Entfernen Sie SCPs aus OUs.
3. Untergeordnete Organisationseinheiten entfernen — Eine Organisationseinheit kann nicht entfernt werden, wenn sie noch Konten oder verschachtelte Organisationseinheiten hat.

Zugehörige Ressourcen

- [the section called “Ziel Connect AWS-Konto s und Regionen”](#)
- [the section called “Migrieren Sie Ihr Netzwerk zu AWS”](#)
- [AWS Control Tower Tower-Benutzerhandbuch](#)
- [AWS Benutzerhandbuch für Organizations](#)
- [AWS IAM Identity Center-Benutzerhandbuch](#)
- [CloudFormation Benutzerhandbuch](#)
- [Landezone Accelerator aktiviert AWS](#)
- [AWS Well-Architected Framework](#)
- [AWS Präskriptive Leitlinien: Bau von Landezonen](#)

Migrieren Sie Ihr Netzwerk zu AWS

Mit AWS Transform können Sie Ihr Netzwerk zu migrieren AWS. AWS Transform übersetzt die Konfiguration Ihrer Quellumgebung in AWS-äquivalente Netzwerkressourcen — VPCs, Subnetze, Sicherheitsgruppen, NAT-Gateways, Transit-Gateways, elastische IPs, Routen und Routing-Tabellen nach Bedarf. Sie können die generierte Netzwerkkonfiguration vor der Bereitstellung überprüfen und ändern. Sie können die Konfiguration mit AWS Transform bereitstellen und die Netzwerkkonnektivität analysieren. Alternativ können Sie sich für die Selbstbereitstellung entscheiden und Infrastructure as Code (IaC) in Ihrem bevorzugten Format erhalten: AWS Cloud Development Kit (AWS CDK) Landing Zone Accelerator (LZA) oder Terraform. HashiCorp

Gehen Sie wie folgt vor, um Ihr Netzwerk zu migrieren:

1. Laden Sie Ihre Quellnetzwerkdatei hoch.
2. Laden Sie zusätzliche Konfigurationsdateien hoch (optional, für RVTools-Umgebungen).
3. Wählen Sie eine Netzwerktopologie aus.
4. Wählen Sie eine Strategie für die Zuordnung von Sicherheitsgruppen aus.
5. Überprüfen und optimieren Sie Ihr Netzwerk.
6. Generieren Sie ein Netzwerkdiagramm (optional).
7. Konfigurieren Sie das Ressourcen-Tagging.
8. Stellen Sie Ihr Netzwerk bereit.

Note

Bei Bereitstellungen mit mehreren Konten müssen Sie kontenübergreifende IAM-Rollen und vertrauenswürdigen Zugriff für AWS Organizations konfigurieren, bevor Sie mit der Netzwerkmigration beginnen. Weitere Informationen zu Migrationstypen finden Sie unter [the section called “Schritt 1: Auswahl des Migrationstyps”](#)

Schritt 1: Zuordnung des Quellnetzwerks

Für die Netzwerkzuweisung müssen Sie eine Konfigurationsdatei aus Ihrer Quellumgebung hochladen. Welches Tool Sie wählen, hängt von Ihrem Quellnetzwerktyp ab:

- Software Defined Networks (SDN): Import/Export für VMware NSX-Netzwerkvirtualisierung oder Cisco ACI-Konfiguration für Cisco Application Centric Infrastructure.
- VMware vSphere-Netzwerke: [RVTools](#). Wenn Sie RVTools-Dateien verwenden, generiert AWS Transform nur Amazon VPC-Konfigurationen. Sicherheitsgruppenkonfigurationen erfordern zusätzliche Eingaben von Firewall- oder softwaredefinierten Netzwerkdateien. Weitere Informationen zur Generierung von Sicherheitsgruppen aus zusätzlichen Dateien finden Sie unter [Zusätzliche Konfigurationsdateien](#).
- Netzwerke, die auf Firewall-Konfigurationsdaten basieren: Exportieren Sie Dateien aus Palo Alto Networks Firewall, Fortinet FortiGate Firewall oder Cisco ACI. Weitere Informationen zu unterstützten Versionen und Anweisungen zur Extraktion finden Sie unter Extrahieren von [Konfigurationsdateien](#).
- Hybride Netzwerke, auf denen sowohl VMware-Workloads als auch Workloads anderer Anbieter ausgeführt werden: AWS [Transform Discovery Tool](#) oder ModelizeIT.
- Andere Dateitypen: Wenn es sich bei Ihrer Konfigurationsdatei nicht um eines der oben aufgeführten unterstützten Formate handelt, wird die Datei automatisch in ein unterstütztes Format konvertiert. Diese Konvertierung kann je nach Dateigröße und Komplexität bis zu zwei Stunden dauern.

 Note

Die maximal unterstützte Größe der Quellnetzwerkdatei beträgt 70 MB.

 Warning

Laden Sie RVTools nur von der offiziellen Dell-Website unter <https://www.dell.com/en-us/shop/vmware/sl/rvtools> herunter. Laden Sie RVTools nicht von inoffiziellen Quellen herunter.

Jedes Quellnetzwerksegment ist einer eigenen VPC zugeordnet. Die Netzwerksegmentierung variiert je nach Quelltyp:

- vNetwork: AWS Transformieren Sie Gruppen-VMs nach vSwitch und virtuellem LAN (VLAN). VLANs können unter mehreren vSwitches (außer VLAN 0) erscheinen.
- NSX-Netzwerke: AWS Transformieren Sie Netzwerksegmente auf der Grundlage von Tier-1 Routern, gruppieren Sie die Router und sammeln Sie ihre Segmente.

Schritt 2: Zusätzliche Konfigurationsdateien

Für RVTools-Quellumgebungen können Sie optional zusätzliche Konfigurationsdateien hochladen, um die Generierung von Sicherheitsgruppen zu ermöglichen. Wenn Sie keine zusätzlichen Konfigurationsdateien hochladen, werden keine Sicherheitsgruppen für Ihre RVTools-based Migration generiert.

AWS Transform unterstützt die folgenden zusätzlichen Konfigurationsdateitypen. Sie können nur eine Konfigurationsdatei von einer Plattform hochladen.

- Cisco Application Centric Infrastructure (ACI) bietet Netzwerkrichtlinienkonfigurationen.
- Palo Alto Networks bietet Firewall-Sicherheitsrichtlinien.
- Fortinet FortiGate bietet Firewall-Sicherheitsrichtlinien.

Wenn Sie eine Firewall oder eine Cisco ACI-Datei hochladen, generiert AWS Transform Netzwerkinfrastruktur und Sicherheitsgruppen. Wenn Sie nur eine RVTools-Datei hochladen, generiert AWS Transform nur die Netzwerkinfrastruktur.

Weitere Informationen zu unterstützten Versionen und Extraktionsanweisungen finden Sie unter [Extrahieren von Konfigurationsdateien](#).

Schritt 3: Netzwerktopologien

Während des Schritts der Netzwerkdefinition wählen Sie eine Netzwerktopologie aus. Sie können die Topologie „Isolierte VPCs“ oder die Topologie „Hub and Spoke“ wählen.

Isolierte VPCs

Was wird bereitgestellt

Isolierte VPCs sind unabhängige Netzwerkumgebungen, die innerhalb von AWS Netzwerken als separate Einheiten agieren. Ihre VPCs sind vollständig isoliert, es gibt keine integrierten Kommunikationswege zwischen ihnen. Diese Trennung bietet ein Höchstmaß an Netzwerkgrenzschutz.

AWS Transform erstellt die folgenden Ressourcen:

- Eine dedizierte VPC für jedes erkannte Quellnetzwerksegment.

- Private Subnetze, die auf Ihrer Quellnetzwerkconfiguration basieren.
- Sicherheitsgruppen (wenn Sie Firewall- oder SDN-Konfigurationsdateien bereitgestellt haben).

Vervollständigen Sie Ihr Setup

AWS Transform stellt die Netzwerkinfrastruktur bereit, überlässt Ihnen jedoch den Internetzugang und die Konnektivität zwischen VPC, sodass Sie die Konfiguration wählen können, die den Anforderungen Ihres Unternehmens entspricht.

Gehen Sie wie folgt vor, um den Internetzugang für eine isolierte VPC zu aktivieren:

1. Erstellen Sie ein [Internet-Gateway](#) und fügen Sie es an die VPC an.
2. Erstellen Sie öffentliche Subnetze in jeder Availability Zone, in der Sie Internetzugang benötigen. Fügen Sie eine Route hinzu, die `0.0.0.0/0` auf das Internet-Gateway verweist. Weitere Informationen zur Subnetzkonfiguration finden Sie unter [Subnetze für Ihre VPC](#).
3. Erstellen Sie [NAT-Gateways](#) in den öffentlichen Subnetzen (eines pro AZ für hohe Verfügbarkeit). Weisen Sie jedem NAT-Gateway eine Elastic IP zu.
4. Aktualisieren Sie Ihre privaten [Subnetz-Routentabellen](#) — fügen Sie eine Route hinzu, die auf das NAT-Gateway in derselben AZ `0.0.0.0/0` verweist.
5. Überprüfen Sie Ihre [Sicherheitsgruppenregeln](#) — stellen Sie sicher, dass die Regeln für ausgehenden Datenverkehr den für Ihre Workloads benötigten Datenverkehr zulassen (HTTPS, DNS usw.).

Richten Sie für die VPC-to-VPC Kommunikation [VPC-Peering](#) oder ein [Transit Gateway](#) ein und aktualisieren Sie die Routentabellen in jeder VPC, um den Verkehr an die Peering-Verbindung oder den TGW-Anhang weiterzuleiten.

Hub und Spoke

In diesem Modell fungiert ein [AWS Transit Gateway](#) als zentraler Hub, der mehrere Workload-VPCs (die Spokes) verbindet.

Was wird bereitgestellt

AWS Transform erstellt die folgenden Ressourcen:

- Spoke-VPCs: Eine VPC pro erkanntem Quellnetzwerksegment mit privaten Subnetzen und einem Transit Gateway Gateway-Anhang.

- **Inspektions-VPC:** Hostet Ihre Firewall-Appliance für die Verkehrsinspektion. Der gesamte VPC-übergreifende Verkehr wird über diese VPC geleitet. Der Transit Gateway Gateway-Anhang verwendet [den Gerätemodus](#), eine Einstellung, die sicherstellt, dass der Datenverkehr für beide Verbindungsrichtungen symmetrisch durch dasselbe Gerät fließt.
- **Eingehende VPC:** Verwaltet den Datenverkehr, der über das öffentliche Internet in Ihr Netzwerk eingeht (Nord-Süd-Eingang). Beinhaltet ein [Internet-Gateway](#) und öffentliche Subnetze in mehreren Availability Zones.
- **Ausgehende VPC:** Verwaltet den Datenverkehr, der Ihr Netzwerk in das öffentliche Internet verläßt (Nord-Süd-Ausgang). Beinhaltet ein Internet-Gateway, [NAT-Gateways](#) mit [elastischen IP-Adressen](#) in jeder Availability Zone für hohe Verfügbarkeit und private Subnetze für den Transit Gateway Gateway-Anhang.
- **Transit Gateway Gateway-Routentabellen:** Zwei Routentabellen leiten den Verkehr durch die Inspection-VPC. Die Tabelle Uninspected ist Spoke-VPCs, Inbound VPC und Outbound VPC zugeordnet — sie leitet den gesamten Traffic weiter (0.0.0. 0/0) zum VPC-Anhang von Inspection und ist die Standard-Routing-Tabelle für Assoziationen. Die Tabelle Inspected ist mit der Inspection-VPC verknüpft — sie enthält propagierte Routen von allen Spoke-VPCs und ist die Standard-Propagierungsroutentabelle.

Bei Bereitstellungen mit mehreren Konten wird das Transit Gateway über [AWS Resource Access Manager \(RAM\)](#) von allen Konten gemeinsam genutzt.

Datenverkehrsfluss

Der gesamte VPC-übergreifende Verkehr folgt diesem Pfad:

1. Der Verkehr von einer Spoke-VPC wird an das Transit Gateway gesendet (Standardroute 0.0.0. 0/0).
2. Die Routentabelle Uninspected leitet den Datenverkehr an die Inspection-VPC VPC.
3. Ihre Firewall in der Inspection-VPC überprüft den Datenverkehr und leitet ihn zurück an das Transit Gateway weiter.
4. Die Tabelle Inspected Route leitet den Datenverkehr mithilfe von propagierten Routen an die Ziel-Spoke-VPC weiter.

Für ausgehenden Internetverkehr leitet die Inspected-Routing-Tabelle den Verkehr an die ausgehende VPC weiter. NAT-Gateways übersetzen private IP-Adressen, bevor der Verkehr an das Internet-Gateway weitergeleitet wird. Die Tabelle der öffentlichen Routing Outbound VPC enthält

spezifische Routen für jeden Spoke-VPC Classless Inter-Domain Routing (CIDR) -Bereich zurück zum Transit Gateway. Diese Routen ermöglichen es dem Rückverkehr, die richtige Spoke-VPC zu erreichen.

Eingehender Internetverkehr erfolgt über das Internet-Gateway der eingehenden VPC und folgt demselben Inspektionspfad, um Spoke-VPCs zu erreichen.

Vervollständigen Sie Ihr Setup

AWS Transform stellt die Netzwerkinfrastruktur bereit, überlässt Ihnen jedoch die Firewall-Konfiguration und die Einrichtung eingehender Dienste, sodass Sie die Sicherheits-Appliances und -richtlinien auswählen können, die den Anforderungen Ihres Unternehmens entsprechen.

 Note

Standardmäßig durchläuft der VPC-übergreifende Datenverkehr die Inspektion-VPC ohne Inspektion. Sie müssen eine Firewall bereitstellen, um die Überprüfung des Datenverkehrs zu ermöglichen.

Eine Firewall bereitstellen: Erstellen Sie zusätzliche Subnetze in der Inspektion-VPC für die Firewall-Endpunkte. AWS Transform erstellt Subnetze nur für den Transit Gateway Gateway-Anhang. Leiten Sie den Verkehr von den TGW-Anhangssubnetzen zu den Firewall-Endpunkten und von den Firewall-Subnetzen zurück zum Transit Gateway. Sie können eine [AWS Network Firewall](#) oder eine Appliance eines Drittanbieters bereitstellen. Weitere Informationen zum Bereitstellen einer Firewall mit einem Transit Gateway finden Sie unter [Erstellen einer Firewall mit einem Transit Gateway](#).

Konnektivität überprüfen: Nachdem Sie die Firewall bereitgestellt haben, testen Sie den ausgehenden Internetzugang von einer Spoke-VPC-Instance aus (z. B. `curl https://aws.amazon.com`). Sie können [Reachability Analyzer](#) verwenden, um Verbindungsprobleme zu beheben.

Eingehende Dienste einrichten: Um öffentlich zugängliche Dienste zu hosten, stellen Sie einen [Application Load Balancer oder Network Load Balancer](#) in den öffentlichen Inbound-VPC-Subnetzen bereit. Konfigurieren Sie Zielgruppen, die über das Transit Gateway auf Instances in Ihren Spoke-VPCs verweisen, und stellen Sie sicher, dass die Inspected-Routing-Tabelle Rückrouten zur Inbound-VPC enthält.

Wenn Sie eine detaillierte Kontrolle über die Kommunikation zwischen den VPCs wünschen, wählen Sie die Option Isolierte VPCs und ändern Sie das generierte Netzwerk, um die spezifischen Kommunikationspfade zu erstellen, die Sie benötigen.

Schritt 4: Zuordnung von Sicherheitsgruppen

Wählen Sie aus, wie Ihre Quell-Sicherheitsrichtlinien in AWS Sicherheitsgruppen übersetzt werden sollen. AWS Transform erstellt Sicherheitsgruppen auf der Grundlage der Konfigurationen Ihrer Quellumgebung. Sicherheitsrichtlinien, Sicherheitsrichtlinienregeln, Gateway-Richtlinien und Gateway-Richtlinienregeln werden in Sicherheitsgruppen umgewandelt.

Important

AWS Transform erstellt Sicherheitsgruppen nach bestem Wissen und Gewissen, um sie an Ihre Quellumgebung anzupassen. Überprüfen und ändern Sie die generierten Sicherheitsgruppen, um sicherzustellen, dass sie den Anforderungen und Sicherheitsrichtlinien Ihres Unternehmens entsprechen.

Referenzierung von Sicherheitsgruppen

Wenn Sicherheitsgruppen generiert werden, verwendet AWS Transform die Referenzierung von Sicherheitsgruppen, sofern dies unterstützt wird. Bei der Referenzierung von Sicherheitsgruppen werden Sicherheitsregeln festgelegt, die auf einer anderen Sicherheitsgruppen-ID und nicht auf bestimmten IP-Adressbereichen (CIDR-Blöcken) basieren. Dieser Ansatz bietet flexiblere und wartbarere Sicherheitskonfigurationen.

Ihre Sicherheitsgruppenregeln können nur auf andere Sicherheitsgruppen innerhalb derselben VPC oder in einer VPC verweisen, die innerhalb derselben Region verbunden ist. Cross-account Verweise werden ebenfalls unterstützt. Sie können nicht auf eine Sicherheitsgruppe in einer nicht verbundenen VPC oder regionsübergreifend verweisen. Für verbundene VPCs unterstützen nur eingehende Regeln VPC-Sicherheitsgruppenverweise — ausgehende Regeln müssen Regeln verwenden. CIDR-based Wie AWS Transform Sicherheitsgruppenregeln erstellt, hängt von der von Ihnen gewählten Netzwerktopologie ab:

- **Hub and Spoke:** Transit Gateway bietet Netzwerkkonnektivität zwischen VPCs. AWS Transform verwendet Referenzierung sowohl für Regeln innerhalb von VPC als auch für Cross-Ingress-Regeln. VPC/cross-account Cross-VPC/cross-account Für ausgehende (ausgehende) Ausgangsregeln werden Regeln verwendet. CIDR-based
- **Isolierte VPCs:** Ihre VPCs haben keine Netzwerkverbindung zwischen ihnen. AWS Transform verwendet Verweise nur für Regeln innerhalb der VPC. Alle VPC- und kontoübergreifenden Regeln verwenden Regeln. CIDR-based

CIDR-based Regeln werden auch verwendet, wenn Quellkonfigurationen nicht symmetrisch sind.

Wählen Sie eine der folgenden Strategien zur Zuordnung von Sicherheitsgruppen:

- **MAP:** Übersetzt Sicherheitsregeln aus Ihrer Quellumgebung in AWS Sicherheitsgruppen und Regeln. Verwenden Sie diese Option für Migrationen mit statischer IP-Adressierung.
- **MAP_DHCP (Mit DHCP-Unterstützung Translate):** Übersetzt Sicherheitsregeln aus Ihrer Quellumgebung mit DHCP-Kompatibilität. DHCP weist IP-Adressen dynamisch aus dem CIDR-Bereich des Subnetzes zu. Infolgedessen werden die VPC-übergreifenden Ausgangsregeln erweitert, sodass sie dem vollständigen CIDR des Zielsubnetzes entsprechen. Ein enger gefasster CIDR würde DHCP-assigned IPs blockieren, die außerhalb dieses Bereichs liegen. Überprüfen Sie diese Regeln nach der Migration.

Verwenden Sie diese Option für DHCP-Unterstützung mit VPC-Transit-Gateway-Kommunikation. Funktioniert auch mit statischen IPs, erzeugt aber möglicherweise umfassendere Regeln als MAP.

- **SKIP:** Übersetzt keine Sicherheitsregeln. Konfigurieren Sie AWS Sicherheitsgruppen nach der Migration manuell. Funktioniert sowohl mit statischen IP- als auch mit DHCP-Umgebungen. Für RVTools-Quellumgebungen ohne zusätzliche Konfigurationsdateien verwendet AWS Transform automatisch SKIP.

Note

Ihre Zuordnungsstrategie bestimmt Ihre IP-Zuweisungsoptionen. MAP unterstützt nur statische IP-Adressen. MAP_DHCP und SKIP unterstützen sowohl statische als auch DHCP.

Ansätze zur IP-Migration

Sie haben zwei Optionen für die Netzwerkkonfiguration für Ihre Migration:

Auswahl des Netzwerkbereichs

- **Bestehende Bereiche beibehalten (Aufbewahrung von IP-Adressbereichen):** Behalten Sie die ursprünglichen IP-Adressbereiche während der Migration bei. Ideal für Migrationen, bei denen Sie Anwendungen AWS ohne Änderungen verschieben (Lift-and-Shift), insbesondere bei älteren Anwendungen mit fest codierten IP-Abhängigkeiten oder bestehenden Firewallregeln.

- Aktualisierung auf neue IP-Bereiche (CIDR-Update): Sie können jeden VPC-CIDR-Bereich während der Migration ändern, und AWS Transform überträgt Änderungen automatisch an Subnetze, Routing-Tabellen und Sicherheitsgruppen.

Zuweisung von IP-Adressen

- Feste IP-Adressen (statisch): AWS Transform weist statische IPs auf der Grundlage des CIDR zu. Dies eignet sich am besten für Anwendungen, die vorhersehbares Netzwerkverhalten, DNS-Management oder IP-based Zugriffskontrolle erfordern. IPs bleiben auch bei Instance-Neustarts über Elastic Network Interfaces (ENIs) bestehen. Dabei handelt es sich um virtuelle Netzwerkkarten, die an Ihre Instances angeschlossen sind.
- Dynamische IP-Zuweisung (AWS DHCP): Ordnen Sie beim Start der Instance automatisch IPs aus Subnetzpools zu. Optimal für Anwendungen, die für die Ausführung in der Cloud und für die auto-scaling von Workloads konzipiert sind. Reduziert den Betriebsaufwand, erfordert jedoch, dass Anwendungen DNS oder Service Discovery verwenden.

Sie können eine der beiden Bereichsauswahlen mit einer der beiden IP-Zuweisungsmethoden kombinieren.

Note

Die Strategie für die Zuweisung von IP-Adressen wird auf Wellenebene festgelegt. Sie können bestimmten Servern unterschiedliche Strategien zuweisen, indem Sie die Wave-Datei anpassen. Wenn Sie beispielsweise einen statischen IP-Adressansatz für die Wave wählen, aber einem bestimmten Server einen dynamischen Ansatz zuweisen möchten, verwenden [RESET_VALUE] Sie den unter [Bearbeiten Ihrer Konfiguration](#) im MGN-Benutzerhandbuch beschriebenen Ansatz.

Schritt 5: Überprüfen und optimieren Sie Ihr Netzwerk

Nachdem AWS Transform Ihre Zielnetzwerkconfiguration generiert hat, können Sie die lokalen Netzwerksegmente überprüfen, die zur AWS Infrastruktur konvergiert wurden. Verwenden Sie die visuelle Oberfläche, um Ihr Netzwerk zu überprüfen, und die Chat-Oberfläche, um Änderungen vorzunehmen und Empfehlungen zu erhalten. AWS Transform führt kaskadierende Folgenabschätzungen durch und implementiert die erforderlichen Änderungen, um die Netzwerkkonsistenz und die Einhaltung von Best Practices zu gewährleisten. [Sie können AWS](#)

[Transform auch bitten, Ihr Netzwerk zu analysieren und Optimierungen vorzuschlagen. Weitere Informationen finden Sie unter Geführte Empfehlungen.](#)

Bestehende VPCs in Ihrem Zielkonto

Wenn Ihr Zielkonto bereits VPCs enthält — aus früheren Migrationsphasen oder parallel Infrastrukturprojekten — erkennt AWS Transform diese automatisch und zeigt sie während des Überprüfungsprozesses zusammen mit Ihren zugewiesenen VPCs an. Bei Migrationen mehrerer Konten erkennt AWS Transform bestehende VPCs in allen Konten in Ihrem Unternehmen. AWS

Diese Transparenz hilft Ihnen zu verstehen, wie Ihr geplantes Netzwerk mit Ihrer bestehenden Infrastruktur zusammenhängt, potenzielle CIDR-Konflikte zu identifizieren und vor der Implementierung fundierte Entscheidungen zu treffen.

Note

AWS Transform erkennt nur vorhandene VPCs (keine Subnetze oder andere Ressourcen). Die Erkennung ist schreibgeschützt — AWS Transform ändert Ihre vorhandenen VPCs nicht.

Optimieren Sie Ihr Netzwerk

Note

Diese Operationen gelten nur für Workload-VPCs. Für Appliance-VPCs in der Hub-and-Spoke-Topologie (Inspection, Inbound, Outbound) wird nur die Änderung der IP-Adresse unterstützt.

Sie können die Operationen Löschen, Zusammenführen und Teilen nicht rückgängig machen. Überprüfen Sie Ihre Konfiguration sorgfältig, bevor Sie diese Änderungen anwenden.

Die folgenden Operationen sind für VPCs verfügbar:

- **Löschen:** Entfernt eine VPC dauerhaft aus der Konfiguration. Verwenden Sie dies für veraltete Netzwerksegmente, zu denen Sie nicht migrieren AWS sollten.
- **Ausschließen:** Entfernen Sie vorübergehend eine VPC aus der Migration für phasenweise Migrationsstrategien. Ausgeschlossene VPCs werden nicht bereitgestellt, können aber später wieder aufgenommen werden.

- **Einbeziehen:** Fügt eine zuvor ausgeschlossene VPC wieder in die Migration ein.
- **Zusammenführen:** Kombinieren Sie zwei VPCs zu einer. Die erste VPC behält ihre Identität und nimmt alle Subnetze der zweiten VPC auf. Sicherheitsgruppen werden in die zusammengeführte VPC verschoben und ihre Zuordnungen werden entsprechend neu erstellt. Das CIDR der ersten VPC wird auf den kleinsten CIDR-Bereich erweitert, der beide ursprünglichen CIDRs enthält, und das Routing wird automatisch aktualisiert. Die zweite VPC wird aus der Konfiguration entfernt.

Anforderungen für das Zusammenführen:

- Subnetz-CIDRs dürfen sich zwischen den beiden VPCs nicht überschneiden.
- Der zusammengeführte CIDR darf /16 nicht überschreiten.
- Bei Bereitstellungen mit mehreren Konten müssen beide VPCs demselben Konto zugewiesen werden.
- **IP-Adresse ändern:** Ändern Sie die Basis-IP-Adresse einer VPC CIDR unter Beibehaltung der gleichen Präfixlänge. AWS Transform übersetzt automatisch alle Subnetz-CIDRs mit demselben Offset. Wenn Sie beispielsweise eine VPC von `10.0.0.0/16` zu ändern, wird ein Subnetz von `10.0.1.0/24` zu `10.20.0.0/16` verschoben. `10.20.1.0/24`

Sicherheitsgruppenregeln, die genau dem alten VPC-CIDR entsprechen, werden automatisch aktualisiert. Regeln, die sich teilweise mit dem alten CIDR überschneiden oder nicht übereinstimmen, werden nicht geändert. Überprüfen Sie diese Regeln nach der Änderung.

- **Umbenennen:** Ändern Sie den Namen einer VPC, sodass er den Benennungskonventionen Ihrer Organisation für Kostenzuweisung, Compliance-Nachverfolgung und Betriebsstandards entspricht.
- **Größe ändern:** Ändern Sie die Präfixlänge eines VPC-CIDR, um den IP-Adressbereich zu erweitern oder zu reduzieren.
 - Verringerung der Präfixlänge (mehr IPs, z. B. /20 bis /16): Subnetze passen immer noch in den größeren Bereich. Es sind keine Änderungen am Subnetz erforderlich.
 - Erhöhung der Präfixlänge (weniger IP-Adressen, z. B. /16 bis /20): Subnetze, die außerhalb des neuen Bereichs liegen, müssen zuerst mithilfe der Subnetzgrößenänderung in der Größe geändert werden.

Sicherheitsgruppenregeln, die genau dem alten VPC-CIDR entsprechen, werden automatisch aktualisiert. Regeln, die sich teilweise mit dem alten CIDR überschneiden oder nicht übereinstimmen, werden nicht geändert. Überprüfen Sie diese Regeln, nachdem Sie die Größe geändert haben.

Anforderungen zum Ändern der Größe:

- Der neue CIDR muss zwischen /16 und /28 liegen.
- Das neue CIDR darf sich nicht mit anderen VPCs im Netzwerk überschneiden (Hub-and-Spoke-Topologie).
- Bei der Reduzierung des CIDR müssen alle vorhandenen Subnetze in das neue CIDR passen. Ändern Sie bei Bedarf zuerst die Größe der Subnetze.
- Aufteilen: Teilen Sie eine VPC auf der Grundlage der von Ihnen angegebenen CIDR-Grenzen in zwei VPCs auf. Subnetze werden der neuen VPC zugewiesen, in deren CIDR sie enthalten sind. Sicherheitsgruppen werden auf beide neuen VPCs geklont, aber die CIDRs für Sicherheitsgruppenregeln werden nicht automatisch aktualisiert. Überprüfen Sie Ihre Regeln nach dem Teilen, um sicherzustellen, dass die VPC-übergreifende Kommunikation wie erwartet funktioniert. Die ursprüngliche VPC wird durch die beiden neuen VPCs ersetzt.

Geteilte Anforderungen:

- Sie müssen genau zwei CIDR-Bereiche angeben.
- Die beiden CIDRs dürfen sich nicht überschneiden.
- Jeder CIDR muss zwischen /16 und /28 liegen.
- Jedes Subnetz muss in genau eines der beiden CIDRs passen. Wenn ein Subnetz nicht passt, wird der Vorgang abgelehnt.

Die folgenden Operationen sind für Subnetze verfügbar:

- IP-Adresse ändern: Ändern Sie die Basis-IP-Adresse eines Subnetz-CIDR unter Beibehaltung der gleichen Präfixlänge.
- Löschen: Entfernt ein Subnetz dauerhaft aus der Konfiguration, ohne dass sich dies auf die übergeordnete VPC auswirkt.
- Größe ändern: Ändern Sie die Präfixlänge eines Subnetz-CIDR, um den IP-Adressbereich zu erweitern oder zu reduzieren.

Anforderungen an die Größenänderung des Subnetzes:

- Der neue CIDR muss zwischen /16 und /28 liegen.
- Das neue CIDR darf sich nicht mit anderen Subnetzen in derselben VPC überschneiden.
- Das neue CIDR muss sich innerhalb des übergeordneten VPC-CIDR befinden.

Nach jedem Vorgang bewertet AWS Transform die Sicherheitsgruppenreferenzierung neu, wodurch CIDR-based Regeln möglicherweise in Sicherheitsgruppenverweise umgewandelt werden oder umgekehrt. Überprüfen Sie Ihre Sicherheitsgruppenregeln, nachdem Sie Änderungen vorgenommen haben, um sicherzustellen, dass sie Ihren Anforderungen entsprechen.

Geführte Netzwerkempfehlungen

AWS Transform analysiert Ihr zugeordnetes Netzwerk und gibt über die Chat-Oberfläche priorisierte Empfehlungen. Empfehlungen basieren auf Ihren Netzwerkdaten und müssen von Ihnen bestätigt werden, bevor Änderungen übernommen werden.

AWS Transform empfiehlt möglicherweise die folgenden Optimierungen:

- **CIDR-Konfliktlösung:** Kennzeichnet überlappende CIDR-Bereiche zwischen Ihren zugewiesenen VPCs und vorhandenen VPCs in allen Konten in Ihrer Organisation. AWS Widersprüchliche VPCs werden zuerst angezeigt. Sie können Konflikte lösen, indem Sie die zugeordnete VPC erneut adressieren, sie ausschließen oder löschen oder den Konflikt bestätigen und ihn nach der Bereitstellung selbst lösen.
- **Standardisierung der Benennung:** Kennzeichnet VPC-Namen, die keinem konsistenten Muster folgen (z. B. Namen, die Hardwarereferenzen enthalten). AWS Transform fragt nach Ihrer Cloud-Namenskonvention, bevor Sie Ersatzprodukte vorschlagen.
- **Überprüfung des Umfangs:** Identifiziert Netzwerksegmente, in die möglicherweise nicht migriert werden muss AWS, wie z. B. Altsysteme oder Konstrukte, deren Außerbetriebnahme noch aussteht. AWS Transform bittet Sie um Ihre Bestätigung, bevor ein Konstrukt ausgeschlossen wird.
- **Richtige Dimensionierung der VPC-Kapazität:** Zeigt VPCs an, bei denen der CIDR für die darin enthaltenen Subnetze zu groß oder zu klein erscheint. AWS Transform zeigt die aktuellen Kapazitätsdaten an und lässt Sie entscheiden, ob Sie die Größe ändern möchten.
- **Sicherheitsüberprüfung:** Kennzeichnet Sicherheitsgruppenregeln, die uneingeschränkten eingehenden Datenverkehr zulassen (0.0.0. 0/0) für Ihre Überprüfung.
- **VPC-Konsolidierung:** Identifiziert fragmentierte VPCs, die anscheinend eher durch physische Infrastrukturgrenzen als durch logische Isolationsanforderungen getrennt sind, und schlägt vor, sie zusammenzuführen.

Note

Alle Empfehlungen bedürfen Ihrer ausdrücklichen Bestätigung, bevor AWS Transform Änderungen vornimmt. AWS Transform geht mit Kompromissen einher, wenn sich eine Empfehlung auf mehrere Aspekte Ihres Netzwerks auswirkt.

Schritt 6: Netzwerkdiagramm

Nachdem Sie die generierten VPC-Konfigurationen überprüft haben, können Sie optional ein Netzwerkdiagramm generieren, um Ihre Netzwerktopologie zu visualisieren. AWS Transform unterstützt die folgenden Diagrammformate:

- Mermaid-Code (.mmd): Dieses Format erzeugt eine textbasierte Diagrammdefinitionsdatei, die Sie mit Werkzeugen rendern können. Mermaid-compatible
- Bild (.png): Dieses Format erzeugt ein gerendertes Bild Ihrer Netzwerktopologie.

Schritt 7: Konfigurieren Sie das Ressourcen-Tagging

Ihre Netzwerkressourcen sind für den Start und die Replikation markiert. Sie können auch benutzerdefinierte Tags und MAP-Tags (AWS Migration Acceleration Program) hinzufügen.

Automatische Tags für Start und Replikation

AWS Transform kennzeichnet Ihre migrierten Netzwerkressourcen (VPCs, Subnetze, Sicherheitsgruppen und Routing-Tabellen) automatisch mit den folgenden Tags:

- Schlüssel: CreatedBy Wert: AWSApplicationMigrationService
- Schlüssel: ATWorkspace Wert: *workspace-id*

Diese Tags ermöglichen die Verwendung der VPC und des Subnetzes zum Starten von Test- und Cutover-Instances in. AWS

Note

Ihre migrierten VPCs und Subnetze bieten standardmäßig keine Internetverbindung und eignen sich daher nicht als Staging-Bereiche für die Replikation.

Um die VPC und das Subnetz auch als Staging-Bereich (Replikation) zu verwenden, fügen Sie manuell die folgenden Tags hinzu:

- Schlüssel: CreatedFor Wert: AWSTransform
- Schlüssel: ATWorkspace Wert: *workspace-id*

Sie können diese Tags auch auf jede vorhandene AWS Netzwerkressource anwenden, um sie für die Replikation verfügbar zu machen.

Finden Sie Ihre Workspace-ID in der URL der AWS Transform-Web-App: <https://... workspace-id / workspace/-id job/job>

Benutzerdefinierte Tags

Zusätzlich zu den von AWS Transform automatisch angewendeten Tags kannst du optional benutzerdefinierte Tags hinzufügen, um deine migrierten Netzwerkressourcen zu organisieren, die Kosten zu verfolgen und die Einhaltung der Vorschriften zu verwalten. Sie können benutzerdefinierte Tags auf zwei Ebenen anwenden:

- Job-level Tags: Gilt für alle Ressourcen, die durch diesen Job erstellt wurden, einschließlich aller VPCs, Subnetze, Sicherheitsgruppen und Routing-Tabellen.
- VPC-level Tags: Auf eine bestimmte VPC anwenden und automatisch auf alle zugehörigen Ressourcen (Subnetze, Sicherheitsgruppen, Routing-Tabellen) kaskadieren.

Note

Maximal 40 Tags pro Anfrage. Für jedes Tag sind ein Schlüssel und ein Wert erforderlich. AWS Es gelten die Tagging-Konventionen.

AWS Transform wendet diese Tags an, wenn es die Infrastructure-as-Code-Vorlagen generiert.

AWS Migration Acceleration Program

Wenn Ihre Migration Teil des AWS Migration Acceleration Program (MAP 2.0) ist, wendet AWS Transform ein MAP-Tag auf Ihre Ressourcen an. Wenn Sie Ihre MPE-ID zu einem früheren Zeitpunkt des Migrationsprozesses angegeben haben, wird das Tag automatisch angewendet. Andernfalls

fragt AWS Transform nach Abschluss der Überprüfung der generierten VPC-Konfigurationen, ob Sie eine MAP-Vereinbarung haben, und fordert Sie auf, Ihre MPE-ID anzugeben — einen 10-stelligen Code mit Großbuchstaben und Zahlen (z. B. ABCDE12345). Das angewendete Tag verwendet das folgende Format:

- Schlüssel: map-migrated Wert: mig`MPE_ID`

Schritt 8: Stellen Sie Ihr Netzwerk bereit

Wählen Sie nach dem Taggen Ihre Bereitstellungsstrategie aus:

- AWS Transform-managed Bereitstellung: AWS Transform verwendet CloudFormation Vorlagen für die Bereitstellung Ihres Netzwerks und führt Reachability Analyzer aus, um die Konnektivität zwischen Subnetzen über mehrere VPCs hinweg und innerhalb derselben VPC zu überprüfen.

Note

Sie müssen eine ausdrückliche Genehmigung einholen, bevor Ihre Anfrage zur Netzwerkbereitstellung ausgeführt wird. Weitere Informationen finden Sie unter [Genehmigungsverfahren für die Bereitstellung](#).

- Self-deployment: AWS Transform generiert IaC-Vorlagen (Infrastructure as Code). CloudFormation Vorlagen werden standardmäßig generiert. Sie können auch zusätzliche Ausgabeformate auswählen:
 - AWS CDK generiert ein TypeScript Projekt für die programmatische Infrastrukturbereitstellung.
 - HashiCorp Terraform generiert HCL-Vorlagen (HashiCorp Configuration Language) für die Verwaltung von Netzwerkressourcen.
 - Landing Zone Accelerator (LZA) generiert eine network-config.yaml-Datei für die LZA-Netzwerkkonfiguration.

Note

Wenn Sie die Bereitstellung über die Landing Zone Accelerator (LZA) -Pipeline durchführen, müssen sich Ihr AWS Transform-Konto und Ihre LZA-Installation in derselben Organisation befinden. AWS Die Bereitstellung schlägt fehl, wenn die Organisations-IDs nicht übereinstimmen.

Verwenden Sie für die Selbstbereitstellung den bereitgestellten Link, um eine ZIP-Datei mit den generierten Vorlagen herunterzuladen. Der ZIP-Ordner enthält eine README.md Datei, in der erklärt wird, wie die generierten Vorlagen verwendet werden.

Um zu überprüfen, ob die heruntergeladene Datei nicht beschädigt oder manipuliert wurde, generieren Sie eine Prüfsumme, laden Sie sie herunter und vergleichen Sie sie dann mithilfe `openssl dgst -sha256 -binary <file.zip> | base64` eines Befehls mit einem lokal generierten Hash.

Genehmigungsverfahren für die Bereitstellung

Um sicherzustellen, dass Netzwerkänderungen den Sicherheitsstandards und Architekturanforderungen Ihres Unternehmens entsprechen, durchlaufen alle Bereitstellungsanfragen einen Genehmigungsworkflow. Sie müssen eine ausdrückliche Genehmigung einholen, bevor Ihre Anfrage zur Netzwerkbereitstellung ausgeführt wird. Wenn Sie eine Bereitstellungsanfrage einreichen, wird sie automatisch über die Registerkarte Genehmigungen AWS transformieren an autorisierte Genehmiger weitergeleitet. Genehmigende Personen validieren sowohl CloudFormation Vorlagen als auch Netzwerkkonfigurationen, um die Einhaltung von Sicherheitsstandards und architektonischen Anforderungen sicherzustellen. Jede Einreichung löst einen neuen Überprüfungszyklus aus, und die Bereitstellung wird erst nach Erhalt der Bestätigung fortgesetzt. Wenn ein Genehmiger Ihre Anfrage ablehnt, wenden Sie sich direkt an ihn, um die erforderlichen Änderungen zu besprechen. AWS Transform verfolgt alle Genehmigungsentscheidungen zu Prüfungszwecken und führt den Bereitstellungsverlauf.

Löscht bereitgestellte Netzwerkressourcen

Wenn Sie eine Bereitstellung rückgängig machen müssen, können Sie die von AWS Transform bereitgestellten Netzwerkressourcen löschen. Sie können Ressourcen sofort nach Abschluss der Bereitstellung löschen. Wenn Sie die bereitgestellten Netzwerkressourcen nach der Bereitstellung ändern, können die Ressourcen nicht automatisch gelöscht werden.

- **AWS Transform-managed Bereitstellungen:** AWS Transform entfernt alle CloudFormation Stapel, die während der Bereitstellung erstellt wurden. Für diese Aktion ist eine Genehmigung über die Registerkarte „Genehmigungen AWS transformieren“ erforderlich.
- **Self-deployments:** Sie müssen die bereitgestellten Ressourcen manuell über die AWS Management Console oder AWS CLI löschen.

Extrahieren der Konfigurationsdatei

Wenn Ihre Quellumgebung Cisco ACI, Palo Alto Networks oder Fortinet verwendet, müssen Sie eine Konfigurationsdatei extrahieren FortiGate, um sie Transform zur Verfügung zu stellen. AWS Sie können diese Dateien als eigenständige Quelldateien verwenden, um Netzwerkinfrastruktur- und Sicherheitsgruppen zu generieren, oder als ergänzende Dateien zusammen mit einem RVTools-Upload, um die Generierung von Sicherheitsgruppen hinzuzufügen. Der Extraktionsprozess ist in beiden Fällen derselbe.

Gehen Sie wie folgt vor, um Konfigurationsdateien aus Ihrer Firewall und Ihren Netzwerkkumgebungen zu extrahieren. Aktuelle Informationen finden Sie in der Herstellerdokumentation.

Fortinet FortiGate

- Die Firmware-Version muss v7.0 oder höher sein.
- Sie benötigen super_admin unsere super_admin_readonly Rechte auf globaler Ebene.
- Schritte:
 1. Stellen Sie über SSH oder den integrierten CLI-Client eine Connect zur Firewall her
 2. Ausführen: `show | grep ""` (`| grep ""` deaktiviert die Paginierung)
 3. Speichert die gesamte Ausgabe ab dem Befehl in einer Datei `show`

Palo Alto Networks

- Die Firmware-Version muss 10.1 oder höher sein.
- Sie benötigen die Superadmin-Rolle.
- Stellen Sie über SSH Connect zur Firewall her, führen Sie die folgenden Befehle aus, um die Paginierung zu deaktivieren, das Ausgabeformat festzulegen, in den Konfigurationsmodus zu wechseln und die Konfiguration und die vordefinierten Objekte zu exportieren. Speichern Sie die Ausgaben:

```
set cli pager off
set cli config-output-format set
configure
show                # Save as palo-conf.txt
show predefined     # Save as palo-default.txt
```

Cisco ACI

- Die Firmware-Version muss 6.0 oder höher sein.
- Sie benötigen die Administratorrolle mit allen Rechten und ein konfiguriertes Secure Copy Protocol (SCP), SSH File Transfer Protocol (SFTP) oder File Transfer Protocol (FTP) -Ziel.
- Schritte:
 1. Stellen Sie über Ihren Browser eine Connect zum Application Policy Infrastructure Controller (APIC) her
 2. Öffnen Sie das Admin-Menü und wählen Sie Config Rollbacks
 3. Wählen Sie im Dialogfeld „Einen Snapshot erstellen“ die Option „Remote-Standort“ und wählen Sie „Jetzt einen Snapshot erstellen“.
 4. Nachdem Sie die Meldung „Übertragung erfolgreich“ erhalten haben, stellen Sie eine Verbindung zum Remote-Standortserver her und rufen Sie die neueste Snapshot-Datei (.gz-Datei) ab

Server migrieren

AWS Transform verwendet AWS Transform MGN (MGN), um Ihre Server auf Amazon EC2 umzuhosten. Der Workflow zur Servermigration führt Sie durch die Einrichtung der einzelnen Migrationswellen, die Validierung Ihres Serverbestands, die Bereitstellung von Replikationsagenten, die Überwachung der Datenreplikation, das Testen migrierter Instances und die Durchführung der endgültigen Umstellung. [Weitere Informationen dazu finden Sie unter Was ist? AWS Transform MGN](#) im MGN-Benutzerhandbuch.

Die Servermigration wird in Wellen organisiert. Jede Welle steht für eine Gruppe von Servern, die zusammen migriert werden. Für jede Welle schließen Sie die folgenden Phasen ab:

Für Wellen mit einer Strategie zur Containerisierung führt AWS Transform anstelle der unten beschriebenen Rehost-Schritte den Workflow zur Containerisierung des Quellcodes aus. Der Containerisierungs-Workflow führt Sie durch das Klonen von Quellcode, das Generieren von Docker-Artefakten, das Veröffentlichen von Container-Images und die Bereitstellung auf Amazon Elastic Container Service oder Amazon Elastic Kubernetes Service. Den vollständigen Workflow zur Containerisierung finden Sie unter. [Containerisierung des Quellcodes](#)

1. Voraussetzungen und Konfiguration der Standardwerte für die Migration
2. Schritt 1: Migrationswelle einrichten

3. Schritt 2: Inventar validieren und bestätigen
4. Schritt 3: Implementieren Sie Replikationsagenten
5. Schritt 4: Datenreplikation
6. Schritt 5: Testen
7. Schritt 6: Umstellung

Voraussetzungen und Konfiguration der Standardeinstellungen für die Migration

Voraussetzungen

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

Note

Wenn Sie alle Schritte eines umfassenden Migrationsauftrags in AWS Transform abgeschlossen haben, sind Ihre Zielkonten und Ihre Inventardatei bereits vorbereitet — die Inventardatei wurde während des Migrationsplanungsschritts für Sie generiert. Die im Rahmen der AWS Transform-Netzwerkmigration eingerichtete Netzwerkinfrastruktur ist ebenfalls bereit. Wenn Sie Ihre Netzwerkinfrastruktur nicht mit AWS Transform erstellt haben, stellen Sie sicher, dass sie im Voraus eingerichtet ist, bevor Sie mit der Rehost-Migration beginnen.

Bevor Sie mit der Rehost-Migration beginnen, stellen Sie sicher, dass Sie über die Netzwerkressourcen und die Infrastruktur für das Hosten Ihrer Server verfügen. Sie können dafür die landing zone- und Netzwerkigrationsfunktionen von AWS Transform oder andere Tools verwenden.

- **Unterstützte Betriebssysteme** — Auf den Quellservern muss ein unterstütztes Betriebssystem ausgeführt werden. Die vollständige Liste finden Sie im MGN-Benutzerhandbuch unter [Unterstützte Betriebssysteme](#).
- **Zielkonten für die Migration** — Die AWS-Konto IDs, zu denen Ihre Server migriert werden sollen. Sie können AWS Transform landing zone oder andere Tools verwenden, um Ihre Infrastruktur einzurichten.

- Netzwerkinfrastruktur vorhanden — bereitgestellte und konfigurierte VPCs, Subnetze und Sicherheitsgruppen. Sie können AWS Transform Network Migration oder andere Tools verwenden, um Ihre Netzwerkinfrastruktur einzurichten.
- Inventardatei — Vorbereitet mit Serverdetails, Wave-Zuweisungen, Zielkontoinformationen und Amazon EC2 EC2-Instance-Typeeinstellungen. Sie können die AWS Transform-Migrationsplanung verwenden, um diese Datei zu generieren.

Konfigurieren Sie die Standardeinstellungen für die Migration

Bevor Sie mit der Ausführung der Migration mehrerer Konten beginnen, sollten Sie Standardeinstellungen konfigurieren, die für alle Ihre Zielkonten gelten. Diese Standardeinstellungen definieren, wie Ihre Amazon EC2 EC2-Instances gestartet werden und wie die allgemeine Migration konfiguriert wird. Sie können diese Standardeinstellungen während der Wave-Einrichtung auf Wave-Ebene überschreiben.

Amazon EC2 EC2-Empfehlungseinstellungen

AWS Transform bietet Empfehlungen zum Amazon EC2 EC2-Instance-Typ, die auf der Nutzungsspezifikation Ihrer Quell-VMs basieren. Sie können Ihre Amazon EC2 EC2-Empfehlungseinstellungen konfigurieren, um zu steuern, wie Instance-Typen für Ihre migrierten Server ausgewählt werden.

Weitere Informationen zum Generieren von Amazon EC2 EC2-Empfehlungen finden Sie unter [Generieren von Amazon EC2 EC2-Empfehlungen](#) unter AWS Migration Hub

Note

Sie können die vorgeschlagenen Amazon EC2 EC2-Instance-Typen so ändern, dass sie Empfehlungen aus dem [Migration Evaluator](#), [AWS Optimization and Licensing Assessment \(OLA\)](#) oder einem AWS Transform-Assessment-Job enthalten.

Initialisierung der Migration

Um die Migration zu starten, initialisiert AWS Transform MGN für alle Konten, AWS-Region in denen Sie migrieren möchten, sowie für alle Zielkonten, in denen der Dienst verwendet werden soll. Während des Initialisierungsprozesses:

- Die erforderlichen IAM-Rollen und -Richtlinien werden erstellt.

- Die erforderlichen Standardvorlagen sind konfiguriert.

Informationen zum Initialisierungsprozess finden Sie unter [Initialisieren AWS Transform MGN mit der Konsole](#) im MGN-Benutzerhandbuch.

Amazon-EC2-Startvorlage

Die Starteinstellungen bestehen aus zwei Teilen: den allgemeinen Starteinstellungen und der Amazon EC2 EC2-Startvorlage, die bestimmt, wie eine Test- oder Cutover-Instance für jeden Quellserver in gestartet wird. AWS

Starteinstellungen, einschließlich der Amazon EC2 EC2-Startvorlage, können auf Kontoebene definiert werden und werden dann jedes Mal, wenn Sie AWS Transform MGN einen Quellserver hinzufügen, automatisch auf jeden Quellserver angewendet. Die in diesem Abschnitt definierten Standardeinstellungen für die Starteinstellungen können automatisch auf alle Ihre Zielkonten angewendet werden.

AWS Transform präsentiert die Liste der verfügbaren Einstellungen für Startvorlagen. Sie können wählen, ob Sie mit den Standardeinstellungen fortfahren oder Ihre Startvorlage konfigurieren möchten. Wenn Sie sich für die Konfiguration entscheiden, stellt AWS Transform einen Link zu einer Human-in-the-Loop (HITL) -Überprüfung bereit, die alle Parameter der Einstellungen für die Startvorlage enthält. Sie können die gewünschten Parameter auch direkt über die Chat-Oberfläche ändern.

[Quellserver](#) werden mit den Einstellungen für die Kontostartvorlage erstellt. Sobald die Quellserver mit diesen Standardeinstellungen erstellt wurden, können Sie sie auf der Ebene der Starteinstellungen für den Quellserver ändern. Sie können die Quellservereinstellungen für jeden Parameter über die Chat-Oberfläche oder für Massenvorgänge mithilfe der Excel-Inventardatei während der Bearbeitung ändern [Schritt 2: Inventar validieren und bestätigen](#).

Eine vollständige Liste der Einstellungen und Einzelheiten der Startvorlage finden Sie unter [Allgemeine Starteinstellungen](#) im MGN-Benutzerhandbuch.

Zusätzliche Änderungen an der Amazon EC2 EC2-Startvorlage

Wenn Sie weitere Änderungen an der Amazon EC2 EC2-Startvorlage vornehmen möchten, sollten Sie diese an der Vorlagen-ID für jedes Zielkonto vornehmen. Diese Option ist im Wave-Setup verfügbar. AWS Transform führt Sie durch den Vorgang und bietet den entsprechenden Link.

Schritt 1: Migrationswelle einrichten

In dieser Phase bereitet AWS Transform die Migrationswelle vor, indem es das Zielkonto konfiguriert, die Dienstberechtigungen überprüft, Ressourcen-Tags einrichtet, Netzwerkdaten zu Ihrem Inventar hinzufügt und die Replikations- und Starteinstellungen konfiguriert.

Migrationsmodus und Kontokonfiguration

AWS Transform unterstützt zwei Migrationsmodi:

- Single-account Migration — Alle Server in der Welle migrieren auf dasselbe Zielkonto, das in Ihrem Connector konfiguriert ist.
- Multi-account Migration — Server werden zu verschiedenen Zielkonten migriert, die in Ihrer Inventardatei angegeben sind. Bei Migrationen mehrerer Konten muss Ihre Inventardatei eine `mgn:account-id` Spalte mit der Zielkonto-ID für jeden Server enthalten.

AWS Transform bestätigt die Konfiguration des Zielkontos und überprüft, ob MGN in jedem Zielkonto initialisiert ist. Wenn MGN noch nicht initialisiert ist, bietet AWS Transform Anweisungen zum Abschluss der Initialisierung. Während der Initialisierung erstellt MGN die folgenden IAM-Dienstrollen für Replikations- und Startvorgänge:

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`
- `AWSApplicationMigrationAgentRole`

Weitere Informationen zu diesen Rollen finden Sie unter [Initialisieren von MGN mit der Konsole](#) oder [Initialisieren von MGN mit der API im MGN-Benutzerhandbuch](#).

Bei Migrationen mit mehreren Konten erstellt AWS Transform während des Initialisierungsschritts auch die folgende Rolle: `AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>` Diese Rolle wird für alle Migrationszielkonten bereitgestellt.

Überprüfung der Kennzeichnung von Ressourcen

Nachdem die Serviceberechtigungen bestätigt wurden, überprüft AWS Transform, ob alle erforderlichen Ressourcen ordnungsgemäß gekennzeichnet sind, damit die Migration vom Agenten erfolgreich durchgeführt werden kann. Wenn bei Ressourcen erforderliche Tags fehlen, stellt AWS Transform einen Link zur Tagging-Seite bereit, auf der Sie die fehlenden Tags anwenden können, bevor Sie fortfahren. Die folgenden Tags sind erforderlich:

- Bestehende Quellserver müssen die Tags `CreatedBy: AWSTransform` und `habenATWorkspace: <workspace_id>`. Wenn Sie bereits mit der Replikation auf Quellservern begonnen und sie im AWS Transform MGN-Dienst erstellt haben, müssen Sie diese Server taggen, damit AWS Transform sie mit den in Ihrer lokalen Umgebung erkannten Quellservern korrelieren kann und so die unnötige Erstellung doppelter Quellserver vermeiden kann. AWS Transform korreliert sie automatisch anhand der vom Benutzer bereitgestellten ID-, FQDN- oder Hostnamenschlüssel.
- Netzwerkressourcen müssen sowohl für die Replikation (Staging-Bereich) als auch für die Start-Instances ordnungsgemäß gekennzeichnet sein. AWS Transform zeigt die vollständige Liste der Netzwerkressourcen in Ihrem Zielkonto an und gibt an, ob die einzelnen Ressourcen bereits markiert sind oder nicht. Sie können die Liste überprüfen und alle Ressourcen ohne Tags auswählen, die Sie hinzufügen möchten. Für jede Ressource, die Sie auswählen, wendet AWS Transform das entsprechende Tag an:
 - `CreatedBy: AWSTransformoderCreatedFor: AWSTransform`, je nach Ressourcentyp.
 - `ATWorkspace: <workspace_id>` wird auf alle ausgewählten Ressourcen angewendet.

VPCs und Subnetze, die vom AWS Transform Network Migration Agent erstellt wurden, werden automatisch markiert.

- Neben VPCs und Subnetzen zeigt AWS Transform auch alle vorhandenen Elastic Network Interfaces (ENIs) an, die sich in Ihrem Zielkonto befinden. Wenn Sie möchten, dass AWS Transform sie als Teil Ihres Instance-Starts verwendet, müssen sie mit und gekennzeichnet werden. `CreatedFor: AWSTransform` `ATWorkspace: <workspace_id>` Weitere Informationen zum Anhängen oder Hinzufügen von ENIs an die Amazon EC2 EC2-Startvorlage finden Sie unter [Detaillierte Überlegungen](#) im MGN-Benutzerhandbuch.

Netzwerkdaten zum Inventar hinzufügen

AWS Transform fügt Netzwerkinformationen aus Ihrer Netzwerkmigration zur Inventardatei hinzu. In diesem Schritt werden Ihre Server den entsprechenden Zielsubnetzen und

Sicherheitsgruppen zugeordnet, basierend auf der während der Netzwerk migrationsphase generierten Netzwerkkonfiguration.

Einstellungen für Replikation und Start

Konfiguration der Replikationseinstellungen

Die Replikationseinstellungen bestimmen, wie Daten von Ihren Quellservern auf repliziert werden. AWS Konfigurieren Sie die Replikationseinstellungen in der Replikationsvorlage, bevor Sie Quellserver zu AWS Transform MGN hinzufügen. AWS Transform zeigt Ihnen alle Parameter der Replikationseinstellungen. Sie können sie über eine spezielle HITL oder über die Chat-Oberfläche konfigurieren.

Weitere Informationen zu den Parametern für die Replikationseinstellungen finden Sie unter [Vorlage für Replikationseinstellungen](#) im MGN-Benutzerhandbuch.

Starten Sie die Vorlageneinstellungen

Mit der Startvorlage können Sie steuern, in AWS welcher Weise AWS Transform MGN Instances startet. Die in der Vorlage definierte Standardkonfiguration wird automatisch auf jeden neu hinzugefügten Server angewendet. Sie können die Einstellungen für die Startvorlage über ein spezielles HITL oder über die Chat-Oberfläche konfigurieren.

Weitere Informationen zu den Einstellungsparametern für die Startvorlage finden Sie unter [Startvorlage](#) im MGN-Benutzerhandbuch.

AWS Transform bietet auch einen Link zur Amazon EC2 EC2-Startvorlagen-ID, die mit der Startvorlage verknüpft ist, sodass Sie zusätzliche Amazon EC2 EC2-Startvorlagenattribute ändern können. Um die Amazon EC2 EC2-Startvorlage zu bearbeiten, folgen Sie den Anweisungen [unter Startvorlage](#) im MGN-Benutzerhandbuch.

Strategie für die IP-Zuweisung

Sie wählen, wie IP-Adressen Ihren migrierten Servern zugewiesen werden:

- **Statische IP** — Die IP-Adresse des Quellserver wird beibehalten. Wenn eine CIDR-Transformation erforderlich ist, konvertiert AWS Transform die IP-Adresse automatisch so, dass sie der neuen CIDR entspricht.
- **Dynamische IP (DHCP)** — Jedem Server wird eine neue IP-Adresse aus dem IP-Pool des Subnetzes zugewiesen.

 Note

Wenn Sie bei der Netzwerkmigration die Strategie zur Zuordnung von MAP-Sicherheitsgruppen ausgewählt haben, ist nur die statische IP-Zuweisung verfügbar. Weitere Informationen finden Sie unter [Zuordnung von Sicherheitsgruppen](#).

Schritt 2: Inventar validieren und bestätigen

Bevor Sie Ihre Serverdaten in MGN laden, bereitet AWS Transform die Inventardatei für Ihre Überprüfung vor. Sie können die Datei im CSV- oder XLSX-Format herunterladen, die Serverkonfigurationen überprüfen und bei Bedarf Änderungen vornehmen.

Die Inventardatei enthält Details wie Servernamen, Betriebssysteme, Empfehlungen für den Amazon EC2 EC2-Instance-Typ, Zielsubnetze, Sicherheitsgruppen, IP-Zuweisungen und Lizenzoptionen. Zu den erforderlichen Feldern gehören:

- Serverinformationen — Servername, VMID und Quellspezifikationen.
- Wellenzuweisung — Gruppierung von Migrationswellen.
- Anwendungsgruppierung — Logische Anwendungszuordnungen.
- Zielkonfiguration — Zielkonto, Region und Amazon EC2 EC2-Instance-Typ.
- Netzwerkkonfiguration — Zielsubnetz und Sicherheitsgruppen.

Sie können die Datei ändern, um die Amazon EC2 EC2-Konfigurationen anzupassen, die Betriebssystem-Lizenzierungsoptionen (BYOL oder License Included) zu ändern und die Tenancy-Einstellungen zu aktualisieren.

Nachdem Sie das Inventar überprüft haben, können Sie es entweder wie abgebildet akzeptieren oder eine geänderte Version hochladen. AWS Transform lädt dann die Daten in MGN, wodurch Quellserverdatensätze für jeden Server in der Welle erstellt werden.

 Note

Entfernen Sie keine Spalten und ändern Sie keine Spaltenüberschriften in der Inventardatei. AWS Für die Transformation ist die ursprüngliche Dateistruktur erforderlich, um die Daten korrekt zu verarbeiten.

 Note

AWS Transform ermöglicht einen Import in ein bestimmtes Ziel AWS-Konto und ein bestimmtes Ziel AWS-Region nach dem anderen. Wenn Sie an mehr als einer Welle gleichzeitig arbeiten oder wenn mehrere Migrationsaufträge mit demselben Zielkonto ausgeführt werden, müssen Sie warten, bis ein Import abgeschlossen ist, bevor Sie einen weiteren Import in einer anderen Welle oder einem anderen Job durchführen können.

Sie können die Lizenzierungsoptionen für das Betriebssystem (BYOL oder Lizenz enthalten) und die Tenancy steuern, indem Sie die Konfiguration in den Spalten `mgn:launch:placement:operating-system-licensing` und in der Inventardatei angeben. `mgn:launch:placement:tenancy` Weitere Informationen finden Sie unter [Importparameter](#) im MGN-Benutzerhandbuch.

Schritt 3: Replikationsagenten bereitstellen

Um mit der Replikation von Daten von Ihren Quellservern auf zu beginnen AWS, installieren Sie den AWS Replication Agent auf jedem Quellserver. AWS Transform bietet drei Installationsmethoden:

- **Organisationstools** — Verwenden Sie die vorhandenen Bereitstellungstools Ihres Unternehmens (wie SCCM, Ansible oder Chef), um Agenten auf Ihren Servern zu installieren. AWS Transform stellt die Installationsbefehle mit zusätzlichen Parametern für die unbeaufsichtigte Installation bereit, darunter `--no-prompt`, `--aws-access-key-id`, `--aws-secret-access-key`, und `--aws-session-token`
- **MGN-Konnektor** — Verwenden Sie einen MGN-Connector, um die Agenteninstallation zu automatisieren. Der Connector stellt über SSH (Linux) oder WinRM (Windows) eine Verbindung zu Quellcomputern her und installiert den Replikationsagenten automatisch. Nach der Konfiguration kann ein Connector für mehrere Wellen und verschiedene Ziele wiederverwendet werden. AWS-Konten Weitere Informationen zum MGN-Anschluss finden Sie unter [Einrichten des MGN-Anschlusses im MGN-Benutzerhandbuch](#).

 Note

Bevor Sie den MGN-Konnektor mit AWS Transform verwenden, müssen Sie die verwaltete Instanz des Connectors in AWS Systems Manager Fleet Manager mit den folgenden Tags kennzeichnen:

- Schlüssel: CreatedFor Wert: AWSTransform
- Schlüssel: ATWorkspace Wert: *workspace-id*

Um die verwaltete Instanz zu taggen, öffnen Sie die AWS Systems Manager Konsole, navigieren Sie unter Node Tools zu Fleet Manager, wählen Sie die verwaltete Instanz Ihres MGN-Connectors aus und wenden Sie die oben genannten Tags an. Finden Sie Ihre Workspace-ID in der URL der AWS Transform-Web-App: `https://.../workspace/workspace-id/job/job-id`.

- Manuelle Installation — Installieren Sie den Agenten direkt auf jedem Quellserver. Diese Methode erfordert direkten Zugriff auf jeden Server, gibt Ihnen jedoch die volle Kontrolle über den Installationsvorgang.

AWS Transformieren Sie die Einrichtung des MGN-Connectors

Der AWS Transform MGN Connector automatisiert die Bereitstellung von Replikationsagenten auf Ihren Quellservern. Der Connector ist ein einfacher Client, der auf einem dedizierten Linux-Computer in Ihrer lokalen Umgebung bereitgestellt wird. Es stellt über SSH (Linux) oder WinRM (Windows) eine Verbindung zu Quellservern her, um Replikationsagenten zu installieren und zu konfigurieren, sodass die manuelle Koordination mehrerer AWS Dienste entfällt.

So funktioniert der Connector

Der Konnektor funktioniert über die folgenden Komponenten:

- Connector-Client — Wird auf einem dedizierten Linux-Computer in Ihrer Umgebung bereitgestellt.
- SSM-Agent — Auf demselben Computer installiert, um eine sichere Kommunikation mit AWS zu ermöglichen.
- SSM-Hybrid-Aktivierung — Verbindet die Connector-Maschine mit AWS Systems Manager für eine sichere Befehlsausführung.
- Verwaltung von Anmeldeinformationen — Ruft Quellserver-Anmeldeinformationen von AWS Secrets Manager ab.

Wenn Sie Agenten bereitstellen, sendet AWS Transform ein SSM-Dokument an den Connector-Computer. Der Connector ruft dann die Quellserver-Anmeldeinformationen von AWS Secrets Manager ab, stellt eine Verbindung zu jedem Quellserver her, überprüft, ob der Quellserver die

Voraussetzungen erfüllt, installiert und konfiguriert den Replikationsagenten und verifiziert die erfolgreiche Installation.

Anforderungen an die Connector-Maschine

Anforderung	Details
Betriebssystem	Unterstütztes Linux-Betriebssystem. Die vollständige Liste finden Sie unter Voraussetzungen für den MGN-Anschluss im MGN-Benutzerhandbuch.
Netzwerkzugriff	Muss alle Quellserver erreichen (Linux über SSH, Windows über WinRM)
Internet-Konnektivität	Ausgehendes HTTPS (443) an AWS Endpunkte (Systems Manager, Secrets Manager, MGN)
Festplattenkapazität	Mindestens 200 MB kostenlos
Berechtigungen	Root- oder Sudo-Zugriff

Note

Der Connector muss auf einem Linux-Computer installiert sein, kann aber Agenten sowohl auf Linux- als auch auf Windows-Quellservern bereitstellen.

Einrichtungsvorgang

AWS Transform führt Sie durch die folgenden Schritte zur Einrichtung des Connectors:

Schritt 1: Konfiguration des Konnektors

Geben Sie einen Namen für Ihren Connector ein, oder verwenden Sie den automatisch generierten Standardnamen. Der Connector kann auf dem Verwaltungskonto oder auf einem delegierten Administratorkonto in MGN installiert werden. Bei Migrationen mehrerer Konten kann der Connector Agenten auf Servern für mehrere Mitgliedskonten bereitstellen.

Schritt 2: Einrichtung der Ressourcen AWS

AWS Transform öffnet eine Einrichtungsseite, die in Ihrem Browser mit Ihren AWS Anmeldeinformationen ausgeführt wird. Sie müssen entweder mit Ihrem AWS Verwaltungskonto oder Ihrem delegierten Administratorkonto bei der Management Console angemeldet sein. Dies muss dasselbe Konto sein, mit dem Ihr AWS Transform-Ziel-Connector verbunden ist.

Auf der Einrichtungsseite werden automatisch die folgenden Ressourcen erstellt:

- IAM-Rollen (idempotent erstellt — übersprungen, falls sie bereits existieren):
 - `AWSApplicationMigrationConnectorManagementRole`— Wird während der Agenteninstallation für den Zugriff auf Anmeldeinformationen verwendet.
 - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>`— Enthält Berechtigungen für die Agenteninstallation.
- SSM-Hybrid-Aktivierung — Ablauffrist von 30 Tagen. Verbindet die Connector-Maschine mit AWS Systems Manager und generiert sichere Aktivierungsdaten.

Alternativ können Sie eine CloudFormation Vorlage von der Einrichtungsseite herunterladen, um die IAM-Rollen selbst bereitzustellen.

Auf der Einrichtungsseite wird ein einzeliger Installationsbefehl mit allen erforderlichen Anmeldeinformationen und Konfigurationen generiert.

Important

Lassen Sie die Einrichtungsseite geöffnet, bis die Installation abgeschlossen ist. Um es zu schließen, muss der Vorgang neu gestartet werden. Alle Anmeldeinformationen existieren nur in Ihrem Browser und werden nicht von AWS Transform gespeichert.

Schritt 3: Installation des Connectors

Installieren Sie den Connector auf einem Linux-Computer in Ihrer Umgebung:

1. Kopieren Sie den Installationslink von der Setup-Seite.
2. Stellen Sie eine SSH-Verbindung zu Ihrem ausgewählten Linux-Computer her.
3. Fügen Sie den Installationsbefehl ein und führen Sie ihn aus.
4. Warten Sie, bis die Installation abgeschlossen ist (normalerweise 2—3 Minuten).

Schritt 4: Quellserver anhängen

Nach der Installation identifiziert AWS Transform alle Quellserver, die zur aktuellen Welle gehören, und verbindet sie automatisch mit dem MGN-Anschluss.

Schritt 5: Anmeldeinformationen konfigurieren

Geben Sie AWS Secrets Manager Manager-ARNs für Ihre Quellserver-Anmeldeinformationen an. AWS Transform bietet drei Konfigurationsoptionen für Anmeldeinformationen:

- Einzelner geheimer Schlüssel für Linux-Server — Ein gemeinsam genutzter geheimer Schlüssel mit SSH-Schlüsseln oder username/password für alle Linux-Quellserver.
- Single Secret für Windows-Server — Ein gemeinsam genutzter geheimer Schlüssel, der Benutzername und Passwort für alle Windows-Quellserver enthält.
- Mehrere Geheimnisse pro Server — Verschiedene Geheimnisse pro Server oder Servergruppe. Verwenden Sie diese Option, wenn Server unterschiedliche Anmeldeinformationen haben. AWS Transform generiert eine CSV-Datei, die bereits mit Ihrer Serverliste gefüllt ist. Sie füllen die `secret_arn` Spalte für jeden Server aus und laden die fertige Datei hoch.

Note

Sie können die Single Secret-Optionen für Linux und Windows kombinieren, wenn Sie beide Servertypen mit jeweils einem gemeinsamen geheimen Schlüssel haben. Die Option für serverseitige geheime Daten schließt sich gegenseitig mit den Optionen für einzelne geheime Daten aus.

Format für geheime Anmeldeinformationen. Weitere Informationen dazu finden Sie unter den [Anmeldeinformationen für den MGN-Connector](#) im MGN-Benutzerhandbuch:

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

Bereitstellung des Agenten

Sobald die Anmeldeinformationen konfiguriert und verifiziert sind, stellt AWS Transform Replikationsagenten auf Ihren Quellservern bereit. Sie können die Bereitstellung auf allen Servern der aktuellen Welle oder auf bestimmten Servern durchführen.

Der Bereitstellungsprozess für jeden Server:

1. AWS Transform sendet Bereitstellungsbefehle über SSM an den Connector.
2. Der Connector ruft Anmeldeinformationen von AWS Secrets Manager ab.
3. Der Connector stellt mithilfe der konfigurierten Anmeldeinformationen eine Verbindung zum Quellserver her.
4. Der Connector überprüft, ob der Quellserver alle Voraussetzungen erfüllt, die für die Ausführung des Replikationsagenten erforderlich sind.
5. Der Connector installiert und konfiguriert den Replikationsagenten.
6. Der Connector überprüft die erfolgreiche Installation und Konnektivität.

Sie können den Bereitstellungsfortschritt in Echtzeit überwachen, indem Sie den Status pro Server verfolgen, einschließlich des aktuellen Installationsschritts, der verstrichenen Zeit und der geschätzten verbleibenden Zeit. Wenn Server ausfallen, zeigt AWS Transform die Fehlerursache an und bietet Wiederholungsoptionen für jeden Server an. Erfolgreich bereitgestellte Server können unabhängig voneinander fortfahren, während ausgefallene Server erneut versucht werden.

Wiederverwendung und Lebenszyklus von Connectoren

Bei der Bereitstellung von Agenten für nachfolgende Wellen können Sie einen vorhandenen Connector wiederverwenden oder einen neuen erstellen. AWS Transform listet alle in Ihrem Konto konfigurierten Connectors auf und zeigt den Namen, den Status (Aktiv oder Abgelaufen), die Anzahl der angeschlossenen Server und das Ablaufdatum der Hybrid-Aktivierung an.

- **Aktiver Connector** — Die Hybrid-Aktivierung ist weiterhin gültig. AWS Transform überprüft die IAM-Rollen für die neue Welle und fährt mit der Konfiguration der Anmeldeinformationen fort. Es ist keine neue Hybrid-Aktivierung erforderlich.
- **Abgelaufener Connector** — Die SSM-Hybrid-Aktivierung ist abgelaufen. Abgelaufene Aktivierungen können nicht erneuert werden. Sie müssen einen anderen Connector auswählen oder einen neuen erstellen.

SSM-Hybrid-Aktivierungen laufen nach 30 Tagen ab. Die Aktivierung ist nur für die Installation des Connectors auf dem Linux-Computer erforderlich. Sobald der Connector installiert ist, können Sie ihn auch nach Ablauf der Aktivierung weiterhin zur Installation von Replikationsagenten auf Quellservern verwenden. Wenn Sie den Connector nach Ablauf der Aktivierung auf einem neuen Computer installieren müssen, müssen Sie während des Einrichtungsvorgangs einen neuen Connector erstellen.

Manuelle Agenteninstallation

Bei der manuellen Installation generieren Sie zunächst AWS Anmeldeinformationen (temporär oder permanent) und installieren dann den Agenten auf jedem Quellserver.

Optionen für Anmeldeinformationen:

- Temporäre Anmeldeinformationen (empfohlen) — Erstellen Sie eine IAM-Rolle mit der `AWSApplicationMigrationAgentInstallationPolicy` verwalteten Richtlinie und verwenden Sie sie dann, um temporäre Anmeldeinformationen `aws sts assume-role` zu generieren. Weitere Informationen dazu finden Sie unter [Berechtigungen zur Agenteninstallation](#) im MGN-Benutzerhandbuch.
- Permanente Anmeldeinformationen — Erstellen Sie einen IAM-Benutzer mit der `AWSApplicationMigrationAgentInstallationPolicy` verwalteten Richtlinie und generieren Sie einen Zugriffsschlüssel.

Schritte zur Installation:

Laden Sie für Linux-Server das Installationsprogramm herunter und führen Sie es aus:

```
wget -O ./aws-replication-installer-init \  
https://aws-application-migration-service-region.s3.region.amazonaws.com/latest/  
linux/aws-replication-installer-init  
sudo chmod +x aws-replication-installer-init  
sudo ./aws-replication-installer-init --region region --user-provided-id server-  
identifizier
```

Laden Sie für Windows-Server das entsprechende Installationsprogramm herunter und führen Sie es PowerShell als Administrator aus:

```
Invoke-WebRequest -Uri "https://aws-application-migration-  
service-region.s3.region.amazonaws.com/latest/windows/  
AwsReplicationWindowsInstaller.exe" `
```

```
-OutFile "C:\AwsReplicationWindowsInstaller.exe"  
C:\AwsReplicationWindowsInstaller.exe --region region --user-provided-id server-  
identifizier
```

Important

Der Parameter `--user-provided-id` muss angegeben werden. *server-identifizier* Ersetzen Sie ihn durch den exakten Wert aus der `mgn:server:user-provided-id` Spalte in Ihrer Inventardatei. Diese Kennung verknüpft den physischen Server mit seinem MGN-Quellservereintrag.

Weitere Informationen zur Agenteninstallation finden Sie unter [Linux-Agent](#) und [Windows-Agent](#) im MGN-Benutzerhandbuch.

Nach der Installation überprüft AWS Transform, ob alle Agents erfolgreich verbunden wurden, indem überprüft wird, ob auf den Servern der INITIATING Replikationsstatus oder angezeigt wird. INITIAL_SYNC

Note

AWS Transform unterstützt keine agentenlose MGN-Replikation. Informationen zur agentenlosen Replikation finden Sie unter [Überblick über die agentenlose Replikation im MGN-Benutzerhandbuch](#).

Note

Sie müssen den Replication Agent auf allen Servern in einer Welle installieren. Trennen und archivieren Sie die Server, auf denen Sie den Replikationsagenten nicht installieren. Sie können den `disconnect-from-service` Befehl verwenden, um die Verbindung zu Servern zu trennen, und den `mark-as-archived` Befehl, um getrennte Server zu archivieren. Der Archivierungsbefehl funktioniert nur für Quellserver mit dem Lebenszyklusstatus. DISCONNECTED

Informationen zu Kontingenten im Zusammenhang mit der Replikation finden Sie unter [Beschränkungen der MGN-Dienstkontingente](#) im MGN-Benutzerhandbuch.

Schritt 4: Datenreplikation

Nach der Installation der Replikationsagenten beginnt die Datenreplikation automatisch. AWS Transform verwendet kontinuierliche Replikation auf Blockebene, um Daten von Quellservern zu synchronisieren. AWS

Der Replikationsprozess besteht aus zwei Phasen:

- **Erste Synchronisierung** — Eine vollständige Kopie der Quellserverdaten auf AWS. Daten werden je nach Ihrem konfigurierten Zielspeichertyp als Amazon Elastic Block Store (Amazon EBS) - Snapshots oder auf Amazon FSx for NetApp ONTAP (FSx for ONTAP) -Volumes im Zielkonto gespeichert. Weitere Informationen finden Sie unter [Zielspeichertyp](#) im MGN-Benutzerhandbuch. Die Dauer hängt vom Datenvolumen und der Netzwerkbandbreite ab.
- **Kontinuierliche Replikation** — Fortlaufende Synchronisation geänderter Blöcke mit minimaler Auswirkung auf die Leistung des Quellservers. Verwaltet eine aktuelle Kopie in AWS.

Replikationsserver sind temporäre Amazon EC2 EC2-Instances, die im Staging-Bereich-Subnetz bereitgestellt werden. Sie erhalten replizierte Daten von Quellservern und werden automatisch von MGN verwaltet. Weitere Informationen dazu finden Sie unter [Replication Server Settings](#) im MGN User Guide.

AWS Transform überwacht den Replikationsfortschritt und bietet Statusaktualisierungen, einschließlich Replikationsstatus, Replikationsverzögerung (Zeitunterschied zwischen Quell- und replizierten Daten) und Bandbreitennutzung.

Während der Replikation durchläuft jeder Server die folgenden Zustände:

- **Nicht bereit** — Der Server durchläuft gerade den ersten Synchronisierungsprozess und ist noch nicht bereit für Tests.
- **Bereit zum Testen** — Der Server wurde erfolgreich hinzugefügt und die Datenreplikation wurde gestartet. Test- oder Cutover-Instanzen können jetzt gestartet werden.

Sobald alle Server in der Welle den NOT_READY Status überschritten haben, ist die Datenreplikationsphase abgeschlossen und Sie können mit dem Testen fortfahren.

Sie können die Replikation für einzelne Server oder die gesamte Welle jederzeit steuern:

- Replizierung unterbrechen — Unterbrechen Sie vorübergehend die Replikation für bestimmte Server oder die gesamte Welle.
- Replizierung fortsetzen — Setzt die zuvor unterbrochene Replikation fort.
- Replizierung beenden — Stoppen Sie die Replikation dauerhaft. Die gestoppte Replikation kann neu gestartet werden, sie beginnt jedoch mit der ersten Synchronisierung.

Schritt 5: Testen

Nach Abschluss der Datenreplikation können Sie Testinstanzen starten, um Ihre migrierten Server zu validieren, bevor Sie die endgültige Umstellung durchführen. Weitere Informationen dazu finden Sie im [MGN-Benutzerhandbuch unter Testinstanzen starten](#). AWS Transform unterstützt zwei Testoptionen:

- Vollwellentests — Starten Sie Testinstanzen für alle Server in der Welle.
- Selektives Testen — Starten Sie Testinstanzen für bestimmte Server, die Sie auswählen, indem Sie deren vom Benutzer bereitgestellte IDs aus der Inventardatei angeben.

AWS Transform startet Amazon EC2 EC2-Instances aus den replizierten Daten und stellt die Instance-IDs bereit, sodass Sie eine Verbindung zu den Test-Instances herstellen und diese validieren können. Nach dem Testen können Sie:

- Fahren Sie mit der Umstellung fort, wenn der Test erfolgreich war.
- Starten Sie neue Testinstanzen für den erneuten Test.
- Beenden Sie Testinstanzen und beheben Sie alle Probleme, bevor Sie den Test erneut durchführen.

Schritt 5b: Markieren Sie Anwendungen als bereit für die Umstellung

Wenn der Test abgeschlossen ist und Sie mit den Ergebnissen zufrieden sind, markieren Sie Ihre Anwendungen als bereit für die Umstellung. AWS Transform überprüft den Replikationsstatus jeder Anwendung und behebt alle Replikationswarnungen, bevor Sie fortfahren können. Nur Anwendungen mit dem Status „Clean Replication“ können für die Umstellung markiert werden.

Schritt 6: Umstellung

Die Umstellung ist der letzte Migrationsschritt, in den Ihre Produktions-Workloads verschoben werden. AWS Weitere Informationen dazu finden Sie unter [Starten von Cutover-Instanzen](#) im MGN-Benutzerhandbuch. Ähnlich wie beim Testen unterstützt AWS Transform Full-Wave-Cutover oder Selective Cutover für bestimmte Server.

Während der Umstellung startet AWS Transform Amazon EC2 EC2-Instances aus den neuesten replizierten Daten und stellt die Instance-IDs für jeden Server bereit. Nachdem Sie die Cutover-Instances verifiziert haben, schließen Sie die Übernahme ab, wodurch die laufende Replikation des Quellcomputers gestoppt wird.

Der Umstellungsprozess umfasst die folgenden Schritte:

1. Cutover-Instances starten — AWS Transform startet Amazon EC2 EC2-Instances für die ausgewählten Server. Sie können zwischen Full-Wave-Cutover oder Selective Cutover wählen.
2. Übernahmeinstanzen überprüfen — Stellen Connect zu den gestarteten Instances her und überprüfen Sie, ob sie ordnungsgemäß funktionieren.
3. Übernahme abschließen — Bestätigen Sie die Umstellung, um die Replikation des Quellcomputers zu beenden. Sie können alle Server in der Welle abschließen oder bestimmte Server auswählen. Die Finalisierung verhindert, dass Replikationsagenten Daten senden, entfernt Replikationsagenten von den Quellservern und sperrt den Lebenszyklusstatus des Servers. Diese Aktion kann nicht einfach rückgängig gemacht werden. Weitere Informationen dazu finden Sie unter [Finalize Cutover im MGN-Benutzerhandbuch](#).
4. Quellserver archivieren (optional) — Nach der Finalisierung können Sie Quellserver als archiviert markieren, um Quellserverkontingent in Ihrem Konto freizugeben.

Important

Durch den Abschluss der Übernahme wird die laufende Replikation des Quellcomputers beendet. Stellen Sie vor dem Abschluss sicher, dass Sie Ihre Übernahmeinstanzen verifiziert haben.

 Note

Zwischen dem Herunterfahren der Quelle und der Verfügbarkeit der Cutover-Instance treten Ausfallzeiten auf. Planen Sie Ihr Umstellungsfenster entsprechend.

Status des Serverlebenszyklus

Während der Migration durchläuft jeder Server die folgenden Lebenszyklusstatus. Weitere Informationen dazu finden Sie unter [Lebenszyklus des Quellservers](#) im MGN-Benutzerhandbuch.

- Nicht bereit — Der Server durchläuft gerade den ersten Synchronisierungsprozess und ist noch nicht bereit für Tests.
- Bereit zum Testen — Die Datenreplikation wurde gestartet und Test- oder Übernahmeinstanzen können gestartet werden.
- Test läuft — Eine Testinstanz wird gerade gestartet.
- Bereit für die Umstellung — Der Server wurde getestet und ist bereit für die Umstellung.
- Umstellung läuft — Eine Übernahmeinstanz wird derzeit gestartet.
- Umstellung abgeschlossen — Der Server wurde umgestellt. Alle Daten wurden auf die Übernahmeinstanz migriert. AWS
- Verbindung getrennt — Der Server wurde von MGN getrennt.

Sie können AWS Transform jederzeit während der Migration nach dem Status Ihrer Server fragen. AWS Transform bietet eine interaktive Wave-Statustabelle, in der alle relevanten Serverinformationen einschließlich des Migrationslebenszyklus, des Replikationsstatus und der empfohlenen nächsten Schritte angezeigt werden. Sie können auch in natürlicher Sprache fragen, zum Beispiel:

- Was ist der Status meiner Server?
- Was ist der Status meiner Welle?
- Was ist der Status des Schritts, in dem ich mich gerade befinde?

Während der Wave-Migration können Sie AWS Transform bitten, den Status einzelner Server zu aktualisieren oder zu ändern. Wenn beispielsweise 9 von 10 Servern in Ihrer Wave die Testphase bestanden haben, einer jedoch ausgefallen ist, können Sie AWS Transform erlauben, die 9 Server

weiterhin in die nächste Phase zu verschieben, während der Test auf dem ausgefallenen Server erneut ausgeführt wird.

Genehmigungen für die Bereitstellung

Einige Migrationsvorgänge erfordern vor der Ausführung eine ausdrückliche Genehmigung. Wenn für einen Vorgang eine Genehmigung erforderlich ist, leitet AWS Transform die Anfrage über die Registerkarte Genehmigungen an autorisierte Genehmiger weiter. Nur Benutzer mit der Administratorrolle in AWS Transform können Bereitstellungsanfragen genehmigen. Bereitstellungen werden erst nach Erhalt der Bestätigung fortgesetzt.

Versionshinweise

Die folgenden Versionshinweise behandeln die neuesten Änderungen von [Migrationen \(einschließlich VMware\)](#). Informationen zu unterstützten AWS Transform-Regionen finden Sie unter [Unterstützte Regionen](#). Informationen zu unterstützten Zielregionen finden Sie auf der [Seite zur Einrichtung des Account-Connectors](#).

Juni 2026

- AWS Transform for Migrations unterstützt jetzt die Lokalisierung. Sie können die Anzeigesprache der Webanwendung ändern, wenn Sie mit Migrationsworkflows arbeiten. [Erfahren Sie mehr über Spracheinstellungen](#).
- AWS Mit Transform können Sie jetzt Ihre Replikationseinstellungen und Starteinstellungen für Ihre Migration konfigurieren. Sie können die Konfiguration für Ihr Zielkonto oder für bestimmte Quellserver festlegen. [Erfahren Sie mehr über Replikations- und Starteinstellungen](#).
- AWS Mit Transform können Sie jetzt bestehende Elastic Network Interfaces (ENIs) an Ihre Startvorlage anhängen. Sie können ENIs in Ihrem Zielkonto taggen, sodass sie beim Start von Instances verwendet werden können. [Erfahren Sie mehr über das Tagging von Netzwerkressourcen](#).
- AWS Transform for Migrations unterstützt jetzt alle AWS Handelsregionen als Migrationsziele, mit Ausnahme des Nahen Ostens (Bahrain) und des Nahen Ostens (VAE). [Erfahren Sie mehr über unterstützte Zielregionen](#).

Mai 2026

- AWS Transform erkennt jetzt bei der Überprüfung der Netzwerkmigration bestehende VPCs in Ihrem Zielkonto. Sie können vorhandene VPCs neben Ihren zugewiesenen VPCs sehen, CIDR-Konflikte identifizieren und diese vor der Bereitstellung lösen. [Erfahren Sie mehr über die bestehende VPC-Erkennung](#).
- AWS Transform unterstützt die Umstellung von Quellcode-Repositorys auf Container während der Migration zu. AWS [Erfahren Sie mehr über Containerisierung](#).

April 2026

- Die Erstellung von Landezonen wurde direkt in den Migrationsworkflows hinzugefügt. AWS Transform sucht nach einer vorhandenen Grundlage, empfiehlt Strukturen und Zielkonten für Organisationseinheiten (OU) und bietet automatische Bereitstellung oder IaC-Ausgabe (Infrastructure as Code) (Formate CloudFormation, AWS CDK, oder Landing Zone Accelerator (LZA)). [Erfahre mehr über die Erstellung von landing zone](#).
- Unterstützung für DHCP mit Sicherheitsgruppenzuweisung während der Netzwerkmigration hinzugefügt. [Erfahren Sie mehr über die Erstellung von Sicherheitsgruppen](#).

März 2026

- Öffentliche APIs für die Netzwerkmigration wurden hinzugefügt, sodass Partner- und programmatischen Zugriff auf Netzwerkigrationsfunktionen erhalten. Weitere Informationen finden Sie in der [API-Referenz zur Netzwerkmigration](#).

Februar 2026

- Die Netzwerkmigration unterstützt jetzt das Einlesen von [Firewall- oder Software-Defined Netzwerkkonfigurationsdateien \(SDN\)](#), ohne dass [RVTools-Erkennungsdaten](#) erforderlich sind. Sie können Firewall- oder SDN-Konfigurationsdateien unabhängig voneinander verwenden oder sie mit RVTools-Exporten kombinieren.

Januar 2026

- Unterstützung für das [Tagging des Migration Acceleration Program \(MAP\) und das benutzerdefinierte Tagging von](#) Netzwerkmigrationselementen wurde hinzugefügt, sodass Sie Migrationsressourcen für MAP-Kredit- und Organisationszwecke verfolgen können.

Dezember 2025

- Es wurde ein neues [Migrationserlebnis](#) mit neu gestaltetem Workflow und verbesserter Benutzerfreundlichkeit hinzugefügt. Weitere Informationen finden Sie unter [Beschleunigte VMware-Migration: Die neue Erfahrung von AWS Transform](#).
- [Netzwerkconfiguration für den Landing Zone Accelerator \(LZA\)](#) für die automatische Einrichtung der landing zone hinzugefügt.
- Es wurde Unterstützung für [mehrere AWS Zielkonten](#) bei der Migrationsausführung hinzugefügt, sodass Sie Workloads kontenübergreifend migrieren können.
- Netzwerkmigrationsunterstützung für die [Quellformate Cisco ACI, Palo Alto und FortiGate ModelizeIT](#) wurde hinzugefügt.

Oktober 2025

- Die Durchführung der Migration wurde um den asiatisch-pazifischen Raum (Osaka) auf [16 Zielregionen](#) ausgeweitet.

September 2025

- Es wurde Unterstützung für die Lizenzconfiguration in [Rehost-Wellen](#) hinzugefügt, sodass Sie pro Welle Optionen mit Bring Your Own License (BYOL) oder im Lieferumfang enthaltene Lizenzen angeben können.
- Es wurde Unterstützung für [Terraform bei der Netzwerkmigration hinzugefügt, sodass Sie die Netzwerkinfrastruktur](#) mithilfe von Terraform-Vorlagen bereitstellen können.
- Unterstützung für die Aktualisierung der Replikationssubnetzconfiguration hinzugefügt, wodurch die Anforderung einer Standard-VPC im Zielkonto entfällt.

August 2025

- Ausweitung der Migrationsausführung (Netzwerkmigration und Rehost) auf [15 Zielregionen](#) mit Hinzufügung von USA Ost (Ohio), Europa (Stockholm) und Europa (Irland).
- Es wurden [flexible CIDR-Bereichsfunktionen](#) für die Netzwerkmigration hinzugefügt, sodass Sie IP-Adressbereiche während der Netzwerkbereitstellung anpassen können.

Mai 2025

- Erster Servicestart von [Migrationen \(einschließlich VMware\)](#), der umfassende Migrationsfunktionen bietet, einschließlich [Erkennung](#), Bewertung, [Migrationsplanung](#), Netzwerkmigration und Server-Rehosting.
- Unterstützte Migrationsausführung in 12 [Zielregionen](#): USA Ost (Nord-Virginia), USA West (Oregon), Kanada (Zentral), Südamerika (São Paulo), Europa (Frankfurt), Europa (London), Europa (Paris), Asien-Pazifik (Mumbai), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), Asien-Pazifik (Singapur) und Asien-Pazifik (Sydney).

Containerisierung des Quellcodes

AWS Transform unterstützt die Umstellung von Anwendungen auf Container während der Migration zu AWS. In diesem Kapitel werden die agentischen KI-Funktionen von AWS Transform zur Automatisierung der Containerisierung Ihres Quellcodes beschrieben. Sie können parallel migrieren und modernisieren und so den Zeitaufwand und die Komplexität der Umstellung von lokalen auf Cloud-native Architekturen reduzieren. Sie können Quellcode aus GitHub Bitbucket- oder .zip-Dateien containerisieren, GitLab, Docker-Images generieren, in Amazon Elastic Container Registry (Amazon ECR) veröffentlichen und in Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) bereitstellen. Dadurch wird die Containerisierung in denselben Workflow integriert, den Sie für die Planung und Ausführung von Rehost-Migrationen verwenden.

Note

Die Containerisierung von Quellcode ist für Anwendungen konzipiert, die noch nicht containerisiert sind. Sie erfordert Zugriff auf den Quellcode Ihrer Anwendung und unterstützt nicht die Migration vorhandener containerisierter Workloads. Verwenden Sie zur Migration vorhandener Container die AWS Standardbereitstellungsmethoden für Amazon Elastic Container Service oder Amazon Elastic Kubernetes Service.

Funktionen und Hauptmerkmale

AWS Transform bietet die folgenden Funktionen für die Containerisierung Ihrer Anwendungen.

- **AI-driven Quellcode-Analyse** — Analysiert den Quellcode Ihrer Anwendung und generiert automatisch Docker-Artefakte, einschließlich Docker-Dateien und zugehöriger Konfigurationsdateien.
- **Erstellung und Veröffentlichung von Container-Images** — Erstellt und testet Container-Images mithilfe von AI-driven Docker-Builds und veröffentlicht sie mit automatisiertem Schwachstellen-Scanning in Amazon Elastic Container Registry.
- **Infrastruktur als Codegenerierung** — Generiert eine Bereitstellungsinfrastruktur für Amazon Elastic Kubernetes Service (Helm-Diagramme) oder Amazon Elastic Container Service (Terraform-Module) mit automatisierter Validierung und Sicherheitsscans.

- Unterstützung für private Abhängigkeiten — Sie können optional AWS CodeArtifact Repositorys (Maven, PyPI, npm) und private Amazon ECR-Basisimages als Abhängigkeitsquellen für Ihre Builds konfigurieren.
- Iterativer Test und Umstellung — Stellt eine Testinfrastruktur zur Validierung bereit und stellt dann die endgültige Infrastruktur für die Produktionsumstellung bereit.

Wie funktioniert die Containerisierung

AWS Transform verwendet einen AI-powered Agenten, der Sie in einem Chat-basierten Workflow durch den Containerisierungsprozess führt. AWS Transform koordiniert spezielle Aufgaben wie Quellcode-Analyse, Docker-Image-Generierung und Infrastrukturerstellung. An wichtigen Punkten des Workflows überprüfen und genehmigen Sie die Ausgabe, bevor Sie fortfahren.

Sie greifen auf die Containerisierung des Quellcodes zu, indem Sie einen VMware-Migrationsauftrag erstellen. Innerhalb des Jobs können Sie die Containerisierung als eigenständigen Workflow oder als Teil einer umfassenden Migration ausführen, wenn die Migrationsstrategie einer Welle auf Containerisierung festgelegt ist. Weitere Informationen zur VMware-Migration finden Sie unter [Migrationen \(einschließlich VMware\)](#).

Voraussetzungen

Beginnen Sie erst, wenn Folgendes vorliegt:

- Ein AWS Transform-Arbeitsbereich. Informationen zum Einrichten eines Workspace finden Sie unter [Erste Schritte](#).
- Ihr Anwendungsquellcode in einem Git-Repository, auf das über zugegriffen werden kann AWS CodeConnections, oder als ZIP-Dateien für den Upload verpackt. Einzelne Dateien dürfen 1 GB nicht überschreiten, und die Gesamtgröße des gesamten Quellcodes darf 8 GB nicht überschreiten.
- (Optional) Ein Amazon ECR-Repository zum Veröffentlichen von Container-Images. Sie können den Amazon ECR-Zugriff später im Workflow konfigurieren, wenn Sie zur Veröffentlichung bereit sind.
- Für Amazon EKS-Bereitstellungen: Ein vorhandener Amazon EKS-Cluster oder Berechtigungen zum Erstellen der erforderlichen Infrastruktur.

- Für Amazon ECS-Bereitstellungen: Berechtigungen zum Erstellen von Amazon ECS-Clustern, -Services und zugehörigen Ressourcen mithilfe von Terraform,, AWS CloudFormation oder. AWS Cloud Development Kit (AWS CDK)

Arbeitsablauf bei der Containerisierung

Der Workflow zur Containerisierung besteht aus den folgenden Schritten. Der AWS Transform-Agent führt Sie durch jeden Schritt in der Chat-Oberfläche.

1. [the section called “Schritt 1: Sicherheitsausschluss”](#)— Lesen und akzeptieren Sie den Sicherheitsausschluss.
2. [the section called “Schritt 2: Quellcode klonen”](#)— Geben Sie den Quellcode Ihrer Anwendung an.
3. [the section called “Schritt 3: Containerisieren”](#)— Der KI-Agent analysiert Ihren Code und generiert Docker-Artefakte.
4. [the section called “Schritt 4: Artefakte überprüfen”](#)— Überprüfen Sie die generierten Artefakte und genehmigen Sie Codeänderungen.
5. [the section called “Schritt 5: Bilder veröffentlichen”](#)— Veröffentlichen Sie Container-Images auf Amazon ECR.
6. [the section called “Schritt 6: IaC generieren”](#)— Generieren Sie Amazon EKS- oder Amazon ECS-Bereitstellungsvorlagen.
7. [the section called “Schritt 7: Stellen Sie die Testinfrastruktur bereit”](#)— Bereitstellung und Validierung der Testinfrastruktur.
8. [the section called “Schritt 8: Bereinigen Sie die Testinfrastruktur”](#)— Testressourcen abbauen.
9. [the section called “Schritt 9: Implementieren Sie die Umstellungsinfrastruktur”](#)— Bereitstellung der Produktionsinfrastruktur.

Starten eines Containerisierungsjobs

Um Ihre Anwendungen zu containerisieren, erstellen Sie zunächst einen VMware-Migrationsauftrag in Ihrem Transform-Workspace. AWS Innerhalb des Jobs können Sie wählen, ob Sie einen eigenständigen Containerisierungs-Workflow oder einen End-to-End-Migrationsablauf ausführen möchten, der die Containerisierung beinhaltet.

- **Eigenständige Containerisierung** — Containerisieren Sie Ihren Quellcode, ohne eine vollständige VMware-Migration durchzuführen. Wählen Sie diese Option, wenn Sie Anwendungen unabhängig von einer Infrastrukturmigration containerisieren möchten.
- **End-to-end Migration mit Containerisierung** — Führen Sie den vollständigen VMware-Migrationsworkflow mit einer Strategie zur Containerisierung aus, die einer oder mehreren Wellen zugewiesen ist. Der Containerisierungs-Workflow wird als Teil der Migration für diese Wellen ausgeführt. Weitere Informationen zur VMware-Migration finden Sie unter. [Migrationen \(einschließlich VMware\)](#)

Um einen Containerisierungsjob zu starten

1. Wähle auf deiner Workspace-Landingpage die Option Job erstellen aus.
2. Wähle VMware-Migration.
3. Wählen Sie, ob Sie einen eigenständigen Containerisierungs-Workflow oder einen umfassenden Migrationsablauf ausführen möchten, der die Containerisierung beinhaltet.
4. AWS Transform führt Sie durch die Workflow-Schritte, beginnend mit. [the section called “Schritt 1: Sicherheitsausschluss”](#)

Berechtigungen für die Containerisierung

Während des Containerisierungs-Workflows stellt AWS Transform Ihnen AWS-Konto eine IAM-Rolle zur Verfügung, die zum Erstellen von Container-Images und zum Bereitstellen der Infrastruktur verwendet wird. Sie werden gebeten, die Erstellung dieser Rolle zu überprüfen und zu genehmigen, bevor der Workflow fortgesetzt wird.

Die Rolle hat einen Namen `AWSTransformCodeBuildExecutionRole` und wird über einen AWS CloudFormation Stack bereitgestellt. Sie umfasst die folgenden verwalteten Richtlinien.

Basisrichtlinie

Stellt Kernberechtigungen für den Containerisierungs-Workflow bereit:

- Amazon S3 — Objekte in `aws-transform-*` Buckets lesen und schreiben
- Amazon ECR — Authentifizieren, Bilder abrufen (markiert mit `Project: atx-migration`) und Bilder in Repositories übertragen, die mit gekennzeichnet sind `CreatedBy: AWSTransform`

- AWS CodeArtifact — Lesen Sie aus Repositorys, die mit `Project: atx-migration` markiert sind, listen Sie Repositorys auf, holen Sie sich Autorisierungstoken und lesen Sie Repository-Endpunkte. Diese Berechtigungen unterstützen sowohl die Auflösung öffentlicher Abhängigkeiten als auch private Abhängigkeitsquellen, die während des Workflows konfiguriert wurden
- Amazon CloudWatch Logs — Protokollgruppen und Streams erstellen und Protokollereignisse für Amazon ECS-Protokollgruppen schreiben
- AWS KMS — Schlüssel beschreiben und entschlüsseln (gilt für Amazon S3 via Service Condition)
- Amazon EC2 — Netzwerkschnittstellen für VPC-enabled Projekte erstellen und verwalten
- AWS CodeConnections — Verwenden Sie Verbindungen, um über den konfigurierten CodeConnections ARN auf Quellcode-Repositorys zuzugreifen

Netzwerkrichtlinie

Verwaltet Netzwerkressourcen für bereitgestellte Anwendungen:

- Elastic Load Balancing — Load Balancer, Zielgruppen, Listener und Regeln erstellen, beschreiben und verwalten (verschlagwortet mit) `CreatedBy: AWSTransform`
- Route 53 — Hosting-Zonen und DNS-Einträge erstellen und verwalten
- AWS Cloud Map — Namespaces und Dienste für die Serviceerkennung erstellen und verwalten (markiert mit) `CreatedBy: AWSTransform`

Speicherrichtlinie

Verwaltet Speicherressourcen für bereitgestellte Anwendungen:

- Amazon S3 — Buckets erstellen und verwalten, einschließlich Verschlüsselung, Versionierung, Lebenszyklus und Zugriffsrichtlinien
- Amazon EFS — Dateisysteme erstellen und verwalten, Ziele einbinden und Zugriffspunkte (markiert mit) `CreatedBy: AWSTransform`
- Amazon EBS — Volumes und Snapshots erstellen und verwalten (markiert mit) `CreatedBy: AWSTransform`

AWS KMS policy

Verwaltet Operationen mit Verschlüsselungsschlüsseln:

- Beschreiben Sie Schlüssel, listen Sie Aliase auf und lesen Sie die Schlüsselrichtlinien
- Datenschlüssel verschlüsseln, entschlüsseln und generieren (gemäß den Servicebedingungen von Amazon CloudWatch Logs, Amazon EFS, Amazon EC2 und Amazon S3)

Amazon ECS-Richtlinie

Verwaltet Amazon Elastic Container Service-Ressourcen für Container-Bereitstellungen:

- Cluster, Services und Aufgabendefinitionen (gekennzeichnet mit `CreatedBy: AWSTransform`) erstellen und verwalten
- Aufgabendefinitionen registrieren und deregistrieren, Aufgaben ausführen
- Übergeben Sie IAM-Rollen an Aufgaben und Services von Amazon ECS
- Lesen Sie die IAM-Rolleninformationen und ACM-Zertifikate
- Beschreiben Sie Amazon EC2 EC2-VPCs, Subnetze, Sicherheitsgruppen und Netzwerkschnittstellen

Amazon EKS-Richtlinie

Verwaltet Amazon Elastic Kubernetes Service Service-Ressourcen für Kubernetes-Bereitstellungen:

- Greifen Sie auf die Kubernetes-API zu, beschreiben Sie Cluster und listen Sie Add-Ons auf
- Übergeben Sie IAM-Rollen an Amazon EKS

Note

Alle Berechtigungen sind auf Sie und Ihre Person beschränkt. AWS-Konto AWS-Region Mit AWS Transform erstellte Ressourcen sind mit `gekennzeichnetCreatedBy: AWSTransform`, und Schreibvorgänge sind gegebenenfalls auf Ressourcen mit diesem Tag beschränkt.

Schritt 1: Sicherheitsausschluss überprüfen

Bevor der Workflow zur Containerisierung beginnt, präsentiert AWS Transform einen Sicherheitsausschluss, den Sie lesen und akzeptieren müssen.

Was der Haftungsausschluss abdeckt

Der Containerisierungsprozess erfordert Internetzugang, um Anwendungsabhängigkeiten herunterzuladen (z. B. Pakete aus öffentlichen Registern wie npm, PyPI oder Maven Central). Der Sicherheitsausschluss informiert Sie darüber, dass:

- Build-Umgebungen verfügen über ausgehenden Internetzugang, um die in der Build-Konfiguration Ihrer Anwendung angegebenen Abhängigkeiten aufzulösen und herunterzuladen.
- Sie sind dafür verantwortlich, die für Ihre Anwendung erforderlichen Abhängigkeiten zu überprüfen und sicherzustellen, dass sie den Sicherheitsrichtlinien Ihres Unternehmens entsprechen.
- Sie können optional private Abhängigkeitsquellen (wie AWS CodeArtifact Repositorys oder private Amazon ECR-Basis-Images) in einem späteren Schritt konfigurieren, um das Herunterladen aus öffentlichen Registern zu vermeiden.

Wichtige Informationen

Um den Sicherheitsausschluss zu lesen und zu akzeptieren

1. Lesen Sie den Sicherheitsausschluss, den AWS Transform präsentiert.
2. Akzeptieren Sie den Haftungsausschluss, um mit dem Workflow zur Containerisierung fortzufahren.

Nachdem Sie den Haftungsausschluss akzeptiert haben, fährt AWS Transform mit dem nächsten Schritt fort, in dem Sie Ihren Quellcode angeben.

Note

Die Connectorkonfiguration für AWS CodeConnections und Amazon ECR ist nicht mehr im Voraus erforderlich. AWS Transform fordert Sie auf, den Zugriff auf diese Services zu einem späteren Zeitpunkt im Workflow zu konfigurieren, und zwar nur bei Bedarf. Sie konfigurieren beispielsweise, CodeConnections wann Sie aus Git-Repositorys klonen möchten, und

Sie konfigurieren den Amazon ECR-Zugriff, wenn Sie bereit sind, Container-Images zu veröffentlichen.

Schritt 2: Quellcode klonen

In diesem Schritt stellen Sie den Quellcode Ihrer Anwendung für AWS Transform bereit. Sie können Quellcode aus Git-Repositorys oder durch Hochladen von ZIP-Dateien bereitstellen.

Option 1: Git-Repositoryn

Sie können Ihren Quellcode aus Git-Repositorys bereitstellen. Wenn Sie noch nicht konfiguriert haben AWS CodeConnections, fordert AWS Transform Sie zu diesem Zeitpunkt auf, Ihren CodeConnections ARN anzugeben. Sie haben zwei Möglichkeiten, Ihre Repositorys anzugeben:

- Laden Sie eine CSV-Datei hoch — Bereiten Sie eine CSV-Datei mit Spalten `repo_name` und `branch` vor. Das `repo_name` muss im `owner/repo-name` Format sein. Die `branch` Spalte ist optional. Lassen Sie sie leer, um den Standardzweig des Repositorys zu verwenden. Beispiel:

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- Geben Sie Repository-Details im Chat an — Teilen Sie AWS Transform die Repository-Namen und Branches direkt im Chat mit, anstatt eine CSV-Datei hochzuladen.

AWS Transform überprüft, ob jedes Repository existiert und über Ihre CodeConnections Konfiguration zugänglich ist, und klonet dann die Repositorys.

Note

Einzelne Dateien dürfen 1 GB nicht überschreiten, und die Gesamtgröße aller Repositorys darf 8 GB nicht überschreiten. AWS Transform klonet mehrere Repositorys gleichzeitig, um die Verarbeitung zu beschleunigen.

 Important

Anwendungen, die sich über mehrere Repositorys erstrecken, werden über die Git-Clone-Option nicht unterstützt. Wenn deine Anwendung Quellcode aus mehreren Repositorys benötigt, packe sie zusammen als Zip-Datei und verwende stattdessen die Zip-Upload-Option.

Option 2: Hochladen einer Zip-Datei

Wenn Sie Ihren Quellcode nicht konfiguriert CodeConnections haben oder lieber direkt hochladen möchten, können Sie ZIP-Dateien hochladen.

Um Quellcode als Zip-Dateien hochzuladen

1. Wenn Sie dazu aufgefordert werden, laden Sie eine ZIP-Datei pro Anwendung hoch. Sie können Dateien in den Chat ziehen oder die Schaltfläche zum Anhängen verwenden.
2. Jede Zip-Datei sollte den Quellcode für eine Anwendung enthalten.
3. Einzelne Dateien dürfen 1 GB nicht überschreiten, und die Gesamtgröße aller Uploads darf 8 GB nicht überschreiten.

Optional: Konfigurieren Sie private Abhängigkeiten

Wenn Ihre Anwendung von Paketen aus privaten Registern abhängt, können Sie in diesem Schritt private Abhängigkeitsquellen konfigurieren. AWS Transform unterstützt die folgenden privaten Abhängigkeitstypen:

- **AWS CodeArtifact Repositorys** — Konfigurieren Sie Maven-, PyPI- oder NPM-Repositorys, die in gehostet werden. AWS CodeArtifact AWS Transform präsentiert eine Liste der verfügbaren Repositorys in Ihrem Konto, aus der Sie auswählen können.
- **Private Amazon ECR-Basis-Images** — Wenn Ihre Dockerfiles Basis-Images aus einem privaten Amazon ECR-Repository verwenden, geben Sie die Repository-Details an, damit die Build-Umgebung diese Images abrufen kann.

Wenn Sie private Abhängigkeiten konfigurieren, fordert AWS Transform Sie auf, eine Verbindung zu dem Ort herzustellen, an AWS-Konto dem diese Ressourcen gehostet werden. Diese Connectorkonfiguration ist nur erforderlich, wenn Sie private Abhängigkeiten verwenden.

Bestätigung der Einstellungen für die Containerisierung

Sobald Ihr Quellcode verfügbar ist, fragt AWS Transform Sie, ob Sie spezifische Anweisungen dafür haben, wie die Containerisierung durchgeführt werden soll. Sie können optional Folgendes angeben:

- Ob ein neues Dockerfile generiert oder ein vorhandenes wiederverwendet werden soll.
- Ob ein bestimmter Service in einem Monorepo oder alle Services verarbeitet werden sollen.
- Alle anderen Einstellungen für den Containerisierungsprozess.

Die Standardwerte sind:

1. Verwenden Sie das Amazon Linux 2023-Basisimage (`public.ecr.aws/amazonlinux/amazonlinux:latest`).
2. Verarbeiten Sie alle Anwendungen im Repository.
3. Verwenden Sie ein vorhandenes Dockerfile, falls vorhanden, mit geringfügigen Änderungen, falls erforderlich.

Sie können bestätigen, dass Sie mit den Standardeinstellungen fortfahren möchten, oder spezifische Anweisungen geben.

Schritt 3: Containerisieren

In diesem Schritt analysiert der AWS Transform AI-Agent Ihren Anwendungsquellcode und generiert Docker-Artefakte. AWS Transform untersucht die Struktur, Abhängigkeiten und Laufzeitanforderungen Ihrer Anwendung, um entsprechende Dockerfiles und zugehörige Konfigurationsdateien zu erstellen.

Was passiert bei der Containerisierung

Der Containerisierungs-Agent führt die folgenden Aufgaben aus:

1. Quellcode-Analyse — AWS Transform untersucht die Projektdateien, Abhängigkeiten, Build-Konfiguration und Laufzeitanforderungen Ihrer Anwendung. AWS Transform ersetzt außerdem hartcodierte Werte (wie Datenbank-IP-Adressen oder DNS-Namen), identifiziert Umgebungsvariablen, erkennt Volumes und versucht, Protokolle zur Standardausgabe umzuleiten.
2. Dockerfile-Generierung — Basierend auf der Analyse generiert AWS Transform ein Dockerfile, das auf Ihre Anwendung zugeschnitten ist.

3. Container-Image erstellen und testen — AWS Transform erstellt das Container-Image und führt einen Test durch, um zu überprüfen, ob das Dockerfile ein funktionierendes Image erzeugt. Wenn der Build fehlschlägt, iteriert AWS Transform automatisch auf dem Dockerfile.
4. Sicherheitsanalyse — AWS Transform durchsucht die generierten Artefakte nach fest codierten Werten wie Anmeldeinformationen, API-Schlüsseln oder anderen sensiblen Daten und markiert alle Ergebnisse zur Überprüfung durch Sie.

Wenn Sie mehrere Repositorys oder ein Monorepo mit mehreren Diensten bereitgestellt haben, werden die einzelnen Dienste parallel verarbeitet.

Unterstützte Anwendungstypen

AWS Transform unterstützt die Containerisierung der folgenden Anwendungstypen:

- .NET 7 und höher — Optimierte Containerisierung für .NET-Anwendungen, die auf Version 7 oder höher ausgeführt werden.
- Allgemeine Anwendungen — Containerisierung für Anwendungen, die mit einer beliebigen Sprache oder einem beliebigen Framework erstellt wurden, einschließlich Java, Python Node.js, Go und anderen.
- Nicht unterstützte Anwendungen — Windows, Xcode oder andere proprietäre Build-Umgebungen werden nicht unterstützt.

Wichtige Informationen

Dieser Schritt wird automatisch ausgeführt. AWS Transform zeigt Fortschrittsaktualisierungen an, während es jede Anwendung analysiert und containerisiert. Wenn AWS Transform auf Probleme stößt, werden Sie möglicherweise um Erläuterungen oder zusätzliche Informationen gebeten.

Wenn die Containerisierung abgeschlossen ist, fährt AWS Transform mit dem nächsten Schritt fort, in dem Sie die generierten Artefakte überprüfen. Die Ausgaben werden im Artifact Store gespeichert.

Schritt 4: Docker-Artefakte und Codeänderungen überprüfen

In diesem Schritt überprüfen Sie die Docker-Artefakte und Codeänderungen, die AWS Transform während der Containerisierung generiert hat.

Änderungen aus Git-Repositorys überprüfen

Wenn Sie Quellcode aus Git-Repositorys bereitgestellt haben, überträgt AWS Transform die Änderungen an der Containerisierung in einem neuen Branch in jedem Repository. Wenn Sie mehrere Repositorys haben, präsentiert AWS Transform alle Änderungen als Batch zur konsolidierten Überprüfung.

Um Änderungen zu überprüfen und zu genehmigen

1. Überprüfen Sie die Code-Diff-Links, die AWS Transform bereitstellt. Jeder Unterschied zeigt alle Dateien, die hinzugefügt oder geändert wurden, einschließlich Docker-Dateien, Konfigurationsdateien und aller Änderungen am Quellcode.
2. Wenn AWS Transform das Genehmigungsdialogfeld anzeigt, können Sie die Änderungen genehmigen oder ablehnen. Bei mehreren Repositorys genehmigen Sie alle Änderungen in einem einzigen Batch-Vorgang.
3. Wenn Sie zustimmen, überträgt AWS Transform die Änderungen an die neuen Branches in Ihren Repositorys.
4. Bestätigen Sie, dass Sie bereit sind, mit dem nächsten Schritt fortzufahren.

Änderungen aus ZIP-Uploads überprüfen

Wenn Sie den Quellcode als Zip-Dateien hochgeladen haben, stellt AWS Transform Download-Links für die containerisierten Artefakte bereit. Laden Sie die Artefakte herunter und überprüfen Sie sie, einschließlich der generierten Docker-Dateien und aller Änderungen am Quellcode.

Änderungen anfordern

Wenn die generierten Artefakte geändert werden müssen, können Sie Feedback geben, damit AWS Transform den Schritt zur Containerisierung mit Ihren aktualisierten Anweisungen neu startet und neue Artefakte zur Überprüfung generiert.

Schritt 5: Bilder veröffentlichen

In diesem Schritt veröffentlicht AWS Transform Ihre Container-Images in Amazon Elastic Container Registry. Wenn Sie den Amazon ECR-Zugriff noch nicht konfiguriert haben, fordert AWS Transform Sie zu diesem Zeitpunkt auf, Ihre Amazon ECR-Repository-Details anzugeben.

Was passiert beim Veröffentlichen

AWS Transform führt für jedes Container-Image die folgenden Aufgaben aus:

1. **Connector-Konfiguration** — Wenn Sie den Amazon ECR-Zugriff noch nicht konfiguriert haben, zeigt AWS Transform ein Connector-Formular an, in dem Sie Ihren Amazon ECR-Repository-ARN angeben und eine Verbindung zu Ihrem herstellen. AWS-Konto
2. **Genehmigungsanfrage** — AWS Transform präsentiert die Liste der zu veröffentlichenden Bilder und bittet Sie um Ihre Genehmigung. Sie können den Veröffentlichungsvorgang genehmigen oder ablehnen.
3. **Image-Push** — Nach der Genehmigung veröffentlicht AWS Transform die Container-Images in Ihrem Amazon ECR-Repository mithilfe von. Wenn Sie über mehrere Services verfügen, veröffentlicht AWS Transform alle Bilder in einem einzigen Batch-Vorgang.
4. **Scannen von Sicherheitslücken** — Amazon ECR scannt die veröffentlichten Bilder automatisch auf bekannte Sicherheitslücken. AWS Transform meldet die Scanergebnisse. Für eine umfassendere Analyse aktivieren Sie das erweiterte AWS ECR-Scannen und die AWS GuardDuty Laufzeitüberwachung.

Note

Die Veröffentlichung von Bildern erfolgt asynchron mit. Wenn Ihre Sitzung während der Veröffentlichung unterbrochen wird, stellt AWS Transform den Vorgang automatisch wieder her, wenn Sie die Verbindung wieder herstellen.

Wichtige Informationen

- Überprüfen Sie die Liste der Bilder, die veröffentlicht werden sollen.
- Genehmigen Sie den Veröffentlichungsvorgang oder lehnen Sie ihn ab. Wenn Sie ablehnen, überspringt AWS Transform die Veröffentlichung von Bildern und Sie können ohne veröffentlichte Bilder mit dem nächsten Schritt fortfahren.
- Überprüfen Sie nach Abschluss der Veröffentlichung die Ergebnisse der Schwachstellensuche.

Nach der Veröffentlichung stellt AWS Transform die Image-URLs bereit, die in den Schritten zur Bereitstellung der Infrastruktur verwendet werden.

Schritt 6: Infrastruktur als Code generieren

In diesem Schritt generiert AWS Transform AWS Infrastrukturvorlagen für die Bereitstellung Ihrer containerisierten Anwendung. Sie wählen zwischen Amazon Elastic Kubernetes Service und Amazon Elastic Container Service als Zielplattform.

Amazon Elastic Kubernetes Service (Kubernetes)

Wenn Sie sich für Amazon EKS entscheiden, generiert AWS Transform Helm-Diagramme mit Kubernetes-Manifesten für Ihre Anwendung. Zu den generierten Vorlagen gehören:

- Bereitstellungen und Dienste
- Regeln für den Zugriff
- ConfigMaps und Ressourcen SecretProviderClass
- Dienstkonten
- Dauerhafte Volumenansprüche (EBS und EFS)
- DNS-Einträge Route 53)
- Konfigurationen Health Integritätsprüfungen

Optional: CloudWatch Protokollierung

AWS Transform fragt, ob Sie die CloudWatch Protokollierung für Ihre Amazon EKS-Bereitstellung einbeziehen möchten. Wenn Sie sich dafür entscheiden, generiert AWS Transform eine Fluent DaemonSet Bit-Konfiguration, die Pod-Logs sammelt und sie an CloudWatch Logs versendet.

Wenn Sie sich für die CloudWatch Protokollierung entscheiden, muss Ihr Clusteradministrator vor der Bereitstellung die folgenden Voraussetzungen erfüllen:

1. Erstellen Sie den `amazon-cloudwatch` Namespace im Cluster.
2. Erstellen Sie eine IAM-Rolle für das Fluent Bit-Dienstkonto mit CloudWatch Logs-Schreibberechtigungen. Während der Bereitstellung werden Sie zur Eingabe des Rollen-ARN aufgefordert.

Amazon Elastic Container Service (Terraform)

Wenn Sie sich für Amazon ECS entscheiden, generiert AWS Transform Terraform-Module für die Bereitstellung Ihrer Anwendung. Zu den generierten Vorlagen gehören:

- ECS-Cluster
- ECS-Service mit Aufgabendefinitionen
- Application Load Balancer mit Zugriffsprotokollierung
- Amazon EFS für persistenten Speicher
- Private gehostete Zonen für die Serviceerkennung
- Konfigurationen Health Integritätsprüfungen

Automatisierte Validierung und Sicherheitsscans

AWS Transform validiert die generierten Infrastrukturvorlagen automatisch, bevor sie Ihnen präsentiert werden. Die Validierung umfasst Folgendes:

- Für Terraform: `terraform fmt` und `terraform validate` um die Richtigkeit von Syntax und Konfiguration zu überprüfen.
- Für Helm: Diagrammvalidierung, um zu überprüfen, ob die generierten Manifeste wohlgeformt sind.
- Sicherheitsscan mit Checkov zur Identifizierung potenzieller Sicherheitsfehlkonfigurationen im generierten Infrastrukturcode.

AWS Transform meldet alle Validierungsprobleme und behebt sie, bevor der Vorgang fortgesetzt wird.

IaC wird ohne veröffentlichte Bilder generiert

Sie können Infrastrukturvorlagen auch dann generieren, wenn Sie im vorherigen Schritt keine Container-Images veröffentlicht haben. Die generierten Vorlagen verwenden Platzhalter-Image-URIs, die Sie später mit Ihren tatsächlichen Image-Speicherorten aktualisieren können.

Wichtige Informationen

Um Infrastrukturvorlagen zu generieren

1. Wenn Sie dazu aufgefordert werden, wählen Sie Ihre Zielplattform aus: Amazon EKS oder Amazon ECS.
2. Wenn Sie Amazon EKS ausgewählt haben, fragt AWS Transform, ob die CloudWatch Protokollierung eingeschlossen werden soll. Antworten Sie mit Ja oder Nein.

3. Wenn Sie dazu aufgefordert werden, geben Sie Details zum Health Check-Endpoint für Ihre Anwendung an (z. B. einen `/health` Pfad).
4. AWS Transform generiert und validiert die Infrastrukturvorlagen. Dieser Schritt wird automatisch ausgeführt und AWS Transform zeigt Fortschrittsaktualisierungen an, einschließlich aller Überprüfungs- oder Sicherheitsscanergebnisse.
5. Überprüfen Sie die generierten Vorlagen, wenn AWS Transform sie präsentiert.

Schritt 7: Testinfrastruktur bereitstellen

In diesem Schritt stellt AWS Transform eine Testinfrastruktur bereit, sodass Sie Ihre containerisierte Anwendung vor der Produktionsumstellung validieren können.

Was passiert während der Testbereitstellung

AWS Transform stellt die im vorherigen Schritt generierten Infrastrukturvorlagen für Ihre AWS-Konto bereit. Für Amazon EKS-Bereitstellungen wird Helm verwendet. Für Amazon ECS-Bereitstellungen wird Terraform verwendet.

Vor der Bereitstellung zeigt AWS Transform ein Formular mit Infrastrukturwerten an, in dem Sie Bereitstellungsparameter wie Ressourcennamen, Anzahl der Replikate und umgebungsspezifische Einstellungen konfigurieren können. AWS Transform generiert außerdem eine Bereitstellungsvorschau, in der angezeigt wird, welche Ressourcen erstellt werden, sodass Sie die Änderungen überprüfen können, bevor Sie sie genehmigen.

Wichtige Informationen

Um die Testinfrastruktur bereitzustellen und zu validieren

1. Füllen Sie das Formular mit den Infrastrukturwerten mit Ihrer Bereitstellungskonfiguration aus. Das Formular enthält Parameter wie Clusternamen, Namespaces, Anzahl der Replikate und andere umgebungsspezifische Einstellungen.
2. Sehen Sie sich die Bereitstellungsvorschau an, in der die Ressourcen angezeigt werden, die erstellt oder geändert werden.
3. Genehmigen Sie die Infrastrukturbereitstellung, wenn AWS Transform sie anfordert.
4. Warten Sie, bis die Bereitstellung abgeschlossen ist. AWS Transform zeigt die Bereitstellungsergebnisse an.

5. Testen Sie Ihre bereitgestellte Anwendung, um sicherzustellen, dass sie in einem Container ordnungsgemäß ausgeführt wird und ob die Infrastruktur Ihren Anforderungen entspricht.
6. Teilen Sie AWS Transform mit, ob Sie mit der Bereitstellung zufrieden sind oder ob Sie die Infrastruktur ändern und erneut bereitstellen möchten.

Iteration an der Infrastruktur

Wenn Sie die Infrastrukturvorlagen ändern müssen, können Sie aktualisierte Vorlagen hochladen und erneut bereitstellen:

1. Teilen Sie AWS Transform mit, dass Sie den IaC ändern möchten.
2. Laden Sie eine ZIP-Datei hoch, die Ihre geänderten Infrastrukturvorlagen enthält.
3. AWS Transform ersetzt die Vorlagen und führt ein inkrementelles Update durch (Terraform Apply oder Helm Upgrade).
4. Überprüfen Sie die aktualisierten Bereitstellungsergebnisse.

Sie können diesen Zyklus wiederholen, bis Sie mit der Bereitstellung zufrieden sind.

Wiederherstellung der Sitzung

Infrastrukturbereitstellungen werden asynchron unter Verwendung von ausgeführt. Wenn Ihre Sitzung während einer Bereitstellung unterbrochen wird, stellt AWS Transform den Vorgang automatisch wieder her, wenn Sie die Verbindung wieder herstellen, und zeigt die Bereitstellungsergebnisse an.

Schritt 8: Testinfrastruktur bereinigen

Nach Abschluss der Validierung baut AWS Transform die Testinfrastruktur ab, um unnötige Kosten zu vermeiden.

Wichtige Informationen

Um die Testinfrastruktur zu bereinigen

1. AWS Transform informiert Sie darüber, dass die Testinfrastruktur abgerissen wird.
2. Genehmigen Sie den Löschvorgang, wenn AWS Transform ihn anfordert.
3. Warten Sie, bis die Bereinigung abgeschlossen ist. AWS Transform zeigt die Ergebnisse an, wenn alle Testressourcen entfernt wurden.

Bei Amazon ECS-Bereitstellungen entfernt dieser Schritt alle Ressourcen, die während der Testbereitstellung erstellt wurden, einschließlich Rechenressourcen, Load Balancer, Speicher und Netzwerkkomponenten.

Bei Amazon EKS-Bereitstellungen wird die Bereinigung je nach Bezeichnung auf Ihr spezifisches Projekt zugeschnitten. Nur Ressourcen, die für diesen Containerisierungs-Workflow gekennzeichnet sind, werden entfernt. Andere Workloads, die auf demselben Amazon EKS-Cluster ausgeführt werden, sind nicht betroffen.

Schritt 9: Implementieren Sie die Cutover-Infrastruktur

In diesem letzten Schritt stellt AWS Transform die fertige Infrastruktur für den Produktionseinsatz bereit. Bei der Umstellung werden dieselben Infrastrukturvorlagen verwendet, die Sie im Schritt der Testbereitstellung validiert haben.

Wichtige Informationen

Um die Cutover-Infrastruktur bereitzustellen

1. Füllen Sie das Formular mit den Infrastrukturwerten mit Ihrer Konfiguration für die Produktionsbereitstellung aus. Sie können die Parameter aus der Testbereitstellung anpassen oder dieselben Werte verwenden.
2. Sehen Sie sich die Bereitstellungsvorschau an, in der die Produktionsressourcen angezeigt werden, die erstellt werden.
3. Genehmigen Sie die Produktionsbereitstellung, wenn AWS Transform sie anfordert.
4. Warten Sie, bis die Bereitstellung abgeschlossen ist. AWS Transform zeigt die Ergebnisse der Cutover-Bereitstellung an.
5. Stellen Sie sicher, dass Ihre Anwendung in der Produktionsumgebung ordnungsgemäß ausgeführt wird.

Important

Überprüfen Sie die generierten Infrastrukturkonfigurationen mit Ihrem Team, um sicherzustellen, dass sie den Sicherheits-, Compliance- und Geschäftsanforderungen Ihres Unternehmens entsprechen. AWS Transform bietet zwar automatische

Konfigurationsempfehlungen, Sie sind jedoch dafür verantwortlich, die Einstellungen zu validieren und an Ihre Bedürfnisse anzupassen, bevor Sie mit der Umstellung fortfahren.

Wiederherstellung von Sitzungen

Produktionsbereitstellungen werden asynchron unter Verwendung von ausgeführt. Wenn Ihre Sitzung während der Bereitstellung unterbrochen wird, stellt AWS Transform den Vorgang automatisch wieder her, wenn Sie die Verbindung wieder herstellen, und zeigt die Bereitstellungsergebnisse an.

Modernisierung von Mainframe-Anwendungen

AWS Transform wurde entwickelt, um die Modernisierung älterer Mainframe-Anwendungen zu beschleunigen. Es orchestriert die Analyse von Mainframe-Codebasen, generiert Dokumentation, extrahiert Geschäftslogik, zerlegt monolithische Strukturen, transformiert veralteten Code und managt bei Bedarf den gesamten Prozess mit menschlichem Input (HITL). Die Transformationsfunktionen von AWS Transform für die Modernisierung und Migration von Mainframe-Anwendungen ermöglichen es Ihnen, Ihre kritischen Mainframe-Anwendungen schneller zu modernisieren und gleichzeitig Ihre geschäftskritische Logik während des gesamten Transformationsprozesses beizubehalten.

Topics

- [Funktionen und Hauptmerkmale](#)
- [High-level Komplettlösung](#)
- [Der Mensch ist auf dem Laufenden \(HITL\)](#)
- [Unterstützte Dateitypen für die Transformation von Mainframe-Anwendungen](#)
- [Unterstützte Regionen und Kontingente für AWS Transformieren Sie den Mainframe](#)
- [High-level Überblick über den Weg zur Mainframe-Modernisierung](#)
- [Transformation von Mainframe-Anwendungen](#)
- [Erstellen und implementieren Sie Ihre modernisierte Anwendung nach dem Refactoring](#)

Funktionen und Hauptmerkmale

AWS Transform bietet die folgenden Funktionen für die Mainframe-Modernisierung:

- Unterstützt die Modernisierung von z/OS Mainframe-Anwendungen, die in COBOL (Common Business-Oriented Language) und PL/I (Programming Language One) geschrieben wurden, mit zugehörigen JCL- (Job Control Language), CICS-Transaktionen (Customer Information Control System), BMS-Bildschirmen (Basic Mapping Support), Db2-Datenbanken und VSAM-Datendateien (Virtual Storage Access Method).
- Unterstützt das Refactoring von Fujitsu GS21-Mainframe-Anwendungen mit PSAM (Presentation Service Access Method), japanischen Zeichensätzen und NDB-Datendateien (Network Data Base).
- Führt zielgerichtete Überlegungen, Analysen, Zerlegung, Planung, Dokumentationserstellung und Code-Refactoring durch.

- Refaktoriert COBOL-based Mainframe-Workloads automatisch in moderne, Cloud-optimierte Java-Anwendungen.
- Orchestriert und integriert sich nahtlos in die zugrunde liegenden Tools, die Analyse, Dokumentation, Zerlegung, Planung und Code-Refactoring durchführen.
- Hilft Ihnen bei der Einrichtung von Cloud-Umgebungen für modernisierte Mainframe-Anwendungen, indem es gebrauchsfertige Infrastructure-as-Code (IaC) -Vorlagen bereitstellt.

High-level Komplettlösung

Hier finden Sie eine ausführliche Anleitung zu AWS Transform für die Modernisierung und Migration von Mainframe-Anwendungen.

1. Starten Sie einen Chat mit AWS Transform und geben Sie ein Ziel ein.
2. Auf der Grundlage Ihres Ziels schlägt AWS Transform einen Modernisierungsplan vor, der das übergeordnete Ziel in Zwischenschritte unterteilt.
3. Je nachdem, welches Ziel Sie angegeben haben, kann AWS Transform:
 - Die Codebasis bewerten und neu erfinden
 - Erstellen Sie einen benutzerdefinierten Job, der auf dem Ziel basiert

Unterwegs fordert AWS Transform möglicherweise Informationen von Ihnen an, um die Aufgaben auszuführen.

Note

Weitere Informationen zu den Refactoring-Funktionen von AWS Transform for Mainframe finden Sie unter [Projekt erstellen](#) in der Dokumentation AWS Transform for Mainframe Refactor.

Der Mensch ist auf dem Laufenden (HITL)

Während der Transformation von Mainframe-Anwendungen können Sie den Fortschritt und den Status der Transformationsaufgaben über die AWS Transform-Weboberfläche überwachen.

AWS Transform wird in den folgenden Szenarien zusätzliche Informationen von Ihnen einholen:

- Wenn zusätzliche Informationen zur Ausführung von Aufgaben benötigt werden.
- Wenn eine Genehmigung für Zwischenartefakte erforderlich ist (z. B. die Zerlegung von Domänen oder die Wellenplanung).
- Wenn Probleme auftreten, die AWS Transform nicht automatisch lösen kann.

Unterstützte Dateitypen für die Transformation von Mainframe-Anwendungen

Zu den unterstützten Dateitypen für z/OS gehören:

- COBOL-Artefakte und zugehörige CPY (Copybooks)
- PL/I Quelldateien
- JCL (Job Control Language) und JCL Procedure (PROC)
- CICS-Systemdefinition (CSD)
- BMS (Basic Mapping Support)
- Db2-Datenbanken
- VSAM (virtuelle Speicherzugriffsmethode)
- IMS TM (Transaktionsmanager)

Zu den unterstützten Dateitypen für Fujitsu GS21 gehören:

- PSAM (Zugriffsmethode für den Presentation Service)
- ADL (AIM-Definitionssprache)
- NDB (Netzwerkdatenbank)

Weitere Informationen zu Fujitsu GS21 finden Sie in den folgenden Themen im Migrationshandbuch AWS Transform for Mainframe:

- [GS21](#)
- [Aufnahme und Wiedergabe — GS21-Terminals](#)
- [Mainframe, AS400, Open VMS und GS21](#)

Unterstützte Regionen und Kontingente für AWS Transformieren Sie den Mainframe

Eine Liste der unterstützten Regionen finden Sie unter [Unterstützte Regionen für AWS Transform](#).

Note

Ihre Daten werden möglicherweise in einer anderen Region verarbeitet als in der Region, in der Sie AWS Transform verwenden. Informationen zur regionsübergreifenden Verarbeitung finden Sie unter [the section called “Cross-region Verarbeitung”](#).

Informationen zu den Kontingentgrenzen finden Sie unter [Kontingente](#).

High-level Überblick über den Weg zur Mainframe-Modernisierung

Die Modernisierung von Mainframe-Anwendungen erfolgt in der Regel in vier Phasen: (a) Bewertung, (b) Mobilisierung, (c) Migration und Modernisierung und (d) Betrieb, Optimierung und Innovation. AWS Jede dieser Phasen wird detailliert beschrieben und enthält Ziele und zugehörige Aktivitäten zur Unterstützung Ihrer Modernisierung.

Phasen

- [Phase 1: Beurteilen](#)
- [Phase 2: Mobilisieren](#)
- [Phase 3: Migration und Modernisierung](#)
- [Phase 4: Betrieb, Optimierung und Innovation](#)

Phase 1: Beurteilen

Ziel: Ihre Modernisierungsbereitschaft zu ermitteln und erste Modernisierungspläne zu entwickeln.

Mit AWS Transform können Sie Ihre Mainframe-Anwendungen, Infrastruktur und Betriebsabläufe bewerten, um den richtigen Modernisierungsansatz für Ihre Geschäftsanforderungen zu ermitteln.

 Note

Jede Phase enthält eine Liste aller möglichen Aktivitäten, die Sie bei der Modernisierung Ihrer Mainframe-Anwendung durchführen können. Sie können einige Aktivitäten überspringen, die nicht zu Ihrem Anwendungsfall oder Ihren Zielen passen.

Aktivitäten

- Beginnen Sie mit einem informellen Gespräch über die Modernisierung und arbeiten Sie an der Chancengleichheit, indem Sie die richtigen Personen ins Gespräch bringen
- Stellen Sie die Chancengleichheit
- Führen Sie beim ersten Gespräch eine Präsentation mit einem Plan zur Zuordnung der Anwendungsabhängigkeiten und der Anwendungsarchitektur durch
- Ermitteln Sie das ROM (grobe Größenordnung), das die Infrastrukturkosten während der Migration, die Kosten für die Migration, die Kosten für die Nachbearbeitung und die Projektdauer umfasst
- Schnelle Portfolioerkennung:
 - Führen Sie eine Bewertung von Mustern und Tools durch
 - Führen Sie eine Quellcode-Analyse durch
 - Identifizieren Sie Kandidaten für den Machbarkeitsnachweis (POC)
- Erstellen Sie Schulungen zur technischen Unterstützung:
 - Tage zum Eintauchen
 - Workshops mit allgemeinen Themen
- Erstellen Sie einen Bericht zur Bewertung der Migrationsfähigkeit (Migration Readiness Assessment, MRA) für große Mainframe-Modernisierungsprojekte oder Neukunden AWS
- Erstellen Sie eine Leistungsbeschreibung für die Mobilisierungsphase

Phase 2: Mobilisieren

Ziel: Schaffung einer Grundlage und Validierung des Ansatzes durch erfolgreiche Machbarkeitsstudien oder Pilotmodernisierungen.

In der Mobilisierungsphase können Sie die erforderlichen Frameworks, Tools und Prozesse einrichten, um die Mainframe-Modernisierung in großem Maßstab zu unterstützen.

Aktivitäten

- Starten Sie den Modernisierungsplan mit einem Pilotprojekt und dem identifizierten POC:
 - Analysieren Sie das Pilotprojekt und richten Sie den Code für die Modernisierung ein
 - Erstellen und testen Sie die modernisierten Pilotdaten
 - Liefern Sie Ergebnisse und überprüfen Sie das Pilotprojekt, um eine detaillierte Lösung für die umfassendere Datenmodernisierung zu entwickeln
- Für die Plattform:
 - Erstellen Sie einen Sicherheits-, Compliance- und Überwachungsplan
 - Richten Sie Landingzone-Umgebungen mit AWS Mainframe-Landezone und Kontostruktur ein
 - Bestimmen Sie Architektur, Infrastruktur, Anwendung, Integration und mehr
- Denken Sie an Menschen und Prozesse:
 - Das Cloud Center of Excellence ist eine gute Ressource
 - Betriebsmodell
- Erstellen Sie eine umfassende Portfolioanalyse für verschiedene Anwendungsszenarien:
 - Umfassende Recherche, einschließlich umfassender Dokumentation
 - Zerlegungsplan (für alle Anwendungen)
 - Muster- und Werkzeuganleitung für alle Anwendungen
 - Erstellen Sie einen ersten Modernisierungs- und Migrationsplan
- Erstellen Sie eine detaillierte Lösung unter Berücksichtigung von Pilotprojekt, Plattform, Mitarbeitern und Prozessen sowie einer umfassenden Portfolioanalyse
- Ermitteln Sie den Geschäftsszenario
- Erfolgreiches Pilotprojekt mit Lösung für die Leistungsbeschreibung für die nächste Phase abschließen

Phase 3: Migration und Modernisierung

Ziel: Abschluss der Modernisierung und Migration innerhalb des geplanten Zeitplans und Budgets.

Während dieser Phase können Sie Ihre Mainframe-Anwendungen und -Daten zu migrieren und zu modernisieren. AWS

Aktivitäten

- Weisen Sie dem produktionsbereiten Anwendungscode Ressourcen zu
- Überprüfen und analysieren Sie den Entwurf anhand der vorhandenen Dokumentation oder durch Befragung von Fachexperten (KMU)
- Definieren Sie Testszenarien
- Richten Sie Modernisierungsumgebungen mit geeigneter Laufzeit, Datenbanken und Software von Drittanbietern ein
- Migrieren und modernisieren Sie Quellcode und Daten:
 - Sie können Ihre Anwendung iterativ auf der Grundlage von Geschäftsdomänen in der Anwendungscodebasis modernisieren
 - Skalieren Sie Modernisierungsumgebungen nach Bedarf, um Ihre Modernisierungs-Workloads zu unterstützen
- Richten Sie eine Pipeline CI/CD (kontinuierliche Integration, kontinuierliche Bereitstellung) ein
- Migrieren Sie ausgewählte Workloads, um Ihre Modernisierung einzuleiten.
- Übertragen Sie Anwendungsprogramme und passen Sie die Umgebungsskalierung nach Bedarf an:
 - Sie können die Umgebungen je nach Bedarf nach oben oder unten skalieren
 - Modernisieren Sie Arbeitspakete, indem Sie Tests zur Überprüfung der Codequalität ausführen
 - Synchronisieren Sie bei Bedarf erneut mit dem Quellcode
- Führen Sie umfassende Tests durch und überprüfen Sie Ihre Migration:
 - Sammeln Sie anfängliche Zustandsdaten
 - Zeichnen Sie Testszenarien auf dem Mainframe auf
 - Umgebung, Anwendung und Daten in der Phase
 - Führen Sie Testszenarien in der Cloud aus
 - Vergleichen Sie Quell- und Zieltestergebnisse
 - Erstellen Sie automatisierte Pipelines zur Ausführung von Testszenarien
 - Generieren Sie KPIs und Berichte
- Validieren Sie Ihre Daten für die Produktionseinrichtung
- Bestätigen Sie Ihren Fortschritt, indem Sie:
 - Durchführung von Integrations- und Systemtests
 - Durchführung von Leistungstests

- Benutzerakzeptanztests werden ausgeführt
- HA/DR Tests werden ausgeführt
- Definieren Sie mit dem Eigentümer der Anwendung einen Plan für die Einführung und erstellen Sie einen Plan für Schulung und Wissenstransfer
- Überlegen Sie sich die Umstellung und führen Sie Produktionsumstellungen durch
- Sorgen Sie für eine nachhaltige Unterstützung für Aktivitäten nach der Produktion wie Betrieb, Überwachung, Kapazitätsplanung und Gewährleistung von Anwendungsfunktionen

Phase 4: Betrieb, Optimierung und Innovation

Ziel: Förderung der betrieblichen Exzellenz und der kontinuierlichen Verbesserung modernisierter Anwendungen.

Nach der Modernisierung können Sie die Leistung, Sicherheit und Kosten Ihrer Anwendungen optimieren und gleichzeitig Services für Innovationen nutzen AWS .

Aktivitäten

- Überwachen Sie die Anwendung auf:
 - Leistungsmetriken
 - Sicherheitspraktiken
 - Richtlinien zur Einhaltung von Vorschriften
 - Kosten
- Einzelheiten protokollieren
- Anwendungsvorgänge verwalten:
 - Verwaltung der Infrastruktur
 - Transaktionen und Auftragsverwaltung
 - Unterstützung für Laufzeitumgebungen
- Optimierung und Modernisierung von Anwendungen
- Anwendungsentwicklung und Wartung:
 - Codierung (IDE)
 - Entwicklung
 - Integration

- Testen
- Bereitstellung

Transformation von Mainframe-Anwendungen

AWS Transform beschleunigt die Transformation Ihrer Mainframe-Modernisierungsanwendungen. In diesem Thema werden die verfügbaren Funktionen beschrieben.

Topics

- [Voraussetzung: Bereiten Sie die Projekteingaben in S3 vor](#)
- [Sammlung von Mainframe-Quellartefakten](#)
- [Sign-in und erstelle einen Job](#)
- [Den Fortschritt der Transformation verfolgen](#)
- [Richten Sie einen Konnektor ein](#)
- [Beurteilen und überdenken Sie den Stellenplan](#)
- [Stellen Sie sich den Jobplan neu vor](#)
- [Benutzerdefinierter Jobplan](#)

Voraussetzung: Bereiten Sie die Projekteingaben in S3 vor

AWS Transform ist in der Lage, komplexe Mainframe-Codebasen zu verarbeiten. Um die Codebasis zu verwenden, stellen Sie sicher, dass Sie alle Ressourcen an Ihrem S3-Standort haben.

Wichtige Projekteingaben:

- **Quellcode:** Sie müssen Ihre Mainframe-Quellcodedateien auf S3 hochladen. Dazu gehören COBOL-Programme, JCL-Skripte, Copybooks und alle anderen relevanten Quelldateien.
- **Datendateien:** Wenn Sie über VSAM-Dateien oder andere Datendateien verfügen, die Ihre Mainframe-Anwendungen verwenden, müssen diese auf S3 hochgeladen werden.
- **Konfigurationsdateien:** Schließen Sie Konfigurationsdateien ein, die für Ihre Mainframe-Umgebung spezifisch sind.

Andere Projekteingaben

- **SMF-Datensätze (System Management Facility):** Laden Sie gegebenenfalls SMF-Datensätze in einen neuen Ordner im S3-Bucket hoch, in dem der Quellcode gespeichert ist. Diese Datensätze sollten im ZIP-Dateiformat vorliegen.
- **Formatierung:** Für die Generierung der technischen Dokumentation können Sie eine optionale Konfigurationsdatei verwenden, um PDF-Dokumente zu generieren, die Ihren erforderlichen Formaten und Standards entsprechen, einschließlich Kopf- und Fußzeilen, Logos und benutzerdefinierten Informationen.
- **Glossar:** AWS Transform nutzt Automatisierung mit generativer KI für die Dokumentationserstellung und die Extraktion von Geschäftsregeln. Das Hinzufügen einer Glossar-CSV-Datei mit Informationen zu wichtigen Abkürzungen und Terminologien in das Stammverzeichnis Ihrer ZIP-Datei trägt zur Verbesserung der Qualität der generierten Dokumentation bei.
- **Testdaten:** Laden Sie, falls verfügbar, Testdatensätze hoch, die zur Validierung der modernisierten Anwendung verwendet werden können. Diese Daten sollten in einem neuen Ordner im S3-Bucket gespeichert werden, in dem der Quellcode gespeichert ist.

Einzelheiten zu den Projekteingaben finden Sie [hier](#).

Sammlung von Mainframe-Quellartefakten

In diesem Thema wird der Prozess zur Erfassung von Mainframe-Quellcode und zugehörigen Artefakten zur Unterstützung von Mainframe-Modernisierungsinitiativen mithilfe von Transform beschrieben. AWS Die korrekte Erfassung und Aufbereitung von Quelltextartefakten ist entscheidend für eine erfolgreiche Analyse, Migrationsplanung und Implementierung.

Inventar des Quellcodes

Typen des Anwendungsquellcodes

Die folgenden Quellcodetypen für Anwendungen werden unterstützt:

- COBOL-Programme
- JCL-Skripte
- Assembler-Programme
- PL/I Programme
- CICS-Transaktionen
- Natürliche Programme

- REXX-Skripte
- Easytrieve-Programme
- Copybooks und beinhaltet
- Proc-Bibliotheken

Datenbank-Assets

Die folgenden Datenbankressourcen werden unterstützt:

- DB2, DCLGEN- und DDL-Skripts.
- IMS-Datenbankdefinitionen (PSBs und DBDs)
- VSAM-Dateideinitionen
- Physikalische und logische Datenbankschemas
- Datenbankprozeduren und Trigger

Dateierweiterungen im Quellcode

Wenn Sie sich der Erweiterung nicht sicher sind, lassen Sie sie leer oder .txt und AWS Transform klassifiziert sie für Sie.

In der folgenden Tabelle sind gängige Dateierweiterungen für Mainframe-Quellartefakte aufgeführt.

Mainframe-Quellcode-Dateierweiterungen

Language/Type	Allgemeine Erweiterungen	Description
COBOL	.cbl, .cob, .cobol	COBOL-Quellprogramme
JCL	.jcl	Skripte in der Job-Control-Sprache
Assembler	.asm	Programme in Assembler-Sprache
PL/I	.pl1	PL/I Sprachprogramme
CICS-Definition	.csd	CICS-Systemdefinition (CSD)
Natürlich	.nat	Natürliche Programme

Language/Type	Allgemeine Erweiterungen	Description
REXX	.rex, .rexx	REXX-Skripte
Einfach abrufen	.ezt	Easytrieve-Berichtsprogramme
Bücher kopieren	.cpy	COBOL-Copybooks
BMS	.bms	Grundlegende Mapping-Unterstützung (BMS)
PL/I Copybooks	.pl1_kopieren	PL/I Copybooks
Db2 DCLGEN	.dcl	Generator für Db2-Deklarationen
Db2-Definition	.sql, .ddl	Db2-Datenbankdefinitionen
IMS-Definition	.ims	Datensatz zur IMS-Ressourcendefinition (IMS-Stufe 1)
MFS	.mfs	IMS MFS (Nachrichtenformatdienst)
PSB	.psb	IMS PSB (Programmspezifikationsblock)
DBD	.dbd	IMS-Datenbankdefinitionen
JCL Proc	.prc, .proc	JCL-Prozedurbibliotheken
JCL beinhaltet	.inc	JCL-Dateien einbeziehen
Makros	.mac	Assembler-Makros
Steuerkarten	.ctl	JCL Utility-Steuerkarten

Methoden zur Erfassung

Extraktion des Quellcodes

Verwenden Sie sichere FTP-Clients (WinSCP/FileZilla) für die interaktive Quellcode-Extraktion aus Mainframe-PDS-Bibliotheken.

Extraktion des DB2-Schemas

Die DB2 LUW-Clientsoftware (Linux, UNIX und Windows) enthält das db2look Hilfsprogramm als Teil des Installationspakets. Das db2look Hilfsprogramm extrahiert DDL-Anweisungen (Data Definition Language) aus einer DB2-Datenbank.

Führen Sie den folgenden Befehl aus:

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg  
-o DATABASE_NAME.sql
```

In der folgenden Liste werden die Parameter beschrieben:

- -d *DATABASE_NAME*: Gibt den Namen der Datenbank an, aus der das Schema extrahiert werden soll
- -i *userid*: Benutzer-ID für die Datenbankauthentifizierung
- -w *password*: Passwort für die Datenbankauthentifizierung
- -a: Extrahiert Autorisierungsinformationen (Zuschüsse)
- -e: Extrahiert alle Datenbankobjekte (Tabellen, Ansichten, Indizes usw.)
- -m: Extrahiert Statistiken und physikalische Eigenschaften
- -l: Extrahiert Tabellen- und Spaltenkommentare
- -x: Extrakte erklären Tabellen
- -f: Formatiert die Ausgabe für eine bessere Lesbarkeit
- -createdb: Beinhaltet Anweisungen zur Datenbankerstellung
- -printdbcfg: Beinhaltet Datenbankkonfigurationsparameter
- -o *DATABASE_NAME*.sql: Gibt den Namen der Ausgabedatei an

Extrahieren von Kataloginformationen aus dem Mainframe

Der Befehl LISTCAT in IDCAMS ist ein Hilfsprogramm zum Abrufen von Kataloginformationen über Datensätze auf dem Mainframe. Dies ist bei Mainframe-Modernisierungsprojekten nützlich, um Datensätze zu inventarisieren und ihre Eigenschaften zu verstehen.

```
//LSTCATJ JOB 'LISTCAT',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID  
//*  
//STEP1 EXEC PGM=IDCAMS  
//*
```

```
//SYSPRINT DD DSN=AWS.M2.CATALOG.LIST,
//          DISP=(NEW,CATLG,DELETE),
//          SPACE=(CYL,(1,1),RLSE),
//          DCB=(RECFM=FBA,LRECL=133,BLKSIZE=0)
//*
//SYSIN DD *
  LISTCAT ENT('AWS.M2.CARDDEMO.*') ALL
  LISTCAT ENT('SYS1.*') ALL
/*
```

Extrahieren von CICS-Definitionen

Das IBM-provided DFHCSDUP-Hilfsprogramm kann CICS-Ressourcendefinitionen aus der CICS-Systemdefinitionsdatei (CSD) extrahieren.

Verwenden Sie die folgende JCL, um bestehende Definitionen aus dem DFHCSD zu entladen:

```
//CSDXTJ JOB 'EXTRACT CSD',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=DFHCSDUP,REGION=0M,
//          PARM='CSD(READONLY),PAGESIZE(60),NOCOMPAT'
//*
//STEPLIB DD DSN=your-hlq.SDFHLOAD,DISP=SHR
//DFHCSD DD DSN=your-hlq.DFHCSD,DISP=SHR
//*
//CBDOUT DD DSN=your-hlq.CSD,
//          DISP=(NEW,CATLG,DELETE),
//          SPACE=(CYL,(1,1),RLSE),
//          DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  EXTRACT GROUP(cics-group) USERPROGRAM(DFH0CBDC) OBJECTS
/*
```

IMS-Definitionen werden extrahiert

Um IMS-Definitionen zu extrahieren, können Sie die IMS-Transaktionsdatei mit dem Hilfsprogramm DFSURDD0 generieren. Dieses Tool erstellt Makroanweisungen der Phase 1, die Sie für Migrationszwecke verwenden können. Derzeit wird nur IMS Stage 1 unterstützt.

Verwenden Sie die folgende JCL, um IMS-Definitionen zu extrahieren:

```
//IMSEXTJ JOB 'IMS STAGE 1',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
```

```

/**
//STEP1 EXEC PGM=DFSURDD0,MEMLIMIT=12G
/**
//STEPLIB DD DISP=SHR,DSN=your-hlq.SDFSRESL
/**
//RDDSDSN DD DISP=SHR,DSN=your-rdds
/**
//SYSOUT DD DSN=your-hlq.STAGE1.IMS,
//          DISP=(NEW,CATLG,DELETE),
//          SPACE=(CYL,(1,1),RLSE),
//          DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
        OUTPUT=MAC
/*

```

Scheduler-Informationen werden extrahiert CA-7

CA-7 Informationen zum Jobplan sind in LJOB-Berichten enthalten. Verwenden Sie das LJOB-Hilfsprogramm mit dem LIST=NODD Parameter, um die Berichte auf dem Mainframe zu generieren. Die Berichte müssen eine .ca7 Erweiterung haben. Jeder Bericht muss in Spalte 1 ANSI-Wagenkontrollzeichen enthalten. Sie können einen Bericht mit Wagensteuerzeichen in Spalte 1 erstellen, indem Sie in der JCL, die zur Ausführung des Dienstprogramms LJOB verwendet wird, den Wert DCB=RECFM=FBA (oder FA) angeben.

Beispiel: LJOB, JOB=ZBN*, LIST=ALL

Weitere Informationen finden Sie in der [Broadcom-Dokumentation](#).

Extrahieren von SMF-Daten

SMF-Datensätze (System Management Facility) enthalten Aktivitätsmetriken, die von Transform verwendet werden, um die AWS Nutzung von Batch-Jobs und CICS-Transaktionen zu analysieren. Die folgenden SMF-Datensatztypen werden unterstützt: 14, 15, 30 (Untertyp 5), 64, 102, 110 (Untertyp 1 mit Datenklasse 1, 3 und 4).

Formatanforderungen für SMF-Datensätze:

- Muss die Datensatztypen 30 und 110 (mindestens) enthalten
- Muss im rohen binären EBCDIC-Format vorliegen und RDW-Bytes (Record Descriptor Word) enthalten
- Muss in einem der folgenden Formate angegeben werden:

- Eine Datei mit bis zu 600 MB, komprimiert im ZIP-Format
- Eine Datei mit bis zu 5 GB, komprimiert im Format.tar.gz oder .gz
- Muss in einem separaten Ordner von Ihrem Quellcode in Amazon S3 gespeichert werden

Stellen Sie SMF-Aufzeichnungen für mindestens 13 Monate bereit, um jährliche Chargenzyklen und saisonale Muster zu erfassen, die in kürzeren Zeiträumen möglicherweise übersehen werden.

Option 1: Extrahieren und sortieren Sie SMF-Datensätze

Verwenden Sie die folgende JCL-Beispieldatei, um SMF-Datensätze zu extrahieren und zu sortieren:

```
//SMFEXTR JOB (ACCT),'EXTRACT SMF',CLASS=A,
//          MSGCLASS=X,NOTIFY=&SYSUID
//*-----*
/** SMF RECORD EXTRACTION TEMPLATE
/** CUSTOMIZE: Job card, dataset names, date range, record types
/**-----*
/**
/** STEP 1: EXTRACT SMF RECORDS
/**
//EXTRACT EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
/**
/** INPUT: Specify your SMF datasets (MAN files or GDG)
/**
//DUMPIN DD DISP=SHR,DSN=SYS1.MAN1
//        DD DISP=SHR,DSN=SYS1.MAN2
//        DD DISP=SHR,DSN=SYS1.MAN3
/**
/** OUTPUT: Extracted SMF records
/**
//DUMPOUT DD DSN=your.hlq.SMF.EXTRACT,
//          DISP=(NEW,CATLG,DELETE),
//          UNIT=SYSDA,
//          SPACE=(CYL,(500,100),RLSE),
//          DCB=(RECFM=VBS,LRECL=32760,BLKSIZE=27998)
/**
/** CONTROL CARDS
/**
//SYSIN DD *
//          INDD(DUMPIN,OPTIONS(DUMP))
//          OUTDD(DUMPOUT,TYPE(14,15,30,110))
```

```

DATE(yyyy/ddd,yyyy/ddd)
START(0000)
END(2359)
/*
/**
/** STEP 2: SORT EXTRACTED RECORDS (OPTIONAL)
/**
//SORT      EXEC PGM=SORT
//SORTIN    DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT   DD DSN=your.hlq.SMF.SORTED,
//           DISP=(NEW,CATLG,DELETE),
//           UNIT=SYSDA,
//           SPACE=(CYL,(500,100),RLSE),
//           DCB=(RECFM=VBS,LRECL=32760)
//SORTWK01  DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK02  DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK03  DD UNIT=SYSDA,SPACE=(CYL,(50))
//SYSOUT    DD SYSOUT=*
//SYSPRINT  DD SYSOUT=*
//SYSIN     DD *
        SORT FIELDS=(11,4,CH,A,7,4,CH,A,15,4,CH,A),EQUALS
/*

```

Passen Sie die folgenden Werte in der vorherigen JCL an:

1. Jobkarte: Konto, Klasse und Nachrichtenklasse aktualisieren
2. DUMPIN: Zeigen Sie auf Ihre SMF-Datensätze
3. DUMPOUT: Geben Sie den Namen des Ausgabedatensatzes und HLQ an
4. TYP: Wählen Sie Datensatztypen aus (14, 15, 30, 110 oder andere)
5. DATUM: Format yyyy/ddd (zum Beispiel 2026/055,2026/056)
6. LEERTASTE: Passen Sie es auf der Grundlage des erwarteten Datenvolumens an
7. Entfernen Sie den SORT-Schritt, falls er nicht benötigt wird

Option 2: Extrahieren Sie SMF-Daten mit DFSORT

Sie können DFSORT verwenden, um historische SMF-Daten zu konsolidieren und zu melden. Dies ist hilfreich, wenn Sie Ihre SMF-Datensätze in einem GDG nach Tag oder Woche speichern. Der folgende Job verwendet DFSORT, um SMF-Datensätze aus der SORTIN-Datei zu konsolidieren und auf der Grundlage der im INCLUDE COND-Parameter angegebenen Datensätze zu filtern.

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=S,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//SORTJES2 EXEC PGM=SORT,REGION=0M
//SYSOUT DD SYSOUT=*
//SORTMSG DD SYSOUT=*
//SORTIN DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT DD DSN=your.hlq.SMF.OUTPUT,
// DISP=(MOD,CATLG,DELETE),
// DCB=(BUFNO=20,
// RECFM=VBS,LRECL=32760,BLKSIZE=27998),
// SPACE=(CYL,(1400,900),RLSE)
//SORTWK1 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK2 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK3 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK4 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SYSIN DD *
OPTION COPY
INCLUDE COND=(6,1,BI,EQ,X'0E',OR,6,1,BI,EQ,X'0F',OR,
6,1,BI,EQ,X'1E',OR,6,1,BI,EQ,X'40',OR,
6,1,BI,EQ,X'50',OR,6,1,BI,EQ,X'59',OR,
6,1,BI,EQ,X'5C',OR,6,1,BI,EQ,X'65',OR,
6,1,BI,EQ,X'66',OR,6,1,BI,EQ,X'6E')
```

Um die Daten herunterzuladen und gleichzeitig die RDW-Daten beizubehalten, können Sie einen FTP-Server verwenden, um die extrahierte Datei zu empfangen. Stellen Sie sicher, dass die Daten im Binärformat übertragen werden und dass die RDW-Option verwendet wird, damit das RDW in der Datenübertragung enthalten ist. Der folgende Job zeigt ein Beispiel für einen FTP-Job zum Übertragen dieser Datei.

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=A,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//STEP1 EXEC PGM=FTP,REGION=2048K
//SYSIN DD *
10.10.10.10
userid
password
type i
LOCSITE RDW
put 'your.hlq.SMF.OUTPUT' SMFREQS.SMF
quit
```

SCRT-Bericht wird hochgeladen

Sie können auch einen SCRT-Bericht (Sub-Capacity Reporting Tool) in Transform hochladen. AWS

Hochladen des Anwendungsinventars

Nachdem Sie alle Artefakte gesammelt haben, führen Sie die folgenden Schritte aus:

1. Organisieren Sie Dateien nach Artefakttyp in Unterordnern (z. B. /cobol, /jcl, /copybooks, /db2, /ims, /cics, /ca7).
2. Komprimieren Sie den Ordner der obersten Ebene in eine einzige ZIP-Datei.
3. Laden Sie die ZIP-Datei in den Amazon S3 S3-Bucket hoch, der mit Ihrem AWS Transform-Workspace verbunden ist.

Note

SMF-Datensätze müssen in einem von Ihrem Quellcode getrennten Ordner innerhalb des Amazon S3 S3-Buckets gespeichert werden und müssen im Format.tar.gz oder .gz vorliegen.

Eine ausführliche Anleitung zum Verbinden Ihres Amazon S3 S3-Buckets mit AWS Transform finden Sie unter [the section called “Richten Sie einen Konnektor ein”](#).

Sign-in und erstelle einen Job

Folgen Sie allen Anweisungen im [Erste Schritte mit AWS Transformieren](#) Abschnitt der Dokumentation, um sich für das AWS Transform-Weberlebnis anzumelden.

Um einen Job zu erstellen und zu starten: Folgen Sie den Schritten unter [Starten Sie Ihr Projekt](#).

Workspace erstellen: Benenne und beschreibe deinen Workspace, in dem Jobs, Mitarbeiter und zugehörige Artefakte gespeichert werden.

Job erstellen: Erstelle einen Job, indem du aus vorkonfigurierten Jobplänen auswählst, oder passe den Jobplan an dein Ziel an, indem du aus der Liste der unterstützten Funktionen auswählst.

Important

AWS Transform lehnt Operationen von Ihnen ab, wenn Sie nicht über die entsprechenden Berechtigungen verfügen. Ein Mitwirkender kann beispielsweise eine Job-Transformation von

Mainframe-Anwendungen nicht abbrechen oder einen Job löschen. Nur ein Administrator kann diese Funktionen ausführen.

Wenn Sie Ihren Job erstellen, können Sie aus den folgenden Funktionen wählen. Der Kickoff-Schritt ist jedoch immer erforderlich, da sich dort der Quellcode für das Projekt befindet. Beim ersten Job, der in einem Workspace eingerichtet wurde, müssen Sie einen Connector zu Ihrem Amazon S3 S3-Bucket einrichten.

Den Fortschritt der Transformation verfolgen

Sie können den Fortschritt der Transformation während des gesamten Prozesses auf zwei Arten verfolgen:

- **Arbeitsprotokoll** — Dies bietet ein detailliertes Protokoll der Aktionen, die AWS Transform ergreift, zusammen mit menschlichen Eingaben und Ihren Antworten auf diese Anfragen.
- **Dashboard** — Dies bietet eine allgemeine Zusammenfassung der Mainframe-Anwendungstransformation. Es zeigt Kennzahlen zur Anzahl der transformierten Jobs, zur angewandten Transformation und zur geschätzten Zeit bis zum Abschluss der Transformation von Mainframe-Anwendungen. Sie können auch Details zu jedem Schritt einsehen, darunter Codezeilen nach Dateitypen, generierte Dokumentation für jeden Dateityp, den zerlegten Code und den Migrationsplan.

Richten Sie einen Konnektor ein

AWS Transform verwendet einen Konnektor, um auf Ressourcen in Ihrem Konto zuzugreifen, die für Mainframe-Modernisierungsfunktionen erforderlich sind. Ihr Connector wird automatisch mit dem ersten Job konfiguriert, den Sie im Workspace ausführen. Je nachdem, welchen Jobplan Sie wählen, führt Sie AWS Transform zur Erstellung Ihres Connectors.

Mainframe-Konnektor neu erfinden

Der Mainframe Reimagine Connector ist für Jobs vorgesehen, bei denen die Workflows Assessment und Reimagine ausgeführt werden. Es verwendet einen S3-Bucket für den Zugriff auf und die Speicherung von Transformationsressourcen sowie einen Amazon Neptune Neptune-Cluster zum Speichern extrahierter Artefakte. Der Neptun-Cluster dient als einheitlicher Wissensgraph, der alle extrahierten Artefakte über Ihren Job speichert, und der Wissensgraph beantwortet alle Fragen in der AWS Transform-Chat-Oberfläche.

Stellen Sie den Amazon Neptune Neptune-Cluster in einer VPC bereit, in der AWS Transform elastische Netzwerkschnittstellen (ENIs) erstellen kann. Dies sind die Netzwerkverbindungen, die es AWS Transform ermöglichen, sicher mit Neptune in Ihrer VPC zu kommunizieren, um Daten zu laden und Ihren Wissensgraphen abzufragen.

AWS CloudFormation

Wir empfehlen, die folgende CloudFormation Vorlage zu verwenden, um die Ressourcen zu erstellen, die für Ihren Mainframe-Reimagine-Connector erforderlich sind. Verwenden Sie bei der Ausführung der Vorlage denselben S3-Bucket, den Sie für den Connector verwenden möchten. CloudFormation Weitere Informationen zur Verwendung von CloudFormation Vorlagen finden Sie unter [Arbeiten mit Vorlagen](#).

Um die CloudFormation Vorlage herunterzuladen, wählen Sie [neptune-kg-setup.yaml](#).

Die Vorlage akzeptiert die folgenden Parameter:

- BucketName – Erforderlich. S3-Bucket-Name für den Neptune-Bulk-Loader-Zugriff. Sie müssen denselben S3-Bucket verwenden, den Sie in Ihrem AWS Transform-Connector verwenden möchten.
- KmsKeyId – Optional. KMS-Schlüssel für Neptune-Verschlüsselung. Akzeptiert Schlüssel-ID, ARN, Aliasnamen oder Alias-ARN. Standardmäßig wird der AWS verwaltete Schlüssel verwendet, wenn er weggelassen wird.

Geben Sie bei der Konfiguration Ihres Connectors die folgenden Details an:

- S3 Bucket-ARN
- Neptun-Cluster ARN
- Ressourcen-ID des Neptun-Clusters
- Subnetz-IDs der Anwendung
- ID der Anwendungssicherheitsgruppe
- Neptune S3 Bulk-Loader-Rolle ARN

 Important

Die Registerkarte Ausgaben der CloudFormation Vorlage enthält die Details, die Sie AWS Transform bei der Konfiguration des Konnektors angeben müssen.

Benutzerdefinierte Konfiguration

Wenn Sie es vorziehen, eine vorhandene VPC oder andere Tools zu verwenden, um die erforderliche Infrastruktur zu erstellen, muss Ihre Umgebung die folgenden Anforderungen erfüllen:

Neptun-Cluster

- Amazon Neptune Serverless mit Engine-Version 1.4.5.1 oder höher
 - IAM-Authentifizierung aktiviert
 - Speicherverschlüsselung aktiviert (AWS verwalteter Schlüssel oder vom Kunden verwalteter KMS-Schlüssel)
- Konfiguration für serverlose Skalierung (empfohlen: 1—128 NCUs)
- (Empfohlen) Lesen Sie das Replikat in einer zweiten Availability Zone für hohe Verfügbarkeit und verbesserte Leseleistung

Netzwerk

- Eine VPC mit DNS-Unterstützung und aktivierten DNS-Hostnamen
- Mindestens zwei Subnetze in separaten Availability Zones. AWS Transform erstellt ENIs in diesen Subnetzen, um auf den Neptune-Cluster zuzugreifen, der sich in denselben Subnetzen oder in dedizierten Subnetzen befinden kann. Passen Sie die Größe der Subnetze auf /20 an, um VPC-Endpunkt- und Anwendungs-ENIs zu berücksichtigen.
- Netzwerkkonnektivität von den Subnetzen zu den folgenden AWS Diensten über VPC-Schnittstellenendpunkte ():AWS PrivateLink
 - AWS Transform Agents API — Koordiniert die Mainframe-Modernisierungsaufgaben
 - Amazon Bedrock Runtime — Ruft grundlegende Modelle zur Analyse und Argumentation auf
 - Amazon Relational Database Service (Amazon RDS) — Neptune-Clusterverwaltung
 - Amazon Elastic Compute Cloud (Amazon EC2) — Verwaltung von ENIs
 - Amazon CloudWatch — Metriken für die AWS Beobachtbarkeit von Transform

- Ein S3-Gateway-Endpunkt, der an die Routing-Tabellen angehängt ist, die Ihren Subnetzen zugeordnet sind. AWS Transform verwendet diesen Endpunkt, um Daten aus dem S3-Bucket in den Neptune-Cluster zu laden.

Sicherheitsgruppen

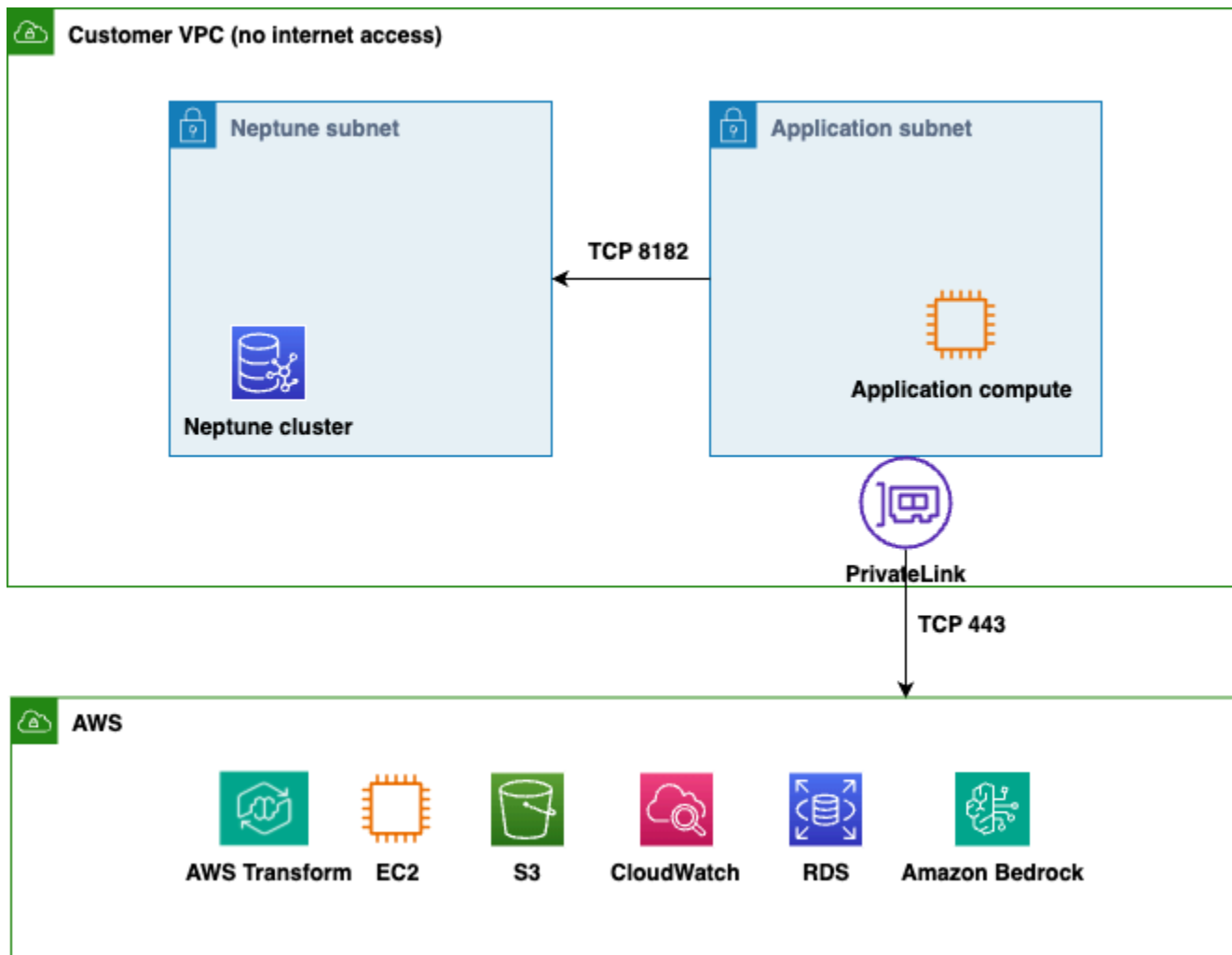
Sicherheitsgruppen sind an ENIs angehängt, nicht an Subnetze. Selbst wenn sich AWS Transform ENIs und Neptune im selben Subnetz befinden, kontrollieren separate Sicherheitsgruppen den Zugriff zwischen ihnen.

- Eine Sicherheitsgruppe (verbunden mit den von Transform erstellten ENIs), die Folgendes ermöglicht: AWS
 - Ausgehender TCP 8182 an die Neptune-Sicherheitsgruppe
 - Ausgehendes TCP 443 zum Erreichen von VPC-Endpunkten
- Eine Sicherheitsgruppe (an den Neptune-Cluster angeschlossen), die Folgendes ermöglicht:
 - Eingehender TCP 8182 von der Anwendungssicherheitsgruppe
- Eine VPC-Endpunkt-Sicherheitsgruppe (an den Schnittstellenendpunkt ENIs angehängt), die Folgendes ermöglicht:
 - Eingehendes TCP 443 aus der Anwendungssicherheitsgruppe

IAM

- Eine IAM-Rolle mit einer Vertrauensrichtlinie für `rds.amazonaws.com` diese Grants `s3:GetObjects``s3:ListBucket`, und in `s3:GetBucketLocation` Ihrem S3-Bucket
- Diese Rolle muss mit dem Neptune-Cluster verknüpft sein, damit Knowledge-Graph-Daten massenweise geladen werden können.

Das folgende Diagramm zeigt die empfohlene Architektur.



S3-Anschluss

Für Jobs mit einem benutzerdefinierten Plan kann AWS Transform einen S3-Connector verwenden. Der S3-Konnektor verwendet einen S3-Bucket für den Zugriff auf und das Speichern von Transformationsressourcen und einen S3-Vektor-Bucket für die indizierte Ausgabe.

Important

Ihre Daten werden im AWS Transform-Artefaktspeicher in Ihrem Workspace gespeichert und dauerhaft gespeichert und nur für die Ausführung des Jobs verwendet.

Optionale Konfiguration des S3-Vektor-Buckets.

In Regionen, in denen S3-Vektor-Buckets verfügbar sind, speichert AWS Transform durchsuchbare Vektorkodierungen der Jobausgabe in diesem S3-Vektor-Bucket in Ihrem Konto, um ein KI-gestütztes Such- und Chat-Erlebnis zu bieten. Daten werden nicht außerhalb dieses Jobs verwendet und auch nicht zum Trainieren von Modellen verwendet. Um dies zu aktivieren, müssen Sie einen S3-Vektor-Bucket erstellen und bereitstellen. AWS Transform erstellt automatisch eine Rolle mit den erforderlichen Schreibberechtigungen für diesen Bucket und fügt sie an.

CORS-Berechtigungen für den S3-Bucket

Nachdem Ihr Connector konfiguriert ist, fügen Sie Ihrem S3-Bucket die folgende CORS-Richtlinie hinzu, damit Sie Artefakte direkt in der AWS Transform-Konsole anzeigen und vergleichen können. Wenn diese Richtlinie nicht korrekt eingerichtet ist, können Sie die Inline-Anzeige- oder Dateivergleichsfunktionen von AWS Transform möglicherweise nicht verwenden.

```
[
  {
    "AllowedHeaders": [],
    "AllowedMethods": [
      "GET"
    ],
    "AllowedOrigins": [
      "https://*.transform.eu-central-1.on.aws",
      "https://*.transform.ap-south-1.on.aws",
      "https://*.transform.ap-northeast-1.on.aws",
      "https://*.transform.ap-northeast-2.on.aws",
      "https://*.transform.ap-southeast-2.on.aws",
      "https://*.transform.ca-central-1.on.aws",
      "https://*.transform.eu-west-2.on.aws",
      "https://*.transform.us-east-1.on.aws",
      "https://*.transform.sa-east-1.on.aws"
    ],
    "ExposeHeaders": [],
    "MaxAgeSeconds": 0
  }
]
```

Beurteilen und überdenken Sie den Stellenplan

Der Jobplan Assess and Reimagine ist ein vordefinierter Arbeitsablauf für die Modernisierung von Mainframe-Anwendungen. Er führt Sie durch zwei Phasen: die Bewertung Ihrer Codebasis zur Identifizierung von Geschäftsfunktionen und die Neugestaltung der von Ihnen ausgewählten

Funktionen. Um stattdessen einzelne Funktionen auszuwählen, verwenden Sie den benutzerdefinierten Jobplan.

Bewerten

Die Modernisierung von Mainframes beginnt in der Regel mit der Evaluierung der Codebasis, um Inhalte zu identifizieren und Zusammenhänge und Abhängigkeiten zu verstehen. Nach dieser Evaluierung können Sie beginnen, Teile des Quellcodes zu zerlegen und auszuwählen, die modernisiert werden sollen. Die Grenzen der Zerlegung werden auf der Grundlage von Geschäftsfunktionen festgelegt.

Der Geschäftsfunktionskatalog zerlegt Ihre Codebasis in einzelne Geschäftsfunktionen, die auf einer Grundlage deterministischer Datenpfade aufbauen, die jede Geschäftsfunktion von Anfang bis Ende abbilden. Ein Datenpfad ist der Weg, den Daten nehmen, angefangen bei einem Geschäftsauslöser bis hin zum letzten Schreibvorgang innerhalb des Mainframe-Codes. Anstatt die Analyse auf einen einzigen Einstiegspunkt zu beschränken, umfasst das System Batch-Jobs, CICS-Transaktionen und deren gemeinsame Datenspeicher, um kohärente Geschäftsbereiche zu identifizieren.

Eine Geschäftsfunktion ist eine Gesamtheit von Aufgaben, die von einem geschäftlichen Auslöser ausgehen und mit einem messbaren Geschäftsergebnis enden. AWS Transform bietet einen Katalog von Geschäftsfunktionen, auf die ein Geschäftsbereich reagieren kann, sodass fundierte Entscheidungen darüber getroffen werden können, was zuerst modernisiert werden muss.

Vorteile der Bewertung Ihrer Codebasis im Hinblick auf die Modernisierung mithilfe von Geschäftsfunktionen:

- Full-estate Transparenz — Erfahren Sie, wie Ihre Batch-Jobs, Online-Transaktionen und Datenspeicher zu sinnvollen Funktionen für Ihr Unternehmen zusammenwirken.
- Umsetzbare Grenzen — Jede identifizierte Geschäftsfunktion ist eine eigenständige Einheit, die von Ihren Geschäftsbereichen für Modernisierungsmaßnahmen überprüft und priorisiert werden kann.
- Konsistenz vom Code bis zur Spezifikation — Dieselben Codeblöcke, die eine Geschäftsfunktion definieren, werden zur Generierung ihrer Spezifikationen verwendet, ohne dass eine Übersetzungsebene oder ein Abgleich erforderlich ist.
- Verkürzte Erkennungszeit — Die automatische Erkennung ersetzt monatelange manuelle Stammesgespräche durch systematische, wiederholbare Analysen.

Die Ergebnisse der Bewertung wurden im Chat bereitgestellt

Die im Chat bereitgestellten Ergebnisse der Bewertung umfassen eine Liste der Geschäftsfunktionen, einschließlich der Anzahl der Datenpfade, des Umfangs der einzelnen Funktionen in Bezug auf Batch- und CICS-Transaktionen sowie eine Unternehmensbeschreibung. Sie erhalten einen Link zu den Artefakten, die im Amazon S3 S3-Bucket generiert wurden, und Sie können auch über den Chat darauf zugreifen. Es werden zwei Artefakte bereitgestellt: Details zur Geschäftsfunktion und Zusammenfassung der Geschäftsfunktionen.

- Zusammenfassung der Geschäftsfunktionen — Enthält eine Liste der Geschäftsfunktionen und eine Beschreibung in natürlicher Sprache, welche Funktionen die Elemente im Code ausführen.
- Details zu den Geschäftsfunktionen — Stellt ein interaktives Diagramm bereit, das die Beziehungen zwischen den einzelnen Quelltexten darstellt.

Um mit dem Diagramm zu interagieren, wählen Sie ein Element aus, um zusätzliche Details anzuzeigen, oder öffnen Sie ein Element, um dessen Details abzufragen. Auf jeder Seite gibt es eine Zusammenfassung aller Elemente auf dieser Ebene und eine grafische Oberfläche, über die Sie mit den einzelnen Komponenten interagieren und mehr über sie erfahren können, einschließlich der folgenden:

- Geschäftsfunktion — Zeigt, welche Geschäftsfunktionen miteinander verbunden sind, und bietet einen Überblick über die einzelnen Geschäftsfunktionen. Wenn Sie eine Geschäftsfunktion auswählen, werden die folgenden Informationen bereitgestellt:
 - Anzahl der Datenpfade
 - Anzahl der Codezeilen
 - Geschäftsbeschreibung: Ein Überblick über die Geschäftsfunktion, in der in natürlicher Sprache beschrieben wird, welche Funktionen die Elemente im Code ausführen.
 - Schnittstellen: beschreibt, wie Datenelemente innerhalb der Geschäftsfunktion zusammenhängen (z. B. austauschen oder schreiben).
- Details zur Geschäftsfunktion — Stellt die Verbindungen zwischen den Datenpfaden innerhalb einer einzelnen Geschäftsfunktion dar, sodass Sie sich eingehender mit der Zusammensetzung der Geschäftsfunktion befassen können. Wenn Sie ein Element auswählen, sehen Sie, wie dieses Element in der gesamten Geschäftsfunktion miteinander verknüpft ist, sowie die folgenden Details:
 - Datenspeicher: Autoren und Leser für den Datenspeicher.

- Weitere Elemente: ein Überblick über den zugehörigen Datenpfad, der in natürlicher Sprache die Aktionen und Ergebnisse beschreibt, die innerhalb des Datenpfads durchgeführt werden, eine Liste der Programme sowie der Leser und Autoren.
- Datenpfade — Zeigt die Details eines Datenpfads und die Beziehung der Elemente innerhalb des Datenpfads zueinander.
 - Beschreibung: Ein Überblick über den Datenpfad, der in natürlicher Sprache die Aktionen und Ergebnisse beschreibt, die innerhalb des Datenpfads vorgenommen wurden.
 - Inhalt des Datenpfads:
 - Einstiegspunkt
 - Reads
 - Writes
 - Programme

Im Chat können Sie die Ergebnisse abfragen, um zu verstehen, welche Elemente in den einzelnen Geschäftsfunktionen enthalten sind, und anhand des Geschäftsfunktionsdiagramms die Grenzen ausloten.

Nachdem Sie die Grenzen Ihrer Modernisierung identifiziert haben, werden Sie im Chat aufgefordert, die Geschäftsfunktionen auszuwählen, die Sie neu definieren möchten. Sie können eine einzelne Geschäftsfunktion oder mehrere Geschäftsfunktionen auswählen. AWS Transform sendet die ausgewählten Grenzen und die erforderlichen Bewertungsergebnisse an den Reimagine-Flow, um die Modernisierung fortzusetzen.

Nachdem Sie Ihre erste Modernisierung abgeschlossen haben, können Sie den Chat verwenden, um weitere Geschäftsfunktionen für die Modernisierung auszuwählen.

Stellen Sie sich neu vor

In der Phase der Neukonzeption können Sie eine oder alle Geschäftsfunktionen auswählen, die bei der Bewertung identifiziert wurden, und sie für die Modernisierung vorbereiten. Dadurch wird die Extraktion der Geschäftslogik ausgelöst, gefolgt von der Generierung von Anforderungen für die ausgewählten Geschäftsfunktionen. Die generierten Anforderungen sind der wichtigste Input für Forward Engineering. Dabei wird das Verständnis der bestehenden Systeme in eine genaue Spezifikation dessen umgesetzt, was die modernisierte Anwendung bieten muss.

Extrahieren Sie Geschäftslogik

Nachdem Sie eine oder mehrere Geschäftsfunktionen ausgewählt haben, beginnt AWS Transform mit der Generierung der Geschäftslogik für die ausgewählten Geschäftsfunktionen. Nach Abschluss der Extraktion speichert AWS Transform die Ergebnisse in einem Amazon S3 S3-Bucket im JSON-Format für die nachgelagerte Verwendung. Sie können den Fortschritt der Extraktion überwachen und etwaige Probleme direkt in der AWS Transform-Konsole überprüfen.

Um die Ergebnisse der Extraktion von Geschäftslogik zu überprüfen

1. Wählen Sie im linken Navigationsbereich den Schritt Geschäftslogik extrahieren aus, um ihn zu erweitern.
2. Sehen Sie sich in den Schrittdetails Folgendes an:
 - S3-Bucket-Link: Der Ort, an dem die extrahierten Ergebnisse der Geschäftslogik im JSON-Format gespeichert werden.
 - Probleme: Eine Liste aller Probleme, die bei der Extraktion der Geschäftslogik aufgetreten sind.

Falls bei Dateien Probleme beim Extrahieren aufgetreten sind, werden für jede betroffene Datei die folgenden Details angezeigt:

- Dateiname: Der Name der Datei, bei der ein Problem aufgetreten ist.
- Dateityp: Der Typ der Datei (z. B. COBOL oder JCL).
- Dateipfad: Der Speicherort der Datei in Ihrer Anwendung.
- Status: Der aktuelle Status der Dateiextraktion.
- Details: Eine Beschreibung des aufgetretenen Problems.

Note

Nach Abschluss des Extraktionsschritts beginnt AWS Transform automatisch mit der Generierung von Anforderungen. Sie werden nicht zur Eingabe zusätzlicher Eingaben aufgefordert, bevor dieser Vorgang gestartet wird.

Generieren Sie Anforderungen

Nach Abschluss der Extraktion der Geschäftslogik verwendet der Agent `Generate Requirements` die extrahierten Artefakte (Codeanalyse, Datenanalyse, Geschäftsregeln) und erstellt Modernisierungsanforderungen. Bei diesen Anforderungen handelt es sich um formelle Funktionsspezifikationen, die technologieunabhängig sind und überprüfbare Akzeptanzkriterien beinhalten. AWS Transform erstellt eine `requirements.md` Datei für jede von Ihnen ausgewählte Geschäftsfunktion und speichert die Ausgabe in einem Amazon S3 S3-Bucket. Um den Amazon S3 S3-Speicherort der Ausgabe anzuzeigen, wählen Sie den Schritt `Anforderungen generieren`.

Jede `requirements.md` Datei ist in die folgenden Teile gegliedert:

- **Titel** — Benennt die Geschäftsfunktion und den Arbeitsablauf, für den sie steht.
- **Globale Voraussetzungen** — Bedingungen, die vor und während der Verarbeitung für den gesamten Workflow gelten müssen. Konfigurierbare Werte werden als Platzhalter für Parameter angezeigt.
- **Nummerierte Workflow-Abschnitte** — Jeder Abschnitt stellt eine separate Phase der Geschäftsfunktion dar. Jeder Abschnitt enthält Folgendes:
 - Eine Benutzergeschichte, in der das Ziel als Rolle, die Aktion, die diese Rolle ausführen möchte, und das daraus resultierende Ergebnis beschrieben wird.
 - Eine Liste von Anforderungen im Format EARS (Easy Approach to Requirements Syntax), jede mit einer eindeutigen Kennung.

Note

Wenn Sie eine zweite Gruppe von Geschäftsfunktionen auswählen, wird der Schritt „Neugestaltung“ für die neu ausgewählten Funktionen neu gestartet. Die Konsole zeigt dann nur Ergebnisse für die neue Auswahl an, sodass alle Probleme mit den Geschäftsregeln aus Ihren vorherigen Geschäftsfunktionen und den Amazon S3 S3-Links, in denen die Ausgaben für die Geschäftslogik und die Anforderungen gespeichert sind, nicht mehr angezeigt werden. Ihre früheren Ausgaben sind nicht verloren gegangen. Sie können weiterhin über den Tab `Artefakte` oder in Ihrem Amazon S3 S3-Bucket auf sie zugreifen.

Rückverfolgbarkeit zwischen Transformationsartefakten

AWS Transform gewährleistet die Rückverfolgbarkeit zwischen den Artefakten, die es während des gesamten Beurteilungs- und Neugestaltungsprozesses generiert. Mithilfe der Rückverfolgbarkeit können Sie jede Anforderung auf Ihre extrahierten Geschäftsregeln oder direkt auf den ursprünglichen Quellcode zurückverfolgen, der die Anforderung erstellt hat.

Mithilfe der Datei können Sie alle Rückverfolgbarkeitsdetails für jede Geschäftsfunktion einsehen. `traceability.yaml` Sie beschreibt, wie jede Geschäftsregel einer Anforderung zugeordnet wird.

Für interaktive Rückverfolgbarkeit können Sie das IDE-Plug-In in VS Code- und Open VSX-kompatiblen Editoren verwenden. Weitere Informationen finden Sie unter [Entwicklertools](#).

Stellen Sie sich den Jobplan neu vor

Für Anwendungen, für die Sie eine Modernisierung geplant haben und die bereit sind, sie neu zu gestalten, können Sie einen eigenständigen Job zur Neugestaltung ausführen. Der Job analysiert Ihren Code und Ihre Daten, extrahiert Geschäftslogik, identifiziert Geschäftsbereiche und generiert Modernisierungsanforderungen für jede Geschäftsdomäne.

Benutzerdefinierter Jobplan

Mit einem benutzerdefinierten Jobplan können Sie Ihren eigenen Modernisierungs-Workflow erstellen, indem Sie die Funktionen auswählen, die Sie ausführen möchten. Er gibt Ihnen die volle Kontrolle darüber, welche Funktionen enthalten sind. Wählen Sie je nach Ihrem Modernisierungsziel aus den folgenden Funktionen. Einige Funktionen hängen davon ab, dass andere zuerst ausgeführt werden. Für die meisten anderen Funktionen ist beispielsweise eine Codeanalyse erforderlich.

Analysieren Sie den Code

Nachdem Sie den Amazon S3 S3-Bucket-Pfad mit AWS Transform geteilt haben, analysiert Transform den Code für jede Datei mit Details wie Dateiname, Dateityp, Codezeilen und deren Pfaden.

Note

Sie können die Codeergebnisse analysieren über den Tab Artefakte auf Job- oder Workspace-Ebene herunterladen. Gehen Sie auf Jobebene im linken Navigationsmenü zur Option „Artefakte“ und öffnen Sie den Ordner „Ergebnisse“. Oder suchen Sie auf

Workspace-Ebene nach dem Namen des Jobs und öffnen Sie den Ordner „Ergebnisse“. Dadurch wird eine ZIP-Datei heruntergeladen, die die Klassifizierungsdatei für den manuellen Klassifizierungs-Workflow, die Asset-Liste, die JSON-Datei für Abhängigkeiten und die Liste der fehlenden Dateien enthält.

Wählen Sie im Jobplan im linken Navigationsbereich die Option Code analysieren aus, um Ihre Ergebnisse anzuzeigen. Sie können Ihre Codeanalyseergebnisse auf verschiedene Arten anzeigen:

- Listenansicht — Alle Dateien im Amazon S3 S3-Bucket, die Sie für den Mainframe transformieren möchten
- Dateityp-Ansicht — Alle Dateien im Amazon S3 S3-Bucket werden pro Dateityp angezeigt. Eine Liste der unterstützten Dateitypen finden Sie unter [Unterstützte Dateien](#).
- Ordneransicht — Alle Dateien im Amazon S3 S3-Bucket werden in der Ordnerstruktur angezeigt.

In den Dateiergebnissen stellt AWS Transform je nachdem, welche Dateiansicht Sie wählen, die folgenden Informationen bereit:

- Name
- Dateityp
- Gesamtzahl der Codezeilen
- Dateipfad
- Kommentarzeilen
- Leere Zeilen
- Effektive Codezeilen
- Anzahl der Dateien
- Zyklomatische Komplexität — Die zyklomatische Komplexität stellt die Anzahl der linear unabhängigen Pfade durch den Quellcode eines Programms dar. AWS Transform zeigt für jede der Dateien eine zyklomatische Komplexität.

Fehlende Dateien — Fehlende Dateien aus der Codeanalyse für die Mainframe-Modernisierung. Diese Dateien sollten idealerweise als Teil der Quelleingabe im Amazon S3 S3-Bucket hinzugefügt werden, und der Analyseschritt sollte erneut ausgeführt werden, um bessere und kohärente Ergebnisse zu erzielen.

Identisch benannt — AWS Transform gibt Ihnen eine Liste von Dateien, die denselben Namen und möglicherweise dieselben Eigenschaften haben (z. B. Anzahl der Codezeilen). Es wird nicht in der Lage sein, den Unterschied zwischen den Inhalten zweier Dateien gleichzeitig zu vergleichen.

Doppelte IDs — Beim Cobol-Programm dient das Feld Programm-ID als eindeutige Kennung der Datei. Diese ID muss eindeutig sein, da sie verwendet wird, um das Programm während Ihres gesamten Projekts aufzurufen. Einige Projekte haben jedoch möglicherweise COBOL-Dateien mit unterschiedlichen Namen, aber derselben Programm-ID. Wenn Sie die Liste dieser Dateien während der Bewertung abrufen, können Sie die Abhängigkeiten zwischen allen Programmen besser verstehen.

 Note

Dies ist spezifisch für COBOL-Code und -Dateien.

Wenn Sie Programme mit doppelten IDs haben, wird empfohlen, die Programm-IDs dieser Dateien so zu ändern, dass für jede dieser Dateien eine eindeutige Kennung im COBOL-Code verwendet wird. Anschließend können Sie Ihren Job erneut ausführen, um genauere und umfassendere Codeanalyseergebnisse zu erhalten.

Durch das Auflösen doppelter Programm-IDs können Sie:

- Verbessern Sie die Klarheit und Wartbarkeit des Codes
- Reduzieren Sie potenzielle Konflikte bei Programmaufrufen
- Verbessern Sie die Genauigkeit der Abhängigkeitszuweisung
- Vereinfachen Sie future Modernisierungsbemühungen

Probleme mit der Codebasis — Mögliche Probleme in der Codebasis, die Sie lösen sollten, bevor Sie mit dem Modernisierungsprojekt fortfahren. Zu diesen Problemen können fehlende Verweise auf zugehörige Anweisungen oder nicht unterstützte Links im Code gehören.

Klassifizierung aktualisieren — Bei der manuellen Reklassifizierung können Sie Dateien mithilfe der Funktion zur Massenaktualisierung reklassifizieren, indem Sie die JSON-Datei mit der neuen Klassifizierung hochladen.

 Important

Dies ist nur für UND-Dateien verfügbar. UNKNOWN TXT

Nach der Reklassifizierung wird AWS Transform:

1. Aktualisiert die Klassifizierungsergebnisse
2. Re-runs Abhängigkeitsanalyse mit den neuen Dateitypen
3. Aktualisiert alle betroffenen Analyseergebnisse

 Note

Sie können Dateien erst reklassifizieren, wenn die erste Analyseschleife abgeschlossen ist.

Inline-Viewer und Dateivergleich

Der Inline Viewer ist eine Funktion der AWS Transform for Mainframe-Funktionen, die zwei wichtige Visualisierungsfunktionen bietet:

- Dateiansicht: Zeigt den Inhalt ausgewählter Legacy-Dateien aus Jobs an
- Dateivergleich: Der Inhalt von zwei älteren Dateien wird nebeneinander verglichen

Anzeige der Eingabedatei

Um Ihre Dateien in der Analysieren Sie den Code Schritt

- Wählen Sie unter Codeanalyseergebnisse anzeigen eine Datei aus, indem Sie das Kontrollkästchen in der Liste verwenden.

Wählen Sie die Aktionsschaltfläche „Anzeigen“ (aktiviert, wenn 1 Element ausgewählt ist).

Der Dateiinhalt wird in der Komponente „Dateiansicht“ auf dem Bildschirm gerendert.

Dateivergleich

Um Dateien zu vergleichen in Analysieren Sie den Code Schritt

1. Wählen Sie unter Codeanalyseergebnisse anzeigen mithilfe der Kontrollkästchen in der Liste zwei Dateien aus.
2. Wählen Sie die Aktionsschaltfläche Vergleichen (nur aktiviert, wenn 2 Elemente ausgewählt sind).
3. Dateien werden in der Komponente „Dateivergleich“ nebeneinander angezeigt.

 Note

Sie können nicht mehr als zwei Dateien auswählen, um Dateien zu vergleichen.

 Important

Wenn Sie Probleme mit dem Inline-Viewer oder dem Dateivergleich haben, stellen Sie sicher, dass der S3-Bucket korrekt eingerichtet ist. Weitere Informationen zur CORS-Richtlinie des S3-Buckets finden Sie unter [the section called “CORS-Berechtigungen für den S3-Bucket”](#).

Datenanalyse

AWS Transform bietet Datenanalysen, um die Auswirkungen von Datenbeziehungen und Elementen auf das Mainframe-Modernisierungsprojekt besser zu verstehen. Die beiden bereitgestellten Ergebnisse sind:

- Datenherkunft: Verfolgt den Lebenszyklus von Daten, indem Beziehungen zwischen Datenquellen, Jobs und Programmen abgebildet werden
- Datenwörterbuch: Dient als Aufbewahrungsort für die Dokumentation der strukturellen Metadaten älterer Datenelemente

Nach Abschluss der Analyse stehen für jede Ausgabe zwei Registerkarten zur Verfügung. Anschließend stehen mehrere Ansichten zur Verfügung, wie unten beschrieben, sowohl für die Datenherkunft als auch für das Wörterbuch.

 Note

Wenn Sie eine Datenanalyse anfordern, führt AWS Transform eine Codeanalyse durch, die für die Datenanalyse erforderlich ist.

Datenherkunft

AWS Transform bietet mehrere Ansichten, die auf den Datenbeziehungen basieren, die in der zu modernisierenden Codebasis verstanden werden müssen. Zu den vier Tabellenansichten, die in Data Lineage verfügbar sind, gehören:

- **Datensätze:** Diese Ansicht bietet eine umfassende Folgenabschätzung, einschließlich der Nachverfolgung von Vorgängen, um zwischen Lesen, Schreiben, Aktualisieren und Löschen unterscheiden zu können
- **Db2-Tabellen:** Stellen Sie die Auswirkungsanalyse für Db2-Tabellen und die Operationen bereit
- **Program-to-data:** Identifizieren Sie, welche COBOL-Programme auf die einzelnen Datensätze verweisen
- **JCL-to-data Beziehungen:** Identifizieren Sie, welche JCL-Skripten auf jeden Datensatz verweisen

Die Zusammenfassung bietet einen Überblick über Datenquellen und ihre Beziehungen zu Programmen und JCLs sowie zusammenfassende Informationen darüber, wie die Datenquellen genutzt werden und wie die gesamten Operationen in der Codebasis gefunden wurden.

Datenwörterbuch

Der nächste Schritt besteht darin, die Datenelemente in den in der Codebasis vorhandenen Datenquellen zu verstehen, um zu erkennen, wie die verschiedenen Datenquellen voneinander abhängen. Das Datenwörterbuch ist ein Datenkatalog, der Metadaten auf Feldebene mit Beschreibungen in Geschäftssprachen für eine genaue Zuordnung von Transformationen bereitstellt.

- **COBOL-Datenstruktur:** Stellt Feldinformationen für alle COBOL-Copybooks und INLINE-Referenzen in der Codebasis bereit, einschließlich Feldeigenschaften und Geschäftsdefinitionen
- **Db2-Tabellen:** Stellt Spalten- und Tabelleneigenschaften für alle in der Codebasis vorhandenen Db2-Tabellen bereit, einschließlich Primär- und Fremdschlüssel, Schema- und Indexinformationen sowie Datentypen

Die Beziehung zwischen Datenherkunft und Wörterbuch ist verfügbar, indem Sie die Datenquelle auswählen und dann die Schaltfläche Datenherkunft oder Datenwörterbuch verwenden, um sich eingehender mit der Beziehung zwischen der Datenquelle und den Datenelementen zu befassen. Die Navigation zwischen Datenherkunft und Wörterbuch bietet eine integrierte Datentransparenz, wobei die Datenherkunft neben dem „Wo“, der Verwendung und der Beziehung auch das „Was“ — Struktur und Bedeutung — bereitstellt.

Analyse von Aktivitätsmetriken

Mit der Analyse von Aktivitätsmetriken können Sie SMF-Datensätze (System Management Facility) der Typen 14, 15, 30, 64, 102 und 110 analysieren. Die Analyse bietet Einblicke in die Verwendung von Elementen in Ihrer Mainframe-Anwendung. Sie kann dabei helfen, ungenutzten Code zurückzuziehen oder Entscheidungen über die Zielarchitektur für die modernisierte Anwendung zu treffen. Wenn Sie die Analyse von Aktivitätsmetriken in Ihren Job einbeziehen, erhalten Sie, wenn Sie zuerst den Schritt der Codeanalyse abschließen, umfangreichere SMF-Ergebnisse, obwohl dies nicht erforderlich ist.

Note

Wenn Sie den Arbeitsplan für die Mainframe-Modernisierung aushandeln, liefert der Abschluss der Schritte zur Codeanalyse und Dekomposition zunächst aussagekräftigere Ergebnisse.

Integrierte SMF-Datensätze zur Analyse

Sie müssen den Speicherort des SMF-Datensatzes in Ihrem Amazon S3 S3-Bucket als ersten Schritt für die SMF-Analyse angeben. Stellen Sie Aufzeichnungen für mindestens 13 Monate bereit, um jährliche Ereignisse zu erfassen, die in kürzeren Zeiträumen möglicherweise übersehen werden. Obwohl 13 Monate empfohlen werden, führt jeder Zeitraum mit nachweisbaren SMF-Aufzeichnungen zu Analyseergebnissen.

Ihr SMF-Extrakt muss die folgenden Formatanforderungen erfüllen:

- Schließen Sie die Typen 14, 15, 30 (Untertyp 5), 64, 102 und 110 ein.
- Verwenden Sie eine unformatierte Binärdatei im EBCDIC-Format.
- RDW-Bytes einbeziehen.

Stellen Sie einen Link zu den SMF-Datensätzen in Ihrem Amazon S3-Bucket bereit und stellen Sie sicher, dass sich die Datensätze in einem Ordner befinden, der von Ihrem Quellcode getrennt ist. Zu den Formatoptionen gehören .zip (bis zu 600 MB) oder .tar.gz (bis zu 5 GB) komprimiert. Wenn Sie einen Link zu einem Ordner angeben, in dem keine SMF-Datensätze erkannt wurden, erhalten Sie eine Fehlermeldung und die Analyse ist nicht abgeschlossen.

Ausgabe der Analyse

Die Analyseausgabe enthält je nach Datensatztyp zwei Komponenten: eine tabellarische Ansicht und eine CSV-Ausgabe (in Ihrem Amazon S3 S3-Bucket verfügbar). In AWS Transform werden die Ausgaben für Typ 30 und 110 angezeigt. Anhand der Artefakte in Ihrem Amazon S3 S3-Bucket können Sie die Analyse anderer Datensatztypen untersuchen. In der Benutzeroberfläche wird in der Kopfzeile der Zeitraum der von Ihnen bereitgestellten Datensätze angezeigt, sodass Sie fehlende Schlüsseldaten identifizieren können. Wenn sich Ihre Datensätze beispielsweise vom 1. Mai bis zum 31. Oktober erstrecken, aber den geschäftigen Tag nach Thanksgiving ausschließen, können Sie feststellen, dass wichtige Datensätze fehlen. Die Zeitstempel in der Webanwendung geben die Zeitzone Ihres Systems und die SMF-Datensätze wieder.

In Amazon S3 verfügbare Artefakte ermöglichen Analysen für jeden Datensatztyp, der in den bereitgestellten Datensätzen gefunden wurde.

Tabellarische Ansicht

Die tabellarische Ansicht, die nur für SMF 30 und 110 verfügbar ist, enthält bis zu drei Hauptkomponenten für Batch-Jobs und CICS-Transaktionen:

- Zusammenfassung — Enthält die wichtigsten Jobs und Transaktionen.
- Analyse von job/CICS Batch-Transaktionen — Bietet aggregierte Analysen für Jobs und Transaktionen.
- Vergleich der Codeanalyse (nur Batch) — Stellt Vergleichsdaten bereit, wenn der Codeanalyseschritt vor der SMF-Analyse ausgeführt wird.

Die Zusammenfassung der Ergebnisse enthält drei Gruppen von Aufträgen und Transaktionen, anhand derer Sie schnell Elemente für eine eingehendere Analyse identifizieren können.

Die Batch-Job- und CICS-Transaktionsanalyse bietet aggregierte Analysen für Jobs und Transaktionen. Einige Spalten in den Analyseergebnissen sind standardmäßig ausgeblendet. Wählen Sie das Zahnradsymbol, um weitere Felder anzuzeigen.

Der Transaktionsschlüssel generiert eine eindeutige Datenaggregation für CICS-Transaktionen und kombiniert vier Felder zu einem einzigen Schlüsselwert:

- Transaktions-ID
- Name des Programms
- SysPlex ID
- SysID

Sie können nach dem vollständigen Schlüssel oder nach einer beliebigen Komponente des Schlüssels in der Analyseausgabe suchen.

Beim Vergleich der Codeanalyse werden Jobs hervorgehoben, die entweder in den SMF-Datensätzen oder im Schritt „Code analysieren“ gefunden wurden, aber nicht in beiden vorhanden sind. Dadurch werden Jobs angezeigt, die während Ihres SMF-Datensatzes nicht ausgeführt wurden oder die im Schritt „Code analysieren“ nicht enthalten waren. Diese Ausgabe ist nur verfügbar, wenn Sie den Codeanalyseschritt vor der SMF-Analyse in Ihrem Job ausführen.

Bewährte Methoden

Um umfassende Ausgaben für Batch-Jobs (Typ 30) zu erhalten, stellen Sie sicher, dass der Name Ihrer JCL-Datei mit dem Jobnamen übereinstimmt, um aussagekräftige Ergebnisse im Vergleich der Codeanalyse zu erhalten.

Generieren Sie technische Dokumentation

Sie können technische Dokumentation für Ihre Mainframe-Anwendungen erstellen, die gerade modernisiert werden. Durch die Analyse Ihres Codes kann AWS Transform automatisch eine detaillierte Dokumentation Ihrer Anwendungsprogramme erstellen, einschließlich Beschreibungen der Programmlogik, Abläufe, Integrationen und Abhängigkeiten, die in Ihren Altsystemen vorhanden sind. Diese Dokumentationsfunktion hilft, Wissenslücken zu schließen, sodass Sie fundierte Entscheidungen treffen können, wenn Sie Ihre Anwendungen auf moderne Cloud-Architekturen umstellen.

Note

Wenn Sie die Generierung von technischer Dokumentation anfordern, führt AWS Transform Codeanalysen, einschließlich Codeabhängigkeitsanalysen, durch, die für die Erstellung der Dokumentation erforderlich sind.

Um technische Dokumentation zu erstellen

1. Wählen Sie im linken Navigationsbereich unter Technische Dokumentation generieren die Option Dateien auswählen und Einstellungen konfigurieren aus.
2. Wählen Sie die Dateien im Amazon S3 S3-Bucket aus, für die Sie Dokumentation generieren möchten, und konfigurieren Sie die Einstellungen auf der Registerkarte Collaboration.

Note

Die ausgewählten Dateien sollten denselben Kodierungstyp haben (d. h. alle in derselben CCSID — UTF8 oder ASCII). Andernfalls enthält die generierte technische Dokumentation möglicherweise leere Felder oder Abschnitte.

3. Wählen Sie die Detailebene der Dokumentation aus:
 - Zusammenfassung — Bietet einen allgemeinen Überblick über jede Datei im Geltungsbereich. Enthält außerdem eine einzeilige Zusammenfassung der einzelnen Dateien.
 - Detaillierte Funktionsspezifikation — Enthält umfassende Informationen zu jeder Datei im Bereich der Mainframe-Anwendungstransformation. Einige Details umfassen Logik und Ablauf, Abhängigkeiten, Eingabe- und Ausgabeverarbeitung sowie verschiedene Transaktionsdetails.

Note

Dokumentation kann nur für COBOL- und JCL-Dateien generiert werden.

4. Klicken Sie auf Weiter.
5. Sobald AWS Transform die Dokumentation generiert hat, überprüfen Sie die Dokumentationsergebnisse, indem Sie dem Amazon S3 S3-Bucket-Pfad in der Konsole folgen, wo die Ergebnisse generiert und gespeichert werden.
6. Sobald die Dokumentation generiert ist, können Sie auch den AWS Transform-Chat verwenden, um Fragen zur generierten Dokumentation zu stellen und über die nächsten Schritte zu entscheiden.

Fügen Sie Benutzerinformationen zur Dokumentation hinzu

```
ARTIFACT_ID.zip  
### app/
```

```
### File1.CBL
### File2.JCL
### subFolder/
#   # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

Optionale Dateien können zur ZIP-Datei hinzugefügt werden, um die Qualität der generierten Dokumentation zu verbessern und ein individuelles PDF-Deckblatt bereitzustellen. Einige davon können sein:

- Datei `glossary.csv`: Sie können wählen, ob Sie ein optionales Glossar in der Zip-Datei im S3-Bucket bereitstellen und hochladen möchten. Das Glossar ist im CSV-Format. Dieses Glossar hilft bei der Erstellung von Dokumentationen mit relevanten Beschreibungen, die dem Kundenvokabular entsprechen. Eine `glossary.csv` Beispieldatei sieht wie folgt aus:

```
LOL,Laugh out loud
ASAP,As soon as possible
WIP,Work in progress
SWOT,"Strengths, Weaknesses, Opportunities and Threats"
```

- `pdf_config.json`: Sie können diese optionale Konfigurationsdatei verwenden, um PDF-Dokumente zu generieren, die den Formaten und Standards ihres Unternehmens entsprechen, einschließlich Kopf- und Fußzeilen, Logos und benutzerdefinierter Informationen. Ein Beispiel sieht wie folgt aus: `pdf_config.json`

```
{
  "header": {
    "text": "Acme Corporation Documentation",
    "logo": "header-logo.png"
  },
  "customSection": {
    "variables": [
      {
        "key": "business Unit",
        "value": "XYZ"
      },
      {
```

```

    "key": "application Name",
    "value": "ABC"
  },
  {
    "key": "xxxxxxxxxxx",
    "value": "yyyyyyyyyyyyyy"
  },
  {
    "key": "urls",
    "value": [
      {
        "text": "Product Intranet Site",
        "url": "https://example.com/intranet"
      },
      {
        "text": "Compliance Policies",
        "url": "https://example.com/policies"
      }
    ]
  }
],
"footer": {
  "text": "This document is intended for internal use only. Do not distribute
without permission.",
  "logo": "footer-logo.png",
  "pageNumber": true
}
}

```

- Kopfzeile:
 - Für die PDF-Datei mit dem Deckblatt ist der Standardtext der Projektname.
 - Für jede Programm-PDF-Datei ist der Standardtext der Programmname.
 - Es gibt kein Standardlogo. Wenn kein Header-Logo konfiguriert ist, wird kein Logo angezeigt.
 - Die Schriftgröße und die Logogröße müssen dynamisch auf der Grundlage der Anzahl der Wörter oder der Größe der Logo-Datei geändert werden.
- Benutzerdefinierter Bereich:
 - Wenn der benutzerdefinierte Abschnitt nicht konfiguriert ist, wird er in der PDF-Datei weggelassen.
 - Der Link muss anklickbar sein.

- Fußzeile:
 - Es gibt keinen Standardtext oder kein Standardlogo für die Fußzeile.
 - Die Seitenzahl wird standardmäßig in der Fußzeile angezeigt, sofern nicht ausdrücklich anders konfiguriert.
 - Die Schriftgröße und die Logogröße werden dynamisch auf der Grundlage der Anzahl der Wörter oder der Größe der Logo-Datei geändert.

Generieren Sie die Dokumentation im Inline-Viewer

Sie können die PDF-Dateien im Schritt „Technische Dokumentation generieren“ anzeigen.

Um die PDF-Dateien anzusehen

1. Navigieren Sie zur Registerkarte „Ergebnisse der Dokumentation überprüfen“.
2. Suchen Sie das PDF in der Tabelle mit den generierten PDF-Dateien.
3. Wählen Sie entweder die Datei und dann Ansicht aus, oder wählen Sie das Linkelement aus, das dem Dateinamen überlagert ist.

Die PDF-Datei wird in AWS Transformieren geöffnet. Sie haben die Option, den Bildschirm oben rechts zu erweitern.

Note

AWS Transform bietet Ihnen auch die Möglichkeit, entweder eine XML- oder eine PDF-Version der generierten technischen Dokumentation herunterzuladen.

Important

Wenn Sie Probleme mit dem Inline-Viewer für die Dokumentation haben, stellen Sie sicher, dass der S3-Bucket korrekt eingerichtet ist. Weitere Informationen zur CORS-Richtlinie des S3-Buckets finden Sie unter [the section called “CORS-Berechtigungen für den S3-Bucket”](#).

Extrahieren Sie Geschäftslogik

Sie können wichtige Geschäftslogik aus Ihren Mainframe-Anwendungen extrahieren, die gerade modernisiert werden. AWS Transform analysiert Ihren Code automatisch, um kritische Geschäftselemente zu identifizieren und zu dokumentieren, einschließlich detaillierter Prozessabläufe und Geschäftslogik, die in Ihre Anwendungen eingebettet ist. Diese Funktion dient mehreren Beteiligten auf Ihrem Weg zur Modernisierung. Geschäftsanalysten können die extrahierte Logik nutzen, um präzise Geschäftsanforderungen zu erstellen und Lücken oder Inkonsistenzen in aktuellen Implementierungen zu identifizieren. Entwickler erhalten die Möglichkeit, komplexe Funktionen älterer Systeme schnell zu verstehen, ohne umfangreiche Mainframe-Kenntnisse zu benötigen.

Note

Wenn Sie die Extraktion von Geschäftslogik anfordern. AWS Transform führt Codeanalysen durch, einschließlich Codeabhängigkeit und Einstiegsanalyse, die für die Extraktion der Geschäftslogik erforderlich sind.

Um Geschäftslogik zu extrahieren

1. Wählen Sie im linken Navigationsbereich unter Geschäftslogik extrahieren die Option Einstellungen konfigurieren aus.
2. Wählen Sie auf der Registerkarte Zusammenarbeit aus, wie Sie Geschäftslogik extrahieren möchten:
 - Anwendungsebene: Generiert Geschäftsdokumente für alle Geschäftsfunktionen, Transaktionen, Batch-Jobs und Dateien. Dadurch werden alle Dateien in der Anwendung ausgewählt.
 - Dateiebene: Generiert Geschäftsdokumente nur für Dateien, die Sie aus der Dateitabelle auswählen.

Note

- Für beide Optionen können Sie „Detaillierte Funktionsspezifikation einbeziehen“ auswählen, sodass AWS Transform den Kontrollfluss und umfassende Geschäftsregeln für die ausgewählten Dateien enthält.

- Die ausgewählten Dateien sollten denselben Kodierungstyp haben (d. h. alle in derselben CCSID — UTF8 oder ASCII). Andernfalls könnte die generierte Dokumentation leere Felder oder Abschnitte enthalten.
- Dokumentation kann nur für COBOL- und JCL-Dateien generiert werden.
- Auf Anwendungsebene werden Programme, die von CICS-Transaktionen und Batch-Jobs verwendet werden, gruppiert, während alle anderen Programme als Nicht zugewiesen kategorisiert werden.

3. Klicken Sie auf Weiter.
4. Sobald AWS Transform die Geschäftslogik extrahiert hat, speichert es die Ergebnisse in einem Amazon S3 S3-Bucket im JSON-Format, sodass Sie sie online anzeigen können.

Note

Die Anzahl der generierten Geschäftsregeldateien ist möglicherweise größer als Ihre ursprüngliche Auswahl. Bei einigen ausgewählten Dateien kann die Extraktion von Geschäftsregeln ausgelöst werden, sodass weitere abhängige Dateien eingeschlossen werden, die ebenfalls in der Ergebnistabelle angezeigt werden.

Sehen Sie sich die extrahierte Geschäftsdokumentation online an

Sie können die Geschäftslogik im Schritt Geschäftsregel extrahieren einsehen. Um das zu tun,

1. Navigieren Sie zu Ergebnisse der Extraktion von Geschäftslogik überprüfen.
2. Wählen Sie das Dokument, das Sie anzeigen möchten, aus der Tabelle aus, und klicken Sie dann auf die Schaltfläche Ergebnis anzeigen.

Die Seite mit der Geschäftsdokumentation wird in einem neuen Browser-Tab geöffnet.

Zersetzung

Sie können Ihren Code in Domänen zerlegen, die Abhängigkeiten zwischen Programmen und Komponenten berücksichtigen. Auf diese Weise können die zugehörigen Dateien und Programme innerhalb derselben Domäne entsprechend gruppiert werden. Es trägt auch dazu bei, die Integrität der Anwendungslogik während des Zerlegungsprozesses aufrechtzuerhalten.

 Note

Wenn Sie eine Zerlegung anfordern, führt AWS Transform eine Codeanalyse durch, einschließlich einer Codeabhängigkeitsanalyse, die für die Zerlegung erforderlich ist. Wir empfehlen außerdem, vor der Zerlegung eine Extraktion der Geschäftslogik durchzuführen, um bessere Ergebnisse zu erzielen.

Gehen Sie wie folgt vor, um mit der Zerlegung Ihrer Anwendung zu beginnen:

1. Wählen Sie im linken Navigationsbereich die Option Code zerlegen aus.

 Note

Eine Domäne, Nicht zugewiesen, wird automatisch für alle Dateien erstellt, die keiner Domäne zugeordnet sind. Bei der ersten Navigation sollten alle Dateien mit „Nicht zugewiesen“ verknüpft werden, es sei denn, Domänen wurden anhand der Extraktion von Geschäftslogik auf Anwendungsebene vorgeschlagen.

2. Erstellen Sie über das Menü Aktionen eine neue Domäne und wählen Sie dann Domäne erstellen.

3. Geben Sie unter Domain erstellen den Domainnamen und eine optionale Beschreibung ein und markieren Sie einige Dateien als Seeds.

- CICS-konfigurierte Dateien (CSD) und Scheduler-konfigurierte Dateien (SCL) können für die automatische Seed-Erkennung verwendet werden.
- Sie können auch nur eine Domäne als gemeinsame Komponente festlegen. Die Dateien in dieser Domäne sind mehreren Domänen gemeinsam.

4. Wählen Sie Erstellen aus.

 Note

Sie können mehrere Domains mit unterschiedlichen Dateien als Seeds erstellen.

5. Nachdem Sie alle Domains und Seeds bestätigt haben, wählen Sie Zerlegen.

6. AWS Transform überprüft die Quellcodedateien und zerlegt sie dann in Domänen mit Programmen und Datensätzen mit ähnlichen Anwendungsfällen und hohen Programmierabhängigkeiten.

AWS Transform bietet Ihnen eine tabellarische und grafische Ansicht der zerlegten Domänen als Abhängigkeiten. Die Diagrammansicht bietet drei Optionen:

- Domänenansicht — In visueller Form können Sie sehen, wie verschiedene Domains zueinander in Beziehung stehen.
- Abhängigkeitsansicht — Kann alle Dateien in jeder Domain als komplexes Abhängigkeitsdiagramm anzeigen. Wenn ein Knoten, der zu einer Domain hinzugefügt wurde, keine Informationen von einem Seed in derselben Domain erhalten hat, wird dieser Knoten entweder als nicht zugewiesen (Knoten hat keine Informationen erhalten), getrennt (in einem Untergraph, der keine Seed-Informationen erhalten hat) oder in eine andere Domain (Knoten hat Informationen von mindestens dieser Domain empfangen) vorhergesagt.
- Untergraphenansicht — Der Benutzer kann Untergraphen erstellen, um eine Teilmenge von Knoten zu visualisieren, um die relationalen Auswirkungen und Grenzen dieser Sammlung von Knoten besser zu verstehen.
 - Um einen Untergraphen zu erstellen, wählen Sie eine Gruppe von Knoten aus und wählen Sie in der Werkzeugleiste die Option Untergraphen extrahieren
 - Das Zusammenführen von Untergraphen ist verfügbar, wenn zusätzlich zu den beiden Untergraphen, die Sie zusammenführen, ein neuer dritter Untergraph erstellt wird.

 Note

Wiederholen Sie diese Schritte, um weitere Domains hinzuzufügen oder Ihre bereits erstellten Domains mit einem anderen Satz von Seeds neu zu konfigurieren, falls Ihnen die aktuelle Domainstruktur nicht gefällt.

7. Wenn Sie fertig sind, wählen Sie Weiter.

Samen

Seeds sind die grundlegenden Eingaben für die Phase der Codezerlegung. Jede Komponente oder Datei (z. B. JCL-, COBOL-, Db2-Tabellen, CSD- und Scheduler-Dateien) kann als Ausgangsdatei nur einer Domäne zugewiesen werden, wodurch klare Grenzen und eine klare Ausrichtung während des Zerlegungsprozesses gewährleistet werden.

Die Identifizierung der Seeds hängt von der Struktur der Anwendung oder des Portfolios ab. Im Fall einer typischen Legacy-Mainframe-Anwendung können Seeds häufig anhand etablierter Namenskonventionen, Gruppierung auf Batch-Ebene im Scheduler und Gruppierung auf

Transaktionsebene, die im CICS-System definiert ist, bestimmt werden. Darüber hinaus können Datenbanktabellen auch als Ausgangswerte dienen und so eine weitere Strukturebene für die Zerlegung bereitstellen.

Dateien mit and/or Aktualisierungsabhängigkeiten importieren

Während der Zerlegung können Sie eine JSON-Datei für die Abhängigkeiten hochladen, die die vorhandenen Dateien ersetzt, die durch die von AWS Transform durchgeführte Abhängigkeitsanalyse generiert wurden.

Mit der Funktion Abhängigkeiten exportieren können Sie die im Zerlegungsschritt generierte JSON-Datei für Abhängigkeiten herunterladen. Nach dem Herunterladen können Sie die Datei gemäß Ihren Anforderungen ändern. Anschließend können Sie Abhängigkeiten mithilfe der Upload-Funktion von AWS Transform importieren, mit der Sie die neue JSON-Datei mit den Abhängigkeiten hochladen können, die die durch die Abhängigkeitsanalyse generierte Datei ersetzt. Danach wird das Diagramm im Zerlegungsschritt aktualisiert.

Um Abhängigkeiten zu exportieren, zu ändern und zu importieren

1. Wählen Sie auf der Seite Zerlegungsergebnisse anzeigen die Option Aktionen aus.
2. Wählen Sie in der Dropdownliste unter Andere Aktionen die Option Abhängigkeitsdatei aktualisieren aus.
3. Im Modal „Abhängigkeitsdatei aktualisieren“
 - a. Laden Sie die Abhängigkeitsdatei AWS Transform herunter, die aus den vorhandenen Analyseergebnissen erstellt wurde.
 - b. Ändern Sie in der heruntergeladenen Datei die Abhängigkeiten je nachdem, was Sie erreichen möchten.
 - c. Speichern Sie diese Datei nach der Änderung und laden Sie sie hoch, indem Sie auf die Schaltfläche Abhängigkeitsdatei hochladen klicken.

Note

Das einzig akzeptierte Dateiformat ist die JSON-Datei.

4. Wählen Sie als Nächstes Import.

AWS Transform importiert die Abhängigkeitsdatei und erstellt auf der Grundlage Ihrer Eingabe ein neues Abhängigkeitsdiagramm.

Domänen importieren und and/or aktualisieren

Für Kunden, denen bereits vor der Zerlegung Domänen, Stammdaten und and/or Dateibeziehungen zugeordnet wurden, können Sie diese Domaindefinition über die Funktion Domain-Datei importieren hochladen, die im Menü Aktionen verfügbar ist. Einige Beispiele dafür, wann diese Funktion verwendet werden kann:

- Zersetzung aus einem anderen Job vorziehen
- Fachexperten, die dieses Mapping zur Verfügung stellen

Sobald die Domänendatei importiert wurde, kann der Benutzer entweder die Zerlegung anhand der Domänendefinition durchführen oder, wenn er zufrieden ist, die Domänendefinition speichern und dann absenden.

Parent/child/neighbor Dateien

In einem Abhängigkeitsdiagramm stehen Programme über verschiedene Arten von Verbindungen zueinander in Beziehung. Das Verständnis dieser Beziehungen hilft Ihnen, Programmabhängigkeiten während der Transformation Ihrer Mainframe-Anwendungen zu analysieren. Es hilft auch dabei, die Grenzen einer Domäne zu verstehen. Wenn Sie beispielsweise eine Domäne und dann eine übergeordnete Ebene auswählen, werden Ihnen die verbundenen Knoten angezeigt.

Beziehungen zu übergeordneten Elementen — Eine übergeordnete Datei ruft andere Programme auf oder steuert sie. Eltern stehen in der Hierarchie über ihren abhängigen Programmen. Sie können Eltern auf einer Ebene oder auf allen Ebenen auswählen.

Beziehungen zwischen Kindern — Eine untergeordnete Datei wird vom übergeordneten Programm aufgerufen oder gesteuert. Kinder befinden sich in der Dateihierarchie unter ihren Eltern.

Nachbarschaftsbeziehungen — Nachbarn sind Dateien auf derselben Hierarchieebene. Sie verwenden dasselbe übergeordnete Programm und können direkt miteinander interagieren.

Code neu fälschen

Reforge verwendet Large Language Models (LLMs), um die Qualität des umgestalteten Codes zu verbessern. Bei der anfänglichen COBOL-to-Java Transformation wird die funktionale Äquivalenz gewahrt, während COBOL-influenced Datenstrukturen und Variablennamen aus dem Altsystem

beibehalten werden. Reforge strukturiert diesen Code neu, sodass er modernen Java-Praktiken und -idiomen folgt, und ersetzt COBOL-style Konstrukte durch native Java-Sammlungen und Namenskonventionen. Dies macht den Code für Java-Entwickler lesbarer und wartbarer.

Note

Die Quoten für Reforge sind:

- 3.000.000 Codezeilen pro Job
- 50.000.000 Codezeilen pro Benutzer und Monat

Forge deinen Code nach dem Refactoring neu, indem du die folgenden Schritte befolgst:

1. Wählen Sie im linken Navigationsbereich die Option Java-Code neu formieren und wählen Sie dann Code-Reforge konfigurieren aus.
2. Geben Sie den S3-Speicherort für Ihr komprimiertes baubares Quellprojekt an und wählen Sie Weiter. Verwenden Sie diese Zip-Struktur:

```
input.zip
  ### PROJECT-pom
  ### PROJECT-entities
  ### PROJECT-service
  ### PROJECT-tools
  ### PROJECT-web (optional)
  ### pom.xml
```

AWS Transform analysiert Ihr Zip-Paket, um Dateien innerhalb des PROJECT-service Verzeichnisses zu finden, sodass es eine auswählbare Liste von Klassen bereitstellt, die Sie neu fälschen können. Diese Klassen haben das Suffix. `ProcessImpl.java`

3. Füllen Sie die Seite „Klassen für die Neuformierung auswählen“ aus und klicken Sie auf Weiter. Verfolge den Status der Neuformierung auf dem Worklog-Tab.
4. Sieh dir die Ergebnisse deiner abgeschlossenen Reforge-Bearbeitung auf der Seite „Ergebnisse anzeigen“ an. Dort wird der Reforge-Status pro Klasse angezeigt. Außerdem wird angegeben, wo sich das Reforge-Ergebnis in Ihrem S3-Bucket befindet.

Sobald AWS Transform diese Eingabe von Ihnen erhält, erhalten Sie eine herunterladbare Datei mit den Reforge-Ergebnissen.

Dies ist die Zip-Struktur, die aus einem erfolgreichen Reforge resultiert:

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project enthält den neu gefälschten Quellcode.
- Dateien, die überarbeitet wurden, deren Kompilierung jedoch nicht erfolgreich abgeschlossen wurde, befinden sich unter und sind benannt. /src/main/resources/reforge/originalClassName.java.incomplete originalClassName.java.incomplete
Vergleichen Sie diese mit den Originalversionen der Dateien, um neue Funktionen auszuwählen, die Sie speichern möchten.
- Für AWS Transform bereitgestellte Quelldateien, die erfolgreich überarbeitet wurden, werden Sicherungskopien erstellt und benannt. src/main/resources/reforge/originalClassName.java.original originalClassName.java.original Die überarbeiteten Versionen der Dateien ersetzen die für Transform bereitgestellten Quelldateien.
AWS

Note

Die originalClassName.java Dateien werden nur dann durch die neu gefälschten Dateien ersetzt, wenn der Neuformierungsvorgang erfolgreich ist. Andernfalls behalten sie den ursprünglichen Inhalt bei.

- reforge.log enthält Protokolle, anhand derer Sie Auftragsfehler diagnostizieren oder bei Problemen dem AWS Support zur Verfügung stellen können.
- tokenizer_map.json enthält eine Zuordnung von Token-IDs zu Ihren Daten, wie z. B. Dateipfaden und class/method Namen, die aus Datenschutzgründen in den Protokollen tokenisiert werden. Sie können diese Datei dem Support im Falle eines Problems zur Verfügung stellen. AWS

Planen Sie das Testen Ihrer modernisierten Anwendungen

Sie können Testpläne für Ihre modernisierten Mainframe-Anwendungen auf der Grundlage von extrahierten Codeattributen, Auftragskomplexität und Scheduler-Pfaden erstellen und verwalten. AWS Transform hilft bei der Priorisierung der zu testenden Jobs und identifiziert die spezifischen

Artefakte, die für jeden Testfall benötigt werden. Der Testplanungsprozess ist in drei Hauptphasen unterteilt: Konfiguration, Umfang und Überprüfung.

Um einen Testplan zu erstellen

1. Konfigurieren Sie die Testplaneinstellungen
 - a. Wählen Sie im linken Navigationsbereich unter Testen planen die Option Einstellungen konfigurieren aus.
 - b. (Optional) Stellen Sie S3-Pfade für Ihre Business Logic Extraction (BLE) bereit. Diese Artefakte verbessern die Qualität des Testplans. Ohne BLE-Artefakte bleiben einige Felder im Testplan möglicherweise unvollständig.
2. Definieren Sie den Umfang des Testplans
 - a. Wählen Sie Einstiegspunkte, wie z. B. Batch-Jobs, aus, die in Ihren Testplan aufgenommen werden sollen.
 - b. Filtern und sortieren Sie Jobs auf der Grundlage mehrerer Attribute:
 - Geschäftsfunktionen (extrahiert aus BRE BLE)
 - Domänen (aus der Zerlegungsphase)
 - Dateipfade und Speicherorte
 - Benutzerdefinierte Suchkriterien
 - c. Wählen Sie einzelne Jobs oder ganze Gruppen zum Testen aus.
 - d. Überprüfen Sie die Arbeitsbeziehungen und Abhängigkeiten.
3. Überprüfen Sie den Testplan und passen Sie ihn an

Der generierte Testplan bietet umfassende Informationen, darunter:

- Bevorzugte Ausführungsreihenfolge basierend auf Abhängigkeiten
- Auftragsgruppenzuweisungen aus dem Scheduler
- Komplexitätswerte, bei denen es sich um aggregierte Ergebnisse für Testfälle handelt
- Assoziationen von Geschäftsdomänen
- Metriken zur zyklomatischen Komplexität
- Abhängigkeiten zwischen Datensätzen und Tabellen
- Zeilen mit Code-Metriken
- Zuordnungen von Geschäftsfunktionen

Optionen zur Anpassung des Testplans

Ihr Testplan kann an spezifische Bedürfnisse angepasst werden. Beispielsweise ist Folgendes möglich:

- Erstellen Sie neue Testfälle, indem Sie mehrere Einstiegspunkte auswählen
- Führen Sie bestehende Testfälle zusammen, um verwandte Funktionen zu kombinieren
- Teilen Sie Testfälle für detailliertere Tests auf
- Entfernen Sie unnötige Testfälle
- Fügen Sie Einstiegspunkte für bestehende Testfälle hinzu oder entfernen Sie sie
- Ändern Sie die Beschreibungen und Attribute von Testfällen
- Passen Sie die Ausführungsreihenfolge an

Detaillierte Informationen zum Testfall

Jeder Testfall enthält Details, die seinen Inhalt und die zugehörigen Datensätze oder Datendateien beschreiben:

- Umfassende Beschreibung des Testumfangs
- Vollständige Liste der Einstiegspunkte enthalten
- Aggregierte Kennzahlen, die Komplexität und Größe aufzeigen
- Geschäftsregeln und automatisierte Anleitung für Testfälle
- Abhängigkeiten zwischen Datensätzen und Tabellen mit direction (input/output)
- Interaktive Visualisierung von Abhängigkeitsdiagrammen
- Voraussetzungen und Anforderungen für die Ausführung

Funktionen zur Datenverwaltung

Diese Details helfen Ihnen dabei, die Daten im Zusammenhang mit dem Testfall zu verstehen. Sie können:

- Datensätze nach input/output Richtung filtern
- Identifizieren Sie die erforderlichen Artefakte für die Testausführung
- Verfolgen Sie Datenabhängigkeiten zwischen Testfällen
- Überwachen Sie die Nutzung von Datensätzen in allen Testplänen

 Note

AWS Transform analysiert automatisch die Abhängigkeiten des Schedulers und weist Komplexitätsbewertungen zu, um die Testbemühungen zu priorisieren. Höhere Komplexitätswerte weisen auf Jobs hin, für die während des Testprozesses möglicherweise gründlichere Tests oder eine Isolierung erforderlich sind.

Geschäftsregeln und Anleitungen für Testfälle

Der AWS Transform-Testplan enthält Empfehlungen für Ihren Testfallplan, der auf der Extraktion von Geschäftsregeln basiert:

- Automatische Verarbeitung von Geschäftsregeln mithilfe von LLM
- Generierung synthetischer Testfälle
- Testleitfaden für spezifische Geschäftsszenarien
- Rückverfolgbarkeit zwischen Regeln und Testfällen

Der endgültige Testplan wird am angegebenen S3-Speicherort gespeichert und enthält alle erforderlichen Informationen, um Ihre Teststrategie effektiv umzusetzen. Sie können den Testplan zur Integration mit anderen Testtools oder Dokumentationssystemen exportieren.

 Note

Es werden zwar Anleitungen für synthetische Testfälle bereitgestellt, die eigentlichen Testartefakte müssen jedoch separat auf der Grundlage der Anleitungen erstellt werden. Der Testplan dient als umfassender Entwurf für Ihre Teststrategie, generiert jedoch weder die Testdaten noch die Ausführungsskripten.

Regeln für die Erstellung von Testfällen — Zusammenfassung

Allgemeine Regeln

- Ein Testfall enthält 1 bis viele JCLs in der Reihenfolge der geplanten Ausführung
- Testfälle werden anhand gültiger unterstützter Scheduler (CA7 und) erstellt Control-M
- Der Test führt JCLs aus, nicht den Scheduler selbst oder geplante Aufgaben

- Eine geplante Aufgabe ist einzigartig und führt nur eine JCL aus
- Eine JCL kann durch mehrere geplante Aufgaben ausgeführt werden
- Eine JCL kann existieren, ohne in einem Zeitplan enthalten zu sein

Standardregeln für die Erstellung von Testfällen

- Wenn sich eine einzelne JCL in einem Testfall befindet:
 - JCL ist nicht an einem Zeitplan beteiligt
 - JCL wird durch eine geplante Aufgabe ausgeführt, die in mehrere Zweige aufgeteilt ist
 - Ein Zweig im Zeitplan enthält nur diese JCL
- Bei mehreren JCLs in einem Testfall: steht für eine lineare Ausführungspfadsequenz innerhalb eines Zeitplanzweigs
- Wenn sich JCL an einer abweichenden geplanten Aufgabe befindet, wird JCL zu einem eigenen separaten Testfall
- Wenn sich JCL in einer konvergenten geplanten Aufgabe befindet: JCL kann einen neuen Testfall starten, wird aber nicht in vorherige Zweige aufgenommen
- Fehlende JCLs werden übersprungen und die Ausführung wird fortgesetzt (mit einer geplanten future Erweiterung, um Testfälle an fehlendem JCL-Punkt zu reduzieren)

Regeln für den Benutzerbetrieb

- Testfall erstellen: Der Benutzer wählt aus verfügbaren JCLs
 - Erfolgreich, wenn JCLs in der Reihenfolge der Zeitplanausführung vorhanden sind
 - Folgt der Reihenfolge der Ausführung des Zeitplans
- Fügen Sie eine JCL zum Testfall hinzu: Der Benutzer wählt aus verfügbaren JCLs aus
 - Erfolgreich, wenn JCL in der geplanten Ausführung des Testfalls vorhanden sein kann branch/path
- JCL aus dem Testfall entfernen: Der Benutzer kann jede JCL aus einem Testfall entfernen
 - Zulässig, auch wenn dies zu Lücken im Ausführungspfad führt
- Testfälle zusammenführen: Der Benutzer wählt zwei Testfälle aus, die kombiniert werden sollen
 - Erfolgreich, wenn JCLs zusammen in derselben Zeitplanausführungsverzweigung existieren können
 - Behält die Reihenfolge der Zeitplanausführung bei

- **Geteilter Testfall:** Der Benutzer wählt eine JCL in einem Testfall für die Aufteilung aus
 - Erzeugt einen neuen Testfall ab dem Split-Punkt
 - Der ursprüngliche Testfall wurde geändert, um JCLs nach dem Splitpoint auszuschließen
- **Testfall löschen:** Der Benutzer kann jeden erstellten Testfall löschen

Note

Sie können keine Testfälle aus einem anderen Scheduler branches/path erstellen, hinzufügen oder zusammenführen. Eine future Erweiterung ist geplant, um Operationen zu ermöglichen, die über divergent/convergent Aufgaben im Scheduler hinausgehen.

Generieren Sie Skripts zur Testdatenerfassung

Sie können JCL-Skripts generieren, um Testdaten von Ihren Mainframe-Systemen auf der Grundlage des im vorherigen Schritt erstellten Testplans zu sammeln. AWS Transform erstellt automatisch Datenerfassungsskripten für Datensätze, Datenbanktabellen und sequentielle Dateien, die für umfassende Tests benötigt werden. Der Datenerfassungsprozess ist in vier Hauptphasen unterteilt: Eingabekonfiguration, Testfallauswahl, Skriptkonfiguration und Skriptgenerierung.

Um Skripten zur Testdatenerfassung zu generieren

1. Geben Sie die Eingabe für den Testplan ein
 - a. Wählen Sie im linken Navigationsbereich unter Testdatenerfassung die Option Testplaneingabe bereitstellen aus.
 - b. Geben Sie unter Planen Sie das Testen Ihrer [modernisierten Anwendungen den S3-Pfad zu Ihrer Testplan-JSON-Datei](#) an.
 - c. Das Eingabefeld ist bereits ausgefüllt, wenn der Testplan in einem früheren Jobschritt generiert wurde.
 - d. Sie können auch einen Testplan aus anderen Jobs auswählen, indem Sie den entsprechenden S3-Standort angeben.
2. Wählen Sie Testfälle für die Datenerfassung aus
 - a. Sehen Sie sich die vollständige Liste der Testfälle aus Ihrem Testplan an.
 - b. Filtern und sortieren Sie Testfälle anhand mehrerer Attribute:

- Geschäftsfunktionen und Domänen
 - Abhängigkeiten von Datenbanktabellen
 - Anforderungen an Datensätze
 - Kennzahlen zur Komplexität
 - Benutzerdefinierte Suchkriterien
- c. Wählen Sie einzelne Testfälle aus oder verwenden Sie Optionen für die Massenauswahl.
 - d. Überprüfen Sie die Testfalldetails, einschließlich Einstiegspunkte, Kennzahlen und Geschäftsregeln, indem Sie auf einen Testfall klicken, um Details anzuzeigen.
3. Konfigurieren Sie Datenerfassungsskripts
- a. Laden Sie Beispielvorlagen und Konfigurationsdateien als Referenz herunter.
 - AWS Transform bietet Beispielvorlagen für das Entladen von Db2-Datenbanken, die REPRO-Funktion von VSAM-Dateien und die sequentielle Verarbeitung von Datensätzen, die als Leitfaden für die Art der Vorlagen dienen, die vom Prozess erwartet werden.
 - Die Standards können von Standort zu Standort variieren. Es wird daher erwartet, dass Kunden diese Vorlagen ändern oder ersetzen, wenn sie ihren eigenen Standards entsprechen.
 - Diese geänderten Vorlagen müssen in einen S3-Bucket hochgeladen werden, wo sie von der Testdatenerfassung verarbeitet werden können.
 - b. Stellen Sie eine variable Konfigurationsdatei (JSON-Format) bereit, die Folgendes enthält:
 - Benutzerpräfixe und umgebungsspezifische Konstanten
 - Datenbank-Konfigurationsparameter
 - Einstellungen für Zielendpunkte und Datenübertragungsparameter
 - Andere erforderliche Parameter, die vom Benutzer definiert wurden und in JCL-Vorlagen verwendet werden sollen
 - c. Laden Sie JCL-Vorlagen für verschiedene Datenerfassungsmethoden hoch:
 - Db2-Vorlage: Zum Entladen von Datenbanktabellen (für BMC, IBM DSN oder andere Entladeprogramme anpassen)
 - VSAM-Vorlage: Für die Verarbeitung von VSAM-Dateien (verwendet normalerweise das REPRO-Hilfsprogramm)

- Vorlage für sequentielle Datensätze: Für die Verarbeitung sequentieller Datensätze, partitionierter Datensätze, GDGs usw.

4. Überprüfe und verwalte generierte Skripte

Die generierten Skripte bieten umfassende Datenerfassungsfunktionen, darunter:

- Separate Skripten für die Datenerfassung „vor“ und „nach“ der Testausführung
- Organisierte Skriptstruktur nach Testfall und Datentyp
- Skripte werden automatisch im S3-Bucket gespeichert, um den Zugriff und die Übertragung zu erleichtern
- Generierte JCL-Skripte sind bereit für die Mainframe-Ausführung
- Die Variablenersetzung basiert auf der in den Vorlagen definierten Benutzerkonfiguration

Funktionen zur Skriptgenerierung

Generierte Skripte werden automatisch auf der Grundlage Ihrer Vorlagen und Konfiguration angepasst:

- Template-based Generierung: Verwendet Ihre bereitgestellten JCL-Vorlagen mit Variablenersetzung
- Umgebung: Beinhaltet Ihre spezifische Mainframe-Konfiguration
- Behandlung von Datentypen: Erstellt geeignete Skripts für sequentielle Datensätze, VSAM-Dateien und Datenbanktabellen
- Sammlung für Testfälle: Generiert sowohl „vor“ als auch „nach“ -Datenerfassungsskripten
- Sequentielle Verarbeitung von Datensätzen: Das AWS mitgelieferte Beispiel bietet eine Dateiübertragungsfunktion, die jedoch an die an Ihrem Standort verfügbaren Komprimierungsprogramme oder an Dienstprogramme wie Connect Direct oder Managed File Transfer usw. angepasst werden kann.

Strategie zur Datenerfassung

Die generierten Skripte unterstützen umfassende Datenerfassungsstrategien:

- Sequentielle Datensatzerfassung: REPRO- und Kopierdienstprogramme für VSAM und Flatfiles
- Entladen von Datenbanktabellen: Anpassbare Db2-Entladeprozesse

- Sequentielle Verarbeitung von Datensätzen: Anpassbare Nachbearbeitung sequentieller Datensätze wie Komprimierung, verwaltete Dateiübertragungsdienste usw.
- Abhängigkeitsmanagement: Koordinierte Erfassung auf der Grundlage der Testfalldefinition

Note

AWS Transform generiert Skripte auf der Grundlage Ihrer Vorlagen und Ihrer Konfiguration. Überprüfen Sie alle generierten JCLs, bevor Sie sie auf Ihrer Mainframe-Umgebung ausführen, um die Kompatibilität mit Ihrer spezifischen Systemkonfiguration und Ihren Sicherheitsanforderungen sicherzustellen.

Anpassung von Vorlagen und bewährte Methoden

ATX Test Data Collection bietet flexible Funktionen zur Anpassung von Vorlagen:

- Multi-utility Unterstützung: Passen Sie Vorlagen für verschiedene Mainframe-Dienstprogramme (BMC, IBM, DSN) an
- Variable-driven Konfiguration: Verwenden Sie Konstanten für umgebungsspezifische Parameter
- Wiederverwendbare Vorlagen: Erstellen Sie standardisierte Vorlagen für eine konsistente Skriptgenerierung
- Datenverarbeitung: Integrieren Sie unternehmensspezifische Anforderungen an die Datenverarbeitung
- Sicherheitsintegration: Schließen Sie angemessene Sicherheits- und Zugriffskontrollen ein
- Leistungsoptimierung: Konfigurieren Sie für eine effiziente Datenerfassung und -übertragung

Generierte Ausgabestruktur

Die generierten Skripte sind in Ihrem S3-Bucket mit der folgenden Struktur organisiert:

- Organisation der Testfälle: Skripte, gruppiert nach zugehörigen Testfällen
- Zeitpunkt der Erfassung: Separate Ordner für die Datenerfassung „vor“ und „nach“
- Klassifizierung von Datentypen: Skripte, die nach sequentiellen Datensätzen, Datenbanktabellen und Übertragungen organisiert sind
- Metadatendateien: Zusammenfassende Informationen und Anleitungen zur Ausführung
- Ready-to-transfer Format: JCL formatiert für den direkten Mainframe-Einsatz

Die endgültige Skriptsammlung wird am angegebenen S3-Speicherort gespeichert und enthält alle erforderlichen JCLs, um Ihre Datenerfassungsstrategie effektiv auszuführen. Sie können die Skripts herunterladen, um sie in Ihre Mainframe-Umgebung zu übertragen oder sie in automatisierte Bereitstellungsprozesse zu integrieren.

 Note

Zwar werden umfassende JCL-Skripts generiert, die tatsächliche Ausführung muss jedoch in Ihrer Mainframe-Umgebung erfolgen. Die Skripts dienen als sofort einsatzbereite Tools zur Datenerfassung, erfordern jedoch entsprechende Zugriffs- und Ausführungsberechtigungen für den Mainframe.

Generierung von Skripten zur Testautomatisierung

Sie können Testautomatisierungsskripte generieren, um Testfälle in Ihrer modernisierten Anwendung auf der Grundlage des im vorherigen Schritt erstellten Testplans auszuführen. AWS Transform erstellt automatisch umfassende Testskripte, die die im Rahmen des Testdatenerfassungsprozesses gesammelten Daten verwenden. Der Prozess der Skriptgenerierung für die Testautomatisierung besteht aus drei Hauptphasen: Eingabekonfiguration, Testfallauswahl und Ergebnisse der Skriptgenerierung.

Um Testskripte zu generieren

1. Geben Sie die Eingabe für den Testplan ein
 - a. Wählen Sie im linken Navigationsbereich unter Generierung von Testautomatisierungsskripten die Option Testplaneingabe bereitstellen aus.
 - b. Geben Sie unter Planen Sie das Testen Ihrer [modernisierten Anwendungen den S3-Pfad zu Ihrer Testplan-JSON-Datei](#) an.
 - c. Das Eingabefeld ist bereits ausgefüllt, wenn der Testplan in einem früheren Jobschritt generiert wurde.
 - d. Sie können auch einen Testplan aus anderen Jobs auswählen, indem Sie den entsprechenden S3-Standort angeben.
 - e. Das System verwendet diesen Testplan als Grundlage für die Generierung von Automatisierungsskripten.
2. Wählen Sie Testfälle für die Skriptgenerierung aus

- a. Sehen Sie sich die vollständige Liste der Testfälle aus Ihrem Testplan an.
- b. Filtern und sortieren Sie Testfälle anhand mehrerer Attribute:
 - Geschäftsfunktionen und Domänen
 - Abhängigkeiten von Datenbanktabellen
 - Anforderungen an Datensätze
 - Kennzahlen zur Komplexität
 - Benutzerdefinierte Suchkriterien
- c. Wählen Sie einzelne Testfälle aus oder verwenden Sie die Optionen für die Massenauswahl mit den Schaltflächen Alle markieren und Alle deaktivieren.
- d. Überprüfen Sie die Testfalldetails, einschließlich Einstiegspunkte, Kennzahlen und Geschäftsregeln, indem Sie auf einzelne Testfälle klicken.

Für die ausgewählten Testfälle werden Automatisierungsskripte für die Ausführung in der modernisierten Anwendung generiert.

3. Überprüfen und verwalten Sie die generierten Testautomatisierungsskripte:
 - Das System zeigt eine Erfolgsmeldung an, die den Abschluss der Skriptgenerierung bestätigt.
 - Generierte Testskripte werden automatisch an Ihrem angegebenen S3-Bucket-Speicherort gespeichert.
 - Greifen Sie auf die vollständige Liste der generierten Testskripte mit ihren jeweiligen S3-Speicherorten zu.
 - Für jeden Testfall ist das entsprechende Automatisierungsskript an einzelnen S3-Standorten gespeichert.
 - Die Skripts sind bereit für die Bereitstellung und Ausführung in Ihrer modernisierten Anwendungsumgebung.

Funktionen von Testautomatisierungsskripten

Die generierten Automatisierungsskripte bieten umfassende Testfunktionen:

- Modernisierte Anwendungstests: Skripte wurden speziell für die Ausführung von Testfällen in Ihrer transformierten Anwendung entwickelt
- Datenintegration: Nutzt die Testdaten, die im vorherigen Schritt der Testdatenerfassung gesammelt wurden. Diese Daten müssen für jeden Testfall in Ordner kopiert werden

- **Automatisierte Ausführung:** Skripte können verwendet werden, um Datenszenen einzurichten, Testfälle auszuführen und Ergebnisse zu vergleichen. Einige Parameter müssen entsprechend Ihrer Bereitstellungsumgebung festgelegt werden
- **Organisierte Struktur:** Die Skripte sind in Ihrem S3-Bucket systematisch nach Testfällen organisiert
- **Ready-to-deploy Format:** Skripte sind für die direkte Bereitstellung in Ihrer Testumgebung formatiert

Generierte Ausgabestruktur

Die generierten Testautomatisierungsskripte sind in Ihrem S3-Bucket mit der folgenden Struktur organisiert:

- **Organisation des Testfalls:** Für jeden Testfall ist ein spezielles Skript in einem individuellen S3-Ordner gespeichert
- **Execution-ready Format:** Skripte werden so formatiert, dass sie sofort bereitgestellt und ausgeführt werden können, nachdem je nach Umgebung eine Variable eingerichtet wurde
- **Zentraler Zugriff:** Auf alle Skripts kann von einem einzigen S3-Bucket-Standort aus zugegriffen werden, um eine einfache Verwaltung zu gewährleisten

Strategie zur Testausführung

Die generierten Skripte unterstützen umfassende Workflows zur Testausführung:

- **Einrichtung der Umgebung:** Skripte enthalten Funktionen zum Einrichten der ersten Daten für die Ausführung des Tests
- **Datenvorbereitung:** Integration der gesammelten Testdaten aus dem Schritt zur Erfassung der Testfalldaten
- **Ausführung von Testfällen:** Automatisierte Ausführung einzelner Testfälle in der modernisierten Anwendung
- **Ergebnisvergleich:** Built-in Funktionen zum Vergleich von Testergebnissen und zur Validierung des Anwendungsverhaltens

Note

AWS Transform generiert Testautomatisierungsskripte auf der Grundlage Ihres Testplans und ausgewählter Testfälle. Die Skripts sind für die Ausführung in Ihrer modernisierten

Anwendungsumgebung konzipiert und verwenden die im vorherigen Schritt gesammelten Testdaten. Überprüfen Sie alle generierten Skripts vor der Bereitstellung, um sicherzustellen, dass sie mit Ihren spezifischen Anwendungskonfigurations- und Testanforderungen kompatibel sind.

Bewährte Methoden für die Testautomatisierung

- **Validierung der Umgebung:** Stellen Sie vor der Ausführung des Skripts sicher, dass Ihre modernisierte Anwendungsumgebung ordnungsgemäß konfiguriert ist
- **Datenüberprüfung:** Stellen Sie sicher, dass die erforderlichen Testdaten aus der Erfassungsphase verfügbar und zugänglich sind
- **Anpassung des Skripts:** Überprüfen Sie die generierten Skripts und passen Sie sie nach Bedarf an Ihre spezifischen Testanforderungen an
- **Überwachung der Ausführung:** Implementieren Sie während der Ausführung des Testskripts eine angemessene Überwachung und Protokollierung
- **Ergebnisanalyse:** Richten Sie Prozesse für die Analyse der Testergebnisse und die Identifizierung von Anwendungsproblemen ein

Die endgültige Sammlung von Testautomatisierungsskripten bietet ein vollständiges Testframework zur Validierung Ihrer modernisierten Anwendungsfunktionalität. Die Skripts können in Ihre kontinuierlichen Testprozesse integriert oder als Teil Ihres Workflows zur Anwendungsvalidierung ausgeführt werden.

Bereitstellungsfunktionen in AWS Transformieren

AWS Transform unterstützt Sie bei der Einrichtung von Cloud-Umgebungen für modernisierte Mainframe-Anwendungen, indem es gebrauchsfertige Infrastructure-as-Code (IaC) -Vorlagen bereitstellt. Über die Chat-Oberfläche von AWS Transform können Sie auf vorgefertigte Vorlagen zugreifen, die wichtige Komponenten wie Rechenressourcen, Datenbanken, Speicher und Sicherheitskontrollen erstellen. Die Vorlagen sind in gängigen Formaten wie CloudFormation (CFN) und Terraform verfügbar. AWS Cloud Development Kit (AWS CDK), sodass Sie Ihre Infrastruktur flexibel bereitstellen können.

Diese Vorlagen dienen als Bausteine, die den Zeit- und Expertenaufwand für die Konfiguration von Umgebungen für Ihre modernisierten Mainframe-Anwendungen reduzieren. Sie können diese

Vorlagen an Ihre Bedürfnisse anpassen und erhalten so eine Grundlage für den Aufbau Ihrer Bereitstellungsumgebung.

Um die IaC-Vorlagen abzurufen, fragen Sie im AWS Transform-Chat nach den Infrastructure-as-Code Vorlagen, die Ihr bevorzugtes Modernisierungsmuster (wie AWS Transform for Mainframe Refactor), Ihre bevorzugte Topologie (Standalone oder Hochverfügbarkeit) und Ihr bevorzugtes Format (CloudFormation gegenüber Cloud Development Kit oder Terraform) verdeutlichen.

Erstellen und implementieren Sie Ihre modernisierte Anwendung nach dem Refactoring

Nachdem Sie den Refactoring-Prozess mit AWS Transform abgeschlossen haben, können Sie Ihre modernisierte Java-Anwendung erstellen und bereitstellen. Dieser Leitfaden führt Sie durch das Abrufen Ihres modernisierten Codes, die Konfiguration Ihrer Umgebung sowie die Bereitstellung und das Testen Ihrer Anwendung.

Note

Zusätzlich zu den hier bereitgestellten Anleitungen wird das von AWS Transform generierte Codepaket ein Dokument zur Einrichtung der AWS automatisierten Refaktor-Entwicklungsumgebung enthalten, das Anweisungen zur Einrichtung einer IDE (Integrated Development Environment) mit Developer Runtime enthält.

Topics

- [Voraussetzungen](#)
- [Schritt 1: Rufen Sie den modernisierten Code ab](#)
- [Schritt 2: Erstellen Sie die modernisierte Anwendung](#)
- [Schritt 3: Konfigurieren Sie die Testumgebung](#)
- [Schritt 4: Stellen Sie die modernisierte Anwendung bereit](#)
- [Schritt 5: Testen Sie die modernisierte Anwendung](#)
- [Weiteres Beispiel](#)

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein Refactoring-Job mit AWS Transform wurde erfolgreich abgeschlossen.
- Zugriff auf Ihren modernisierten Code.
- Auf Ihrem Entwicklungscomputer installierter und konfigurierter Build-Software-Tool-Stack, z. B. [Apache Maven oder Apache Tomcat](#). Weitere Informationen zur Runtime-Versionierung finden Sie in den Versionshinweisen zu [AWS Transform for Mainframe Runtime](#).
- Amazon Corretto oder eine Version von Java Runtime installiert und konfiguriert. Weitere Informationen zur Installation von Amazon Corretto finden Sie unter [Amazon Corretto](#) 24.
- Zugriff zum Erstellen und Konfigurieren von Amazon Aurora PostgreSQL-Datenbanken für Runtime-Komponenten, falls erforderlich. Weitere Informationen zur Erstellung der Aurora PostgreSQL-Datenbank finden Sie unter [Working with Amazon Aurora PostgreSQL](#).
- Administratorzugriff zur Bereitstellung von Anwendungen in Ihrer Laufzeitumgebung.
- In den Konzepten von [AWS Transform for Mainframe Runtime wurden grundlegende Konzepte](#) zu Anwendungen, die mit einer AWS automatisierten Refactoring-Lösung modernisiert wurden, geprüft.

Schritt 1: Rufen Sie den modernisierten Code ab

Um den modernisierten Code abzurufen

1. Laden Sie das generierte Codepaket herunter und extrahieren Sie es.
2. Öffnen `codebase/app-pom/pom.xml` und notieren Sie sich die erforderliche Runtime-Engine-Version. Zum Beispiel `<gapwalk.version>4.6.0</gapwalk.version>`.
3. Suchen Sie im heruntergeladenen Codepaket nach dem Dokument `Setup the AWS Automated Refactor Development Environment` als Referenz.

Schritt 2: Erstellen Sie die modernisierte Anwendung

Um Ihre modernisierte Anwendung zu erstellen

1. Greifen Sie über die Toolbox AWS Transform for Mainframe auf die Runtime zu.
2. Laden Sie die entsprechende Runtime-Version (angegeben unter [the section called “Schritt 1: Rufen Sie den modernisierten Code ab”](#)) herunter und installieren Sie sie auf Ihrem lokalen Entwicklungscomputer.

 Note

Zusätzliche Informationen zur Installation der Laufzeitabhängigkeiten auf Ihrem lokalen Computer finden Sie in Abschnitt 3.1 des Dokuments [Setup the AWS Automated Refactor Development Environment](#).

3. Öffnen Sie die Befehlszeile und navigieren Sie zum Stammverzeichnis Ihrer Anwendung.
4. Um bereitstellbare Pakete für die modernisierte Anwendung zu erstellen, führen Sie den Befehl `Maven build` aus:

```
mvn package
```

Einzelheiten zur grundlegenden [Organisation des modernisierten Codes finden Sie auf der Seite Anwendungsorganisation](#). Bei einer modernisierten Anwendung, die eine Frontend-Webanwendung enthält, können Sie beispielsweise zusätzlich zu den Laufzeitkomponenten mindestens die folgenden bereitstellbaren `.war` Aggregate erwarten:

- Serviceprojekt: Enthält ältere Elemente zur Modernisierung der Geschäftslogik

```
<business-app>-service.*.war
```

- Webprojekt: Enthält die Modernisierung von Elementen im Zusammenhang mit der Benutzeroberfläche

```
<business-app>-web.*.war
```

Schritt 3: Konfigurieren Sie die Testumgebung

Um Ihre Testumgebung zu konfigurieren

1. Konfigurieren Sie Ihre modernisierte Anwendungslaufzeit. Weitere Informationen finden Sie im Abschnitt [Konfiguration für Runtime einrichten](#) im AWS Mainframe Modernization Benutzerhandbuch.

 Note

In Abschnitt 5 des Handbuchs zur Einrichtung der AWS automatisierten Refaktor-Entwicklungsumgebung finden Sie Konfigurationsbeispiele für Laufzeitkomponenten.

2. Bereiten Sie Eingabe- und Ausgabedatensätze (I/O) für modernisierte Anwendungen vor. Modernisierte Anwendungen können sequentielle I/O Datensätze, VSAM-Datensätze oder andere verarbeiten.

 Note

Beispiele finden Sie in Abschnitt 6 der Entwicklungsumgebung „AWS Automatisierte Refaktor-Entwicklungsumgebung einrichten“.

3. Eine Laufzeitumgebung — Sie können Ihre bestehende Laufzeitumgebung verwenden oder eine neue Laufzeitumgebung erstellen.
 - Informationen zur Konfiguration einer nicht verwalteten Laufzeitumgebung finden Sie unter [Eine nicht verwaltete Anwendung einrichten](#).
 - Informationen zur Konfiguration einer verwalteten Laufzeitumgebung finden Sie unter [Eine verwaltete Anwendung einrichten](#).

Nach der Konfiguration der Testumgebung fahren Sie mit dem nächsten Schritt der Bereitstellung der modernisierten Anwendung fort.

Schritt 4: Stellen Sie die modernisierte Anwendung bereit

Stellen Sie die Anwendungsartefakte in der Runtime bereit, die Sie erstellt haben und in den [the section called “Schritt 3: Konfigurieren Sie die Testumgebung”](#) Abschnitten [the section called “Schritt 2: Erstellen Sie die modernisierte Anwendung”](#) und and/or konfiguriert haben.

Weitere Anleitungen zur Bereitstellung der modernisierten Anwendung finden Sie unter den folgenden Links:

- [Auf Amazon EC2 bereitstellen](#)
- [Bereitstellung auf Containern auf Amazon ECS und Amazon EKS](#)
- [Erstellen Sie eine AWS Mainframe Modernization Anwendung](#)

Schritt 5: Testen Sie die modernisierte Anwendung

Nach der Bereitstellung

1. Sehen Sie sich die verfügbaren [Runtime-APIs](#) an, um herauszufinden, wie Sie mit den modernisierten Anwendungen interagieren können.
2. Testen Sie Ihre Anwendung, um ihre funktionale Äquivalenz mit der Legacy-Anwendung in Einklang zu bringen. Weitere Informationen finden Sie beispielsweise unter [Testen einer Beispielanwendung](#) im AWS Mainframe Modernization Benutzerhandbuch.

Weiteres Beispiel

Ein konkretes Beispiel für die Modernisierung einer Mainframe-Anwendung mit AWS Transform finden Sie unter [Modernisierung der CardDemo](#) Mainframe-Anwendung.

Full-stack Windows-Modernisierung

AWS Transform bietet eine umfassende Windows-Modernisierung, einschließlich .NET-Modernisierung und SQL Server-Modernisierung.

Der AWS Transform-Agent für .NET kann Ihnen helfen, Ihre .NET-Anwendungen so zu modernisieren, dass sie mit plattformübergreifendem .NET kompatibel sind. [Sie können .NET mithilfe der .NET-Web-App oder der .NET-IDE modernisieren.](#)

AWS Transform for [SQL Server Modernization](#) ist ein AI-powered Service, der die Full-Stack-Modernisierung von Microsoft SQL Server-Datenbanken und den zugehörigen .NET-Anwendungen auf Amazon Aurora PostgreSQL automatisiert. Der Service orchestriert den gesamten Migrationsprozess von der Schemakonvertierung über die Datenmigration bis hin zur Änderung des Anwendungscode, sodass er dem neuen Ziel-PostgreSQL entspricht. Dadurch werden Ihre Teams produktiver, indem komplexe und arbeitsintensive Aufgaben automatisiert werden.

Themen

- [Modernisieren.NET mit AWS Transformieren](#)
- [Modernisierung von SQL Server](#)

Modernisieren.NET mit AWS Transformieren

Der AWS Transform Agent for .NET kann Ihnen helfen, Ihre .NET-Anwendungen so zu modernisieren, dass sie mit plattformübergreifendem .NET kompatibel sind. Diese Funktion wird als .NET-Modernisierung bezeichnet. Anschließend können Sie [AWS Transformieren Sie die Umgebung](#) in AWS Transform einen Transformationsjob für die .NET-Modernisierung erstellen.

Umgebungen

AWS Transform ist in verschiedenen Ausführungen verfügbar:

- Webkonsole: für die groß angelegte Transformation von bis zu 500 Repositorys gleichzeitig.
- Visual Studio IDE: Von Entwicklern geleitete Transformation einer Lösung oder eines Projekts in interaktiver und iterativer Zusammenarbeit mit dem Agenten. Empfohlen für mittlere bis große Projekte.

Sie können frei zwischen Webkonsole und IDE wechseln, um an einem Transformationsjob zu arbeiten.

Sie können AWS Transform auch von anderen IDEs und KI-Code-Begleitern aus aufrufen:

- Kiro: Verwandle dich von Kiro, indem du die Kraft „AWS Transformation für Kiro“ verwendest.
- Weitere KI-Code-Begleiter: Verwandeln Sie sich mit AWS Transform MCP-Agenten von Ihren bevorzugten KI-Programmierassistenten.

Fähigkeiten und Hauptmerkmale

- Analysieren Sie .NET Framework-Codebasen von Ihren Quellcodeverwaltungssystemen aus. Dazu gehören private NuGet Unterstützung, die Identifizierung von Abhängigkeiten zwischen verschiedenen Repositories und die Bereitstellung eines Analyseberichts.
- Automatisierte Transformation älterer .NET Framework-Anwendungen in plattformübergreifendes .NET, E-Mail-Benachrichtigungen und ein zusammenfassender Transformationsbericht.
- Einfache Integration mit den Quellcodeverwaltungsplattformen (BitBucket, GitHub, und GitLab), um vorhandenen Code aufzunehmen und transformierten Code an einen neuen Branch zu übergeben.
- Validierung von transformiertem Code durch Komponententests.

Unterstützte Versionen und Projekttypen

AWS Transform unterstützt die Transformation für diese Versionen von .NET-Versionen:

- .NET Framework 3.5 oder höher
- .NET Core 3.1
- .NET 5.x und höher
- .NET 8

AWS Transform kann in die folgenden .NET-Zielversionen transformiert werden:

- .NET 8
- .NET 10

AWS Transform unterstützt die Transformation dieser Arten von Projekten (nur C#):

- Klassenbibliotheken
- Konsolenanwendungen
- ASP.NET:
 - Model View Controller (MVC), einschließlich Razor Views im Frontend-Modus
 - SPA-Backends (Single Page Application) (Ebenen der Geschäftslogik)
 - Web-API
 - Webformulare
- Unit-Test-Projekte (NUnit, xUnit und MSTest)
- Dienste der Windows Communication Foundation (WCF)
- Projekte mit bereitgestellten plattformübergreifenden Versionen für Pakete von Drittanbietern oder private NuGet Pakete. Wenn ein plattformübergreifendes Äquivalent fehlt oder nicht verfügbar ist, versucht AWS Transform for .NET eine bestmögliche Konvertierung.

AWS Transform kann auch die folgenden Projekttypen in modernes .NET umwandeln. Dies ist eine Vorschaufunktion, die möglicherweise nicht so vollständig transformiert wird wie die unterstützten Projekttypen.

- WinForms Desktop-Projekte.
- WPF-Desktop-Projekte.
- Mobile Xamarin-Projekte.
- Projekte geschrieben in. VB.NET

Einschränkungen

Weitere Informationen zu Kontingenten und Einschränkungen für AWS Transform finden Sie unter [Kontingente für AWS Transformieren](#).

AWS Transform transformiert Folgendes nicht:

- Blazor-UI-Komponenten
- Win32-DLLs ohne kernkompatible Bibliotheken
- Repositories, die keine Lösungen enthalten.

AWS Transform ändert die ursprünglichen Repo-Branches nicht und kann nur in einen separaten Ziel-Branch schreiben, der in Ihrem Transformationsplan angegeben ist.

Menschliches Eingreifen

Während der Portierung von .NET Framework-Anwendungen auf plattformübergreifendes .NET werden Sie in den folgenden Szenarien möglicherweise um Eingaben oder Genehmigungen gebeten:

- Richten Sie einen Konnektor für Ihren Quellcode und Ihre Berechtigungen ein
- Bestätigen Sie den vorgeschlagenen Modernisierungsplan
- Laden Sie fehlende Paketabhängigkeiten hoch als NuGets
- Überprüfe und akzeptiere den transformierten Code

Weitere Informationen

Sie können Ihren .NET-Code modernisieren, indem Sie entweder die AWS Transform-Webanwendung oder das AWS Toolkit für verwenden. Visual Studio

- [Modernisieren Sie Ihren .NET-Code mithilfe der AWS Transformieren Sie die Webanwendung](#)
- [Modernisieren.NET in der IDE](#)
- [Bewährte Methoden für .NET-Transformationen](#)

Modernisieren Sie Ihren .NET-Code mithilfe der AWS Transformieren Sie die Webanwendung

AWS Transform for .NET ist ein neuer generativer AI-powered Agent, der entwickelt wurde, um ältere .NET-Anwendungen zu modernisieren. Sie können Ihren veralteten .NET-Code mithilfe der AWS Transform-Webanwendung oder der Visual Studio AWS Toolkit-Erweiterung modernisieren.

Gehen Sie wie folgt vor, um Ihren .NET-Code mithilfe der AWS Transform-Webanwendung zu modernisieren, indem Sie zur Webanwendung navigieren:

1. [Erstellen der AWS .NET-Jobplan transformieren](#)
2. [Einen Konnektor für ein Quellcode-Repository erstellen](#)
3. [Bestätigen Sie Ihre Repositories, um die Transformation vorzubereiten](#)

4. [Auflösen von Paketabhängigkeiten zur Vorbereitung der Transformation](#)
5. [Überprüfung Ihres Plans zur Vorbereitung auf die Transformation](#)
6. [Transformieren Sie Ihren .NET-Code](#)

Erstellen der AWS .NET-Jobplan transformieren

Nachdem Sie Ihren Workspace erstellt haben, wählen Sie auf der Registerkarte Jobs die Option Job erstellen aus. Folge dann den Anweisungen von AWS Transform im Chat-Bereich in natürlicher Sprache. Dies sind die typischen Schritte zum Erstellen einer .NET-Modernisierungsjobs.

1. AWS Transform fragt Sie, welche Art von Transformationsjob Sie erstellen möchten. Geben Sie im Chat .NET Modernization ein.
2. AWS Transform schlägt einen Jobnamen vor und fragt Sie, ob Sie den Jobnamen ändern möchten. Wenn Sie den Jobnamen ändern möchten, teilen Sie AWS Transform in natürlicher Sprache mit, ändern Sie den Jobnamen beispielsweise in ExampleCorpDotNet1. Andernfalls können Sie im Chat den vorgeschlagenen Jobnamen akzeptieren. Nachdem Sie den Jobnamen akzeptiert haben, werden Sie von AWS Transform im Chatfenster darüber informiert, dass der Job gerade erstellt wird.
3. AWS Transform erstellt den Transformationsjob.

Bestandteile des AWS .NET-Jobplan transformieren

Die AWS Transform.NET-Jobanzeige besteht aus 5 Registerkarten, die Sie aus den vertikalen Symbolen ganz links auswählen können: Aufgaben, Dashboard, Genehmigungen, Artefakte und Arbeitsprotokoll. Jede Registerkarte hat einen linken Bereich und einen mittleren Chat-Bereich. Manchmal erscheint ein rechter Bereich für die Zusammenarbeit, in dem zusätzliche Details angezeigt werden und menschliche Eingaben angefordert werden.

Aufgaben (Jobplan)

Auf dieser Registerkarte wird Ihr Jobplan im linken Bereich angezeigt. Ein .NET-Job besteht aus 5 Schritten:

1. Ressourcen für die Transformation bereitstellen: In dieser Phase erstellen Sie einen Konnektor zu Ihrem Code-Repository mithilfe von AWS CodeConnections. Abhängig von Ihren Repository-Berechtigungen muss ein Administrator des Code-Repositorys den Konnektor möglicherweise genehmigen und AWS Transform Zugriff auf das Repository gewähren.

2. Entdecken Sie Ressourcen für die Transformation: In dieser Phase erkennt AWS Transform Repositorys in der Quellcodeverwaltung, und Sie wählen einige oder alle von ihnen für die Bewertung aus.
3. Analysieren Sie den Code für die Transformation: Ausgewählte Repositorys werden bewertet, und Sie können Bewertungsberichte einsehen.
4. Bereiten Sie sich auf die Transformation vor: In dieser Phase benachrichtigt Sie AWS Transform, wenn in Ihren Repositorys Abhängigkeiten fehlen. Sie können die fehlenden Abhängigkeiten hochladen oder ignorieren. Wenn Sie kein Administrator für das Repo sind, muss möglicherweise ein Administrator den endgültigen Transformationsplan genehmigen.
5. Transformation: In dieser Phase AWS transformiert Transform Ihr Repo und informiert Sie über den aktuellen Status der Transformation, bis diese abgeschlossen ist. Sie können sich die Transformationsberichte ansehen, um zu verstehen, was geändert wurde und warum.

Sie können den Status für jeden Schritt einsehen:

- Nicht gestartet
- Warten Sie auf Benutzereingaben
- In Bearbeitung
- Completed

Dashboard

Die Registerkarte „Dashboard“ bietet eine allgemeine Zusammenfassung der Transformation. Hier werden Kennzahlen zur Anzahl der transformierten Jobs, zur angewandten Transformation und zur voraussichtlichen Zeit bis zum Abschluss der Transformation angezeigt. Unter dem Dashboard befindet sich eine Tabelle mit Repositorys und deren Status — In-progress „Fehlgeschlagen“ oder „Erfolgreich“.

Genehmigungen

Genehmigungsanfragen für den Job werden auf dieser Registerkarte angezeigt und abgeschlossen.

-Artefakte

Jjob-related Artefakte werden von dieser Registerkarte hoch- oder heruntergeladen.

Arbeitsprotokoll

AWS Transform protokolliert seine Aktionen auf der Registerkarte Worklog. Das Worklog enthält ein detailliertes Protokoll der Aktionen, die AWS Transform ergreift, zusammen mit menschlichen Eingaben und Ihren Antworten auf diese Anfragen.

Einen Konnektor für ein Quellcode-Repository erstellen

[Erstellen der AWS .NET-Jobplan transformieren](#) Danach werden auf der Registerkarte Aufgaben im linken Bereich des AWS Transformationsfensters die Phasen des Transformationsjobs aufgeführt. Die erste Phase lautet Ressourcen abrufen, die transformiert werden sollen. In dieser Phase können Sie Mitarbeiter einladen und ein Quellcode-Repository Connect. Im rechten Bereich des AWS Transformationsfensters geben Sie die Details an.

Jeder Transformationsauftrag muss nur über einen Quellcode-Repository-Connector verfügen. Der AWS Transform-Agent verwendet diesen Connector, um deine .NET-Codebasis von GitHub, GitLab, oder Bitbucket herunterzuladen, indem du [AWS CodeConnections](#) Du musst dich AWS CodeConnections in derselben Region wie dein AWS Transform-Job einrichten. Alternativ können Sie anstelle eines [Quellcode-Repositorys eine Connect zum Quellcode in Amazon S3](#) herstellen.

Note

Wenn Sie bereits über einen Quellcode-Repository-Connector verfügen, werden Sie von AWS Transform benachrichtigt. Wählen Sie Bestehenden Konnektor verwenden aus, um diesen Konnektor zu verwenden. Wenn Sie den vorhandenen Konnektor nicht verwenden möchten, lesen Sie weiter [Löschen eines vorhandenen Connectors](#) oben [Einen neuen Connector hinzufügen](#). Sie können nur einen Quell-Repository-Connector pro Job haben.

Einen neuen Connector hinzufügen

Um einen neuen Quellcode-Repository-Connector zu erstellen:

1. Geben Sie die AWS Kontonummer ein, die Sie für den AWS CodeConnections Connector verwenden möchten.
2. Wenn Sie nicht AWS CodeConnections für dasselbe AWS Konto eingerichtet haben, klicken [Sie auf Einrichten AWS CodeConnections](#).
3. Verwende die [AWS Developer Tools Console](#), um eine Verbindung zu deinem [Bitbucket GitHub](#), [GitHub Enterprise Server](#) oder [AzureDevOps](#) Repository herzustellen. [GitLab](#)

4. Kopieren Sie den Amazon-Ressourcennamen (ARN) der Verbindung, die Sie erstellt haben.
5. Kehren Sie zu AWS Transform zurück und fügen Sie den ARN der Verbindung ein, die Sie erstellt haben.
6. Geben Sie einen Namen für den Konnektor ein.

 Note

Geben Sie keine persönlichen Informationen als Teil des Connectornamens ein.

7. Wählen Sie Konnektorerstellung initiieren aus.
8. AWS Transform stellt die Anforderung zur Erstellung eines Connectors für das von Ihnen eingegebene AWS Konto in derselben Region wie der aktuelle Transformationsjob und benachrichtigt Sie, dass eine Genehmigungsanfrage bereit ist, von Ihrem AWS Administrator in der AWS Management Console genehmigt zu werden. Wählen Sie Bestätigungslink kopieren aus.
9. Wenn Sie der AWS Administrator sind, melden Sie sich AWS bei dem Konto an und klicken Sie auf den Bestätigungslink, um die Verbindungsanfrage zu genehmigen. Wenn Sie nicht der AWS Administrator sind, geben Sie den Bestätigungslink an Ihren AWS Administrator weiter.
10. Nachdem der AWS Administrator die Connector-Anfrage genehmigt hat, wählen Sie Connector finalisieren aus, um den Connector-Erstellungsprozess abzuschließen. Wenn Sie einen anderen Connector verwenden möchten, wählen Sie Restart aus, um den Connector-Erstellungsprozess neu zu starten.

Die Registerkarte Zusammenarbeit enthält auch Details zu Ihrem Connector, darunter:

- Status — Genehmigt oder Genehmigung steht noch aus
- AWS Konto-ID
- AWS Region
- Verbindung ARN

Löschen eines vorhandenen Connectors

Note

Wenn Sie über einen vorhandenen Quellcode-Repository-Connector verfügen, werden Sie von AWS Transform benachrichtigt. Wählen Sie entweder Bestehenden Connector verwenden oder Löschen und erstellen Sie einen neuen Connector.

Wenn Sie sich dafür entscheiden, eine bestehende Quellcode-Repository-Verbindung zu löschen, warnt AWS Transform Sie, bevor der Connector tatsächlich gelöscht wird.

1. Sie können einen vorhandenen Connector auf verschiedene Arten löschen:
 - a. Wenn Sie von AWS Transform dazu aufgefordert werden, können Sie Löschen auswählen und einen neuen Connector erstellen.
 - b. Sie können in der Aufforderung auch „Neu starten“ auswählen. Um diesen Konnektor zu ändern, müssen Sie neu starten.
2. AWS Transform warnt Sie davor, dass der Connector durch einen Neustart gelöscht wird. Um den Connector zu löschen, wählen Sie erneut Neu starten.
3. AWS Transform warnt dich erneut, dass durch das Löschen des Connectors die Verbindung zu deinem Drittanbieter-Repository wie Bitbucket, GitHub, und GitLab entfernt wird. Außerdem schlagen alle AWS Transform-Jobs fehl, die diesen Connector verwenden, wenn der Connector gelöscht wird. Um den Löschvorgang zu bestätigen, geben Sie delete ein und wählen Sie Löschen aus.
4. Informationen zum Hinzufügen eines neuen Quellcode-Repository-Connectors finden Sie unter [Einen neuen Connector hinzufügen](#).

Connect zum Quellcode in Amazon S3 her

Als Alternative zum Verbinden eines [Quellcode-Repositorys können Sie AWS Transform mit dem Quellcode in Amazon S3 verbinden](#).

Organisation des S3-Buckets

Der ursprüngliche Quellcode und der transformierte Code werden in einem gemeinsamen S3-Bucket gespeichert, der wie unten gezeigt organisiert ist. Sie müssen Ihren S3-Bucket in derselben Region wie Ihren AWS Transform-Job einrichten. Laden Sie Ihren Quellcode als Zip-Datei auf Root-Ebene

in den Bucket hoch. Die ZIP-Datei muss für jedes Repository einen Ordner der obersten Ebene enthalten.

Während der AWS Transformation erstellt Transform einen Transformationsausgabeordner und speichert die Transformationsergebnisse in diesem Ordner. Die Transformation erstellt eine ZIP-Datei mit dem Namen transformed-code.zip, die den transformierten Code enthält. Dazu gehört ein Bericht über Codeunterschiede (Dateiname diff.txt), in dem Dateiänderungen auf Projektebene hervorgehoben werden.

```
<customer-bucket>/  
### source-code.zip  
    ### repo 1  
    ### repo 2  
    ### .....  
    ### repo n  
### transform-output/  
    ### transformed-code.zip
```

Einen neuen S3-Connector hinzufügen

So erstellen Sie einen neuen S3-Quellcode-Repository-Connector:

1. Erstellen Sie in der AWS Konsole einen S3-Bucket.
2. Laden Sie Ihren Quellcode als Zip-Datei in den S3-Bucket hoch.
3. Starten Sie in der AWS Transform-Web-App einen .NET-Transformationsjob. Wählen Connect im Schritt Ein Quellcode-Repository Connect die Option Ihren Quellcode im S3-Bucket verbinden und dann Speichern aus.
4. Geben Sie auf der nächsten Seite Ihre S3-Bucket-Details ein und wählen Sie Senden aus.
 - a. Name des Connectors
 - b. AWS Konto-ID
 - c. S3 Bucket Arn
 - d. S3-Bucket-Verschlüsselungsschlüssel (optional)
5. Genehmigen Sie den Konnektor:
 - a. Kopieren Sie auf der nächsten Seite den Bestätigungslink.
 - b. Lassen Sie einen Genehmiger den Link aufrufen, um zur Seite mit der Anfrage zur Erstellung des AWS Transform-Connectors zu gelangen.

- c. Wählen Sie, ob Sie eine neue Rolle erstellen oder eine bestehende Rolle verwenden möchten.
 - d. Nachdem Sie die Anfrage geprüft haben, wählen Sie Speichern und genehmigen, um sie zu genehmigen.
6. Geben Sie den Speicherort der S3-Zip-Datei an:
- a. Warten Sie in der AWS Transform-Web-App, bis der Status Genehmigt angezeigt wird.
 - b. Geben Sie auf der Seite „Asset-Speicherort angeben“ eine S3-URL für die Code-Zip-Datei im Format `s3://bucket-name/zip-file-name` und wählen Sie „Zur AWS Transformation senden“.
 - c. Der Job wird mit dem Discovery-Schritt fortgeführt, um die Transformation fortzusetzen.

Löschen eines S3-Connectors

Um einen vorhandenen S3-Connector zu löschen:

1. Wählen Sie in der AWS Transform-Web-App oben rechts die Option Konnektoren verwalten aus.
2. Wählen Sie im Fenster „Konnektoren verwalten“ den Konnektor aus.
3. Wählen Sie Löschen aus.

Bestätigen Sie Ihre Repositorys, um die Transformation vorzubereiten

[Einen Konnektor für ein Quellcode-Repository erstellen](#) Bestätigen Sie anschließend Ihre Repositorys als ersten Schritt zur Vorbereitung der Transformation. Sie können:

- Überprüfen und ändern [Standardeinstellungen](#), die sich auf den Inhalt des Plans auswirken.
- Prüfen Sie die erkannten Repositorien und wählen Sie aus, welche im Hinblick auf die Transformation bewertet werden sollen.
- Lesen Sie den [Bericht zur Bewertung des Repositorys](#) und unterhalten Sie AWS sich mit Transform über dessen Inhalt.
- [Verwenden Sie den Plan, der generiert wurde von AWS Transformieren](#).
- [Passen Sie den Transformationsplan an](#) Verwenden Sie die Web-App oder laden Sie eine JSON-Datei herunter, ändern Sie sie und laden Sie sie in AWS Transform hoch.

Standardeinstellungen

Im Bereich Jobdetails der Registerkarte Zusammenarbeit können Sie Folgendes festlegen:

Auf der Registerkarte Aufgaben können Sie im Schritt Für die Transformation vorbereiten — Bestätigen Sie die zu transformierenden Repositorys Folgendes festlegen:

- Geben Sie den Namen des Ziel-Branches an, in den der transformierte Code in Ihr Repository geschrieben wird.
- Legen Sie die Ziel-.NET-Version fest:
 - .NET 8: transformiere alle Projekte in .NET 8
 - .NET 10: transformiere alle Projekte in .NET 10
- Sie können die standardmäßigen Auftragseinstellungen aktualisieren oder sie unverändert lassen. Dazu zählen:
 - .NET-Standardprojekte vom Transformationsplan ausschließen Diese Einstellung ist standardmäßig ausgewählt. Wenn diese Option ausgewählt ist, schließt AWS Transform alle .NET-Standardprojekte aus dem Transformationsplan aus. Wenn Sie diese Einstellung deaktivieren, werden .NET-Standardprojekte transformiert, sodass sie nicht mehr mit dem .NET Framework kompatibel sind.
 - Überprüfen Sie die NuGet Quellen und holen Sie sich .NET-kompatible Paketversionen. Erlauben Sie AWS Transform, nach .NET-kompatiblen Paketversionen für den Code zu suchen und diese abzurufen, den Sie transformieren möchten.

Lesen Sie den Bewertungsbericht für das Repository

Der Bericht zur Bewertung des Endlagers bietet eine tabellarische Ansicht der Informationen zu jedem von AWS Transform erkannten Endlager. Dies umfasst:

- Besitzer des Repositoriums
- Bewertete Filiale
- Anzahl der Lösungen
- Anzahl der Projekte
- Gesamtzahl der Codezeilen
- Erkannte .NET-Versionen
- Entdeckte Projekttypen
- Anzahl der privaten Nuget-Abhängigkeiten
- Anzahl der öffentlichen Nuget-Abhängigkeiten
- Komplexität der Transformation

Um die Datei herunterzuladen:

1. Wählen Sie in Ihrem Workspace den Tab Zusammenarbeit aus.
2. Wählen Sie im Bereich Repositorys auswählen die Option Herunterladen aus und wählen Sie Als HTML herunterladen oder Als JSON herunterladen

Chatten Sie über den Repository-Zusammenfassungsbericht

Ihre Repository-Zusammenfassung kann sehr lang sein. Verwenden Sie den Chat, um den Inhalt besser zu verstehen. Ihr Bericht ist für den Chat verfügbar, wenn Sie diese Meldung auf der Registerkarte Arbeitsprotokoll sehen: Der Bewertungsbericht ist jetzt im Chat für Rückfragen verfügbar. Um den Chat zu öffnen, klicken Sie auf das lila sechseckige Symbol in der unteren rechten Ecke der Webkonsole. Hier sind einige Beispielaufforderungen:

- Listet alle entdeckten oder bewerteten Repositorys auf.
- Wie viele .NET 6-Projekte wurden bei der Bewertung entdeckt?
- Welche Projekte haben die höchste Komplexität?

Verwenden Sie den Plan, der generiert wurde von AWS Transformieren

Sie können den AWS Transform-Plan verwenden, der anhand der Suche nach Repositorys mit einer höheren Erfolgswahrscheinlichkeit der Transformation erstellt wurde. Dieser Plan umfasst die zuletzt geänderten Repositorys, Root-Repositorys und voneinander abhängige Repositorys.

AWS Transform listet einige allgemeine Details zum Transformationsplan auf, darunter:

- Gesamtzahl der erkannten Repositorys Diese Anzahl älterer .NET-Repositorys, die AWS Transform mithilfe Ihres Quellcode-Repository-Connectors entdeckt hat. AWS Transform kann in jedem Auftrag maximal 1.000 Repositorys scannen. Wenn Sie mehr Repositorys scannen oder transformieren müssen, können Sie mehrere Transformationsaufträge erstellen.
- Ausgewählte Repositorys Die Anzahl der älteren .NET-Repositorys, die AWS Transform für die Transformation ausgewählt hat.
- Ausgewählte Abhängigkeiten Die Anzahl der Abhängigkeiten, die die ausgewählten Repositorys benötigen, die AWS Transform automatisch erkannt und dem Transformationsplan hinzugefügt hat.

In der Tabelle Ausgewählte Repositorys sind die ausgewählten Repositorys aufgeführt. Sie können Repositorys nach Namen durchsuchen, zu weiteren Seiten mit Repositorys navigieren und eine

Datei im JSON-Format herunterladen, in der die ausgewählten Repositorys und ihre Abhängigkeiten aufgeführt sind. In dieser Ansicht können Sie alle Änderungen vornehmen.

In der Tabelle Ausgewählte Repositorys sind die folgenden Details zu den Repositorys aufgeführt, die Transform für die AWS Transformation ausgewählt hat:

- Repository-Name
- Quell-Verzweigung
- Datum und Uhrzeit der letzten Änderung
- Codezeilen Auf diese Weise können Sie feststellen, ob Sie Ihre Kontingentgrenzen erreichen. Weitere Informationen finden Sie unter [Kontingente für AWS Transformieren](#).
- Abhängige Repositorys Sie können auf die Anzahl der abhängigen Repositorys klicken, um weitere Informationen zu diesen Abhängigkeiten anzuzeigen.

Wenn Sie mit dem von AWS Transform generierten Transformationsplan zufrieden sind, wählen Sie Repositories bestätigen aus.

Wenn Sie Änderungen am von AWS Transform generierten Transformationsplan vornehmen möchten, wählen Sie [Passen Sie den Transformationsplan an](#).

Passen Sie den Transformationsplan an

Wenn Sie dies nicht möchten [Verwenden Sie den Plan, der generiert wurde von AWS Transformieren](#), können Sie die Liste der zu transformierenden Repositorys mithilfe einer der folgenden Optionen anpassen:

1. Wählen Sie in der Tabelle Ausgewählte Repositorys die Option Repositorys aus.
 - a. Wenn Sie dem Plan ein Repository hinzufügen, wählt AWS Transform die Abhängigkeiten des Repositorys für Sie aus und fügt sie automatisch dem Transformationsplan hinzu.
 - b. Sie können die Auswahl von Repositorys in der Tabelle auch aufheben.
2. Laden Sie die von AWS Transform generierte JSON-Liste der Repos und Branches herunter.
 - a. Wählen Sie Herunterladen und dann Als JSON herunterladen aus.
 - b. Überprüfen und ändern Sie die JSON-Datei. Sie können Repositorys oder Lösungen innerhalb von Repositorys entfernen, die Sie nicht transformieren möchten.
 - c. Laden Sie die überarbeitete JSON-Datei hoch, indem Sie Benutzerdefinierten Plan hochladen auswählen.

- d. Wenn der JSON-Upload erfolgreich war, werden in der Tabelle Ausgewählte Repositorys die von Ihnen getroffene Auswahl angezeigt.
3. Sie können „Abhängige Repos anzeigen“ auswählen, um die Liste der Repositorys anzuzeigen, bei denen AWS Transform festgestellt hat, dass es sich um Abhängigkeiten der ausgewählten Repositorys handelt.
4. Sie können diese Schritte bei Bedarf wiederholen. Wenn Sie mit Ihrem individuellen Plan zufrieden sind, wählen Sie Repositorys bestätigen aus.

Auflösen von Paketabhängigkeiten zur Vorbereitung der Transformation

Wenn AWS Transform anschließend fehlende Paketabhängigkeiten feststellt, müssen Sie diesen Schritt ausführen. [Bestätigen Sie Ihre Repositorys, um die Transformation vorzubereiten](#) Sie können ein PowerShell Windows-Skript ausführen, um die fehlenden Paketabhängigkeiten von demselben Gerät wie Ihre Visual Studio Entwicklungsumgebung abzurufen, oder Sie können die fehlenden Pakete manuell abrufen. Laden Sie dann die fehlenden Pakete hoch.

Die fehlenden Paketabhängigkeiten können auf zwei Arten aktualisiert werden:

- Mithilfe von Artifact Connector lösen: Beheben Sie das Problem, indem Sie ein Artifact Repository (ADO NuGet Connector) mithilfe eines speziellen Connect Artifact Repository-HITL-Workflows konfigurieren, der angezeigt wird, wenn kein Artifact Connector konfiguriert ist und Pakete fehlen.
- Fehlendes Paket aktualisieren: AWS Transform listet die fehlenden Pakete in der Tabelle mit den Abhängigkeiten fehlender Pakete auf. Sie können im Suchfeld anhand des Namens nach einem fehlenden Paket suchen. Diese Tabelle enthält die folgenden Details zu den fehlenden Paketen:
 - Name
 - Zugehörige Repositorys
 - Status der Framework-Version
 - Status der Kernversion

Um die fehlenden Paketabhängigkeiten zu beheben, [Laden Sie die fehlenden Pakete hoch](#).

Laden Sie die fehlenden Pakete hoch

1. Wenn Sie möchten, können Sie ein PowerShell Windows-Hilfsskript herunterladen, um die fehlenden Paketabhängigkeiten aus Ihrer Visual Studio Entwicklungsumgebung abzurufen. Sie können die fehlenden Pakete auch manuell finden.

Um das PowerShell Windows-Skript zu verwenden:

- a. Wählen Sie PowerShell Windows-Skript herunterladen.
 - b. Führen Sie das Skript lokal mit einer aktiven Verbindung zu den Repositorys aus, die die fehlenden Paketabhängigkeitsdateien enthalten.
 - c. Dieses Skript ermöglicht es Ihnen, die fehlenden Paketabhängigkeiten in Ihre lokale Umgebung herunterzuladen.
2. Das Skript erstellt eine einzige Zip-Datei, die Sie hochladen können und die alle Abhängigkeiten in einem Archiv enthält. Sie können auch einzelne Dateien .nupkg oder ZIP-Dateien für jede Abhängigkeit hochladen.
 3. Wählen Sie Paketdateien hochladen aus.
 4. Wählen Sie im Modal Abhängigkeitsdateien hochladen die Option Dateien auswählen aus und suchen Sie nach dem Speicherort der komprimierten fehlenden Paketdateien auf Ihrem Gerät.
 5. Wählen Sie Hochladen aus.
 6. AWS Transform validiert die von Ihnen hochgeladenen Dateien. Während der Validierung können Sie keine Aktualisierungen vornehmen. AWS Transform meldet den Validierungsstatus oberhalb der Tabelle Fehlende Paketabhängigkeiten.
 7. AWS Transform aktualisiert auch die Statusspalten in der Tabelle mit fehlenden Paketabhängigkeiten von Fehlend auf Aufgelöst. Wenn ein Paket nicht validiert werden kann, erhält es den Status Ungültig. Gehen Sie bei ungültigen Dateien wie folgt vor:
 - a. Wählen Sie in der Tabelle Fehlende Paketabhängigkeiten mit dem Kontrollkästchen das ungültige Paket aus.
 - b. Wählen Sie Hochgeladene Datei entfernen aus.
 - c. Dadurch wird der Status wieder auf Fehlend geändert.
 8. Nachdem Sie die fehlenden Pakete hochgeladen und die Paketabhängigkeiten behoben haben, wählen Sie Weiter zur Überprüfung aus.

Wenn Sie „Mit der Überprüfung fortfahren, ohne die fehlenden Paketabhängigkeiten zu lösen“ auswählen, werden Sie von AWS Transform gefragt, ob Sie die Transformationsaufgabe ohne die fehlenden Pakete starten möchten. Wenn Sie die Option Fehlende Paketabhängigkeiten ignorieren auswählen, verwendet AWS Transform Assemblyverweise, um den Code zu transformieren. Wenn Sie mit dieser Aktion fortfahren, kann sich dies auf verwandte Ressourcen auswirken.

Anforderungen an die Ordnerstruktur

Für NuGet Uploads benötigt AWS Transform entweder:

- Die .nuspec Datei, die für manuell hochgeladene Pakete auf der Root-Ebene platziert werden soll, oder
- Verwendung des bereitgestellten PowerShell Skripts zur Generierung der richtigen Struktur

Anforderungen, die der Version entsprechen

- Framework-Status: AWS Transform versucht, die in der .csproj Datei (Quellcode) angegebene Version der Abhängigkeit mit der Version der hochgeladenen Abhängigkeit abzugleichen. Eine exakte Übereinstimmung führt zu einem Erfolgsstatus.
- Kernstatus: AWS Transform erwartet eine Angabe der Kernversion im Abschnitt „Abhängigkeiten“ der hochgeladenen .nuspec Datei. Wenn eine gefunden wird, lautet der Kernstatus Success.

Beispielformat:

```
<dependencies>
  <group targetFramework="net8.0" />
</dependencies>
```

Zu den gängigen Versionen gehören:

- .NET 5.0 (net5.0)
- .NET 6.0 (net6.0)
- .NET 7.0 (net7.0)
- .NET 8.0 (net8.0)

Überprüfung Ihres Plans zur Vorbereitung auf die Transformation

Nach [Bestätigen Sie Ihre Repositorys, um die Transformation vorzubereiten](#) und [Auflösen von Paketabhängigkeiten zur Vorbereitung der Transformation](#) muss der AWS Kontoadministrator den Transformationsplan überprüfen und ihn in AWS Transform genehmigen.

AWS Transform zeigt die Liste der Repositorys, abhängigen Repositorys und abhängigen Pakete des Jobs an, die für die Transformation ausgewählt wurden.

Überprüfung des Transformationsplans

AWS Transform zeigt die Liste der Repositorys, abhängigen Repositorys und abhängigen Pakete des Jobs an, die für die Transformation ausgewählt wurden.

Note

AWS Transform kann maximal 100 Abhängigkeiten und Repositorys pro Transformationsplan transformieren.

1. Wenn Sie nicht der AWS Kontoadministrator sind, überprüfen Sie den Jobplan, und wenn Sie ihn akzeptieren, wählen Sie Zur Genehmigung senden aus.
2. Wenn Sie der AWS Kontoadministrator sind, müssen Sie den Plan überprüfen und ihn genehmigen, wenn Sie bereit sind, um mit der Transformation zu beginnen. Nachdem Sie den Jobplan überprüft haben, wählen Sie eine der folgenden Optionen aus:
 - a. Ablehnen Wenn der Job von einem Benutzer erstellt wurde, der nicht der AWS Kontoadministrator ist, empfehlen wir Ihnen, den Job-Ersteller zu benachrichtigen, damit er den Job neu starten kann.
 - b. Genehmigen Sie die Transformation und starten Sie sie.

Die Stellenbewertung umfasst die folgenden Details:

1. Zusammenfassung der Stellenausschreibung Dazu gehören:
 - a. Der Zielzweig, in dem AWS Transform den transformierten Code platzieren wird.
 - b. Die .NET-Zielversion, .NET 8.0 oder .NET 10.
 - c. Die Jobeinstellungen:
 - i. .NET-Standardprojekte ausschließen
 - d. Anzahl der für die Transformation ausgewählten Repositorys
 - e. Anzahl der abhängigen Repositorien
 - f. Anzahl der privaten Pakete NuGet
 - g. Gesamtzahl der Codezeilen für den Job
2. Ausgewählte Repositorys Dies sind die Repositorys, die für die Transformation ausgewählt wurden. Dabei muss es sich entweder um MVC-, Web-, Windows Communication Foundation

(WCF), Konsole, Klassenbibliothek, UI Framework — Razor Pages oder Unit-Test-Pakete handeln. Diese Tabelle enthält die folgenden Informationen:

- a. Name
 - b. Quell-Verzweigung
 - c. Unterstützte Projekte
 - d. Codezeilen
 - e. Projekte erkannt
 - f. Projekte wurden übersprungen
 - g. Abhängigkeiten wurden erkannt
3. Abhängige Repositorys hinzugefügt Dies sind die abhängigen Repositorys, die zur Transformation hinzugefügt wurden. Dabei muss es sich entweder um MVC-, Web-, Windows Communication Foundation (WCF), Konsole, Klassenbibliothek, UI Framework — Razor Pages oder Unit-Test-Pakete handeln. Diese Tabelle enthält die folgenden Informationen:
- a. Name
 - b. Benötigt von
 - c. Quell-Verzweigung
 - d. Unterstützte Projekte
 - e. Codezeilen
 - f. Projekte erkannt
 - g. Projekte wurden übersprungen
4. Abhängige Pakete Dies sind die abhängigen Pakete, die zur Transformation hinzugefügt wurden. Sie müssen entweder MVC-, Web-, Windows Communication Foundation (WCF), Konsole, Klassenbibliothek, UI-Framework — Razor-Seiten oder Unit-Test-Pakete sein. Diese Tabelle enthält die folgenden Informationen:
- a. Name
 - b. Zugehörige Repositories
 - c. Status der Framework-Version
 - d. Status der Kernversion

Transformieren Sie Ihren .NET-Code

Nachdem der AWS Kontoadministrator den Vorgang abgeschlossen hat [Überprüfung Ihres Plans zur Vorbereitung auf die Transformation](#), können Sie den Transformationsfortschritt auf der Registerkarte „Dashboard“ Ihres Transformationsjobs einsehen.

Note

Transform transformiert nicht nur Repositorys und Abhängigkeiten, AWS sondern kann auch vollständig transformierte Unittest-Projekte (ohne Build-Fehler) ausführen. AWS Transform hat vor der Transformation keinen Zugriff auf Unit-Test-Ergebnisse und kann nur Ergebnisse nach der Transformation teilen. Anschließend können Sie Ihre Ausgangsdaten vor der Transformation mit den Ergebnissen nach der Transformation vergleichen, um mögliche Lücken zu ermitteln.

In der oberen rechten Ecke sehen Sie den Auftragsstatus, der einen der folgenden Werte hat:

- Wartet auf Benutzereingaben
- Die Zeit ist abgelaufen
- In Ausführung

Sie können auch die folgenden Symbole sehen:

- Ein Symbol „Transformation beenden“
- Ein Aktualisierungssymbol
- Ein Einstellungssymbol

Das Dashboard bietet eine allgemeine Zusammenfassung der Transformation. Es zeigt Kennzahlen für die Anzahl der transformierten Jobs und der angewandten Transformation sowie die geschätzte Zeit bis zum Abschluss der Transformation.

Das Dashboard umfasst:

1. Der Abschnitt mit den Details des Transformationsauftrags, in dem die Standardeinstellungen und Details des Transformationsauftrags aufgeführt sind, darunter:

- a. Ziel-Branch-Ziel Um Ihren Code zu AWS transformieren, erstellt Transform einen neuen Zweig für den transformierten Code in Ihrem Code-Repository.
 - b. .NET-Zielversion, .NET 8.0 oder .NET 10
 - c. Die ID des AWS Transform-Jobs.
 - d. Die Jobeinstellungen:
 - i. .NET-Standardprojekte ausschließen
2. Der Abschnitt mit der Zusammenfassung der Transformation enthält:
- a. Die Anzahl der für die Transformation ausgewählten Repositories
 - b. Die Anzahl der Projekte, die transformiert werden sollen
 - c. Die Gesamtzahl der Codezeilen in diesen Repositories und Projekten

Nach dem Start der Transformation werden in den Abschnitten Repository-Status, Paketstatus und Unit-Teststatus Kreisdiagramme angezeigt, die den Fortschritt in Echtzeit anzeigen. Der Unit-Test-Status zeigt den Status der Unit-Tests in Ihren Repositories, die AWS Transform nach der Transformation ausführt, um den transformierten Code zu testen. AWS Transform teilt die ausgeführten Testergebnisse zusammen mit dem individuellen Testnamen, sodass Kunden die Liste der bestandenen und fehlgeschlagenen Komponententests überprüfen können.

 Note

Im Abschnitt Repositories sind die Repositories aufgeführt, die AWS Transform empfiehlt oder die Sie für die Transformation ausgewählt haben. Wählen Sie JSON herunterladen aus, um eine Liste der Repositories, Abhängigkeiten und Pakete in Ihrem Transformationsplan herunterzuladen.

Sehen Sie sich die Transformationsberichte an

Nach Abschluss eines Transformationsjobs können Sie [Transformationsberichte](#) herunterladen:

- [Zusammenfassungsbericht zur Transformation](#): Dieser Bericht bietet einen Überblick über die Transformation im HTML- oder JSON-Format. Laden Sie den zusammenfassenden Bericht zur Transformation von der Registerkarte Dashboard herunter. Wählen Sie „Herunterladen“ und dann „Als HTML herunterladen“ oder „Als JSON herunterladen“.
- [Detailbericht zur Transformation](#): Dieser Bericht enthält ausführliche Informationen zu einer Transformation im HTML-Format. Laden Sie Detailberichte zur Transformation von der

Registerkarte Dashboard herunter. Wählen Sie in der Repository-Liste den Link Detaillierten Bericht herunterladen aus, um einen detaillierten Bericht herunterzuladen.

Chatten Sie mit AWS Transform über den Transformationsbericht

Sie können mit AWS Transform über den Transformationsbericht chatten, nachdem ein Repository vollständig verarbeitet wurde oder nachdem der Transformationsjob abgeschlossen ist. Auf der Registerkarte Worklog wird diese Meldung für jedes Repository angezeigt, das für den Chat verfügbar ist: Details zur *repository_name* Repository-Transformation sind jetzt im Chat für Anfragen verfügbar. Es wird diese Meldung angezeigt, wenn der Transformationsjob abgeschlossen ist: Der AWS Transformationsjob ist abgeschlossen.

Um den Chat zu öffnen, klicken Sie auf das lila sechseckige Symbol in der unteren rechten Ecke der Webkonsole.

Hier sind einige Beispielaufforderungen:

- Welche Projekte wurden erfolgreich transformiert?
- Welche Projekte wurden teilweise portiert?
- Welche Änderungen wurden am `repo_name` Repository vorgenommen?
- Welche Pakete wurden im `project_name` Projekt aktualisiert?

Modernisieren.NET in der IDE

AWS Transform beinhaltet einen interaktiven, agentischen KI-Assistenten im AWS Toolkit für Visual Studio. Er ermöglicht es Ihnen, Anwendungen mithilfe einer dialogorientierten, schrittweisen Benutzerführung direkt in Ihrer IDE zu modernisieren. Um eine .NET-Lösung oder -Projekt zu AWS transformieren, analysiert der Transform-Agent Ihre Codebasis, ermittelt die für die Portierung Ihrer Anwendung erforderlichen Updates und generiert vor Beginn der Transformation einen Bewertungsbericht und einen Transformationsplan.

Die Visual Studio IDE-Umgebung unterstützt nur die Authentifizierung durch IAM Identity Center. Weitere Informationen finden Sie unter [Benutzer im IAM Identity Center hinzufügen](#).

Das IDE-Erlebnis bietet autonome und interaktive Modi. Verwenden Sie den autonomen Modus für die unbeaufsichtigte Transformation, der sich für Aufträge über Nacht oder lang andauernde Aufgaben eignet. Verwenden Sie den interaktiven Modus, um mit dem Agenten im Chat

zusammenzuarbeiten. Dabei erhalten Sie einen umfassenden Überblick über die Transformation, einen anpassbaren Transformationsplan und eine schrittweise Überprüfung jedes Projekts. Sie können iterieren, um die Ergebnisse zu verfeinern, oder die Richtung ändern, bis Sie zufrieden sind.

Wenn ein Transformationsjob aktiv ist, können Sie mit drei Fenstern interagieren:

- Das Chat-Fenster ist Ihr primärer Interaktionspunkt mit dem Transformationsagenten. Verwenden Sie den Chat, um Fragen zu stellen, Optionen zu besprechen, die Transformation zu steuern und zu iterieren.
- Im Fenster „Jobplan AWS transformieren“ werden Fortschrittsschritte angezeigt. Hier können Sie Artefakte herunterladen oder hochladen oder Unterschiede bei Codeänderungen anzeigen.
- Das Worklog-Fenster zeigt ein Protokoll der Transformationsaktivitäten in natürlicher Sprache.

AWS Transform führt vier wichtige Aufgaben aus, um .NET-Anwendungen nach Linux zu portieren:

- Führt ein Upgrade von .NET- und Sprachversionen durch — Führt ein Upgrade von älterem .NET-C#-Code auf aktuelle .NET- und Sprachversionen durch.
- Migrieren von .NET Framework zu plattformübergreifendem .NET – migriert Projekte und Pakete vom Windows-abhängigen .NET Framework zu plattformübergreifendem .NET, das mit Linux kompatibel ist
- Umschreiben von Code zugunsten der Linux-Kompatibilität – nimmt einen Faktorwechsel für veraltete und ineffiziente Codekomponenten vor und schreibt sie neu
- Generiert einen Bericht zur Linux-Kompatibilität — Für offene Aufgaben, bei denen Benutzereingriffe erforderlich sind, damit der Code unter Linux erstellt und ausgeführt werden kann, bietet AWS Transform einen detaillierten Bericht über die Aktionen, die zur Konfiguration Ihrer Anwendung nach der Transformation erforderlich sind.

Weitere Informationen darüber, wie Transform AWS .NET-Transformationen durchführt, finden Sie unter. [Wie AWS Transform modernisiert.NET-Anwendungen](#)

Informationen zur Modernisierung Ihres .NET-Codes mithilfe von AWS Transform aus der Visual Studio IDE finden Sie im Folgenden:

- [Modernisieren von.NET mit AWS Verwandeln Sie sich in Visual Studio](#)
- [Wie AWS Transform modernisiert.NET-Anwendungen](#)
- [Beheben von Problemen mit .NET-Transformationen in der IDE](#)

Kontingente

Informationen zu AWS Transformationskontingenten für .NET-Transformationen in der IDE finden Sie unter [Kontingente für AWS Transformieren](#).

Modernisieren von .NET mit AWS Verwandeln Sie sich in Visual Studio

Gehen Sie wie folgt vor, um Visual Studio 2026 oder Windows-based 2022 eine .NET-Anwendung mit AWS Transform auf eine Linux-compatible plattformübergreifende .NET-Anwendung zu portieren.

Schritt 1: Voraussetzungen

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die [AWS Toolkit-Erweiterung mit Amazon Q](#) vom Visual Studio Marketplace heruntergeladen und installiert haben. Lesen Sie die AWS [Transform-Funktionen](#) und [Einschränkungen](#) für die .NET-Modernisierung, um sicherzustellen, dass Ihr Code transformiert werden kann.

Schritt 2: Authentifizieren Sie sich in Visual Studio

Um vom Toolkit for Visual Studio aus eine Verbindung zu Ihren AWS Konten herzustellen, öffnen Sie die Benutzeroberfläche Erste Schritte mit dem AWS Toolkit (Verbindungs-UI):

1. Navigieren Sie im Visual Studio-Hauptmenü zu Erweiterungen > AWS Toolkit > Erste Schritte, um die Seite Erste Schritte: AWS Toolkit zu öffnen.
2. Wählen Sie Authentifizierung AWS transformieren aus.
3. Wählen Sie ein vorhandenes Profil aus oder erstellen Sie ein neues. Wenn Sie ein neues Profil erstellen, geben Sie einen Namen für das Profil und Ihre AWS Transform-Start-URL ein, die Sie per E-Mail erhalten haben, nachdem Sie von Ihrem Administrator zu IAM Identity Center hinzugefügt wurden.
4. Wählen Sie Connect aus. Folgen Sie den Anweisungen, um sich über Ihren Webbrowser anzumelden und Zugriffsberechtigungen zu erteilen. In Visual Studio sollte Connected with IAM Identity Center angezeigt werden.
5. Nach der Anmeldung werden Sie zum AWS Transform-Dashboard weitergeleitet. Von dieser Landing Page aus können Sie Folgendes tun:
 - Wählen Sie ein AWS Transform-Profil (Region)
 - Wählen Sie einen Workspace aus oder erstellen Sie ihn
 - Status von Transformationsaufträgen anzeigen

Schritt 3: Transformieren Sie Ihre Anwendung

Sie können Ihre .NET-Lösung oder Ihr Projekt wie folgt transformieren:

Starten Sie die Transformation

1. Öffnen Sie eine C#- oder VB.NET basierte Lösung oder ein Projekt Visual Studio, das Sie transformieren möchten.
2. Klicken Sie im Projektmappen-Explorer mit der rechten Maustaste auf eine Lösung oder ein Projekt, das Sie transformieren möchten, und wählen Sie „Mit AWS Transformation portieren“.
3. Das Dialogfeld „Port with AWS Transform“ wird angezeigt.
 - a. Erstellen Sie in der Dropdownliste „Arbeitsbereich auswählen“ einen Arbeitsbereich oder wählen Sie einen vorhandenen aus. Workspaces machen deine Aktivität in der AWS Transform-Webanwendung sichtbar. Dort kannst du Mitarbeiter einladen, sich Transformationsjobs anzusehen und über sie zu chatten.
 - b. Wählen Sie im Dropdown-Menü Choose a .NET target die .NET-Version aus, auf die Sie aktualisieren möchten.
 - c. Wählen Sie als Transformationsmodus Autonom für unbeaufsichtigte Transformation oder Interaktiv für interaktive Transformation aus.
 - d. Wählen Sie Start, um mit der Transformation zu beginnen.
4. Sobald der Transformationsjob gestartet wird, werden die Fenster „Jobplan AWS transformieren“, „Chat“ und „Arbeitsprotokoll“ angezeigt.

Bewertungs- und Transformationsplan

1. Nachdem AWS Transform Ihren Code analysiert hat, werden im Chat ein Bewertungsbericht und ein Transformationsplan angezeigt. Im interaktiven Modus wird der Chat angehalten, damit Sie sie überprüfen können. Wenn Sie es vorziehen, nicht im Chat zu überprüfen, können Sie diese Alternativen verwenden:
 - Um die Bewertung oder den Plan im Code-Editor anzuzeigen, wählen Sie im Fenster „Jobplan transformieren“ die Option „Bewertung anzeigen“ oder „AWS Transformationsplan anzeigen“.
 - Verwenden Sie das Download-Symbol im Fenster Jobplan, um die Bewertung oder den Plan herunterzuladen.
2. Ändern Sie optional den Transformationsplan. Sie können den Plan im Chat besprechen, z. B. andere Optionen ausloten. Sie nehmen Planänderungen vor, indem Sie Anweisungen im Chat

geben oder indem Sie über das Download-Symbol im Fenster „Jobplan“ einen überarbeiteten Transformationsplan hochladen. Sie können Schritte nach Belieben hinzufügen, entfernen oder ändern. Der Chat bestätigt mit einem überarbeiteten Plan, ob er Ihre Anweisungen verstanden hat.

3. Laden Sie optional Lenkungsdokumente hoch. Verwenden Sie im Chat-Fenster das Upload-Symbol, um Steuerungsdokumente wie Anwendungsspezifikationen, technische Einstellungen und Konventionen der Organisation oder Programmierbeispiele hochzuladen. Nachdem Sie ein Steuerungsdokument hochgeladen haben, beschreiben Sie es im Chat-Fenster, um dem Agenten einen Kontext zu geben.
4. Wenn Sie mit dem Plan zufrieden sind, geben Sie Ihre Zustimmung im Chat und die Transformation beginnt.
5. Im interaktiven Modus können Sie Checkpoints so einrichten, dass sie beendet werden, nachdem ein Projekt zur Überprüfung transformiert wurde. Die Schritte unter Code transformieren im Fenster „Jobplan“ werden mit runden Checkpoint-Symbolen angezeigt. Bei allen Projekten sind Checkpoints standardmäßig aktiviert. Verwenden Sie die Kontrollkästchen, um einen Checkpoint zu löschen oder festzulegen.

Transformations- und Checkpoint-Überprüfungen

1. AWS Transform beginnt mit der Transformation Ihres Codes. Sie können den Fortschritt der Transformationsschritte im Fenster „Jobplan AWS transformieren“ überwachen. Im Fenster „Jobplan“ werden die geschätzte maximale verbleibende Zeit und Ihre Job-ID angezeigt.
2. Bei der Transformation von Projekten werden Zusammenfassungen im Chat angezeigt und die Codeänderungen werden übernommen.
3. Wenn im interaktiven Modus ein Checkpoint erreicht ist, hält der Agent eine Pause an, sodass Sie die Ergebnisse überprüfen können. Im Fenster „Jobplan“ sehen Sie für den Schritt, bei dem der Vorgang unterbrochen wurde, eine Schaltfläche „Ergebnisse anzeigen“, über die Sie die Codeunterschiede überprüfen können. Nachdem Sie die Änderungen überprüft haben, können Sie im Chat nach weiteren Änderungen fragen oder selbst Codeänderungen vornehmen. Visual Studio
4. Sie können am Checkpoint beliebig oft iterieren. Wenn Sie zufrieden sind, weisen Sie den Chat an, fortzufahren, und es wird mit dem nächsten Projekt fortgefahren.

Ende der Transformation

1. Nach der Transformation Ihrer Projekte löst der .NET-Agent ein lokales Build-In aus Visual Studio, um zu bestätigen, dass der Code erfolgreich auf Ihrem lokalen Computer erstellt wurde. Wenn es Fehler gibt, funktioniert er, um sie zu beheben.
2. Sobald die Transformation abgeschlossen ist, sind möglicherweise weitere Schritte erforderlich, z. B. Transformationsaufgaben, die AWS Transform nicht ausführen konnte, oder Änderungen, die aus Gründen der Linux-Kompatibilität erforderlich sind. Eine Markdown-Datei für die nächsten Schritte (NextSteps.md) steht zum Herunterladen zur Verfügung, die Sie als Eingabeaufforderung für einen KI-Code-Begleiter verwenden können. Verwenden Sie zum Herunterladen die Download-Schaltfläche des Jobplan-Fensters NextSteps.md.
3. Sie können weiterhin im Chat interagieren, um Fragen zu stellen oder zusätzliche Änderungen zu beantragen.
4. Teilen Sie dem Chat mit, wann Sie bereit sind, Ihren Transformationsjob zu beenden.

Wie AWS Transform modernisiert .NET-Anwendungen

In den folgenden Abschnitten finden Sie Einzelheiten zur Funktionsweise der .NET-Transformation mit AWS Transform.

Analysieren Ihrer Anwendung und Erstellen eines Transformationsplans

Bevor eine Transformation beginnt, erstellt AWS Transform Ihren Code lokal, um zu überprüfen, ob er erstellbar und korrekt für die Transformation konfiguriert ist. Wenn der Code nicht erstellt werden kann, fragt AWS Transform, ob mit der Transformation fortgefahren werden soll. AWS Transform lädt dann Ihren Code in eine sichere und verschlüsselte Build-Umgebung hoch AWS, analysiert Ihre Codebasis und ermittelt, welche Updates für die Portierung Ihrer Anwendung erforderlich sind.

Während dieser Analyse unterteilt AWS Transform Ihre .NET-Lösung oder Ihr Projekt in Codegruppen. Eine Codegruppe ist ein Projekt mit all seinen Abhängigkeiten, die zusammen eine erstellbare Codeeinheit wie eine Dynamic Link Library (DLL) oder eine ausführbare Datei erzeugen. Selbst wenn Sie nicht alle zu transformierenden Projektabhängigkeiten ausgewählt haben, bestimmt AWS Transform die Abhängigkeiten, die für die Erstellung Ihrer ausgewählten Projekte erforderlich sind, und transformiert sie ebenfalls, sodass Ihre transformierte Anwendung baubar und einsatzbereit ist.

Nach der Analyse Ihres Codes generiert AWS Transform einen Transformationsplan, in dem die vorgeschlagenen Änderungen beschrieben werden, einschließlich einer Liste der Codegruppen und ihrer Abhängigkeiten, die transformiert werden sollen.

Transformieren Ihrer Anwendung

Um die Transformation zu starten, erstellt AWS Transform Ihren Code erneut in der sicheren Build-Umgebung, um zu überprüfen, ob er remote erstellt werden kann. AWS Transform beginnt dann mit der Portierung Ihrer Anwendung. Dabei wird von unten nach oben vorgegangen, beginnend mit der niedrigsten Abhängigkeitsebene. Wenn AWS Transform beim Portieren einer Abhängigkeit auf ein Problem stößt, wird die Transformation gestoppt und es werden Informationen darüber bereitgestellt, was den Fehler verursacht hat.

Die Transformation umfasst die folgenden Aktualisierungen Ihrer Anwendung:

- Ersetzen veralteter C#-Codeversionen durch Linux-compatible C#-Versionen
- Aktualisieren von .NET Framework auf plattformübergreifendes .NET, einschließlich:
 - Identifizieren und iteratives Ersetzen von Paketen, Bibliotheken und APIs
 - NuGet Pakete und APIs aktualisieren und ersetzen
 - Übergehen zur plattformübergreifenden Laufzeit
 - Einrichten von Middleware und Aktualisieren von Laufzeitkonfigurationen
 - Ersetzen von privaten Paketen oder Paketen von Drittanbietern
 - Umgehen mit IIS- und WCF-Komponenten
 - Debuggen von Build-Fehlern
- Umschreiben von Code aus Gründen der Linux-Kompatibilität, einschließlich Durchführung eines Faktorwechsels und Umschreiben von veraltetem und ineffizientem Code zur Portierung von vorhandenem Code

Überprüfung des Transformationsberichts und Annahme von Änderungen

Nach Abschluss der Transformation stellt AWS Transform einen Transformationsbericht mit Informationen zu den vorgeschlagenen Aktualisierungen Ihrer Anwendung bereit, einschließlich der Anzahl der geänderten Dateien, aktualisierten Pakete und geänderten APIs. Es kennzeichnet alle erfolgreichen Transformationen, einschließlich der betroffenen Dateien oder Teile von Dateien und der Fehler, die bei einem Build-Versuch aufgetreten sind. Sie können sich auch eine Build-Zusammenfassung mit Build-Protokollen ansehen, um mehr darüber zu erfahren, welche Änderungen vorgenommen wurden.

Der Transformationsbericht enthält auch einen Linux-Portierungsstatus, der angibt, ob zusätzliche Benutzereingaben erforderlich sind, um die Anwendung Linux-kompatibel zu machen. Wenn für eines der Elemente in einer Codegruppe Eingaben von Ihnen erforderlich sind, laden Sie einen Linux-Bereitschaftsbericht herunter, der Windows-specific Überlegungen enthält, die AWS Transform zum Zeitpunkt der Erstellung nicht berücksichtigen konnte. Falls Eingaben für Codegruppen oder Dateien erforderlich sind, finden Sie im Bericht Einzelheiten darüber, welche Art von Änderung noch vorgenommen werden muss, und gegebenenfalls Empfehlungen zur Aktualisierung Ihres Codes. Diese Änderungen müssen manuell vorgenommen werden, bevor Ihre Anwendung unter Linux ausgeführt werden kann.

Sie können die vorgeschlagenen Änderungen, die AWS Transform vorgenommen hat, in einer Vergleichsansicht überprüfen, bevor Sie sie als direkte Aktualisierungen Ihrer Dateien akzeptieren. Nachdem Sie Ihre Dateien aktualisiert und alle Punkte im Linux-Bereitschaftsbericht behandelt haben, ist Ihre Anwendung bereit, auf plattformübergreifendem .NET ausgeführt zu werden.

Sie können eine Next Steps-Markdown-Datei mit Eingabeaufforderungen zur weiteren AWS Transformation mit Transform oder einem AI-Code-Begleiter herunterladen. Um die Datei herunterzuladen, klicken Sie oben rechts im Bericht auf die Schaltfläche „Nächste Schritte herunterladen“.

Beheben von Problemen mit .NET-Transformationen in der IDE

Verwenden Sie die folgenden Abschnitte, um häufig auftretende Probleme bei .NET-Transformationen in der IDE mit AWS Transform zu beheben.

Woher weiß ich, ob ein Auftrag Fortschritte verzeichnet?

Sie sollten regelmäßige Aktivitäten im Worklog-Fenster sehen. Wenn AWS Transform anscheinend viel Zeit mit einem Schritt im Fenster „Jobplan AWS transformieren“ verbringt, können Sie in den Ausgabeprotokollen überprüfen, ob der Job noch aktiv ist. Wenn Diagnosemeldungen generiert werden, ist der Auftrag noch aktiv.

Um die Ausgaben zu überprüfen, wählen Sie unter „Ausgabe“ die Registerkarte „Ausgabe“ Visual Studio. Wählen Sie im Menü Show output from: die Option Amazon Q Language Client aus.

Der folgende Screenshot zeigt ein Beispiel für die Ausgaben, die AWS Transform während einer Transformation generiert.

```

Output
Show output from: Amazon Q Language Client
Info: [2024-07-29T22:24:59.263Z] Calling getTransform request with job Id: e5fed4b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.263Z] send request to get transform api: ("transformationJobId":"e5fed4b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:24:59.686Z] response received from get transform api: ("transformationJob":{"jobId":"e5fed4b-8286-4fae-b08b-e98876627c53","transformationspec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime
Info: [2024-07-29T22:24:59.612Z] aws/detTransform/getTransformPlan
Info: [2024-07-29T22:24:59.612Z] Calling getTransformPlan request with job Id: e5fed4b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.612Z] send request to get transform plan api: ("transformationJobId":"e5fed4b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:25:00.016Z] received response from get transform plan api: ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design time build on the code a
Info: [2024-07-29T22:25:00.017Z] Transformation plan for job Id e5fed4b-8286-4fae-b08b-e98876627c53 is ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.039Z] aws/detTransform/getTransform
Info: [2024-07-29T22:25:10.039Z] Calling getTransform request with job Id: e5fed4b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.039Z] send request to get transform api: ("transformationJobId":"e5fed4b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:25:10.375Z] response received from get transform api: ("transformationJob":{"jobId":"e5fed4b-8286-4fae-b08b-e98876627c53","transformationspec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime
Info: [2024-07-29T22:25:10.377Z] aws/detTransform/getTransformPlan
Info: [2024-07-29T22:25:10.377Z] Calling getTransformPlan request with job Id: e5fed4b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.377Z] send request to get transform plan api: ("transformationJobId":"e5fed4b-8286-4fae-b08b-e98876627c53")
Info: [2024-07-29T22:25:10.750Z] received response from get transform plan api: ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design time build on the code a
Info: [2024-07-29T22:25:10.750Z] Transformation plan for job Id e5fed4b-8286-4fae-b08b-e98876627c53 is ("transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t

```

Warum wurden einige Projekte nicht für die Transformation ausgewählt?

AWS Transform kann nur unterstützte.NET-Projekttypen transformieren. Eine Liste der unterstützten Projekttypen und anderer Voraussetzungen für die Transformation Ihrer .NET-Projekte finden Sie unter [Schritt 1: Voraussetzungen](#).

Wie kann ich Unterstützung erhalten, wenn mein Projekt oder meine Lösung nicht transformiert wird?

Wenn Sie nicht in der Lage sind, Probleme selbst zu beheben, können Sie sich an Support oder Ihr AWS-Konto Team wenden, um einen Support-Fall einzureichen.

Um Support zu erhalten, geben Sie die ID des Transformationsauftrags an, damit AWS Sie einen fehlgeschlagenen Job untersuchen können. Um eine Transformationsauftrags-ID zu finden, wählen Sie die Registerkarte Ausgabe unter Visual Studio. Wählen Sie im Menü Show output from: die Option Amazon Q Language Client aus.

Wie kann ich verhindern, dass meine Firewall Transformationsaufträge stört?

Wenn Ihre Organisation eine Firewall verwendet, kann dies die Transformationen in Visual Studio beeinträchtigen. Sie können die Sicherheitschecks vorübergehend deaktivieren Node.js , um Fehler zu beheben oder zu testen, was die Ausführung der Transformation verhindert.

Die Umgebungsvariable NODE_TLS_REJECT_UNAUTHORIZED steuert wichtige Sicherheitsprüfungen. Wenn NODE_TLS_REJECT_UNAUTHORIZED Sie auf „0“ setzen, wird die Ablehnung nicht autorisierter TLS/SSL Zertifikate deaktiviert Node.js. Das bedeutet Folgendes:

- Self-signed Zertifikate werden akzeptiert
- Abgelaufene Zertifikate werden zugelassen.
- Zertifikate mit nicht übereinstimmenden Hostnamen sind zulässig.
- Alle anderen Fehler bei der Zertifikatvalidierung werden ignoriert.

Wenn Ihr Proxy ein selbstsigniertes Zertifikat verwendet, können Sie die folgenden Umgebungsvariablen festlegen, anstatt NODE_TLS_REJECT_UNAUTHORIZED zu deaktivieren:

```
NODE_OPTIONS = -use-openssl-ca  
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

Andernfalls müssen Sie die CA-Zertifikate angeben, die der Proxy zur Deaktivierung von `NODE_TLS_REJECT_UNAUTHORIZED` verwendet.

Um `NODE_TLS_REJECT_UNAUTHORIZED` unter Windows zu deaktivieren:

1. Öffnen Sie das Startmenü und suchen Sie nach Umgebungsvariablen.
2. Wählen Sie Systemumgebungsvariablen bearbeiten aus.
3. Wählen Sie im Fenster Systemeigenschaften die Option Umgebungsvariablen aus.
4. Wählen Sie unter Systemvariablen die Option Neu aus.
5. Legen Sie den Variablennamen auf `NODE_TLS_REJECT_UNAUTHORIZED` und den Variablenwert auf 0 fest.
6. Klicken Sie auf OK, um die Änderung zu speichern.
7. Starten Sie Visual Studio neu.

Portierung von Code auf UI-Ebene

AWS Transform kann die UI-Ebene von ASP.NET Websites auf UI-Frameworks portieren, die mit ASP.NET Core kompatibel sind und unter Linux ausgeführt werden können. Die folgenden Transformationen sind verfügbar:

- Portierung der MVC Razor-Benutzeroberfläche
- Portierung von Web Forms auf Blazor UI

Portierung der MVC Razor-Benutzeroberfläche

ASP.NET MVC-Projekte mit Razor Views-Benutzeroberfläche können auf MVC Razor Views auf ASP.NET Core portiert werden, wobei dasselbe UI-Framework verwendet wird. Obwohl die Razor-Ansichten zwischen ASP.NET und ASP.NET Core ähnlich sind, gibt es Unterschiede, die eine Portierung von Codeänderungen erfordern:

- ASP.NET MVC Razor Views verwenden den `System.Web.Mvc` Namespace und sind eng mit dem .NET Framework verknüpft.

- ASP.NET Core Razor Views sind modular aufgebaut und verfügen über eine verbesserte Dependency Microsoft.AspNetCore.Mvc Injection.
- ASP.NET Core verfügt über neue Funktionen wie Tag Helpers und View Components.

AWS Transform erkennt und portiert häufig auftretende inkompatible Komponenten und Konstrukte in Razor Views.

Portierung von Web Forms auf Blazor UI

ASP.NET Die Web Forms-Benutzeroberfläche hat kein Gegenstück auf ASP.NET Core. AWS Transform kann den Code der Web Forms-Benutzeroberflächenebene auf Blazor Server auf ASP.NET Core portieren. Der Code der UI-Ebene wird für das Ziel-UI-Framework neu geschrieben.

Um die Portierung von Web Forms auf Blazor UI zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie die Jobeinstellung UI ASP.NET Web Forms to Blazor transformieren.

Einzelheiten zur Transformation

Ihr Web Forms-Projekt wird in ein Blazor-Projekt mit serverseitigem Hosting konvertiert. Die folgenden Projekt- und Dateiänderungen werden während der Transformation vorgenommen:

Zuordnung der Dateitransformation

From	Bis	Description
*.aspx, *.ascx	*.razor	.aspx-Seiten und benutzerdefinierte .ascx-Steuer-elemente werden zu .razor-Dateien
Web.config	appsettings.json	Web.config Einstellungen werden zu appsettings.json-Einstellungen
Global.asax	Program.cs	Global.asax Program.cs Code wird Code
*.master	*layout.razor	Masterdateien werden zu Layout.razor-Dateien

Post-transformation Struktur des Projekts

Nach der Transformation befinden sich die transformierten Dateien an den folgenden Projektspeicherorten:

- **Komponentenordner:** Alle Razor-Komponenten (*.razor) werden in einem Komponentenordner platziert, der auf derselben Ebene wie die CSPROJ-Datei des Projekts erstellt wurde.
- **Seitenzuordnung:** Web Forms-Seiten (*.aspx) werden in die Ordnerstruktur konvertiert. Components/Pages
- **Zuordnung von Steuerelementen:** Web Forms-Steuerelemente (*.ascx) werden direkt im Ordner Components platziert.

Einschränkungen und nicht unterstützte Funktionen

Die folgenden Funktionen werden derzeit nicht unterstützt. Wenn Ihre Workloads diese Funktionen verwenden, muss dieser Code nach der Transformation manuell oder mit einem KI-Codebegleiter portiert werden.

- .svc-Dateien (Servicedateien)
- .ashx-Dateien (generische Handlerdateien)
- Dienstreferenzen und Webreferenzen (Reference.map-, reference.cs-, .wsdl-Dateien)
- Mischungen von .aspx-Dateien (Web Forms) und .cshtml-Dateien (Razor) im selben Projekt
- Abhängigkeiten von Projekttypen, die von Transform for .NET noch nicht unterstützt werden AWS
- Third-party Benutzeroberfläche des Anbieters libraries/controls
- Webseitenprojekte

Nur Webanwendungsprojekte (die eine CSPROJ-Datei enthalten) werden unterstützt. Informationen zum Konvertieren eines Website-Projekts in ein Webanwendungsprojekt finden Sie in der Microsoft-Anleitung [Konvertieren eines Website-Projekts in ein Webanwendungsprojekt](#).

Transformationsberichte

Nach Abschluss Ihres .NET-Transformationsauftrags sind diese Transformationsberichte verfügbar:

- [Zusammenfassungsbericht zur Transformation](#)
- [Detailbericht zur Transformation](#)

Zusammenfassungsbericht zur Transformation

Nach Abschluss eines Transformationsauftrags ist in der Webkonsole ein zusammenfassender Transformationsbericht verfügbar. Laden Sie den zusammenfassenden Bericht zur Transformation

von der Registerkarte Dashboard herunter. Wählen Sie „Transformationszusammenfassungsbericht herunterladen“ und wählen Sie „Als HTML herunterladen“ oder „Als JSON herunterladen“.

Der Transformationszusammenfassungsbericht bietet einen Überblick über die Transformation und spezifische Informationen zu den einzelnen Repositories, die transformiert wurden, einschließlich:

- Auftragsdetails
 - Überblick über die Transformationsjobs
 - Überblick über die Transformationsergebnisse
 - Überblick über die Dateien
- Liste der Repositories und für jedes Repository:
 - Überblick über Repository-Namen
 - Zusammenfassung der Transformation der Lösung
 - Projektdetails, einschließlich Status, Typ, .NET-Version, Gesamtzahl der Codezeilen, transformierten Codezeilen und geänderte Dateien

Detailbericht zur Transformation

Nach Abschluss eines Transformationsauftrags sind Transformationsdetailberichte sowohl für Webkonsolen- als auch für IDE-Benutzer verfügbar.

- Benutzer der Webkonsole: Für jedes transformierte Repository ist ein detaillierter Bericht verfügbar. Verwenden Sie auf der Registerkarte Dashboard die Links Detaillierten Bericht herunterladen in der Repository-Liste, um einen detaillierten Bericht herunterzuladen.
- IDE-Benutzer: Laden Sie den Transformationsbericht über das Download-Symbol aus dem Fenster AWS Transform Job Plan herunter.

Der Transformationsdetailbericht ist ein interaktiver HTML-Bericht. Er enthält ausführliche Informationen über die Transformation, einschließlich der Gründe für Dateiänderungen und umsetzbare Fehlerdetails. Die Informationen sind in der folgenden Hierarchie angeordnet:

- Informationen zur Job
- Für jede Lösung:
 - Zusammenfassung der Transformation der Lösung
 - Überblick über die Transformation

- Projekte
- Für jedes Projekt:
 - Zusammenfassung des Projekts
 - Zusammenfassung der Build-Fehler
 - NuGet Änderungen an Paketen
 - Änderungen an der Datei
 - Fehler beim Erstellen
- Ergebnisse des Komponententests
- Bericht zur Linux-Eignung

Einen Überblick über die einzelnen Abschnitte des Transformationsberichts mit Beispielen finden Sie im Blogbeitrag [Announcing AWS Transform for .NET — detaillierte Transformationsberichte](#).

Bewährte Methoden für .NET-Transformationen

Folgen Sie dieser Anleitung, um bessere Ergebnisse bei der .NET-Modernisierung mit AWS Transform zu erzielen. Diese bewährten Methoden gelten für den .NET Conversational AI Assistant, der derzeit für Visual Studio IDE verfügbar ist.

Themen

- [Bevor Sie transformieren](#)
- [Bewertung und Planung](#)
- [Transformieren Sie interaktiv oder autonom](#)
- [Validierung und Finalisierung](#)

Bevor Sie transformieren

Lesen Sie sich die folgenden Empfehlungen durch, bevor Sie einen .NET-Transformationsjob starten.

Verwenden Sie den .NET-Konversations-Assistenten für KI

Verwenden Sie den neuen .NET-Agenten, um die besten Transformationsergebnisse zu erzielen. Der Konversations-AI-Assistent ist Visual Studio über das [AWS Toolkit for Visual Studio](#) verfügbar. Über die MCP-Agenten Kiro Power for [Kiro](#) AWS Transform und AWS Transform ist er auch für andere IDEs verfügbar. Der neue .NET-Agent ist noch nicht in der Webkonsole verfügbar.

Verwenden Sie andere Tools, wenn das Ziel nicht die Umwandlung von .NET zu .NET ist

AWS Transform for .NET eignet sich für die Modernisierung von .NET Framework zur .NET-Codemodernisierung und .NET-Upgrades auf spätere Versionen. Es ist nicht für Transformationen geeignet, die Nicht-.NET-Sprachen wie Java oder Nicht-.NET-Frameworks wie React beinhalten. Es bietet auch kein Refactoring der Anwendungsarchitektur. Verwenden Sie [AWS Transform benutzerdefiniert](#) oder Kiro für diese Art der Modernisierung.

Verwenden Sie eine stabile Version von Visual Studio, vorzugsweise VS2026

Verwenden Sie eine GA-Version von Visual Studio anstelle einer Vorschau- oder Insiders-Edition, um Komplikationen durch Vorschau-Software zu vermeiden. Das AWS Toolkit kann mit Visual Studio 2026 oder 2022 verwendet werden. VS2026 wird empfohlen, da es bei geringerem Speicherverbrauch eine bessere Leistung erbringt.

Verwenden Sie die neueste AWS Toolkit für Visual Studio

Bleiben Sie auf der neuesten Version von AWS Toolkit for Visual Studio für Bugfixes und Feature-Updates. Sie können Ihre Toolkit-Version und das Upgrade unter Erweiterungen > Erweiterungen verwalten > Installiert überprüfen.

Arbeiten Sie in Visual Studio IDE für Projekte mittlerer oder höherer Komplexität

Die IDE-Erfahrung bietet Ihnen einen umfassenden Überblick über die Transformation. Sie können bei der Transformation von Projekten mit dem .NET-Agenten zusammenarbeiten. Verwenden Sie für Projekte mit mittlerer, hoher oder kritischer Komplexität eher die IDE als die Webkonsole.

Haben Sie einen Validierungsplan

Entscheiden Sie, wie Sie Ihre Anwendung nach der Transformation auf ihre Richtigkeit überprüfen möchten. Post-transformation, müssen Sie sicherstellen, dass sich die Anwendung bei der Ausführung korrekt verhält und aussieht und dass die Sicherheitskontrollen, die Geschäftslogik und der Datenspeicher intakt sind. Wird die Validierung manuell and/or mithilfe von Testautomatisierung durchgeführt? Wenn Ihre Lösung Komponententests enthält, portiert AWS Transform diese für Sie und führt sie aus. Die Ergebnisse werden im Transformationsbericht angezeigt.

Stellen Sie bereit NuGet Abhängigkeiten von privaten Paketen

Wenn Ihre Lösung von privaten Paketen abhängt, stellen Sie sicher, dass diese auf Ihrem lokalen Computer verfügbar sind, damit die IDE und AWS Transform sie finden können.

Geben Sie Ersatzpakete an oder fragen Sie nach Empfehlungen des Kundendienstmitarbeiters

Bei Paketen, für die es keine modernen.NET-Versionen gibt, können Sie entweder den Transformationsplan so anpassen, dass Ihre geplanten Paketersetzungen spezifiziert werden, oder Sie können den Agenten um Empfehlungen bitten.

Beenden Sie Ihre Arbeit erst, wenn Sie sicher sind, dass Sie keine weiteren Änderungen wünschen

Beenden Sie Ihren Job nach Abschluss der Transformation nicht sofort, falls Sie weitere Änderungen wünschen. Die Transformation ist erst abgeschlossen, wenn Sie sagen, dass sie abgeschlossen ist. Sie können nach Änderungen fragen, bis Sie den Auftrag als abgeschlossen markieren.

Nach der Transformation übergibst du sie an einen KI-Code-Begleiter, um deine App fertigzustellen

Erwarten Sie, AWS Transform mit einem KI-Code-Begleiter wie Kiro zu kombinieren. Ein gängiges Muster besteht darin, zuerst mit AWS Transform for .NET zu transformieren und dann an einen KI-Code-Begleiter zu übergeben, um die Anwendung fertigzustellen. Diese Finalisierungsarbeiten könnten das Identifizieren und Korrigieren von Laufzeitfehlern, Verhaltensproblemen und UX-Styling beinhalten.

Stellen Sie sich AWS Transform auf dem Weg zur Modernisierung als die Expressreise vor, die Sie Ihrem Ziel ein gutes Stück näher bringt, und einen KI-Code-Begleiter als die lokale Reise, die Sie zu Ihrem Bestimmungsort bringt.

Um die Übergabe von AWS Transform an KI-Code-Begleiter zu erleichtern, stellt AWS Transform am Ende der Transformation einen HTML-Transformationsbericht und ein Markdown-Dokument mit den nächsten Schritten zur Verfügung.

Bewertung und Planung

Nachdem Sie einen Transformationsjob gestartet haben, analysiert AWS Transform Ihren Code und erstellt einen Bewertungsbericht und einen Transformationsplan. Verwenden Sie die folgenden bewährten Methoden, um das Beste aus dieser Phase herauszuholen.

Sehen Sie sich die Bewertung an und stellen Sie Fragen, um Ihre Erwartungen zu formulieren

Prüfen Sie die Ergebnisse der Bewertung sorgfältig, um zu verstehen, welche Projekte schwierig zu transformieren sein werden und warum. Der Projektmitarbeiter stellt Projekte mit einem Komplexitätsgrad (niedrig, mittel, hoch, kritisch) vor und erklärt, warum sie diese Bewertung erhalten haben.

Stellen Sie Fragen, um mehr über schwierige Bereiche zu erfahren. Beispiel:

- Fragen Sie den Agenten nach seinem Vertrauensniveau in Bezug auf eine Projekttransformation oder einen Anwendungsfall.
- Fragen Sie den Agenten, welche Aufgaben nach der Transformation wahrscheinlich zusammen mit einem KI-Code-Begleiter erforderlich sein werden.

Überprüfen Sie den Plan und besprechen Sie die Optionen mit dem Agenten

Der Mitarbeiter stellt Ihnen einen Transformationsplan zur Überprüfung zur Verfügung. Sie können diesen Plan besprechen und ändern. Machen Sie sich zunächst mit Ihren Optionen vertraut. Fragen Sie den Agenten, welche Alternativen es zu einem Teil des Plans gibt.

Im Transformationsplan könnte beispielsweise vorgeschlagen werden, WCF-Dienste in ASP.NET Web-APIs umzuwandeln. Ihre Organisation zieht es jedoch vor, bei WCF zu bleiben. Sie fragen den Agenten nach Optionen und erfahren, dass eine Alternative darin besteht, sie in Optionen umzuwandeln. CoreWCF

Laden Sie Dokumente zur Steuerung hoch, um einen maßgeschneiderten Plan für Ihr Unternehmen zu erstellen

Der ursprüngliche Transformationsplan wird erstellt, ohne die Anforderungen und Präferenzen Ihres Unternehmens zu verstehen. Sie können den Mitarbeiter über organisatorische Konventionen, Anwendungsspezifikationen, den bevorzugten Technologie-Stack und bevorzugte Beispiele für Codierungsmuster informieren.

Nachdem Sie ein Steuerungsdokument hochgeladen haben, erläutern Sie es, um dem Agenten einen Kontext zu geben. Mit den zusätzlichen Informationen aus den Steuerungsdokumenten kann der Mitarbeiter einen Plan erstellen, der auf die Arbeitsweise Ihres Unternehmens zugeschnitten ist.

Passen Sie den Plan nach Belieben an

Der .NET-Agent ist flexibel und Sie können den Transformationsplan innerhalb der Domäne von .NET- zu .NET-Transformation frei anpassen. Sie können im Chat nach Planänderungen fragen oder, wenn Sie es vorziehen, mit Markdown-Dateien arbeiten. Überprüfe und verfeinere den Plan, bis du zufrieden bist.

Wenn ein Plan von mehreren Beteiligten geprüft werden muss, können Sie den Plan als Markdown-Datei herunterladen, teilen und später einen benutzerdefinierten Plan hochladen.

Sie überprüfen beispielsweise den Transformationsplan und entscheiden, dass die Klassenbibliotheksprojekte in .NET Standard statt in .NET 10 umgewandelt werden sollen. Im

Chat sagen Sie: „Überarbeiten Sie den Plan, alle Klassenbibliotheken auf .NET Standard 2.0 umzuwandeln“, und der Agent präsentiert Ihnen einen überarbeiteten Plan.

Transformieren Sie interaktiv oder autonom

Das Visual Studio IDE-Erlebnis bietet autonome und interaktive Modi, mit denen Sie den Grad der Interaktivität während der Transformation steuern können.

Verwenden Sie interaktive und autonome Modi, um den Grad der Interaktivität zu steuern

Sie wählen den Modus aus, wenn Sie eine Transformation starten, und Sie können ihn jederzeit über ein Drop-down-Menü oben im Chatfenster ändern.

- Verwenden Sie den autonomen Modus für die unbeaufsichtigte Transformation, der sich für Jobs über Nacht oder lang andauernde Jobs eignet. Am Ende des Jobs haben Sie immer noch die Möglichkeit, die Ergebnisse zu überprüfen und nach Änderungen zu fragen.
- Verwenden Sie den interaktiven Modus, um während des gesamten Transformationsprozesses mit dem Agenten im Chat zusammenzuarbeiten. Dabei erhalten Sie einen anpassbaren Transformationsplan, einen umfassenden Einblick in die Transformationsdetails und eine schrittweise Überprüfung jedes Projekts. Sie können iterieren, um die Ergebnisse zu verfeinern, oder die Richtung ändern, bis Sie zufrieden sind.

Sie können Modi kombinieren. Beginnen Sie beispielsweise im interaktiven Modus, um den Transformationsplan zu überprüfen und anzupassen, und wechseln Sie dann in den autonomen Modus, um die Projekte automatisch zu transformieren.

Bitten Sie den Agenten, die Codeänderungen zu erklären

Wenn Sie Codeänderungen sehen, die Sie nicht verstehen, bitten Sie den Agenten, sie zu erklären.

Verwenden Sie Checkpoints, um bei Projekten anzuhalten, um sie zu überprüfen oder zu ändern

Im interaktiven Modus können Sie nach der Genehmigung Ihres Plans Checkpoints für jedes Projekt festlegen oder löschen. Wenn ein Projekt mit einem Checkpoint transformiert wurde, wird der transformierte Code in der IDE auf das Projekt angewendet und der Agent macht eine Pause zur Überprüfung durch Sie. Sie können die Ergebnisse überprüfen, und wenn sie Ihnen nicht gefallen, können Sie weitere Änderungen beantragen.

Wenn Sie an einem Checkpoint angehalten sind, können Sie:

- Überprüfen Sie die Ergebnisse, wie sie im Chat präsentiert wurden, und stellen Sie im Chat Fragen. Zum Beispiel: „Warum haben Sie die Kryptografie-API in Datei X geändert?“
- Zeigen Sie Codeänderungen an, indem Sie im Fenster „Arbeitsplan AWS transformieren“ auf die Schaltfläche „Ergebnisse anzeigen“ für das Projekt klicken.
- Verfeinern Sie die Transformation, indem Sie nach weiteren Änderungen fragen. Zum Beispiel: „Ändern Sie dies, um Logger X zu verwenden“ oder „Ändern Sie dies, um Paket X anstelle von Paket Y zu verwenden“.
- Versuchen Sie die Transformation erneut und wiederholen Sie sie mit anderen Anweisungen. Zum Beispiel: „Ändern Sie diese Klassenbibliothek auf .NET Standard statt auf .NET 10 als Ziel“ oder „Versuchen Sie diese Transformation erneut und ändern Sie das Ziel von Blazor zu MVC Razor Pages“.
- Nehmen Sie Ihre eigenen Codeänderungen in der IDE vor.
- Bitten Sie den Agenten, mit dem nächsten Projekt-Checkpoint fortzufahren.

Iterieren Sie, bis Sie zufrieden sind

Die Modernisierung ist von Natur aus iterativ, und Sie können davon ausgehen, dass Sie mit dem Agenten iterieren werden. Sie können Änderungen an den Checkpoints des Projekts und auch am Ende der Transformation vornehmen. Iterieren Sie nach Bedarf, bis Sie zufrieden sind. Die Transformation ist erst abgeschlossen, wenn Sie sagen, dass sie abgeschlossen ist.

Kodieren Sie zusammen mit dem Agenten, wenn er an einem Checkpoint angehalten wird

Sie können Ihre eigenen Codeänderungen vornehmen, während Sie mit dem Agenten zusammenarbeiten. Wenn Sie an einem Checkpoint angehalten haben, können Sie Codedateien in Visual Studio bearbeiten. Ihre Änderungen werden synchronisiert, wenn Sie den Agenten anweisen, fortzufahren.

Validierung und Finalisierung

Nachdem die Transformation abgeschlossen ist, validieren Sie Ihre transformierte Anwendung und stellen Sie sie für den produktiven Einsatz fertig.

Lesen Sie den Transformationsbericht und die nächsten Schritte, um zu verstehen, was getan wurde und was noch übrig ist

Lesen Sie den Bericht zur HTML-Transformation, um zu erfahren, was getan wurde. Sehen Sie sich die Markdown-Datei „Nächste Schritte“ an, um zu erfahren, welche Aufgaben noch zu erledigen sind. Bitten Sie den Mitarbeiter, alle Unklarheiten zu klären.

Verwenden Sie einen KI-Code-Begleiter, um Ihre Anwendung zu validieren, zu debuggen und abzuschließen

Überprüfen Sie Ihre transformierte Anwendung auf ihre Richtigkeit. Verwenden Sie einen KI-Code-Begleiter [Kiro](#), um beispielsweise Probleme zu lösen.

Validieren Sie Komponententests

Wenn Ihre Lösung Unit-Test-Projekte (NUnit,xUnit, oderMSTest) enthält, AWS portiert Transform diese auf das moderne .NET und führt die Tests für Sie aus. Die Ergebnisse der Komponententests finden Sie im HTML-Transformationsbericht. Korrigieren Sie fehlgeschlagene Tests mit einem KI-Code-Begleiter.

Überprüfen Sie die Funktionalität der Anwendung

Führen Sie Ihre Anwendung aus und stellen Sie sicher, dass ihre Funktionalität mit der des Originals übereinstimmt. Notieren Sie funktionale Probleme und Laufzeitfehler. Korrigieren Sie mit einem AI-Code-Begleiter.

Überprüfen Sie die Benutzeroberfläche der Anwendung

Führen Sie Ihre Anwendung aus und stellen Sie sicher, dass sie wie das Original aussieht und sich verhält, einschließlich Navigation und Routing. Wenn Ihre Anwendung kein Styling hat, befinden sich die CSS-Dateien möglicherweise nicht am richtigen Speicherort. Korrigieren Sie das Problem mit einem KI-Code-Begleiter.

Modernisierung von SQL Server

AWS Transform for SQL Server Modernization ist ein AI-powered Service, der die Full-Stack-Modernisierung von Microsoft SQL Server-Datenbanken und den zugehörigen .NET-Anwendungen auf Amazon Aurora PostgreSQL automatisiert. Der Service orchestriert den gesamten Migrationsprozess von der Schemakonvertierung über die Datenmigration bis hin zur Änderung des Anwendungscodes, sodass er dem neuen Ziel-PostgreSQL entspricht. Dadurch werden Ihre Teams produktiver, indem komplexe und arbeitsintensive Aufgaben automatisiert werden.

Unterstützte -Regionen

AWS Transform for SQL Server ist in USA Ost (Nord-Virginia) verfügbar — us-east-1

Cross-Region Verwendung: Für Datenbanken in nicht unterstützten Regionen können Sie die Datenbank zur Transformation in eine unterstützte Region klonen und die Ergebnisse dann wieder in Ihrer Zielregion bereitstellen.

Funktionen und Hauptmerkmale

Datenbank-Transformation

- Schemakonvertierung: Konvertiert automatisch SQL Server-Schemas in Aurora PostgreSQL, einschließlich Tabellen, Ansichten, Indizes, Einschränkungen und Beziehungen
- Transformation gespeicherter Prozeduren: Konvertiert T-SQL gespeicherte Prozeduren mit Genauigkeit PL/pgSQL AI-enhanced
- Datenmigration: Migriert Daten mit Integritätsprüfung mithilfe des AWS Database Migration Service (DMS)
- Datenbankobjekte: Unterstützt Trigger, Funktionen, Ansichten, berechnete Spalten und Identitätsspalten
- Validierung: Automatisierte Überprüfung der Datenintegrität und Prüfungen der referentiellen Integrität

Transformation von Anwendungen

- Entity Framework-Transformation: Aktualisiert die Konfigurationen Entity Framework 6.3-6.5 und EF Core 1.0-8.0 für PostgreSQL
- ADO.NET Transformation: Konvertiert ADO.NET Datenzugriffscode von SQL Server zu PostgreSQL-Anbietern.
- Aktualisierungen der Verbindungszeichenfolge: Aktualisiert automatisch alle Datenbankverbindungszeichenfolgen auf die neue PostgreSQL-Zieldatenbank
- Änderungen am Datenbankanbieter: Ersetzt SQL Server-Anbieter durch Npgsql (PostgreSQL-Anbieter)
- ORM-Konfigurationsupdates: Ändert Datentypzuordnungen, Identitätsspalten und datenbankspezifische Konfigurationen

&Validierung der Orchestrierung

- Wave-based Modernisierung: Organisiert große Anlagen in logische Migrationsphasen
- Zuordnung von Abhängigkeiten: Identifiziert Beziehungen zwischen Anwendungen und Datenbanken
- Human-in-the-loop (HITL) -Checkpoints: Ermöglicht Prüf- und Genehmigungstermine in kritischen Phasen
- Automatisierte Validierung: Testet Schemakompatibilität, Datenintegrität und Anwendungsfunktionalität
- CI/CD Integration: Lässt sich in bestehende Entwicklungspipelines integrieren

Bereitstellung

- Bereitstellung von Amazon ECS und Amazon EC2: Automatisierte Bereitstellung in Containern mit Unterstützung für auto-scaling
- Infrastructure-as-code Generierung: Erstellt oder CDK-Vorlagen CloudFormation AWS
- Automatisierte Bereitstellungsvalidierung: Überprüft die erfolgreiche Bereitstellung anhand von Integritätsprüfungen
- Rollback-Funktionen: Unterstützt Rollback-Verfahren, falls Probleme auftreten

Unterstützte Versionen und Projekttypen

SQL Server-Versionen

AWS Transform unterstützt die folgenden SQL Server-Versionen:

SQL Server-Version	Status des Support
SQL Server 2022	Unterstützt
SQL Server 2019	Unterstützt
SQL Server 2017	Unterstützt
SQL Server 2016	Unterstützt

SQL Server-Version	Status des Support
SQL Server 2014	Unterstützt
SQL Server 2012	Unterstützt
SQL Server 2008 R2	Unterstützt

Note

Alle SQL Server-Editionen werden unterstützt (Express, Standard, Enterprise). SQL Server kann auf AWS (Amazon RDS for SQL Server oder SQL Server auf Amazon EC2) oder außerhalb von AWS gehostet werden.

.NET-Versionen

.NET-Version	Status des Support
.NET 10	Unterstützt
.NET 8	Unterstützt
.NET 7	Unterstützt
.NET 6 (Kern)	Unterstützt
.NET Framework 4.x und früher	Nicht unterstützt

Important

Legacy-.NET Framework 4.x und frühere Versionen werden nicht unterstützt. Wenn Ihre Anwendung .NET Framework verwendet, müssen Sie zunächst mithilfe von AWS Transform für die .NET-Modernisierung auf .NET Core 6+ aktualisieren, bevor Sie die Transformationsfunktionen von SQL Server nutzen können.

Entity Framework-Versionen

Framework	Unterstützte Versionen
Entity Framework 6	6.3, 6.4, 6.5
Kern von Entity Framework	1.0 bis 8.0
ADO.NET	Alle Versionen (GA)

Quellcode-Repositoryn

AWS Transform unterstützt die folgenden Quellcode-Plattformen:

- GitHub und GitHub Enterprise Server
- GitLab.com und GitLab Self-Managed
- Bitbucket Cloud und Bitbucket-Rechenzentrum
- Azure DevOps und Azure Server DevOps
- Amazon S3

Zieldatenbank

AWS Transform zielt auf Amazon Aurora PostgreSQL (PostgreSQL 15+ kompatibel) ab und unterstützt die neuesten Aurora-Funktionen und -Optimierungen.

Technische Anforderungen

Datenbankanforderungen

- Microsoft SQL Server Version 2008 R2 bis 2022
- SQL Server gehostet auf AWS (Amazon RDS for SQL Server oder SQL Server auf Amazon EC2) oder außerhalb von AWS
- Bei AWS-gehosteten Datenbanken müssen sich die Datenbank und AWS Transform in derselben AWS Region befinden.
- Für Datenbanken, die außerhalb von gehostet werden AWS, ist eine Netzwerkkonnektivität zum AWS Transform-Dienst erforderlich.

- Datenbankbenutzer mit den Berechtigungen VIEW DEFINITION und VIEW DATABASE STATE
- Datenbankkennwörter, die nur druckbare ASCII-Zeichen enthalten (ausgenommen '/', '@', '"' und Leerzeichen)
- Die VPC, die den Quell-SQL-Server enthält, muss Subnetze in mindestens 2 verschiedenen Availability Zones haben (erforderlich für DMS-Replikationssubnetzgruppen)

Anforderungen an die Anwendung

- .NET Core 6-, 7- oder 8-Anwendungen
- Entity Framework 6.3-6.5 oder Entity Framework Core 1.0-8.0 oder ADO.NET
- Datenbankverbindungen, die im Quellcode auffindbar sind
- Anwendungen werden erfolgreich erstellt und ausgeführt
- Quellcode auf unterstützten Repository-Plattformen

AWS Kontoanforderungen

- AWS Konto mit Administratorzugriff
- IAM Identity Center ist aktiviert
- Erforderliche Servicerollen wurden erstellt (siehe Anweisungen zur Einrichtung unten)
- VPC mit entsprechender Netzwerkkonfiguration

Datenverarbeitung und Speicherung

Ort der Verarbeitung

- Die Schemaverarbeitung erfolgt in einer DMS-Instanz innerhalb Ihrer VPC
- Die Datenmigration ist optional und kann bei Bedarf ausgeschlossen werden
- Transformationsartefakte werden in der AWS Transform-Serviceregion gespeichert

Gespeicherte Artefakte

Die folgenden Artikel werden in der Serviceregion gespeichert:

- Agent-Protokolle
- Bewertungsergebnisse

- SQL-Schemadateien
- DMS-Ausgabeartefakte

Important

Wichtig für die Datenresidenz: Auch wenn die Datenmigration deaktiviert ist, werden Metadaten und Verarbeitungsartefakte in der Serviceregion gespeichert. Dies ist wichtig für Organisationen mit strengen Anforderungen an die Datenresidenz.

Verwaltung von Artefakten

- Kundenoption für Verschlüsselung mit Ihren eigenen KMS-Schlüsseln
- Definierter TTL-Zeitraum (Time-to-Live) für alle Artefakte
- Artefakte können für die Offline-Speicherung heruntergeladen werden

Anforderungen für SQL Server

Datenbankanforderungen

Extern gehostete Datenbanken

Außerhalb von gehostete Datenbanken AWS werden unterstützt. Um eine extern gehostete Datenbank zu verwenden, müssen Sie die Netzwerkkonnektivität zwischen der Datenbank und dem AWS Transform-Dienst sicherstellen.

SSIS-Arbeitslasten

- Einschränkung: Die SQL Server Integration Services (SSIS) -Transformation wird nicht unterstützt.
- Umgehung: Verwenden Sie AWS Glue oder andere ETL-Dienste für die SSIS-Migration.

Verknüpfte Server

- Einschränkung: Externe Datenbankverbindungen über verknüpfte Server erfordern eine menschliche Konfiguration.
- Umgehung: Konfigurieren Sie die Verbindungsserver nach der Migration neu oder verwenden Sie alternative Ansätze wie Datenbanklinks oder Integration auf Anwendungsebene.

Komplexe Muster T-SQL

- Einschränkung: Einige fortgeschrittene T-SQL Muster erfordern möglicherweise menschliches Eingreifen.
- Umgehung: Verwenden Sie Amazon Kiro CLI für komplexe SQL-Konvertierungen. AWS Transform kennzeichnet diese zur Überprüfung während des Transformationsprozesses.

Anforderungen an die Bewerbung

Legacy-.NET-Framework

- Einschränkung: .NET Framework 4.x und frühere Versionen werden nicht unterstützt.
- Problemumgehung: Verwenden Sie AWS Transform for .NET, um zuerst auf .NET Core 6+ zu aktualisieren, und verwenden Sie dann die SQL Server-Transformation.

Entity Framework-Versionen

- Einschränkung: Nur Entity Framework 6.3-6.5 und EF Core 1.0-8.0 werden unterstützt.
- Problemumgehung: Führen Sie vor der Transformation ein Upgrade auf eine unterstützte Entity Framework-Version durch.

VB.NET Anwendungen

- Einschränkung: VB.NET wird nicht unterstützt.
- Problemumgehung: Konvertieren Sie in C# oder verwenden Sie AWS Transform custom, um von C# VB.NET zu konvertieren.

Cross-database Abhängigkeiten

- Einschränkung: Herausforderungen, wenn Datenbankschemas über mehrere Datenbanken hinweg interagieren.
- Problemumgehung: Überprüfen und überarbeiten Sie datenbankübergreifende Abfragen vor der Migration. Erwägen Sie die Konsolidierung von Datenbanken oder die Verwendung von PostgreSQL-Schemas.

- **Auswirkung:** Bei komplexen datenbankübergreifenden Szenarien ist möglicherweise menschliches Eingreifen erforderlich.

Repository-database Kopplung

- **Einschränkung:** Herausforderungen, wenn ein einzelnes Repository mehrere Datenbanken bedient.
- **Problemumgehung:** Ziehen Sie eine Umstrukturierung des Repositorys oder einen schrittweisen Migrationsansatz in Betracht.
- **Auswirkung:** Möglicherweise ist eine zusätzliche Planung für wellenbasierte Migrationen erforderlich.

Anforderungen an die Infrastruktur

account/region Einzeln pro Auftrag

- **Einschränkung:** Jeder Transformationsauftrag zielt auf ein AWS Konto und eine Region ab.
- **Umgehung:** Erstellen Sie mehrere Transformationsaufträge für Bereitstellungen mit mehreren Konten oder mehreren Regionen.

Bereitstellungsziele

- **Einschränkung:** Amazon ECS- und Amazon EC2 EC2-Bereitstellungen werden unterstützt.

Anforderungen an das Repository

Private NuGet Pakete

- **Einschränkung:** Private NuGet Pakete erfordern eine zusätzliche Konfiguration.
- **Problemumgehung:** Konfigurieren Sie private NuGet Feeds in den Transformationseinstellungen, bevor Sie den Job starten.

SQL Server-Setup

Führen Sie diese Schritte in Ihrer SQL Server-Umgebung aus, um die AWS Transform-Modernisierung zu aktivieren.

Einrichtung und Konfiguration der Datenbank

Schritt 1: Erstellen Sie einen Datenbankbenutzer mit den erforderlichen Berechtigungen

Erstellen Sie einen dedizierten Datenbankbenutzer für AWS Transform mit den erforderlichen Berechtigungen. Wenn Sie bereits einen Benutzer für DMS Schema Conversion haben, können Sie ihn wiederverwenden.

Connect zu Ihrer SQL Server-Instanz her und führen Sie die folgenden Befehle aus:

```
-- Create the login in master database
USE master;
CREATE LOGIN [atx_user] WITH PASSWORD = 'YourStrongPassword123!';

-- Switch to your application database
USE [YourDatabaseName];
CREATE USER [atx_user] FOR LOGIN [atx_user];

-- Grant required permissions
GRANT VIEW DEFINITION TO [atx_user];
GRANT VIEW DATABASE STATE TO [atx_user];
ALTER ROLE [db_datareader] ADD MEMBER [atx_user];

-- Grant master database permissions
USE master;
GRANT VIEW SERVER STATE TO [atx_user];
GRANT VIEW ANY DEFINITION TO [atx_user];
```

Note

Wiederholen Sie die datenbankspezifischen Befehle (USE, CREATE USER, GRANT) für jede Datenbank, die Sie modernisieren möchten.

Die Rolle db_datareader ist nur für die Datenmigration erforderlich, nicht nur für die Schemakonvertierung.

- Die Rolle db_datareader gewährt Lesezugriff auf alle Tabellen in der Datenbank
- Diese Rolle ist NUR bei der Durchführung einer Datenmigration erforderlich.
- Nur für die Schemakonvertierung (ohne Datenmigration) ist die Rolle db_datareader NICHT erforderlich

- Die anderen Berechtigungen (VIEW DEFINITION, VIEW DATABASE STATE usw.) reichen für die Schemakonvertierung aus

Schritt 2: Speichern Sie die Anmeldeinformationen in AWS Secrets Manager

Speichern Sie Ihre Datenbankanmeldedaten sicher in AWS Secrets Manager. Überspringen Sie diesen Schritt, wenn Sie bereits ein Geheimnis für DMS erstellt haben.

1. Navigieren Sie in der Konsole zu AWS Secrets Manager
2. Wählen Sie Neues Geheimnis speichern
3. Konfigurieren Sie das Geheimnis:
 - Geheimtyp: Anmeldeinformationen für eine andere Datenbank
 - Datenbank: Microsoft SQL Server
 - Benutzername: atx_user (oder der von Ihnen gewählte Benutzername)
 - Passwort: Das Passwort, das Sie erstellt haben
 - Servername: Ihr SQL Server-Endpunkt
 - Datenbankname: Ihr Datenbankname
 - Port: 1433 (oder Ihr benutzerdefinierter Port)
4. Wählen Sie Weiter
5. Geben Sie den geheimen Namen ein: atx-db-modernization-sqlserver
6. Fügen Sie die erforderlichen Tags hinzu (diese Tags sind verpflichtend):
 - Schlüssel: Projekt, Wert: atx-db-modernization
 - Schlüssel: Besitzer, Wert: database-connector
7. Wählen Sie in den verbleibenden Bildschirmen Weiter
8. Wähle Store
9. Notieren Sie sich den geheimen ARN zur Verwendung im nächsten Schritt

Important

Datenbankkennwörter dürfen nur druckbare ASCII-Zeichen enthalten, ausgenommen '/', '@', '' und Leerzeichen. Geheimnisse, die gelöscht werden sollen, können zu Transformationsfehlern führen.

Schritt 3: Erstellen Sie die erforderlichen DMS-Rollen

AWS Transform erfordert spezielle IAM-Rollen für DMS-Operationen. Stellen Sie diese Rollen mithilfe der folgenden CloudFormation Vorlage bereit.

Note

Wenn in Ihrem AWS Konto bereits DMS-related Rollen vorhanden sind, ändern Sie diese Vorlage, um diese Ressourcen wiederzuverwenden, anstatt Duplikate zu erstellen.

Erstellen Sie eine Datei mit dem Namen `dms-roles.yaml` mit dem folgenden Inhalt:

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'DMS Service Roles for AWS Transform SQL Server Modernization'

Resources:
  DMSCloudWatchLogsRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-cloudwatch-logs-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

  DMSS3AccessRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-s3-access-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
```

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

Policies:

- PolicyName: S3TaggedAccess

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- s3:GetBucketLocation
- s3:GetBucketVersioning
- s3:PutObject
- s3:PutBucketVersioning
- s3:GetObject
- s3:GetObjectVersion
- s3:ListBucket
- s3:DeleteObject

Resource: arn:aws:s3:::atx-db-modernization-*

Condition:

StringEquals:

aws:ResourceAccount: !Ref AWS::AccountId

DMSecretsManagerRole:

Type: AWS::IAM::Role

Properties:

RoleName: dms-secrets-manager-role

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

Policies:

- PolicyName: SecretsManagerTaggedAccess

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- secretsmanager:GetSecretValue

```
- secretsmanager:DescribeSecret
Resource: '*'
Condition:
  StringEquals:
    secretsmanager:ResourceTag/Project: atx-db-modernization
    secretsmanager:ResourceTag/Owner: database-connector
```

DMSVPCRole:

```
Type: AWS::IAM::Role
Properties:
  RoleName: dms-vpc-role
  AssumeRolePolicyDocument:
    Version: '2012-10-17'
    Statement:
      - Effect: Allow
        Principal:
          Service:
            - dms.amazonaws.com
            - schema-conversion.dms.amazonaws.com
        Action: sts:AssumeRole
  ManagedPolicyArns:
    - arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole
```

DMSServerlessRole:

```
Type: AWS::IAM::ServiceLinkedRole
Properties:
  AWSServiceName: dms.amazonaws.com
  Description: 'Service Linked Role for AWS DMS Serverless'
```

Outputs:

```
DMSCloudWatchLogsRoleArn:
  Description: ARN of the DMS CloudWatch Logs Role
  Value: !GetAtt DMSCloudWatchLogsRole.Arn
DMSS3AccessRoleArn:
  Description: ARN of the DMS S3 Access Role
  Value: !GetAtt DMSS3AccessRole.Arn
DMSSecretsManagerRoleArn:
  Description: ARN of the DMS Secrets Manager Role
  Value: !GetAtt DMSSecretsManagerRole.Arn
DMSVPCRoleArn:
  Description: ARN of the DMS VPC Role
  Value: !GetAtt DMSVPCRole.Arn
Export:
  Name: !Sub ${AWS::StackName}-VPCRole
```

```
DMSServerlessRoleArn:
  Description: ARN of the DMS Serverless Role
  Value: !Sub 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/
dms.amazonaws.com/AWSServiceRoleForDMSServerless'
  Export:
    Name: !Sub ${AWS::StackName}-ServerlessRole
```

Stellen Sie den CloudFormation Stack mit AWS CLI bereit:

```
aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1
```

Oder mit der AWS Konsole bereitstellen:

1. Navigieren Sie CloudFormation in der AWS Konsole zu
2. Wählen Sie „Stapel erstellen“
3. Wählen Sie Eine Vorlagendatei hochladen
4. Laden Sie die Datei dms-roles.yaml hoch
5. Geben Sie den Stacknamen ein: dms-roles
6. Bestätigen Sie die IAM-Fähigkeiten
7. Wählen Sie Stack erstellen

Schritt 4: Netzwerksicherheit konfigurieren

Stellen Sie die richtige Netzwerkkonnektivität zwischen AWS Transform, Ihrer SQL Server-Datenbank und anderen AWS Diensten sicher.

Konfiguration der Sicherheitsgruppe (empfohlener Ansatz)

Empfohlener Ansatz: Verwenden Sie eine auf Sicherheitsgruppen basierende Zugriffskontrolle anstelle von IP-basierten Regeln. Dies bietet eine bessere Sicherheit, eine einfachere Verwaltung und funktioniert nahtlos mit der Architektur von AWS Transform.

Warum Group-Based Sicherheitszugriffskontrolle?

- DMS-Schemakonvertierung erstellt Elastic Network Interfaces (ENIs) in Ihrer VPC

- Ihre Datenbanken müssen nicht öffentlich zugänglich sein
- AWS Transform legt keine privaten IP-Adressen offen, was die IP-based Regeln komplex macht
- Sicherheitsgruppenreferenzen bieten dynamische, automatische Updates, wenn die Ressourcen skalieren

Konfigurieren Sie Ihre SQL Server-Sicherheitsgruppe

Wenn Sie das Instanzprofil für die DMS-Schemakonvertierung in AWS Transform konfigurieren, geben Sie eine Sicherheitsgruppe für die DMS SC-Instanz an. Ihre Datenbanksicherheitsgruppe sollte eingehenden Datenverkehr von dieser DMS SC-Sicherheitsgruppe zulassen.

Step-by-step Konfiguration:

1. Identifizieren Sie die Sicherheitsgruppe für die DMS-Schemakonvertierung:
 - Dies wird bei der Erstellung des Instanzprofils in AWS Transform angegeben
 - Notieren Sie sich die Sicherheitsgruppen-ID (z. B. sg-0123456789abcdef0)
2. Aktualisieren Sie Ihre eingehenden SQL Server-Sicherheitsgruppenregeln:
 - Typ: Benutzerdefiniertes TCP
 - Port: 1433 (oder Ihr benutzerdefinierter SQL Server-Port)
 - Quelle: Die Sicherheitsgruppen-ID für die DMS-Schemakonvertierung
 - Beschreibung: „Zugriff auf die DMS-Schemakonvertierung zulassen“
3. Für das Aurora PostgreSQL-Ziel (nach der Erstellung):
 - Typ: PostgreSQL
 - Port: 5432 (oder Ihr benutzerdefinierter PostgreSQL-Port)
 - Quelle: Die Sicherheitsgruppen-ID für die DMS-Schemakonvertierung
 - Beschreibung: „Zugriff auf die DMS-Schemakonvertierung zulassen“

Important

Wichtig für Sicherheitsmodelle mit den wenigsten Rechten: Wenn Ihre Organisation ein Sicherheitsmodell mit den geringsten Rechten verwendet, das standardmäßig den gesamten Datenverkehr blockiert, müssen Sie eingehenden Datenverkehr von der Sicherheitsgruppe für die DMS-Schemakonvertierung zu Ihrem Datenbankport ausdrücklich zulassen. Öffnen Sie Port 1433 nicht für alle Quellen oder IP-Bereiche.

Erforderlich AWS Service-Konnektivität

Stellen Sie sicher, dass Ihre VPC kommunizieren kann mit:

- AWS Transformieren Sie Service-Endpunkte
- AWS DMS Endpunkte
- Aurora PostgreSQL-Endpunkte
- S3-Endpunkte für die Speicherung von Artefakten
- AWS Secrets Manager Endpunkte
- AWS CodeConnections Endpunkte

VPC-Endpunkte: Konfigurieren Sie für private Netzwerke VPC-Endpunkte für erforderliche AWS Dienste, um Internet-Gateway-Abhängigkeiten zu vermeiden.

Anforderungen für extern gehostete Datenbanken

Wenn Ihre SQL Server-Datenbank außerhalb von gehostet wird, stellen Sie sicher AWS, dass die folgenden Voraussetzungen erfüllt sind, und schließen Sie dann die Einrichtungsschritte ab, bevor Sie mit der Modernisierung beginnen.

Voraussetzungen

- Ein AWS Konto bei einer VPC
- Netzwerkkonnektivität zwischen der VPC und der externen Datenbank. Informationen zur Konfiguration der Netzwerkkonnektivität finden Sie unter [Konfiguration der Netzwerkkonnektivität](#) im AWS DMS Benutzerhandbuch.

Schritte zur Einrichtung

1. Erstellen Sie ein geheimes AWS Secrets Manager Konto mit den Verbindungsdetails für die externe Datenbank. Weitere Informationen finden Sie unter [the section called “Schritt 2: Speichern Sie die Anmeldeinformationen in AWS Secrets Manager”](#).
2. Wenn Sie dazu aufgefordert werden, geben Sie die VPC-ID und die Sicherheitsgruppen-ID für die Verbindung mit der externen Datenbank ein. AWS Transform fordert Sie zur Eingabe dieser Informationen auf, da der Datenbank-Hostname im Secret nicht innerhalb des Kontos aufgelöst werden kann. AWS

AWS Transformieren Sie das Setup

Beginnen Sie Ihre Modernisierungsreise, indem Sie auf die AWS Transform-Konsole zugreifen und ein neues Modernisierungsprojekt initiieren. In diesem Schritt werden Ihr Workspace und die grundlegende Konfiguration für Ihre Full-Stack-Transformation eingerichtet.

Zu erledigende Aktionen:

- Navigieren Sie in der AWS Management Console zu AWS Transform Service
- Wählen Sie Microsoft Modernization aus den Serviceoptionen
- Wählen Sie Neues Modernisierungsprojekt erstellen
- Geben Sie den Projektnamen und die Beschreibung an
- Wählen Sie Ihre AWS Zielregion aus (muss mit Ihrem SQL Server-Standort übereinstimmen)
- Überprüfen und bestätigen Sie die Projekteinstellungen

Note

Bewährtes Verfahren: Verwenden Sie aussagekräftige Projektnamen, die den Namen der Anwendung und die Zielumgebung enthalten (z. B. 'CustomerPortal-Production-Modernization'), um Projekte in Mehrwellenszenarien leicht identifizieren zu können.

Erstellen Sie einen Auftrag zur Modernisierung von SQL Server

Datenbank und Quellcode-Repo Connect

Datenbankkonnektor konfigurieren

Stellen Sie eine sichere Konnektivität zu Ihren SQL Server-Datenbanken her, indem Sie Datenbankconnectors konfigurieren. Der Konnektor führt Umgebungsanalysen und die Erkennung von Abhängigkeiten durch und ermöglicht AWS Transform den Zugriff auf Ihre Datenbankschemas und Metadaten zur Bewertung und Konvertierung.

Abzuschließende Aktionen:

- Wählen Sie im Setup-Assistenten die Option Datenbank-Connector konfigurieren aus

- Wählen Sie die Verbindungsmethode: Neue Verbindung oder Bestehende Verbindung
- Geben Sie die SQL Server-Verbindungsdetails (Endpunkt, Port, Datenbanknamen) an
- Konfigurieren Sie die Authentifizierung und testen Sie die Konnektivität
- Überprüfen Sie die erkannten Datenbanken und bestätigen Sie die Auswahl

 Note

Netzwerkonnektivität: Stellen Sie sicher, dass Ihre SQL Server-Sicherheitsgruppen und NACLs eingehende Verbindungen von AWS Transform-Dienstendpunkten zulassen.

Quellcode-Repository Connect

Aktivieren Sie AWS Transform, um auf den Quellcode Ihrer .NET-Anwendung zuzugreifen. AWS Transform unterstützt drei Methoden zur Bereitstellung von Quellcode: einen Personal Access Token (PAT) -Connector (empfohlen) oder Amazon S3. AWS CodeConnections Diese Integration ermöglicht es dem Service, Ihren Anwendungscode zu analysieren, Datenbankabhängigkeiten zu identifizieren und automatisierte Codetransformationen für die PostgreSQL-Kompatibilität durchzuführen.

Abzuführende Aktionen:

- Navigieren Sie zum Abschnitt Connect Source Code Repository
- Wählen Sie Ihre Authentifizierungsmethode: PAT Connector (empfohlen) oder Amazon S3 AWS CodeConnections
- Wählen Sie Repositories, die .NET-Anwendungen enthalten
- Geben Sie den Zweig für die Analyse an (in der Regel main/master für die Entwicklung)
- Validieren Sie den Repository-Zugriff und die Codestruktur

 Note

Repository Discovery: AWS Transform scannt Ihre Repositories automatisch, um .NET-Projekte, Entity Framework-Konfigurationen, Datenbankverbindungszeichenfolgen und SQL-Abhängigkeiten zu identifizieren.

 Note

Sicherheitshinweis: AWS Transform benötigt nur Lesezugriff auf Ihre Repositorys und erstellt neue Feature-Branches für transformierten Code. Ihr Hauptzweig bleibt unberührt.

Der Mensch ist auf dem Laufenden

AWS Transform verwendet Human-in-the-Loop (HITL) -Mechanismen, um die Qualität sicherzustellen und es Ihnen zu ermöglichen, wichtige Transformationsentscheidungen zu überprüfen und zu genehmigen. Die folgenden Checkpoints erfordern Ihre Aufmerksamkeit:

Überprüfung und Genehmigung des Wellenplans

Was Sie überprüfen: Die vorgeschlagenen Migrationswellen, einschließlich der Gruppierung von Datenbanken und Anwendungen und der Reihenfolge der Migrationswellen.

Sie können:

- Genehmigen Sie den Wellenplan
- Passen Sie Wellen an, indem Sie Datenbanken zwischen Wellen verschieben
- Ändern Sie die Wellensequenz
- Wellen teilen oder zusammenführen

Nach der Genehmigung fährt AWS Transform mit der Schemakonvertierung fort.

Überprüfung der Schemakonvertierung

Was Sie überprüfen: Konvertierte Datenbankobjekte, einschließlich Tabellen, gespeicherten Prozeduren, Funktionen und Triggern. Aktionspunkte heben Objekte hervor, die Aufmerksamkeit erfordern.

Sie können:

- Konvertierten Code akzeptieren
- Konvertierten Code ändern
- Markierung, die nach der Transformation von Menschen überprüft werden kann
- Sehen Sie sich den direkten Vergleich von Originalcode und konvertiertem Code an

Was passiert nach der Genehmigung: AWS Transform wendet das Schema auf Aurora PostgreSQL an und fährt mit der Datenmigration fort (falls konfiguriert).

Überprüfung des Anwendungscodes

Was Sie überprüfen: Alle Änderungen am Anwendungscode, einschließlich Entity Framework-Konfigurationen, Verbindungszeichenfolgen, Datenzugriffscode und Aufrufe gespeicherter Prozeduren.

Sie können:

- Änderungen für jede Datei akzeptieren
- Modifizieren Sie den transformierten Code
- Änderungen ablehnen (nicht empfohlen)
- Fügen Sie Kommentare für Ihr Team hinzu
- Laden Sie den transformierten Code zur lokalen Überprüfung herunter

Was passiert nach der Genehmigung: AWS Transform überträgt die Änderungen in einen neuen Branch in Ihrem Repository und fährt mit der Validierung fort.

Überprüfung der Validierungsergebnisse

Was Sie überprüfen: Automatisierte Validierungsergebnisse, einschließlich Schemakompatibilität, Datenintegritätsprüfungen und Status der Anwendungsentwicklung.

Sie können:

- Überprüfe die bestandenen Tests
- Untersuchen Sie gescheiterte Tests
- Adressieren Sie Warnungen
- Fahren Sie mit der Bereitstellung fort oder kehren Sie zurück, um Probleme zu beheben

Was passiert nach der Genehmigung: AWS Transform bereitet die Bereitstellung in Ihrer Zielumgebung vor.

Genehmigung der Bereitstellung

Was Sie überprüfen: Bereitstellungsconfiguration einschließlich Infrastructure-as-Code-Vorlagen, ECS-Servicekonfiguration und Bereitstellungseinstellungen.

Sie können:

- Die Bereitstellungseinstellungen überprüfen und anpassen
- Genehmigen Sie die Bereitstellung, um fort
- Verzögern Sie die Bereitstellung für weitere Tests
- Laden Sie den Infrastrukturcode zur Überprüfung herunter

Nach der Genehmigung stellt AWS Transform Ihre modernisierte Anwendung und Datenbank in der Zielumgebung bereit.

Bewertung und Wellenplanung

landing zone einrichten

Konfigurieren Sie die Zielinfrastrukturumgebung, in der Ihre modernisierten Anwendungen bereitgestellt werden. Die Einrichtung der landing zone umfasst die Bereitstellung von Aurora PostgreSQL, die Netzwerkkonfiguration und Referenzbereitstellungskonfigurationen.

Zu erledigende Aktionen:

- Wählen Sie im Konfigurationsmenü die Option Landing Zone einrichten
- Aurora PostgreSQL-Ziel konfigurieren (Version, Instanzklasse,) Multi-AZ
- Netzwerk- und Sicherheitseinstellungen konfigurieren (VPC, Subnetze, Sicherheitsgruppen)

Note

Kostenüberlegung: Für Aurora PostgreSQL-Instances fallen laufende Kosten an. Erwägen Sie die Verwendung von Aurora Serverless v2 für development/testing Umgebungen.

Bewertung

Führen Sie eine umfassende Analyse Ihrer Datenbankschemas, Ihres Anwendungscode und Ihrer Abhängigkeiten durch. In der Bewertungsphase wird die Komplexität der Transformation bewertet, potenzielle Herausforderungen identifiziert und detaillierte Berichte erstellt.

Abzuschließende Aktionen:

- Wählen Sie Repository Branch für die Codeanalyse aus
- Wählen Sie Repositorien und Datenbanken für die Transformation aus
- Überprüfen Sie die Bewertungsergebnisse und die Einstufungen der Komplexität
- Generieren Sie einen Bewertungsbericht mit Aufwandsprognosen
- Exportieren Sie den Bericht zur Überprüfung und Genehmigung durch die Interessengruppen

Note

Einblicke in die Bewertung: Die Bewertung bietet eine detaillierte Analyse von Schemaobjekten, gespeicherten Prozeduren und Anwendungsabhängigkeiten und schätzt, wie viel menschliches Eingreifen erforderlich ist.

Planung von Wellen

Organisieren Sie Ihre Modernisierung auf der Grundlage der Transformationskomplexität, der Geschäftsprioritäten und der Anwendungsabhängigkeiten in überschaubare Phasen. AWS Transform generiert intelligente Wellenempfehlungen, die Sie anpassen können.

Zu erledigende Aktionen:

- Überprüfen Sie den AI-Generated Wave-Plan und die Empfehlungen
- Passen Sie die Wave-Konfiguration an Ihre Geschäftsprioritäten an
- Validieren Sie Abhängigkeiten zwischen Anwendungen und Datenbanken
- Finalisieren Sie Wave Plan mithilfe der Konversationsoberfläche
- Legen Sie Prioritäten für die Ausführung von Wellen fest und weisen Sie Verantwortlichkeiten zu

Note

AI-Powered Empfehlungen: Sie können mithilfe natürlicher Sprache mit der KI interagieren, um die Empfehlungen anzupassen: „Move CustomerDB to Wave 1“ oder „Kombinieren Sie diese beiden Anwendungen in derselben Welle“.

 Note

Bewährtes Verfahren: Beginnen Sie mit einer Pilotwelle mit 1-2 Datenbanken mit geringer Komplexität, um Prozesse festzulegen und das Vertrauen des Teams zu stärken.

Datenmigration für jede Welle

Schemakonvertierung für jede Welle

Transformieren Sie SQL Server-Datenbankschemas mithilfe AI-enhanced von Konvertierungsfunktionen in PostgreSQL-compatible Entsprechungen. Dieser Prozess konvertiert Tabellen, gespeicherte Prozeduren, Funktionen, Trigger und andere Datenbankobjekte.

Abzuschließende Aktionen:

- Geben Sie Ziele für die Schemakonvertierung an und konfigurieren Sie Einstellungen
- Führen Sie die automatische Konvertierung mithilfe des DMS-Schemakonvertierungsdienstes aus
- Überprüfen Sie die Konvertierungsergebnisse und identifizieren Sie menschliche Eingriffe
- Führen Sie manuelle Eingriffe mithilfe von HITL-Eingabeaufforderungen durch
- Validieren Sie menschliche Korrekturen und führen Sie die Konvertierung bei Bedarf erneut durch

 Note

Häufige manuelle Eingriffe: Verbindungsserver, benutzerdefinierte Typen, erweiterte T-SQL Muster und herstellerspezifische SQL-Funktionen erfordern in der Regel eine Überprüfung und Korrektur durch einen Mitarbeiter.

Datenmigration für jede Welle

Übertragen Sie Daten mithilfe der AWS Database Migration Service (AWS DMS) -Integration von SQL Server nach Aurora PostgreSQL. Wählen Sie zu Testzwecken zwischen der Migration von Produktionsdaten oder der Generierung synthetischer Daten.

Zu erledigende Aktionen:

- Wählen Sie die Migration von Produktionsdaten oder die Generierung synthetischer Daten

- Konfigurieren Sie die DMS-Replikationsinstanz für die Datenübertragung
- Überwachen Sie den Migrationsfortschritt und behandeln Sie Dateninkonsistenzen
- Überprüfen Sie die Datenintegrität und referenzielle Einschränkungen
- Bestätigen Sie den erfolgreichen Abschluss, bevor Sie fortfahren

Note

Automatisierte DMS-Integration: AWS Transform abstrahiert die Komplexität der DMS-Konfiguration und übernimmt automatisch die Endpunkterstellung, Aufgabenkonfiguration und Datentypzuordnungen.

Note

Datenvalidierung: Der Service führt empirische Tests durch, indem identische Abfragen für Quell- und Zieldatenbanken ausgeführt werden, um die Datenkonsistenz sicherzustellen.

Code-Migration für jede Welle

Transformieren Sie .NET-Anwendungscode so, dass er mit Aurora PostgreSQL funktioniert, einschließlich Entity Framework-Konfigurationsupdates, Änderungen von Verbindungszeichenfolgen, SQL-Abfrageanpassungen und Framework-spezifischen Anpassungen.

Abzuführende Aktionen:

- Führen Sie die automatisierte Codeanalyse für SQL Server-Abhängigkeiten aus
- Führen Sie die Framework-Transformation durch (Entity Framework-Anbieterupdates)
- Passen Sie die SQL-Abfragesyntax an PostgreSQL-compatible SQL an
- Konfigurieren Sie Target Branch Management für transformierten Code
- Bewältigen Sie manuelle Eingriffe bei komplexen Mustern

Workflow zur Modernisierung von SQL Server

Dieser Abschnitt bietet eine schrittweise Anleitung zum vollständigen Modernisierungsprozess von SQL Server mithilfe von AWS Transform.

Schritt 1: Erstellen Sie einen SQL Server-Modernisierungsauftrag

Beginnen Sie Ihre Modernisierung, indem Sie in der Transform-Konsole einen neuen AWS Transformationsauftrag erstellen.

1. Melden Sie sich bei der AWS Transform-Konsole an
2. Wählen Sie Modernisierungsauftrag erstellen
3. Wählen Sie Windows-Modernisierungsauftrag und anschließend SQL Server-Modernisierung
4. Geben Sie die Jobdetails ein:
 - Jobname: Beschreibender Name für Ihr Projekt
 - Beschreibung: Optionale Beschreibung
 - Zielregion: AWS Region für den Einsatz
5. Wählen Sie Create job (Auftrag erstellen) aus.

Important

Nehmen Sie in Ihrem Berufsnamen keine personenbezogenen Daten (PII) auf.

Schritt 2: Connect zur SQL Server-Datenbank herstellen

Verbinden Sie AWS Transform mit Ihrer SQL Server-Datenbank, um die Schemaanalyse und -konvertierung zu ermöglichen.

Erstellen Sie einen Datenbankkonnektor

1. Navigieren Sie in Ihrem SQL Server-Modernisierungsauftrag zu Connect zu Ressourcen herstellen
2. Wählen Sie Mit SQL Server-Datenbank verbinden
3. Wählen Sie Neuen Connector erstellen
4. Geben Sie die Konnektordinformationen ein:
 - Steckernamen: Beschreibender Name
 - AWS Konto-ID: Konto, auf dem SQL Server gehostet wird
5. Nach der Bestätigung erhalten Sie einen Link zur Genehmigung. Kopieren Sie den Genehmigungslink, um von Ihrem AWS Administrator die Genehmigung für das Konto zu erhalten. Sobald sie genehmigt wurden, können Sie mit dem nächsten Schritt fortfahren.

6. Nachdem Ihr Administrator die Connector-Anfrage genehmigt hat, klicken Sie auf Senden, um mit der Einrichtung der Quellcode-Verbindung fortzufahren.

Schritt 3: Quellcode-Repository Connect

AWS Transform benötigt Zugriff auf den Quellcode Ihrer .NET-Anwendung, um den Code zu analysieren und zu transformieren, der mit Ihrer SQL Server-Datenbank interagiert. AWS Transform unterstützt drei Methoden zur Bereitstellung von Quellcode.

Wählen Sie Ihre Authentifizierungsmethode

PAT-Konnektor (Personal Access Token) (empfohlen)

Ideal für Teams, die benutzerdefinierte Rechtebereiche, selbst gehosteten Anbietersupport oder Zugriff auf anbieterspezifische APIs wie Secrets benötigen. GitHub Sie erstellen in Ihrem Quellcode-Anbieter eine PAT mit benutzerdefinierten Berechtigungen, speichern sie dort AWS Secrets Manager, und AWS Transform ruft sie bei Bedarf ab. Sie sind für die Verwaltung der Rotation und des Ablaufs von Token verantwortlich.

AWS CodeConnections

Am besten für Teams geeignet, die eine automatisierte Verwaltung von Anmeldeinformationen wünschen. AWS CodeConnections verwendet eine verwaltete Anbieterintegration, die die Authentifizierung über einen OAuth 2.0-Autorisierungsablauf abwickelt. AWS verwaltet den gesamten Lebenszyklus von Anmeldeinformationen, einschließlich der automatischen Aktualisierung und Rotation von Token. Es ist keine manuelle Verwaltung von Anmeldeinformationen erforderlich.

Amazon S3

Laden Sie Ihren Quellcode direkt in einen Amazon S3 S3-Bucket hoch. AWS Transform greift während des Transformationsjobs auf den Code aus dem Bucket zu.

Feature	PAT-Konnektor (empfohlen)	AWS CodeConnections
Verwalten von Anmeldeinformationen	Manuell (vom Kunden verwaltet)	Automatisch (AWS-verwaltet)
Token-Lebenszyklus	Manuelle Rotation erforderlich	Automatische Aktualisierung

Feature	PAT-Konnektor (empfohlen)	AWS CodeConnections
Flexibilität bei Genehmigungen	Vollständig anpassbare Bereiche	Feste Berechtigungen
Self-hosted Unterstützung für Anbieter	Unterstützt	Nicht verfügbar
Komplexität der Einrichtung	Moderat (manuelle Token-Erstellung und Speicherung)	Niedrig (einmalige Autorisierung)
Token-Speicher	Die des Kunden AWS Secrets Manager	AWS-verwaltet

Richten Sie einen PAT-Konnektor ein (empfohlen)

Mit einem PAT-Konnektor erstellen Sie in Ihrem Quellcode-Anbieter ein persönliches Zugriffstoken mit benutzerdefinierten Berechtigungen, speichern es sicher darin AWS Secrets Manager und AWS Transform ruft es bei Bedarf ab. Sie sind für die Verwaltung des Token-Lebenszyklus einschließlich Rotation und Ablauf verantwortlich. AWS Transform erstellt automatisch die erforderliche IAM-Rolle mit Berechtigungen für den Zugriff auf Ihr Geheimnis.

Der PAT-Konnektor unterstützt die folgenden Anbieter, einschließlich selbst gehosteter und benutzerdefinierter DNS/URL Versionen:

- GitHub und GitHub Enterprise Server
- GitLab.com und GitLab Self-Managed
- Bitbucket Cloud und Bitbucket-Rechenzentrum
- Azure DevOps und Azure Server DevOps

Erstellen Sie ein persönliches Zugriffstoken

Erstellen Sie eine PAT in Ihrem Quellcode-Anbieter. Die erforderlichen Berechtigungen variieren je nach Anbieter. Wählen Sie die Registerkarte für Ihren Anbieter.

⚠ Important

Kopieren Sie das Token sofort nach der Erstellung. Sie können es nicht erneut anzeigen. Legen Sie das Ablaufdatum für die Dauer des Transformationsjobs fest. Stellen Sie das Ablaufdatum nicht so ein, dass es niemals abläuft.

⚠ Warning

Speichern Sie PAT-Token niemals in Code-Repositorys oder geben Sie sie nicht über unsichere Kanäle weiter. Bewahren Sie sie immer in AWS Secrets Manager

GitHub

Navigieren Sie zu Einstellungen, Entwicklereinstellungen, Persönliche Zugriffstoken, Fine-grained Token. Wählen Sie die Repositorys aus, die Sie transformieren möchten, und gewähren Sie die folgenden Berechtigungen.

Repository-Berechtigungen

Berechtigung	Zugriff	Zweck
Inhalt	Lesen und schreiben	Liest den Quellcode und schreibt den transformierten Code zurück in das Repository
Metadaten	Read-only	Greift auf grundlegende Repository-Informationen zu

Organisationsberechtigungen (erforderlich für Organisations-Repositorys)

Berechtigung	Zugriff	Zweck
Mitglieder	Read-only	Listet Organisationen auf, auf die das Token für die Repository-Erkennung zugreifen kann

GitLab

Navigieren Sie zu Profil bearbeiten, Zugriffstoken. Wählen Sie die folgenden Bereiche aus.

Scope	Zweck
<code>read_api</code>	Liest Repository-Metadaten, Projektinformationen und Benutzerdetails und listet Gruppen und Zweige auf
<code>read_repository</code>	Liest Quellcodedateien und die Repository-Struktur zur Analyse
<code>write_repository</code>	Schreibt transformierten Code zurück in das Repository

Bitbucket

Navigieren Sie zu Kontoeinstellungen, Sicherheit, API-Token erstellen und verwalten. Die erforderlichen Bereiche hängen von Ihrem Tokentyp ab.

Workspace/Repository Token (ATCT — Bearer Auth, kein Benutzername erforderlich)

Berechtigung	Zugriff	Zweck
Repositorien	Lesen und schreiben	Listet Repos auf, liest Branches und schreibt transformierten Code per Git-Push

Konto-API-Token (ATAT — Standardauthentifizierung mit E-Mail) oder App-Passwort (ATBB — Standardauthentifizierung mit Benutzername)

Scope	Zweck
<code>read:account</code>	Identifiziert den authentifizierten Benutzer, um die Repository-Mitgliedschaft aufzulösen
<code>read:workspace:bitbucket</code>	Listet die Workspaces auf, auf die das Token zugreifen kann, sodass AWS Transform ihre Repositories auflisten kann. Nicht erforderlich, wenn Sie im Secret eine Liste mit Arbeitsbereichen angeben.

Scope	Zweck
<code>read:repository:bitbucket</code>	Listet Repositorys auf und liest Metadaten und Branch-Informationen
<code>write:repository:bitbucket</code>	Schreibt transformierten Code per Git-Push zurück in das Repository

Azure DevOps

Navigieren Sie zu Benutzereinstellungen, Persönliche Zugriffstoken. Wählen Sie Benutzerdefinierte Bereiche aus. Wählen Sie als Organisationsbereich die Option Alle zugänglichen Organisationen (empfohlen) aus, oder geben Sie eine einzelne Organisation an.

Scope	Zugriff	Zweck
Code	Lesen und schreiben	Liest Quellcode, listet Repositorys und Branches auf und schreibt transformierten Code zurück
Benutzerprofil	Lesen	Überprüft den Token-Zugriff und ermittelt die Benutzeridentität für die Suche nach Organisationen
Verwaltung der Ansprüche von Mitgliedern	Lesen	Führt Organisationen auf, auf die das Token für die Repository-Erkennung zugreifen kann

Speichern Sie das PAT in AWS Secrets Manager

1. Öffnen Sie die AWS Secrets Manager Konsole.
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Als Secret-Typ wählen Sie Anderer Secret-Typ aus.
4. Fügen Sie je nach Anbieter und Hostingtyp Schlüssel-Wert-Paare hinzu:
 - Cloud-hosted Anbieter — Fügen Sie einen Schlüssel token mit Ihrem PAT als Wert hinzu.

- Fügen Sie für Azure DevOps mit einer bestimmten Organisation auch einen Schlüssel hinzu, der `organization` mit Ihrem Organisationsnamen benannt ist.
- Füge für Bitbucket-App-Passwörter (ATBB) auch einen Schlüssel hinzu, der `username` mit deinem Bitbucket-Benutzernamen benannt ist. Füge für API-Token (ATAT) für Bitbucket-Konten einen Schlüssel hinzu, der `email` mit deiner Bitbucket-E-Mail-Adresse benannt ist.
- Self-hosted und benutzerdefinierte DNS/URL Anbieter — Füge die folgenden Schlüssel hinzu: `host` (deine Server-URL, zum Beispiel `https://github.mycompany.com`), `provider_type` (`github` `gitlab` `bitbucket`, oder `ado`) und `token` (deine PAT).
- Fügen Sie für Azure DevOps mit einer bestimmten Organisation auch einen Schlüssel hinzu, der `organization` mit Ihrem Organisationsnamen benannt ist.
- Füge für Bitbucket-App-Passwörter (ATBB) auch einen Schlüssel hinzu, der `username` mit deinem Bitbucket-Benutzernamen benannt ist. Füge für API-Token (ATAT) für Bitbucket-Konten einen Schlüssel hinzu, der `email` mit deiner Bitbucket-E-Mail-Adresse benannt ist.

Das folgende Beispiel zeigt, wie ein Secret bei einem in der Cloud gehosteten AWS Secrets Manager Anbieter aussieht: GitHub

```
{
  "token": "your-github-personal-access-token"
}
```

Das folgende Beispiel zeigt ein Bitbucket-App-Passwort (ATBB):

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

Das folgende Beispiel zeigt eine selbst GitLab gehostete Instanz:

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```

5. Wählen Sie Weiter aus.

6. Geben Sie beispielsweise `github-pat-myproject` einen geheimen Namen ein.

7. (Optional) Wählen Sie einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung aus.
8. Schließen Sie den Assistenten ab und wählen Sie Store aus.
9. Kopieren Sie den geheimen ARN. Sie benötigen diesen Wert, wenn Sie den AWS Transform-Job konfigurieren.

Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel zur Verschlüsselung Ihres Geheimnisses verwenden (anstelle des standardmäßig AWS verwalteten Schlüssels), müssen Sie die KMS-Schlüsselrichtlinie aktualisieren, damit AWS Transform das Geheimnis entschlüsseln kann. Fügen Sie Ihrer vom Kunden verwalteten KMS-Schlüsselrichtlinie die folgende Erklärung hinzu:

```
{
  "Sid": "Allow AWS Transform to decrypt secrets",
  "Effect": "Allow",
  "Principal": {
    "Service": "transform.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.REGION.amazonaws.com",
      "kms:EncryptionContext:SecretARN": "YOUR-SECRET-ARN"
    }
  }
}
```

Ersetze es *REGION* durch deine AWS Region (zum Beispiel us-east-1) und *YOUR-SECRET-ARN* durch den ARN deines Geheimnisses. Die `kms:ViaService` Bedingung stellt sicher, dass der KMS-Schlüssel nur über den AWS Secrets Manager Dienst verwendet werden kann. Die `kms:EncryptionContext:SecretARN` Bedingung beschränkt die Entschlüsselung auf Ihr spezifisches Geheimnis.

So aktualisieren Sie Ihre KMS-Schlüsselrichtlinie:

1. Öffnen Sie die AWS KMS-Konsole unter <https://console.aws.amazon.com/kms>.
2. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.

3. Wählen Sie Ihren KMS-Schlüssel aus.
4. Wählen Sie im Tab Schlüsselrichtlinie die Option Bearbeiten aus.
5. Fügen Sie die Richtlinienerklärung der vorhandenen Richtlinie hinzu.
6. Wählen Sie Änderungen speichern aus.

 Note

Wenn Sie den standardmäßigen AWS verwalteten Schlüssel (aws/secretsmanager) verwenden, müssen Sie keine KMS-Schlüsselrichtlinie ändern.

Konfigurieren Sie AWS Job transformieren

1. Navigieren Sie in Ihrem AWS Transform-Job zu Connect to resources.
2. Wählen Sie Connect Source Code Repository.
3. Wählen Sie PAT Connector als Authentifizierungsmethode aus.
4. Geben Sie den geheimen ARN aus Schritt 2 ein.
5. (Optional) Geben Sie den KMS-Schlüssel-ARN ein, wenn Sie einen vom Kunden verwalteten KMS-Schlüssel verwendet haben.
6. Wählen Sie Ihr Repository und Ihren Branch aus.
7. Klicken Sie auf Weiter.

AWS Transform erstellt automatisch eine IAM-Rolle mit den Berechtigungen, die für den Zugriff auf Ihr Geheimnis erforderlich sind.

Rotation und Wartung von Tokens

Sie sind dafür verantwortlich, PAT-Token zu rotieren, bevor sie ablaufen. Um ein Token zu rotieren:

1. Generieren Sie eine neue PAT in Ihrem Quellcode-Anbieter mit denselben Berechtigungen.
2. Aktualisieren Sie den geheimen Wert in AWS Secrets Manager.
3. Stellen Sie sicher, dass Ihr AWS Transform-Job mit dem neuen Token auf das Repository zugreifen kann.
4. Widerrufen Sie die alte PAT in Ihrem Quellcode-Anbieter.

Beheben Sie Probleme mit dem PAT-Connector

Zugriff verweigert — Ungültiger PAT

Stellen Sie sicher, dass die PAT nicht abgelaufen ist. Vergewissern Sie sich, dass das PAT die für Ihren Anbieter erforderlichen Bereiche hat. Vergewissern Sie sich, dass das PAT korrekt gespeichert ist. [AWS Secrets Manager](#)

Das Geheimnis kann nicht abgerufen werden

Stellen Sie sicher, dass der geheime ARN korrekt ist. Überprüfen Sie die Auftragsprotokolle, um sicherzustellen, dass AWS Transform die IAM-Rolle erstellt hat. Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel verwenden, überprüfen Sie die Schlüsselrichtlinie.

Unzureichende Berechtigungen

Dem PAT fehlen möglicherweise die für den Vorgang erforderlichen Bereiche. Generieren Sie die PAT mit den erforderlichen Bereichen neu und aktualisieren Sie den geheimen Wert in. [AWS Secrets Manager](#)

Einrichten AWS CodeConnections

AWS CodeConnections verwendet eine verwaltete Anbieterintegration, die automatisch temporäre OAuth-Anmeldeinformationen über einen OAuth 2.0-Autorisierungsablauf abrufen. Die Berechtigungen werden in der Anbieter-App konfiguriert und vollständig von verwaltet. AWS Sie autorisieren die App einmal und übernehmen die AWS gesamte Verwaltung der Anmeldeinformationen.

1. Navigieren Sie in Ihrem SQL Server-Modernisierungsauftrag zu Connect Ressourcen herstellen.
2. Wählen Sie Connect Source Code Repository.
3. Wenn Sie noch keine Verbindung haben, wählen Sie Verbindung erstellen.
4. Wählen Sie Ihren Repository-Anbieter aus:
 - GitHub / GitHub Unternehmen
 - GitLab.com
 - Bitbucket Cloud
 - Azure-Repositorien
5. Folgen Sie dem Autorisierungsablauf für Ihren Anbieter.
6. Wählen Sie nach der Autorisierung Connect.

Wählen Sie Ihr Repository und Ihren Branch aus

1. Wählen Sie Ihr Repository aus der Liste aus.
2. Wählen Sie den Zweig aus, den Sie transformieren möchten (normalerweise Main, Master oder Develop).
3. (Optional) Geben Sie ein Unterverzeichnis an, falls sich Ihre .NET-Anwendung nicht im Stammverzeichnis des Repositorys befindet.
4. Klicken Sie auf Weiter.

Note

AWS Transform erstellt einen neuen Zweig für den transformierten Code. Sie können die Änderungen mithilfe Ihres normalen Codeüberprüfungsprozesses überprüfen und zusammenführen.

Genehmigung des Zugriffs auf das Repository

Für GitHub und einige andere Plattformen muss der Repository-Administrator die Verbindungsanfrage genehmigen:

1. AWS Transform zeigt einen Bestätigungslink an.
2. Teilen Sie diesen Link mit Ihrem Repository-Administrator.
3. Der Administrator prüft und genehmigt die Anfrage in seinen Repository-Einstellungen.
4. Nachdem der Administrator die Anfrage genehmigt hat, ändert sich der Verbindungsstatus in Genehmigt.

Important

Der Genehmigungsprozess kann je nach den Richtlinien Ihrer Organisation einige Zeit in Anspruch nehmen. Planen Sie diese Ausfallzeit ein.

Schritt 4: Bereitstellungsconnector erstellen (optional)

Wenn Sie die transformierten Anwendungen in Ihrem AWS Konto bereitstellen möchten, haben Sie die Möglichkeit, einen Deployment Connector auszuwählen.

Richten Sie den Bereitstellungsconnector ein

1. Wählen Sie Ja, wenn Sie Ihre Anwendungen bereitstellen möchten. Wenn Sie Nein wählen, wird dieser Schritt übersprungen.
2. Fügen Sie Ihr AWS Konto hinzu, in dem Sie die transformierten Anwendungen bereitstellen möchten.
3. Fügen Sie einen Namen hinzu, mit dem Sie sich den Connector leicht merken können
4. Reichen Sie die Konnektoranfrage zur Genehmigung ein.

Genehmigung des Deployment-Connectors

Ihr AWS Kontoadministrator muss die Verbindungsanforderung für den Deployment Connector genehmigen.

1. AWS Transform zeigt einen Bestätigungslink an
2. Teilen Sie diesen Link mit Ihrem AWS Kontoadministrator
3. Der Administrator überprüft und genehmigt die Anfrage in seinen Repository-Einstellungen
4. Nach der Genehmigung ändert sich der Verbindungsstatus in Genehmigt

Important

Der Genehmigungsprozess kann je nach den Richtlinien Ihrer Organisation einige Zeit in Anspruch nehmen. Planen Sie diese Ausfallzeit ein.

Schritt 5: Bestätigen Sie Ihre Ressourcen

Nachdem Sie eine Verbindung zu Ihrer Datenbank und Ihrem Repository hergestellt haben, überprüft AWS Transform, ob alle erforderlichen Ressourcen zugänglich und bereit für die Transformation sind.

Was AWS Transform verifiziert

- Datenbankkonnektivität: Die Verbindung ist aktiv, der Benutzer hat die erforderlichen Berechtigungen, auf Datenbanken kann zugegriffen werden, die Version wird unterstützt
- Repository-Zugriff: Auf das Repository kann zugegriffen werden, eine Verzweigung ist vorhanden, .NET-Projektdateien wurden erkannt, Datenbankverbindungen sind auffindbar
- Bereitschaft zur Umgebung: Die VPC-Konfiguration unterstützt DMS, erforderliche AWS Servicerollen sind vorhanden, Netzwerkkonnektivität hergestellt, Regionskompatibilität bestätigt

Sehen Sie sich die Checkliste vor dem Flug an

1. Navigieren Sie im Jobplan zu Bestätigen Sie Ihre Ressourcen
2. Sehen Sie sich die Punkte der Checkliste an:
 - # Datenbankverbindung verifiziert
 - # Der Zugriff auf das Repository wurde bestätigt
 - # .NET-Version wird unterstützt
 - # Entity Framework oder ADO.NET erkannt
 - # Netzwerkkonfiguration gültig
 - # Erforderliche Berechtigungen wurden erteilt
3. Wenn alle Elemente als abgeschlossen angezeigt werden, wählen Sie Weiter
4. Wenn bei einigen Elementen Warnungen oder Fehler angezeigt werden, beheben Sie diese, bevor Sie fortfahren

Schritt 6: Entdeckung und Bewertung

AWS Transform analysiert Ihre SQL Server-Datenbank und .NET-Anwendung, um den Umfang und die Komplexität der Modernisierung zu verstehen.

Was wird entdeckt

- Datenbankobjekte: Tabellen, Ansichten, Indizes, gespeicherte Prozeduren, Funktionen, Trigger, Einschränkungen, Datentypen, berechnete Spalten, Identitätsspalten, Fremdschlüsselbeziehungen
- Anwendungscode: .NET-Projektstruktur, Entity Framework-Modelle und -Konfigurationen, ADO.NET Datenzugriffscode, Datenbankverbindungszeichenfolgen, Aufrufe gespeicherter Prozeduren, SQL-Abfragen im Code

- Abhängigkeiten: Welche Anwendungen verwenden welche Datenbanken, datenbankübergreifende Abhängigkeiten, gemeinsam genutzte gespeicherte Prozeduren, gemeinsame Datenzugriffsmuster

Discovery-Prozess

- AWS Transform beginnt nach Bestätigung der Ressource automatisch mit der Erkennung
- Die Erkennung dauert je nach Datenbankgröße und Anwendungskomplexität in der Regel 5 bis 15 Minuten
- Überwachen Sie den Fortschritt im Arbeitsprotokoll
- AWS Transform zeigt Aktualisierungen in Echtzeit an, sobald Objekte entdeckt werden

Überprüfen Sie die Discovery-Ergebnisse

Gehen Sie nach Abschluss der Untersuchung zu Ermittlung und Bewertung, um Folgendes zu überprüfen:

Datenbankanalyse:

- Anzahl der Objekte: Anzahl der Tabellen, Ansichten, gespeicherten Prozeduren, Funktionen, Trigger
- Komplexitätsbewertung: Bewertung der Transformationskomplexität (niedrig, mittel, hoch)
- Aktionspunkte: Objekte, die möglicherweise menschliche Aufmerksamkeit erfordern
- Unterstützte Funktionen: Datenbankfunktionen, die automatisch konvertiert werden
- Nicht unterstützte Funktionen: Funktionen, für die Behelfslösungen erforderlich sind

Anwendungsanalyse:

- Projekttyp: ASP.NET Core, Konsolen-App, Klassenbibliothek usw.
- .NET-Version: .NET Core-Version erkannt
- Datenzugriffsframework: Entity Framework-Version oder ADO.NET
- Datenbankverbindungen: Anzahl der gefundenen Verbindungszeichenfolgen
- Komplexität des Codes: Bewertung der Transformationskomplexität

Übersicht der Abhängigkeiten:

- Visuelle Darstellung der Beziehungen zwischen Anwendungen und Datenbanken
- Cross-database Abhängigkeiten
- Gemeinsam genutzte Komponenten

Komplexitätsbeurteilung verstehen

AWS Transform unterteilt Ihre Modernisierung in drei Kategorien:

Komplexität	Merkmale	Erwartetes Ergebnis
Niedrig (Klasse A)	Standard-SQL-Muster (ANSI SQL), einfache gespeicherte Prozeduren, grundlegende Datentypen, Entity Framework mit Standardkonfigurationen	Minimales menschliches Eingreifen erwartet, hohe Erfolgsquote bei der Automatisierung
Mittel (Klasse B)	Fortgeschrittene T-SQL Muster, komplexe gespeicherte Prozeduren mit Geschäftslogik, benutzerdefinierte Funktionen, berechnete Spalten	Ein gewisses menschliches Eingreifen ist erforderlich, eine Überprüfung durch einen Experten wird empfohlen
Hoch (Klasse C)	CLR-Assemblies, Verbindungsserver, Service Broker, komplexe Volltextsuche	Umfangreiches manuelles Refactoring erforderlich, ein schrittweises Vorgehen ist in Betracht zu ziehen

Bewertungsbericht

AWS Transform generiert einen detaillierten Bewertungsbericht, der Folgendes beinhaltet:

- Zusammenfassung mit umfassendem Überblick
- Vollständiges Datenbankinventar
- Inventar der Anwendungen
- Prozentsatz der Transformationsbereitschaft
- Schätzung des Aufwands
- Strategien zur Risikobewertung und Risikominderung

- Empfohlener Ansatz

Sie können den Bewertungsbericht herunterladen, um ihn offline zu überprüfen und mit allen Beteiligten zu teilen.

Schritt 7: Generieren und überprüfen Sie den Wellenplan

Für große Grundstücke mit mehreren Datenbanken und Anwendungen generiert AWS Transform einen Wellenplan, der die Modernisierung in logischen Gruppen sequenziert.

Was ist ein Wellenplan?

Ein Wellenplan organisiert Ihre Modernisierung in Phasen (Wellen) auf der Grundlage von:

- Abhängigkeiten zwischen Datenbanken und Anwendungen
- Geschäftsprioritäten
- Risikotoleranz
- Verfügbarkeit von Ressourcen
- Technische Komplexität

Jede Welle enthält eine Gruppe von Datenbanken und Anwendungen, die gemeinsam modernisiert werden können, ohne dass Abhängigkeiten unterbrochen werden.

Überprüfen Sie den Wellenplan

1. Navigieren Sie im Jobplan zu Wave Planning
2. Überprüfe die vorgeschlagenen Wellen
3. Überprüfe für jede Welle:
 - Datenbanken eingeschlossen
 - Anwendungen eingeschlossen
 - Abhängigkeiten von anderen Wellen
 - Geschätzte Transformationszeit
 - Grad der Komplexität
 - Bereitstellbare Anwendungen

Passen Sie den Wave-Plan an

Sie können den Wave-Plan auf zwei Arten an Ihre Geschäftsanforderungen anpassen:

Verwenden von JSON:

1. Wählen Sie Alle Wellen herunterladen, um eine JSON-Datei mit allen Wellen zu erhalten
2. Ändern Sie Wellen im JSON wie folgt:
 - Datenbanken zwischen Wellen verschieben
 - Wellen in kleinere Gruppen aufteilen
 - Wellen zusammenfügen
 - Wellensequenz ändern
 - Datenbanken hinzufügen oder aus dem Geltungsbereich entfernen
3. Laden Sie die JSON-Datei zurück auf die Konsole hoch, indem Sie Wellenplan hochladen wählen
4. AWS Transform validiert Ihre Änderungen und warnt, wenn Abhängigkeiten verletzt werden
5. Wählen Sie Wellen bestätigen, um den Wellenplan zu aktualisieren

Chat verwenden:

Sie können die Wave-Pläne ändern, indem Sie mit dem Agenten chatten und ihn bitten, die Repositories und Datenbanken in bestimmte Waves zu verschieben. Dieser Ansatz funktioniert gut, wenn Sie kleinere Änderungen an den Wellen vornehmen müssen.

Important

Stellen Sie sicher, dass bei der Anpassung der Wellen die Abhängigkeiten berücksichtigt werden. Das Transformieren einer abhängigen Anwendung vor ihrer Datenbank kann zu Problemen führen.

Modernisierung einer einzelnen Datenbank

Wenn Sie eine einzelne Datenbank und Anwendung AWS modernisieren, erstellt Transform einen einfachen Plan mit einer Welle. Sie können ohne Wellenplanung direkt mit der Transformation fortfahren.

Genehmigen Sie den Wellenplan

1. Wählen Sie nach der Überprüfung und Anpassung (falls erforderlich) die Option Wellenplan genehmigen
2. AWS Transformieren sperrt den Wellenplan und fährt mit der Transformation fort
3. Sie können den Plan später immer noch ändern, indem Sie Wellenplan bearbeiten wählen

Schritt 8: Schemakonvertierung

AWS Transform konvertiert Ihr SQL Server-Datenbankschema in Aurora PostgreSQL, einschließlich Tabellen, Ansichten, gespeicherten Prozeduren, Funktionen und Triggern.

So funktioniert die Schemakonvertierung

AWS Transform verwendet die mit generativer KI erweiterte AWS DMS-Schemakonvertierung, um:

- Analysieren Sie SQL Server-Schemas und -Beziehungen
- Ordnen Sie Datentypen von SQL Server PostgreSQL-Äquivalenten zu
- T-SQL Transformieren zu PL/pgSQL
- Behandeln Sie Identitätsspalten, berechnete Spalten und Einschränkungen
- Überprüfen Sie die Konvertierung und die referenzielle Integrität
- Generieren Sie Aktionspunkte für Objekte, die einer menschlichen Überprüfung bedürfen

Unterstützte Konvertierungen

Automatisch konvertiert:

- Tabellen, Ansichten und Indizes
- Primärschlüssel und Fremdschlüssel
- Überprüfen Sie Einschränkungen und Standardwerte
- Die gängigsten Datentypen
- Einfache gespeicherte Prozeduren
- Grundlegende Funktionen und Auslöser
- Identitätsspalten (konvertiert in SERIAL oder GENERATED)
- Die meisten berechneten Spalten

Möglicherweise ist eine Überprüfung durch einen Menschen erforderlich:

- Komplexe gespeicherte Prozeduren mit fortgeschrittenen T-SQL
- Server-specific SQL-Funktionen (GETUTCDATE, SUSER_SNAME usw.)
- Berechnete Spalten mit komplexen Ausdrücken
- Full-text Indizes durchsuchen
- Operationen des XML-Datentyps
- HIERARCHYID-Datentyp (erfordert die Erweiterung Itree)

Nicht automatisch konvertiert:

- CLR-Assemblys
- Verknüpfte Server
- Service-Broker
- Aufträge für den SQL Server-Agenten

Starten Sie die Schemakonvertierung

1. Navigieren Sie im Jobplan zu Schemakonvertierung
2. Überprüfen Sie die Konvertierungseinstellungen:
 - PostgreSQL-Zielversion
 - Erweiterungsoptionen (Itree, PostGIS usw.)
 - Namenskonventionen
3. Wählen Sie Konvertierung starten
4. Überwachen Sie den Fortschritt im Arbeitsprotokoll
5. Die Konvertierung dauert in der Regel 10 bis 30 Minuten, abhängig von der Anzahl der Datenbankobjekte

Überprüfen Sie die Konvertierungsergebnisse

Navigieren Sie nach Abschluss der Konvertierung zu Schemakonvertierung überprüfen:

Zusammenfassung der Konvertierung:

- Konvertierte Objekte: Anzahl der erfolgreich konvertierten Objekte
- Aktionspunkte: Objekte, die menschliche Aufmerksamkeit erfordern
- Warnungen: Mögliche Probleme, die überprüft werden müssen
- Fehler: Objekte, die nicht konvertiert werden konnten

Überprüfung nach Objekttyp:

- Tabellen: Datentypzuordnungen, Einschränkungen, Indizes
- Gespeicherte Prozeduren: zur Konvertierung T-SQL PL/pgSQL
- Funktionen: Funktionssignatur und Logikänderungen
- Trigger: Änderungen der Trigger-Syntax und des Timings

Überprüfen Sie die Aktionspunkte

1. Wählen Sie „Aktionspunkte anzeigen“

2. Überprüfen Sie für jeden Aktionspunkt Folgendes:

- Objektname: Das Datenbankobjekt
- Art des Problems: Was erfordert Aufmerksamkeit
- Schweregrad: Kritisch, Warnung oder Info
- Empfehlung: Vorgeschlagene Lösung
- Originalcode: SQL Server-Version
- Konvertierter Code: PostgreSQL-Version

3. Für jeden Aktionspunkt können Sie:

- Akzeptieren: Verwenden Sie den konvertierten Code
- Ändern: Bearbeiten Sie den konvertierten Code
- Für später markieren: Nach der Transformation zur Überprüfung durch einen Menschen markieren

Beispiel: Konvertierung gespeicherter Prozeduren

SQL Server T-SQL:

```
CREATE PROCEDURE GetProductsByCategory
```

```
@CategoryId INT,  
@PageSize INT = 10  
AS  
BEGIN  
    SET NOCOUNT ON;  
  
    SELECT TOP (@PageSize)  
        ProductId,  
        Name,  
        Price,  
        DATEDIFF(DAY, CreatedDate, GETUTCDATE()) AS DaysOld  
    FROM Products  
    WHERE CategoryId = @CategoryId  
    ORDER BY Name  
END
```

Konvertiertes PostgreSQL PL/pgSQL:

```
CREATE OR REPLACE FUNCTION get_products_by_category(  
    p_category_id INTEGER,  
    p_page_size INTEGER DEFAULT 10  
)  
RETURNS TABLE (  
    product_id INTEGER,  
    name VARCHAR(255),  
    price NUMERIC(18,2),  
    days_old INTEGER  
) AS $$  
BEGIN  
    RETURN QUERY  
    SELECT  
        p.product_id,  
        p.name,  
        p.price,  
        EXTRACT(DAY FROM (NOW() - p.created_date))::INTEGER AS days_old  
    FROM products p  
    WHERE p.category_id = p_category_id  
    ORDER BY p.name  
    LIMIT p_page_size;  
END;  
$$ LANGUAGE plpgsql;
```

Vorgenommene Änderungen:

- Die Prozedur wurde in eine Funktion umgewandelt, die TABLE zurückgibt
- Parameternamen mit dem Präfix p_
- TOP wurde in LIMIT umgewandelt
- DATEDIFF wurde in EXTRACT konvertiert
- GETUTCDATE () wurde in NOW () umgewandelt
- In Kleinbuchstaben umgewandelte Spaltennamen (PostgreSQL-Konvention)

Genehmigen Sie die Schemak

1. Nachdem Sie alle Aktionspunkte überprüft und die erforderlichen Änderungen vorgenommen haben
2. Wählen Sie Schemakonvertierung genehmigen
3. AWS Transform bereitet das konvertierte Schema für die Bereitstellung in Aurora PostgreSQL vor

 Note

Sie können das konvertierte Schema als SQL-Skripts zur Offline-Überprüfung oder Versionskontrolle herunterladen.

Schritt 9: Datenmigration (optional)

AWS Transform bietet Optionen für die Migration von Daten von SQL Server nach Aurora PostgreSQL. Die Datenmigration ist optional und kann übersprungen werden, wenn Sie nur eine Schema- und Codetransformation benötigen.

Optionen für die Datenmigration

Option 1: Migration von Produktionsdaten

Migrieren Sie Ihre tatsächlichen Produktionsdaten mit AWS DMS:

- Vollständiges anfängliches Laden aller Daten
- Kontinuierliche Replikation während des Tests (CDC)
- Umstellung auf minimale Ausfallzeiten

- Datenvalidierung und Integritätsprüfungen

Option 2: Datenmigration überspringen

Nur Schema und Code transformieren:

- Nützlich für development/testing Umgebungen
- Wann werden Daten separat migriert
- Für Proof-of-Concept-Projekte

Konfigurieren Sie die Datenmigration

1. Navigieren Sie im Jobplan zu Datenmigration
2. Wählen Sie Ihre Migrationsoption:
 - Migrieren Sie Produktionsdaten
 - Datenmigration überspringen
3. Wenn Sie Produktionsdaten migrieren, konfigurieren Sie:
 - Migrationstyp: Volllast oder Volllast + CDC
 - Validierung: Aktivieren Sie die Datenvalidierung
 - Leistung: Größe der DMS-Instanz
 - Wählen Sie >Migration starten

Prozess der Migration von Produktionsdaten

Wenn Sie sich für die Migration von Produktionsdaten entscheiden:

1. Erste Synchronisierung: AWS DMS führt das vollständige Laden aller Tabellen durch
2. Kontinuierliche Replikation: (Wenn CDC aktiviert ist) Sorgt dafür, dass die Daten synchronisiert werden
3. Validierung: Überprüft die Zeilenanzahl und die Datenintegrität
4. Vorbereitung der Umstellung: Bereitet die endgültige Synchronisation vor

Zeitplan für die Migration:

- Kleine Datenbanken (< 10 GB): 30 Minuten — 2 Stunden

- Mittlere Datenbanken (10-100 GB): 2-8 Stunden
- Große Datenbanken (> 100 GB): mehr als 8 Stunden

Datenvalidierung

AWS Transform validiert migrierte Daten mit den folgenden Prüfungen:

- Vergleich der Zeilenanzahl (Quelle und Ziel)
- Integrität des Primärschlüssels
- Beziehungen mit Fremdschlüsseln
- Kompatibilität mit Datentypen
- Berechnete Spaltenergebnisse
- Behandlung von Nullwerten

Schritt 10: Transformation des Anwendungscodes

AWS Transform transformiert Ihren .NET-Anwendungscode so, dass er mit Aurora PostgreSQL statt mit SQL Server funktioniert. Es fragt nach einem Ziel-Branchnamen in Ihren Repositorys, um den transformierten Quellcode zu übertragen. Sobald Sie den Branch-Namen eingegeben haben, erstellt AWS Transform einen neuen Branch und initiiert die Transformation, die der PostgreSQL-Datenbank entspricht.

Was wird transformiert

Änderungen am Entity Framework:

- Datenbankanbieter: `UseSqlServer ()` → `UseNpgsql ()`
- Verbindungszeichenfolgen: SQL Server-Format → PostgreSQL-Format
- Datentypzuordnungen: SQL Server-Typen → PostgreSQL-Typen
- DbContext Konfigurationen: SQL → Server-specific PostgreSQL-specific
- Migrationsdateien: Aus Gründen der PostgreSQL-Kompatibilität aktualisiert

ADO.NET Änderungen:

- Verbindungsklassen: `SqlConnection` → `NpgsqlConnection`

- Befehlsklassen: SqlCommand → NpgSqlCommand
- Datenleser: SqlDataReader → NpgSqlDataReader
- Parameter: SqlParameter → NpgSqlParameter
- SQL-Syntax: T-SQL → PostgreSQL SQL

Änderungen an der Konfiguration:

- Verbindungszeichenfolgen in appsettings.json
- Pakete NuGet für Datenbankanbieter
- Konfigurationen zur Dependency-Injektion
- Startup/Program.cs Konfigurationen

Starten Sie die Codetransformation

1. Navigieren Sie im Jobplan zu Anwendungstransformation
2. Überprüfen Sie die Transformationseinstellungen:
 - .NET-Zielversion (falls aktualisiert)
 - PostgreSQL-Anbieterversion
 - Einstellungen für den Codestil
3. Wählen Sie Transformation starten
4. Überwachen Sie den Fortschritt im Arbeitsprotokoll
5. Die Transformation dauert je nach Größe der Codebasis in der Regel 15-45 Minuten

Schritt 11: Überprüfen Sie die Transformationsergebnisse

Bevor Sie mit der Bereitstellung fortfahren, überprüfen Sie die vollständigen Transformationsergebnisse, um sicherzustellen, dass alles testbereit ist.

Sie können den transformierten Code aus dem Repository-Zweig herunterladen für:

- Lokales Testen und Validieren
- Codeüberprüfung in Ihrer IDE
- Integration mit Ihrer CI/CD Pipeline

- Commit zur Versionskontrolle

Sie können auch die Zusammenfassung der Transformation herunterladen, um die Änderungen in natürlicher Sprache zu überprüfen, die AWS Transform im Rahmen der Transformation vorgenommen hat.

Zusammenfassung der Transformation

1. Navigieren Sie im Jobplan zur Zusammenfassung der Transformation
2. Sehen Sie sich die Gesamtergebnisse an:
 - Schemakonvertierung: Konvertierte Objekte, Aktionspunkte, Warnungen
 - Datenmigration: Migrierte Tabellen, übertragene Zeilen, Validierungsstatus
 - Codetransformation: Dateien geändert, Zeilen geändert, Probleme gelöst
 - Bereitschaftsbewertung: Allgemeine Bereitschaft zur Bereitstellung

Transformationsbericht erstellen

AWS Transform generiert einen umfassenden Transformationsbericht:

1. Wählen Sie Bericht erstellen
2. Wählen Sie den Berichtstyp aus:
 - Zusammenfassung: High-level Überblick für Interessengruppen
 - Technische Details: Vollständige Transformationsdokumentation
 - Aktionspunkte: Liste der erforderlichen menschlichen Aufgaben
3. Wählen Sie Bericht herunterladen

Der Bericht beinhaltet:

- Umfang und Ziele der Transformation
- Objekte und Code wurden transformiert
- Aufgetretene Probleme und Lösungen
- Validierungsergebnisse
- Bewertung der Einsatzbereitschaft
- Empfehlungen für Tests

Schritt 12: Validierung und Testen

Stellen Sie vor der Bereitstellung in der Produktion sicher, dass die transformierte Anwendung ordnungsgemäß mit Aurora PostgreSQL funktioniert.

Arten der Validierung

Automatisierte Validierung: AWS Transform führt automatisierte Prüfungen durch:

- Schemavalidierung anhand der Quelldatenbank
- Überprüfung der Datenintegrität
- Äquivalenztests abfragen
- Überprüfung der Verbindungszeichenfolge
- Überprüfung der Konfiguration

Validierung durch einen Menschen: Sie sollten zusätzliche Tests durchführen:

- Funktionstests von Anwendungsfunktionen
- Integrationstests mit anderen Systemen
- Leistungstests und Benchmarking
- Tests zur Benutzerakzeptanz
- Sicherheitstests

Führen Sie eine automatisierte Validierung durch

1. Navigieren Sie im Jobplan zu Validierung
2. Wählen Sie Validierung ausführen
3. AWS Transform führt Validierungstests aus:
 - Datenbankkonnektivität
 - Schemakompatibilität
 - Datenintegrität
 - Anwendung erstellen
 - Grundlegende Funktionalität
4. Überprüfen Sie die Validierungsergebnisse:
 - Bestanden: Tests, die erfolgreich waren

- Fehlgeschlagen: Tests, die Aufmerksamkeit erfordern
- Warnungen: Mögliche Probleme, die überprüft werden müssen

Checkliste zum Testen

Datenbank-Funktionalität:

- Auf alle Tabellen kann zugegriffen werden
- Gespeicherte Prozeduren werden korrekt ausgeführt
- Funktionen geben erwartete Ergebnisse zurück
- Löst das Feuer entsprechend aus
- Einschränkungen wurden ordnungsgemäß durchgesetzt
- Indizes verbessern die Abfrageleistung

Funktionalität der Anwendung:

- Die Anwendung wird erfolgreich gestartet
- Datenbankverbindungen wurden hergestellt
- CRUD-Operationen funktionieren korrekt
- Aufrufe gespeicherter Prozeduren sind erfolgreich
- Die Transaktionen commit/rollback wurden ordnungsgemäß durchgeführt
- Die Fehlerbehandlung funktioniert wie erwartet

Datenintegrität:

- Die Anzahl der Zeilen entspricht der Quelle
- Einzigartige Primärschlüssel
- Gültige Fremdschlüssel
- Die berechneten Spalten sind korrekt
- Null-Behandlung ist angemessen
- Kompatible Datentypen

Leistung:

- Akzeptable Antwortzeiten für Anfragen
- Verbindungspooling konfiguriert
- Indizes optimiert
- Keine Probleme mit N+1-Abfragen
- Effizienter Batch-Betrieb
- Angemessene Ressourcennutzung

Schritt 13: Bereitstellung

Nach erfolgreicher Validierung stellen Sie Ihre modernisierte Anwendung und Datenbank für die Produktion bereit.

Optionen für die Bereitstellung

- Amazon ECS und Amazon EC2 Linux

Pre-deployment Checkliste

Vor der Bereitstellung in der Produktion:

- Alle Validierungstests wurden bestanden
- Die Leistungstests wurden abgeschlossen
- Sicherheitsüberprüfung abgeschlossen
- Backup- und Rollback-Plan dokumentiert
- Überwachung und Alarmierung konfiguriert
- Das Team wurde in der neuen Umgebung geschult
- Die Interessengruppen wurden über den Einsatz informiert
- Wartungsfenster geplant

Auf Amazon ECS bereitstellen

1. Navigieren Sie im Jobplan zu Deployment
2. Wählen Sie Deploy to ECS
3. Konfigurieren Sie die Bereitstellungseinstellungen:

- Cluster: Wählen oder erstellen Sie einen ECS-Cluster
 - Service: ECS-Dienst konfigurieren
 - Aufgabendefinition: Überprüfen Sie die generierte Aufgabendefinition
 - Load Balancer: Konfigurieren ALB/NLB
 - Auto-scaling: Legen Sie Skalierungsrichtlinien fest
4. Überprüfen Sie die Infrastruktur als Code (Vorlage oder CDK-Code) CloudFormation AWS
 5. Wählen Sie Deploy

Überwachen Sie die Bereitstellung

AWS Transform stellt Ihre Anwendung bereit:

1. Erstellt einen Aurora PostgreSQL-Cluster
2. Wendet das Datenbankschema an
3. Lädt Daten (falls zutreffend)
4. Stellt Anwendungscontainer bereit
5. Konfiguriert den Load Balancer
6. Richtet die auto-scaling ein

Überwachen Sie den Bereitstellungsfortschritt und überprüfen Sie:

- Bereitstellung der Infrastruktur
- Initialisierung der Datenbank
- Bereitstellen von Anwendungen
- Gesundheitschecks bestanden
- Anwendung zugänglich
- Datenbankverbindungen funktionieren
- Protokolle, die den normalen Betrieb zeigen

Post-deployment Validierung

Nach der Bereitstellung:

Rauchtests:

- Überprüfen Sie wichtige Funktionen
- Testen Sie die Workflows wichtiger Benutzer
- Überprüfen Sie die Integrationspunkte
- Überwachen Sie die Fehlerquoten

Überwachung der Leistung:

- Verfolgen Sie die Antwortzeiten
- Überwachen Sie Datenbankabfragen
- Überprüfen Sie die Ressourcenauslastung
- Überprüfen Sie die Anwendungsprotokolle

Benutzervalidierung:

- Führen Sie Benutzerakzeptanztests durch
- Sammeln Sie Feedback
- Gehen Sie auf alle Probleme ein
- Dokumentieren Sie die gewonnenen Erkenntnisse

Rollback-Verfahren

Falls nach der Bereitstellung Probleme auftreten:

Sofortiges Rollback:

- Zur vorherigen Anwendungsversion zurückkehren
- Wechseln Sie zurück zu SQL Server (falls noch verfügbar)
- Bei Bedarf aus dem Backup wiederherstellen

Teilweises Rollback:

- Führen Sie ein Rollback bestimmter Komponenten durch
- Behalten Sie die Datenbankänderungen bei
- Nur Anwendungscode rückgängig machen

Fix weiterleiten:

- Hotfix auf Aurora PostgreSQL-Version anwenden
- Stellen Sie den aktualisierten Anwendungscode bereit
- Überwachen Sie die Lösung

Important

Halten Sie Ihre SQL Server-Datenbank für einen Zeitraum nach der Umstellung verfügbar, um bei Bedarf ein Rollback zu ermöglichen.

Post-deployment Optimierung

Nach erfolgreicher Bereitstellung:

Leistungsoptimierung:

- Optimieren Sie langsame Abfragen
- Passen Sie die Einstellungen des Verbindungspools an
- Fine-tune Aurora PostgreSQL-Parameter
- Überprüfen und optimieren Sie Indizes

Kostenoptimierung:

- Right-size Aurora-Instanz
- Konfigurieren Sie die auto-scaling entsprechend
- Überprüfen Sie die Speichereinstellungen
- Optimieren Sie die Aufbewahrung von Backups

Einrichtung der Überwachung:

- CloudWatch Dashboards konfigurieren
- Richten Sie Warnmeldungen ein
- Erweiterte Überwachung aktivieren
- Performance Insights konfigurieren

Dokumentation:

- Runbooks aktualisieren
- Änderungen an der Dokumentarchitektur
- Betriebsteam für Züge
- Erstellen Sie Anleitungen zur Fehlerbehebung

Testen und implementieren Sie nach der Transformation

Stellen Sie Ihre transformierten Anwendungen in der landing zone bereit, überprüfen Sie die Konnektivität zwischen Ihren Anwendungen und der transformierten Datenbank und richten Sie optional CI/CD Pipelines ein. Als Referenz werden CI/CD Beispiel-Pipeline-Konfigurationen generiert, die Ihnen bei der Implementierung Ihrer Bereitstellungsautomatisierung helfen sollen. In dieser letzten Phase wird die vollständige Modernisierung validiert.

Ressourcen konfigurieren

Sie müssen die bei der Bereitstellung verwendeten Ressourcen wie IAM-Rollen, Instanzprofile und S3-Bucket konfigurieren. AWS Transform ist nicht berechtigt, S3-Buckets zu erstellen oder Änderungen an Ihrem IAM vorzunehmen. Diese Aktion muss von einem Benutzer ausgeführt werden, der über die Berechtigungen zum Erstellen neuer Rollen verfügt. Normalerweise ist es der Kontoadministrator.

Um den Vorgang zu vereinfachen, stellen wir ein Setup-Skript zur Verfügung, das automatisch:

- Führt die erforderlichen CloudFormation Vorlagen aus
- Erstellt die ECS-Rolle Service-Linked
- Richtet alle erforderlichen IAM-Ressourcen ein

Important

Führen Sie das bereitgestellte Setup-Skript unverändert aus. Ändern Sie keine Ressourcennamen in den Vorlagen oder im Skript, da dies den Bereitstellungsprozess beeinträchtigen kann.

Für Linux:

```
./setup.sh --region <YOUR-Region>
```

Für Windows:

```
./setup.ps1 -Region <YOUR-Region>
```

Überprüfen Sie die Sicherheitsgruppen in Ihrer VPC

AWS Transform stellt die Anwendungen in demselben Subnetz und derselben Sicherheitsgruppe wie die Aurora PostgreSQL-Instance bereit.

Damit die Anwendung eine Verbindung zur Aurora-Instance herstellen kann, stellen Sie sicher, dass diese Sicherheitsgruppe über Regeln für ausgehende Verbindungen mit derselben Sicherheitsgruppe und über Regeln für eingehende Verbindungen von derselben Sicherheitsgruppe verfügt.

Wählen und konfigurieren Sie Anwendungen

Die AWS Transform-Benutzeroberfläche zeigt eine Liste von Anwendungen, die bereitgestellt werden können. Wählen Sie die Anwendung aus und klicken Sie auf **Configure and Commit**, um ein Konfigurationsfenster zu öffnen, in dem Sie Folgendes angeben können:

- Zielinfrastruktur für die Anwendungen: Wählen Sie ECS oder eine der EC2-Instances
- Anwendungs- oder Instanzparameter

Nachdem Sie das Konfigurationsfenster abgeschlossen und geschlossen haben, AWS transformieren Sie:

- Generiert Bereitstellungsartefakte auf der Grundlage Ihrer Konfiguration
- Übergibt diese Artefakte in Ihr Repository, einschließlich:
 - Bereitstellungsskripte
 - CloudFormation Vorlagen
 - Beispiele für CI/CD Pipeline-Konfigurationen (die Sie als Referenz für die Einrichtung Ihrer Bereitstellungsautomatisierung verwenden können)

Sobald der Commit abgeschlossen ist, ändert sich der Status der Anwendung in **Konfiguriert** und **bestätigt**. Anschließend können Sie die Anwendungen auswählen und mit der Schaltfläche **Bereitstellen** oben rechts die Bereitstellung starten.

ECS-Bereitstellung

Alle Anwendungen mit Ziel-ECS werden in einem neuen ECS-Cluster bereitgestellt, der in Ihrem Konto erstellt wird. Jede Anwendung wird in einem eigenen dedizierten Container bereitgestellt — mehrere Anwendungen pro Container werden nicht unterstützt. Sie konfigurieren Container-Parameter für jede Anwendung einzeln, z. B. die erforderliche CPU und den erforderlichen Arbeitsspeicher.

EC2-Bereitstellung

Sie können eine der vorgeschlagenen EC2-Instances auswählen und deren Parameter wie den Instance-Typ konfigurieren. Auf derselben EC2-Instance können mehrere Anwendungen bereitgestellt werden:

- Um mehrere Anwendungen auf einer einzigen Instance bereitzustellen, wählen Sie bei der Konfiguration dieselbe EC2-Zielinstanz für jede dieser Anwendungen aus.
- Alle Anwendungen, für die dieselbe Instanz als Ziel ausgewählt wurde, werden auf dieser Instance bereitgestellt und ihnen werden nach dem Zufallsprinzip unterschiedliche Ports zugewiesen.
- Beachten Sie, dass sich die Änderungen auf alle Anwendungen auswirken, die auf dieser Instanz bereitgestellt werden, wenn Sie die Instanzparameter für eine Anwendung bearbeiten und dann eine andere Anwendung bearbeiten, die auf dieselbe Instanz abzielt.

Die Bereitstellung war erfolgreich

Nach erfolgreicher Implementierung laufen Ihre Anwendungen auf Aurora PostgreSQL mit reduzierten Lizenzkosten, verbesserter Leistung und cloudnativer Skalierbarkeit. Der Job bleibt geöffnet, sofern er nicht ausdrücklich gestoppt wird. Dies ermöglicht die Option einer möglichen erneuten Bereitstellung mit aktualisierten Bereitstellungsparametern.

Bewährte Methoden und Problembehebung

Bewährte Verfahren und häufig auftretende Probleme und deren Behebung während des Modernisierungsprozesses.

ECS-Anwendungsprotokolle

CloudWatch Logs

- Alle ECS-Container-Protokolle werden automatisch an CloudWatch Logs gesendet

- Greifen Sie in der CloudWatch Konsole unter Protokollgruppen auf Protokolle zu
- Benennungsformat für Protokollgruppen: /aws/ecs/{Anwendungsname}
- Jede Container-Instance erstellt einen neuen Log-Stream innerhalb der Gruppe

Anzeigen von Protokollen

Über die AWS Konsole:

- Navigieren Sie zu CloudWatch > Protokollgruppen
- Wählen Sie die Protokollgruppe Ihrer Anwendung aus
- Wählen Sie den entsprechenden Protokollstream aus, um die Container-Logs anzuzeigen

Verwenden von AWS CLI:

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-stream-name
```

Allgemeine Protokollspeicherorte

- Anwendungsprotokolle: CloudWatch Protokolle
- ECS-Dienstereignisse: ECS-Konsole > Cluster > Dienst > Registerkarte Ereignisse
- Container health/status: ECS-Konsole > Cluster > Service > Registerkarte „Aufgaben“

Verwaltung der Datenbankverbindung

Anwendungen verwenden Umgebungsvariablen für Datenbankverbindungseinstellungen

Wenn Verbindungsprobleme auftreten:

- Überprüfen Sie die aktuellen Verbindungseinstellungen in Ihren Umgebungsvariablen
- Aktualisieren Sie die Umgebungsvariablen, um die Datenbankverbindungszeichenfolgen nach Bedarf zu ändern
- Änderungen an der Verbindungszeichenfolge können durch Aktualisierungen von Umgebungsvariablen vorgenommen werden, ohne dass die Anwendung erneut bereitgestellt werden muss

Probleme mit der Datenbankverbindung

Problem: AWS Transform kann nicht mit SQL Server verbunden werden

Lösungen:

- Überprüfen Sie die Netzwerkkonnektivität zwischen AWS Transform und SQL Server
- Überprüfen Sie die Sicherheitsgruppenregeln auf den ordnungsgemäßen Portzugriff (1433)
- Bestätigen Sie die Datenbankanmeldedaten in Secrets Manager
- Testen Sie die Datenbankberechtigungen mit dem erstellten Benutzer
- Stellen Sie sicher, dass SQL Server für die Authentifizierung im gemischten Modus konfiguriert ist
- Stellen Sie sicher, dass der geheime Schlüssel die erforderlichen Tags enthält (Projekt: atx-db-modernization, Besitzer: database-connector)

Probleme mit Firewalls und Sicherheitsgruppen

Problem: Verbindungstimeout oder Fehler „Datenbank kann nicht erreicht werden“

Hauptursache: Sicherheitsgruppen oder Netzwerk-ACLs blockieren den Datenverkehr

Lösungen:

1. Überprüfen Sie die Konfiguration der Sicherheitsgruppe:

- Vergewissern Sie sich, dass Ihre SQL Server-Sicherheitsgruppe über eine Regel für eingehenden Datenverkehr verfügt, die Port 1433 aus der Sicherheitsgruppe DMS-Schemakonvertierung zulässt
- Vergewissern Sie sich, dass es sich bei der Quelle um die Sicherheitsgruppen-ID handelt (z. B. sg-0123456789abcdef0), nicht um eine IP-Adresse
- Stellen Sie sicher, dass die Sicherheitsgruppe für die DMS-Schemakonvertierung im Instanzprofil korrekt angegeben ist
- Stellen Sie sicher, dass es keine widersprüchlichen Ablehnungsregeln gibt

2. Überprüfen Sie die Netzwerk-ACLs:

- Stellen Sie sicher, dass Netzwerk-ACLs auf Subnetzebene eingehenden Datenverkehr auf Port 1433 zulassen
- Stellen Sie sicher, dass Netzwerk-ACLs ausgehenden kurzlebigen Datenverkehr für den Rückverkehr zulassen

- Überprüfen Sie sowohl das Datenbanksubnetz als auch das DMS-Subnetz-Netzwerk-ACLs
3. Überprüfen Sie die VPC-Konfiguration:
- Vergewissern Sie sich, dass sich die DMS-Schemakonvertierungsinstanz und der SQL Server in derselben VPC befinden oder über das richtige VPC-Peering verfügen
 - Überprüfen Sie, ob Routentabellen Datenverkehr zwischen Subnetzen zulassen
 - Stellen Sie sicher, dass keine Firewall-Appliances den Verkehr blockieren
4. Konnektivität testen:
- Starten Sie eine EC2-Testinstanz im selben Subnetz wie die DMS-Schemakonvertierung
 - Hängen Sie dieselbe Sicherheitsgruppe wie DMS Schema Conversion an
 - Testen Sie die Verbindung zu SQL Server mithilfe von Telnet oder SQL Server Management Studio
 - Wenn der Test erfolgreich ist, liegt das Problem bei der AWS Transform-Konfiguration. Schlägt er fehl, liegt das Problem network/firewall

Häufiger Fehler: Öffnen von Port 1433 auf 0.0.0. 0/0 (alle Quellen) stellt ein Sicherheitsrisiko dar. Verwenden Sie immer eine auf Sicherheitsgruppen basierende Zugriffskontrolle, um den Zugriff nur auf die Sicherheitsgruppe DMS Schema Conversion zu beschränken.

Probleme mit der Schemakonvertierung

Problem: Bei der Schemakonvertierung werden viele Aktionspunkte angezeigt

Lösungen:

- Überprüfen Sie die Aktionspunkte im Konversionsbericht
- Priorisieren Sie basierend auf der Wirkung
- Verwenden Sie Amazon Q Developer für komplexe SQL-Konvertierungen
- Wenden Sie sich für weitere Informationen an den AWS Support
- Ziehen Sie einen schrittweisen Ansatz für komplexe Datenbanken in Betracht

Probleme bei der Anwendungstransformation

Problem: Die Anwendungstransformation kann nicht erstellt werden

Lösungen:

- Überprüfen Sie die Build-Fehler im Transformationsbericht
- Konfigurieren Sie bei Bedarf private NuGet Feeds
- Aktualisieren Sie bei Bedarf die Paketreferenzen
- Suchen Sie nach Windows-specific Abhängigkeiten
- Überprüfen Sie die Transformationsprotokolle auf detaillierte Fehler

Probleme bei der Datenmigration

Problem: Die Validierung der Datenmigration schlägt fehl

Lösungen:

- Überprüfen Sie den Validierungsbericht auf bestimmte Fehler
- Überprüfen Sie die Datentypzuordnungen
- Überprüfen Sie die Konfiguration der Identitätsspalte (STANDARDMÄSSIG GENERIERT oder IMMER GENERIERT)
- Überprüfen Sie die berechneten Spaltenausdrücke
- Wenden Sie sich AWS bei komplexen Datenproblemen an den Support

Probleme bei der Bereinigung von Ressourcen

Problem: Der Transformationsjob schlägt aufgrund von Ressourcenfehlern fehl

Lösungen:

- Suchen Sie nach vorhandenen DMS-Ressourcen (Migrationsprojekte, Datenanbieter, Instanzprofile)
- Bereinigen Sie fehlgeschlagene oder unvollständige Ressourcen aus früheren Versuchen
- Stellen Sie sicher, dass das Löschen von Geheimnissen nicht geplant ist
- Überprüfen Sie die Servicekontingente für DMS und Aurora PostgreSQL
- Wenden Sie sich an den AWS Support, wenn das Problem durch die Bereinigung nicht behoben werden kann

Bereitstellungsprobleme

Problem: Die transformierte Anwendung kann keine Verbindung zu Aurora PostgreSQL herstellen

Lösungen:

- Überprüfen Sie das Format der Verbindungszeichenfolge für PostgreSQL
- Überprüfen Sie die Sicherheitsgruppenregeln
- Überprüfen Sie die Datenbankanmeldedaten in Secrets Manager
- Stellen Sie sicher SSL/TLS , dass es richtig konfiguriert ist
- Testen Sie die Verbindung mit psql oder pgAdmin

Weitere Hilfe

Wenn Sie sich an den AWS Support wenden, geben Sie bitte Folgendes an:

- ID des Transformationsauftrags
- AWS Konto-ID
- Region
- Fehlermeldungen und Screenshots
- Transformationsprotokolle (in der AWS Transform-Konsole verfügbar)

Sicherheit bei AWS Transformieren

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen 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, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der [AWS](#). Weitere Informationen zu den Compliance-Programmen, die für AWS Transform gelten, finden Sie unter [AWS Services im Umfang nach Compliance-Programmen AWS](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von AWS Transform anwenden können. In den folgenden Themen erfahren Sie, wie Sie AWS Transform konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Transform-Ressourcen unterstützen.

Topics

- [Datenschutz in AWS Transform](#)
- [Identitäts- und Zugriffsmanagement für AWS Transformieren](#)
- [Konformitätsvalidierung für AWS Transformieren](#)
- [Resilienz in AWS Transformieren](#)
- [AWS Transform und Schnittstellenendpunkte \(AWS PrivateLink\)](#)
- [Zugriff auf AWS Transform Webanwendung aus einer VPC](#)

Datenschutz in AWS Transform

Das [Modell der AWS gemeinsamen Verantwortung](#) gilt für den Datenschutz in AWS Transform. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und AWS-Services die Verwaltungsaufgaben der von Ihnen verwendeten Geräte verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS-Modell der geteilten Verantwortung](#) und die GDPRAWS im Blog zur -Sicherheit.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsdienste wie Amazon Macie, die Sie bei der Erkennung und Sicherung sensibler Daten unterstützen, die in gespeichert sind Amazon S3.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in [Tags](#) oder Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der API AWS Management Console, AWS Command Line Interface () AWS Transform AWS CLI oder den AWS-Services SDKs arbeiten oder diese anderweitig verwenden. AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Weitere Informationen zur AWS Transform Verwendung von Inhalten finden Sie unter [AWS Transform Verbesserung des Service](#).

AWS Transform speichert Ihre Fragen, deren Antworten und zusätzlichen Kontext wie Konsolenmetadaten und Code in Ihrer IDE, um Antworten auf Ihre Fragen zu generieren. Weitere Informationen zur Verschlüsselung von Daten finden Sie unter [Datenverschlüsselung in AWS Transform](#). Informationen darüber, wie wir einige von Ihnen gestellte Fragen AWS Transform und deren Antworten verwenden AWS können, um unsere Dienste zu verbessern, finden Sie unter [AWS Transform Verbesserung des Service](#).

AWS Transform In werden Ihre Daten in der AWS Region gespeichert, in der Ihr AWS Transform Profil erstellt wurde.

Bei Querverweisen AWS Transform können Ihre Anfragen an in einer anderen Region innerhalb der Region bearbeitet werden, in der Ihre Daten gespeichert sind. [Weitere Informationen finden Sie unter Cross-Region Inferenz](#).

Topics

- [Cross-region Verarbeitung in AWS Transform](#)
- [Datenverschlüsselung in AWS Transform](#)
- [AWS Transform Verbesserung des Service](#)

Cross-region Verarbeitung in AWS Transform

In den folgenden Abschnitten wird beschrieben, wie regionsübergreifende Inferenz und regionsübergreifende Aufrufe zur Bereitstellung des Dienstes verwendet werden. AWS Transform

Cross-region Inferenz

AWS Transform wird von Amazon Bedrock unterstützt und verwendet regionsübergreifende Inferenz, um den Datenverkehr auf verschiedene zu verteilen, um die Leistung und Zuverlässigkeit von Large Language Model (LLM) -Inferenzen AWS-Regionen zu verbessern. Regionsübergreifende Inferenz bietet folgende Vorteile:

- Höherer Durchsatz und größere Stabilität in Zeiten hoher Nachfrage
- Verbesserte Leistung
- Zugriff auf neu eingeführte AWS Transform Funktionen und Funktionen, die auf den leistungsstärksten LLMs basieren, die auf Amazon Bedrock gehostet werden

Cross-region Inferenzanfragen werden innerhalb der Region aufbewahrt AWS-Regionen , die Teil der Region ist, in der sich die Daten ursprünglich befinden. Beispielsweise wird eine Anfrage, die über eine AWS Transform Konfiguration in den USA gestellt wird, innerhalb der AWS-Regionen USA aufbewahrt. Die regionsübergreifende Inferenz ändert zwar nichts daran, wo Ihre Daten gespeichert werden, aber Ihre Anfragen und Ausgabeergebnisse können sich außerhalb der Region bewegen, in der sich die Daten ursprünglich befinden. Alle Daten werden bei der Übertragung über das sichere Netzwerk von Amazon verschlüsselt. Für die Nutzung von regionsübergreifender Inferenz fallen keine zusätzlichen Kosten an.

Regionsübergreifende Inferenz hat keinen Einfluss darauf, wo Ihre Daten gespeichert sind. Informationen darüber, wo Daten gespeichert werden, wenn Sie sie verwenden AWS Transform, finden Sie unter [Datenschutz in AWS Transform](#).

Unterstützte Regionen für AWS Transform Regionsübergreifende Inferenz

Für bestimmte Anfragen, die Sie stellen, sind AWS Transform möglicherweise regionsübergreifende Anrufe erforderlich. In der folgenden Tabelle wird beschrieben, in welche Regionen Ihre Anfragen je nach dem Bereich weitergeleitet werden können, aus dem die Anfrage stammt.

Quellregion	Zielregionen
USA Ost (Nord-Virginia): (us-east-1)	USA Ost (Nord-Virginia): (us-east-1) USA Ost (Ohio): (us-east-2) USA West (Oregon): (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (Paris) (eu-west-3)
Asien-Pazifik (Mumbai): (ap-south-1)	Asien-Pazifik (Tokyo) (ap-northeast-1)

Quellregion	Zielregionen
	Asien-Pazifik (Seoul): (ap-northeast-2) Asien-Pazifik (Osaka) (ap-northeast-3) Asien-Pazifik (Mumbai): (ap-south-1) Asien-Pazifik (Hyderabad) (ap-south-2) Asien-Pazifik (Singapur): (ap-southeast-1) Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)
Asien-Pazifik (Tokyo) (ap-northeast-1)	Asien-Pazifik (Tokyo) (ap-northeast-1) Asien-Pazifik (Osaka) (ap-northeast-3)
Asien-Pazifik (Seoul): (ap-northeast-2)	Asien-Pazifik (Tokyo) (ap-northeast-1) Asien-Pazifik (Seoul): (ap-northeast-2) Asien-Pazifik (Osaka) (ap-northeast-3) Asien-Pazifik (Mumbai): (ap-south-1) Asien-Pazifik (Hyderabad) (ap-south-2) Asien-Pazifik (Singapur): (ap-southeast-1) Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)
Asien-Pazifik (Sydney): (ap-southeast-2)	Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)

Quellregion	Zielregionen
Europa (London) (eu-west-2)	Europa (Frankfurt) (eu-central-1) Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (London) (eu-west-2) Europa (Paris) (eu-west-3)
Kanada (Zentral): (ca-central-1)	Kommerziell AWS-Regionen + Kanada (Zentral) (ca-central-1)
Südamerika (São Paulo) (sa-east-1)	Kommerziell AWS-Regionen + Südamerika (São Paulo) (sa-east-1)

Eine vollständige Liste der Regionen, die Sie verwenden können AWS Transform, finden Sie unter [Unterstützte Regionen für AWS Transform](#)

Cross-Region Wissen

Wenn Sie eine allgemeine Frage zu AWS Transform Diensten, Transformationsworkflows oder verwandter AWS Dokumentation stellen, richten Sie AWS Transform möglicherweise regionsübergreifende Anfragen an USA Ost (Virginia) (us-east-1) für US-Regionen oder Europa (Frankfurt) (eu-central-1) für alle anderen Regionen, um Dokumentation abzurufen und Ihre Anfrage zu bearbeiten. Wenn Sie beispielsweise Fragen zur Nutzung anderer AWS Dienste wie Lambda stellen, AWS Transform können Sie einen regionsübergreifenden Anruf tätigen, um die entsprechende AWS Dokumentation zur Beantwortung Ihrer Frage abzurufen. In der folgenden Tabelle wird beschrieben, in welche Regionen Ihre Anfragen je nach dem Bereich weitergeleitet werden können, aus dem die Anfrage stammt.

Quellregion	Zielregionen
USA Ost (Nord-Virginia): (us-east-1)	USA Ost (Nord-Virginia): (us-east-1)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1)
Europa (London) (eu-west-2)	Europa (Frankfurt) (eu-central-1)
Asien-Pazifik (Tokyo) (ap-northeast-1)	Europa (Frankfurt) (eu-central-1)
Asien-Pazifik (Sydney): (ap-southeast-2)	Europa (Frankfurt) (eu-central-1)
Asien-Pazifik (Seoul): (ap-northeast-2)	Europa (Frankfurt) (eu-central-1)
Asien-Pazifik (Mumbai): (ap-south-1)	Europa (Frankfurt) (eu-central-1)
Kanada (Zentral): (ca-central-1)	Europa (Frankfurt) (eu-central-1)
Südamerika (São Paulo) (sa-east-1)	Europa (Frankfurt) (eu-central-1)

Diese Einstellung ist standardmäßig aktiviert. Ein Kontoadministrator kann diese Einstellung ändern. Die Deaktivierung dieser Funktion führt zum Verlust des Zugriffs auf Funktionen, die das Abrufen von Wissen aus anderen Regionen erfordern AWS Transform . Dies kann zu weniger genauen Antworten führen.

So deaktivieren Sie regionsübergreifende Anrufe von AWS Transform:

1. Navigieren Sie bei der ersten Einrichtung AWS Transform zur Seite Erste Schritte und schließen Sie die Konfiguration ab. Für eine bestehende AWS Transform Konfiguration navigieren Sie zur Seite Einstellungen.
2. Schalten Sie die Option Regionsübergreifende Anrufe zur Beantwortung allgemeiner AWS Fragen aktivieren bis zur ausgeschalteten Position um.

AWS Transform für regionsübergreifende Windows-Inferenz

Die folgende Tabelle zeigt die Quellregionen, von denen aus Sie das Inferenzprofil aufrufen können sowie die Zielregionen, an die Anfragen weitergeleitet werden können:

Quellregion	Zielregionen ableiten
USA Ost (Nord-Virginia): (us-east-1)	USA Ost (Nord-Virginia): (us-east-1) USA Ost (Ohio): (us-east-2) USA West (Oregon): (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (Paris) (eu-west-3)
Asien-Pazifik (Tokyo) (ap-northeast-1)	Asien-Pazifik (Tokyo) (ap-northeast-1) Asien-Pazifik (Osaka) (ap-northeast-3)
Asien-Pazifik (Sydney): (ap-southeast-2)	Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)
Asien-Pazifik (Seoul): (ap-northeast-2)	Alle Handelsregionen
Asien-Pazifik (Mumbai): (ap-south-1)	Alle Handelsregionen
Kanada (Zentral): (ca-central-1)	Alle Handelsregionen

AWS Transform für regionenübergreifende Rückschlüsse auf Migrationen

Die folgende Tabelle zeigt die Quellregionen, von denen aus Sie das Inferenzprofil aufrufen können sowie die Zielregionen, an die Anfragen weitergeleitet werden können:

Quellregion	Inferenz: Zielregionen
USA Ost (Nord-Virginia): (us-east-1)	Alle Handelsregionen
Europa (Frankfurt) (eu-central-1)	Alle Handelsregionen
Europa (London) (eu-west-2)	Alle Handelsregionen
Asien-Pazifik (Tokyo) (ap-northeast-1)	Asien-Pazifik (Tokyo) (ap-northeast-1) Asien-Pazifik (Osaka) (ap-northeast-3)
Asien-Pazifik (Sydney): (ap-southeast-2)	Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)
Asien-Pazifik (Seoul): (ap-northeast-2)	Alle Handelsregionen
Asien-Pazifik (Mumbai): (ap-south-1)	Alle Handelsregionen
Kanada (Zentral): (ca-central-1)	Alle Handelsregionen

AWS Transform für regionsübergreifende Mainframe-Inferenz

AWS Transform für Mainframe verwendet Amazon Bedrock Geographic Cross-Region Inference. Das bedeutet, dass einige Ihrer Anrufe möglicherweise an Orte AWS-Regionen außerhalb Ihrer Quellregion weitergeleitet werden. Die folgende Tabelle zeigt die Quellregionen, von denen aus Sie das Inferenzprofil aufrufen können sowie die Zielregionen, an die Anfragen weitergeleitet werden können:

Quellregion	Zielregionen ableiten
USA Ost (Nord-Virginia): (us-east-1)	USA Ost (Nord-Virginia): (us-east-1) USA Ost (Ohio): (us-east-2) USA West (Oregon): (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1)

Quellregion	Zielregionen ableiten
	Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (Paris) (eu-west-3)
Europa (London) (eu-west-2)	Europa (Frankfurt) (eu-central-1) Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (London) (eu-west-2) Europa (Paris) (eu-west-3)
Asien-Pazifik (Tokyo) (ap-northeast-1)	Asien-Pazifik (Tokyo) (ap-northeast-1) Asien-Pazifik (Osaka) (ap-northeast-3)
Asien-Pazifik (Sydney): (ap-southeast-2)	Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)
Asien-Pazifik (Seoul): (ap-northeast-2)	Alle Handelsregionen
Asien-Pazifik (Mumbai): (ap-south-1)	Alle Handelsregionen

Quellregion	Zielregionen ableiten
Kanada (Zentral): (ca-central-1)	Kanada (Zentral): (ca-central-1) USA Ost (Nord-Virginia): (us-east-1) USA Ost (Ohio): (us-east-2) USA West (Oregon): (us-west-2)
Südamerika (São Paulo) (sa-east-1)	Alle Handelsregionen

AWS Transform Benutzerdefiniert

AWS Transform custom verwendet die geografische regionsübergreifende Inferenz von Amazon Bedrock. Das bedeutet, dass einige Ihrer Anrufe möglicherweise an Orte AWS-Regionen außerhalb Ihrer Quellregion weitergeleitet werden. Die folgende Tabelle zeigt die Quellregionen, von denen aus Sie das Inferenzprofil aufrufen können sowie die Zielregionen, an die Anfragen weitergeleitet werden können:

Quellregion	Zielregionen ableiten
USA Ost (Nord-Virginia): (us-east-1)	USA Ost (Nord-Virginia): (us-east-1) USA Ost (Ohio): (us-east-2) USA West (Oregon): (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (Paris) (eu-west-3)

Quellregion	Zielregionen ableiten
Europa (London) (eu-west-2)	Europa (Frankfurt) (eu-central-1) Europa (Stockholm) (eu-north-1) Europa (Mailand) (eu-south-1) Europa (Spanien) (eu-south-2) Europa (Irland) (eu-west-1) Europa (London) (eu-west-2) Europa (Paris) (eu-west-3)
Asien-Pazifik (Tokyo) (ap-northeast-1)	Alle Handelsregionen
Asien-Pazifik (Sydney): (ap-southeast-2)	Asien-Pazifik (Sydney): (ap-southeast-2) Asien-Pazifik (Melbourne) (ap-southeast-4)
Asien-Pazifik (Seoul): (ap-northeast-2)	Alle Handelsregionen
Asien-Pazifik (Mumbai): (ap-south-1)	Alle Handelsregionen
Kanada (Zentral): (ca-central-1)	Kanada (Zentral): (ca-central-1) USA Ost (Nord-Virginia): (us-east-1) USA Ost (Ohio): (us-east-2) USA West (Oregon): (us-west-2)

Datenverschlüsselung in AWS Transform

Dieses Thema enthält spezifische AWS Transform Informationen zur Verschlüsselung bei der Übertragung und Verschlüsselung im Ruhezustand.

AWS Transform bietet standardmäßig Verschlüsselung zum Schutz vertraulicher Kundendaten im Speicher durch Verschlüsselung mit AWS eigenen Schlüsseln.

Verschlüsselungstypen

Verschlüsselung während der Übertragung

Die Kommunikation zwischen Kunden und zwischen AWS Transform und zwischen AWS Transform und ihren nachgelagerten Abhängigkeiten wird durch Verbindungen mit TLS 1.2 oder höher geschützt.

Important

Wenn Sie [ein Discovery-Konto Connect](#), erstellt AWS Transform in Ihrem Namen einen Amazon S3 S3-Bucket in diesem Konto. Dieser Bucket SecureTransport ist standardmäßig nicht aktiviert. Wenn Sie möchten, dass die Bucket-Richtlinie sicheren Transport beinhaltet, müssen Sie die Richtlinie aktualisieren. Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden für Amazon S3](#).

Verschlüsselung im Ruhezustand

AWS Transform speichert Daten im Ruhezustand mithilfe von Amazon DynamoDB und Amazon Simple Storage Service (Amazon S3). Die Daten im Ruhezustand werden standardmäßig mithilfe von AWS Verschlüsselungslösungen verschlüsselt. AWS Transform verschlüsselt Ihre Daten mit Verschlüsselung unter Verwendung AWS eigener Schlüssel von AWS Key Management Service (AWS KMS). Sie müssen keine Maßnahmen ergreifen, um die AWS verwalteten Schlüssel, die Ihre Daten verschlüsseln, zu schützen. Weitere Informationen finden Sie unter [AWS -eigene Schlüssel](#) im AWS Key Management Service -Entwicklerhandbuch.

Datentyp	AWS-eigene Schlüssel verschlüsselung	Vom Kunden verwaltete Schlüsselverschlüsselung (optional)
Bucket-Daten des Kunden	Aktiviert	Aktiviert
Kundeneingaben und -ausgaben wie Code und Dokumentation, die in einem Amazon S3 S3-Bucket gespeichert sind		

Datentyp	AWS-eigene Schlüssel verschlüsselung	Vom Kunden verwaltete Schlüsselverschlüsselung (optional)
Shop für Artefakte Zwischenartefakte als Teil der Codetransformation, gespeichert in einem S3- Bucket	Aktiviert	Aktiviert
Zielsetzung der Job Die Absicht des Kunden für den Auftrag, der in einem Amazon S3 S3-Bucket gespeichert ist	Aktiviert	Aktiviert
Chat-Nachrichten Nachrichten zwischen dem Kunden und in einem Amazon S3 S3-Bucket AWS Transform gespeichert	Aktiviert	Aktiviert
Chat-Wissensdatenbank Indexierte Daten, die für den Kundenchat relevant sind AWS Transform und in Amazon gespeichert OpenSearch und über AWS Bedrock verarbeitet werden	Aktiviert	Aktiviert

Hinweis: Der Kunde kann seinen eigenen Customer Managed Key (CMK) registrieren, der für die Verschlüsselung aller oben genannten Datentypen verwendet wird.

Kundenverwaltete Schlüssel sind KMS-Schlüssel in Ihrem AWS Konto, die Sie erstellen, besitzen und verwalten, um den Zugriff auf Ihre Daten direkt zu kontrollieren, indem Sie den Zugriff auf den KMS-Schlüssel kontrollieren. Es werden nur symmetrische Schlüssel unterstützt. Informationen zum Erstellen Ihres eigenen KMS-Schlüssels finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, AWS Transform werden KMS-Zuschüsse verwendet, sodass autorisierte Benutzer, Rollen oder Anwendungen einen KMS-Schlüssel verwenden können. Wenn sich ein AWS Transform Administrator dafür entscheidet, während der Konfiguration einen vom Kunden verwalteten Schlüssel für die Verschlüsselung zu verwenden, wird ihm ein Zuschuss gewährt. Diese Berechtigung ermöglicht es dem Endbenutzer, den Verschlüsselungsschlüssel für die Datenverschlüsselung im Ruhezustand zu verwenden. Weitere Informationen zu Berechtigungen finden Sie unter [Berechtigungen in AWS KMS](#).

AWS Eigene Schlüssel (Standard)

Note

AWS eigene Schlüssel — AWS Transform verwendet diese Schlüssel standardmäßig, um persönlich identifizierbare Daten automatisch zu verschlüsseln. Sie können AWS eigene Schlüssel nicht einsehen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme zum Schutz der Schlüssel ändern, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie unter AWS Eigene Schlüssel im AWS Key Management Service Developer Guide.

Die standardmäßige Verschlüsselung von Daten im Ruhezustand trägt dazu bei, den betrieblichen Aufwand und die Komplexität zu reduzieren, die mit dem Schutz vertraulicher Daten verbunden sind. Gleichzeitig können Sie damit sichere Anwendungen erstellen, die strenge Verschlüsselungsvorschriften und gesetzliche Auflagen erfüllen.

Sie können diese Verschlüsselungsebene zwar nicht deaktivieren oder einen anderen Verschlüsselungstyp auswählen, aber Sie können eine zweite Verschlüsselungsebene über den vorhandenen AWS eigenen Verschlüsselungsschlüssel hinzufügen, indem Sie bei der Erstellung Ihrer Transformation einen vom Kunden verwalteten Schlüssel auswählen:

Vom Kunden verwaltete Schlüssel (optional)

Vom Kunden verwaltete Schlüssel — AWS Transform unterstützt die Verwendung eines symmetrischen, vom Kunden verwalteten Schlüssels, den Sie selbst erstellen, besitzen und verwalten, um eine zweite Verschlüsselungsebene gegenüber der bestehenden Verschlüsselung mit AWS eigenen Schlüsseln hinzuzufügen. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von -Tags
- Erstellen von Schlüsselaliasen
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von -Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen
- Weitere Informationen finden Sie unter [Kundenseitig verwalteten Schlüssel](#) im Entwicklerhandbuch zum AWS Key Management Service.

Note

AWS Transform aktiviert automatisch die Verschlüsselung im Ruhezustand mithilfe AWS eigener Schlüssel, um personenbezogene Daten kostenlos zu schützen. Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter [AWS Key Management Service Preisgestaltung](#).

Weitere Informationen zu AWS KMS finden Sie unter [Was ist AWS Key Management Service?](#)

Wie AWS Transform verwendet Zuschüsse in AWS Key Management Service

AWS Transform erfordert einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn Sie einen [Ressourcennamen] erstellen, der mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, AWS Transform erstellt in Ihrem Namen einen Zuschuss, indem Sie eine CreateGrant Anfrage an den AWS Key Management Service. Grants in AWS Key Management Service werden verwendet, um AWS Transform Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

AWS Transform setzt voraus, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwendet:

- Senden Sie [KMS-API] -Anfragen an, um AWS KMS zu überprüfen, ob die symmetrische, vom Kunden verwaltete KMS-Schlüssel-ID, die Sie bei der Erstellung von [Ressourcenname] eingegeben haben, gültig ist.
- Senden Sie [KMS-API] -Anfragen an, AWS KMS um Datenschlüssel zu generieren, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.
- Senden Sie [KMS-API] -Anfragen an AWS KMS, um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zur Verschlüsselung Ihrer Daten verwendet werden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, können Sie auf AWS Transform keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, [Ressourcenname] von einem verschlüsselten [Ressourcennamen] abzurufen, der nicht darauf zugreifen kann, würde der Vorgang einen AccessDeniedException Fehler zurückgeben.

Erstellen eines kundenseitig verwalteten Schlüssels

Sie können mithilfe der AWS Management Console oder der AWS Key Management Service APIs einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen.

Um einen symmetrischen, vom Kunden verwalteten Schlüssel zu erstellen, folgen Sie den Schritten unter [Erstellen eines symmetrischen kundenverwalteten Schlüssels im AWS Key Management Service Entwicklerhandbuch](#).

Um Ihren vom Kunden verwalteten Schlüssel mit Ihren AWS Transform Ressourcen zu verwenden, müssen die folgenden API-Operationen in der Schlüsselrichtlinie zulässig sein:

kms: CreateGrant — Fügt einem vom Kunden verwalteten Schlüssel einen Zuschuss hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der den Zugriff für Grant-Operationen AWS

Transform erfordert. Weitere Informationen zum [Verwenden von Zuweisungen](#) finden Sie im Entwicklerhandbuch für AWS Key Management Service .

Auf diese Weise können AWS Transform Sie Folgendes tun:

- Rufen Sie [KMS-API ([GenerateDataKeyWithoutPlainText/GenerateDatakey](#))] auf, um einen verschlüsselten Datenschlüssel zu generieren und zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.
- Rufen Sie [KMS API ([Decrypt](#))] auf, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- Einen Prinzipal für die Außerbetriebnahme einrichten, damit der Service in den Status [RetireGrant](#) wechseln kann.
- [kms: DescribeKey](#) — Stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, damit [Service Name] den Schlüssel validieren kann.

Verschlüsselung für die SQL-Modernisierung

Während des [SQL Server-Modernisierungsprozesses](#) werden Ressourcen in Ihrem Konto AWS Transform erstellt, z. B. EC2-Instances, ECS-Cluster, ECR-Images und S3-Objekte. Sie haben die Möglichkeit, einen vom Kunden verwalteten Schlüssel zur Verschlüsselung der Daten in Ihrem Konto bereitzustellen. Sie müssen Ihren KMS-Schlüssel mit dem Schlüssel CreatedFor und dem Wert awsTransform kennzeichnen. In dieser Beispielrichtlinie sind die Mindestberechtigungen aufgeführt, die in Ihrer Schlüsselrichtlinie erforderlich sind, wenn Sie keine Standardschlüsselrichtlinie haben. Wenn Sie über eine Standard-Schlüsselrichtlinie verfügen, müssen Sie den KMS-Schlüssel zusätzlich zu Ihrer Standard-Schlüsselrichtlinie trotzdem manuell aktualisieren, damit ECS Ihren Schlüssel verwenden kann.

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
```



```

    "StringLike": {
      "kms:ViaService": "s3.*.amazonaws.com",
      "kms:EncryptionContext:aws-transform": "*"
    },
    "ArnLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "ec2.*.amazonaws.com"
      },
      "ArnLike": {
        "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "ec2.*.amazonaws.com",
          "ecr.*.amazonaws.com"
        ]
      }
    }
  },

```

```

    "Bool": {
      "kms:GrantIsForAWSResource": "true"
    },
    "ArnLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "fargate.amazonaws.com"
    },
    "Action": "kms:GenerateDataKeyWithoutPlaintext",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "fargate.amazonaws.com"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": "Decrypt"
      }
    }
  }
]

```

Verschlüsselung für die Datenbankmigration

AWS Transform Verwendet während des Datenbankmigrationsprozesses den AWS Database Migration Service (DMS), um Ihre Datenbankdaten zu migrieren. Sie können optional einen vom

Kunden verwalteten Schlüssel bereitstellen, um Ihre Datenbankdaten während der Migration zu verschlüsseln.

Die folgende Richtlinie enthält drei Aussagen. Die erste Anweisung gewährt Root-Kontoberechtigungen für den AWS KMS Schlüssel. Die zweite Anweisung ermöglicht es der Connector-Rolle, den Schlüssel während der Erkennung zu überprüfen. Die dritte Anweisung ermöglicht es der Connector-Rolle, den Schlüssel für DMS-Operationen zu verwenden.

```
"Statement": [
  {
    "Sid": "Enable IAM User Permissions",
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
    "Action": "kms:*",
    "Resource": "*"
  },
  {
    "Sid": "Allow connector role to validate key during discovery",
    "Effect": "Allow",
    "Principal": { "AWS": "connector-role-arn" },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "Allow connector role to use key via DMS",
    "Effect": "Allow",
    "Principal": { "AWS": "connector-role-arn" },
    "Action": [
      "kms:CreateGrant",
      "kms:Decrypt",
      "kms:DescribeKey",
      "kms:Encrypt",
      "kms:GenerateDataKey*",
      "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "dms.us-east-1.amazonaws.com"
      }
    }
  }
]
```

]

Verwenden von vom Kunden verwalteten KMS-Schlüsseln

Nach der Erstellung eines vom Kunden verwalteten KMS-Schlüssels muss ein AWS Transform Administrator den Schlüssel in der AWS Transform Konsole angeben, um ihn zum Verschlüsseln von Daten zu verwenden.

Um einen vom Kunden verwalteten Schlüssel zum Verschlüsseln von Daten einzurichten AWS Transform, benötigen Administratoren Nutzungsberechtigungen. AWS KMS

Um Funktionen nutzen zu können, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind, benötigen Benutzer Zugriffsberechtigungen für den AWS Transform Zugriff auf den vom Kunden verwalteten Schlüssel.

Wenn Ihnen bei der Verwendung ein Fehler im Zusammenhang mit KMS-Zuschüssen angezeigt wird AWS Transform, müssen Sie wahrscheinlich Ihre Berechtigungen aktualisieren, um Zuschüsse erstellen AWS Transform zu können. Um die benötigten Berechtigungen automatisch zu konfigurieren, rufen Sie die AWS Transform Konsole auf und wählen Sie im Banner oben auf der Seite die Option Berechtigungen aktualisieren aus. Um die Erstellung von Zuschüssen AWS Transform zu ermöglichen, müssen Sie die Berechtigungen auf der AWS Transform Konsoleseite aktualisieren.

Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf AWS Transform Zugriff auf vom Kunden verwaltete Schlüssel

Das folgende Beispiel für eine Richtlinienerklärung gewährt Benutzern Berechtigungen für den Zugriff auf Funktionen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt wurden, indem der AWS Transform Zugriff auf den Schlüssel gewährt wird. Diese Richtlinie muss verwendet werden, AWS Transform wenn ein Administrator einen vom Kunden verwalteten Schlüssel für die Verschlüsselung eingerichtet hat.

Note

Diese Informationen gelten nicht für den Workflow zur Bereitstellung der SQL Server-Modernisierung mithilfe von CMK.

"Statement": [

```
{
  "Sid": "QKMSDecryptGenerateDataKeyPermissions",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:ReEncryptFrom",
    "kms:ReEncryptTo"
  ],
  "Resource": [
    "arn:aws:kms:arn:aws::111122223333:key/[[key_id]]"
  ],
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "q.us-east-1.amazonaws.com"
      ]
    }
  }
}
```

AWS Transform Verbesserung des Service

Um die relevantesten Informationen AWS Transform bereitzustellen, können wir bestimmte Inhalte AWS Transform, wie z. B. von Ihnen gestellte Fragen AWS Transform und deren Antworten, zur Serviceverbesserung verwenden. Auf dieser Seite wird erklärt, welche Inhalte wir verwenden und wie Sie sich abmelden können.

AWS Transform Inhalte, die zur Serviceverbesserung verwendet werden

Wir können bestimmte Inhalte von AWS Transform zur Verbesserung des Dienstes verwenden. AWS Transform können diese Inhalte beispielsweise verwenden, um bessere Antworten auf häufig gestellte Fragen zu geben, AWS Transform betriebliche Probleme zu beheben, Fehler zu beheben oder Modelle zu schulen.

Zu den Inhalten, die zur Serviceverbesserung verwendet werden AWS können, gehören beispielsweise Ihre Fragen, die Antworten AWS Transform und der generierte Code. AWS Transform

So melden Sie sich ab

Wie Sie die AWS Transform Nutzung von Inhalten zur Serviceverbesserung ablehnen, hängt von der Umgebung ab, in der Sie sie verwenden AWS Transform.

Informationen zur AWS Transform Konfiguration einer Opt-Out-Richtlinie für KI-Dienste finden Sie unter AWS Organizations. Weitere Informationen finden Sie unter [Opt-Out-Richtlinien für KI-Services](#) im Benutzerhandbuch für AWS Organizations .

Gehen Sie wie folgt vor, um das Teilen Ihrer Inhalte in der Visual Studio IDE zu deaktivieren.

Gehen Sie zu Tools -> Optionen -> AWS Toolkit -> Amazon Q

Schalten Sie Amazon-Q-Inhalte teilen mit AWS auf Wahr oder Falsch um.

Gehen Sie wie folgt vor, um die gemeinsame Nutzung Ihrer Telemetriedaten im AWS Toolkit für Visual Studio zu deaktivieren:

1. Wählen Sie unter Tools die Optionen aus.
2. Wählen Sie im Bereich Optionen AWS Toolkit und dann Allgemein aus.
3. Deaktivieren Sie die Option AWS Toolkit erlauben, Nutzungsinformationen zu sammeln.

Identitäts- und Zugriffsmanagement für AWS Transformieren

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Transform-Ressourcen zu verwenden AWS . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Transform funktioniert mit IAM](#)
- [Identity-based Richtlinienbeispiele für AWS Transformieren](#)
- [Fehlerbehebung AWS Transformieren Sie Identität und Zugriff](#)

- [Verwenden von serviceverknüpften Rollen für AWS Transform](#)
- [AWS verwaltete Richtlinien für AWS Transformieren](#)
- [AWS Referenz zu Transformationsberechtigungen](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe [Fehlerbehebung AWS Transformieren Sie Identität und Zugriff](#)).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe [Wie AWS Transform funktioniert mit IAM](#)).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe [Identity-based Richtlinienbeispiele für AWS Transformieren](#)).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter [So melden Sie sich bei Ihrem AWS-Konto an](#) im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter [AWS Signature Version 4 for API requests](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der

Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Tasks that require root user credentials](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern 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.

Eine [IAM-Gruppe](#) spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie [von einer Benutzer- zu einer IAM-Rolle \(Konsole\) wechseln](#) AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter [Methoden, um eine Rolle zu übernehmen](#) im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) 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 definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcen und unter welchen Bedingungen durchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter [Choose between managed policies and inline policies](#) im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#).

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im -IAM-Benutzerhandbuch.
- **Service-Kontrollrichtlinien (SCPs)** – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.
- **Ressourcen-Kontrollrichtlinien (RCPs)** – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter [Ressourcen-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter [Bewertungslogik für Richtlinien](#) im IAM-Benutzerhandbuch.

Wie AWS Transform funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AWS Transform zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit Transform verfügbar sind. AWS

IAM-Feature	AWS Unterstützung für Transform
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein

IAM-Feature	AWS Unterstützung für Transform
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-linked Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Transform und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identity-based Richtlinien für AWS Transformieren

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. 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 [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

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. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Identity-based Richtlinienbeispiele für AWS Transformieren

Beispiele für identitätsbasierte AWS Transform-Richtlinien finden Sie unter [Identity-based Richtlinienbeispiele für AWS Transformieren](#)

Resource-based Richtlinien innerhalb AWS Transformieren

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. 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 gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Transformieren

Unterstützt Richtlinienaktionen: Ja

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. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS Transform-Aktionen finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform](#) in der Serviceautorisierungsreferenz.

Eine Liste der Aktionen für AWS Transform custom finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform custom](#) in der Serviceautorisierungsreferenz.

Richtlinienaktionen in AWS Transform verwenden vor der Aktion das folgende Präfix:

```
transform
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
    "transform:action1",  
    "transform:action2"  
]
```

Beispiele für identitätsbasierte AWS Transform-Richtlinien finden Sie unter [Identity-based Richtlinienbeispiele für AWS Transformieren](#)

Politische Ressourcen für AWS Transformieren

Unterstützt Richtlinienressourcen: Ja

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. Als Best Practice geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS Transform-Ressourcentypen und ihrer ARNs sowie die Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform](#) in der Serviceautorisierungsreferenz.

Eine Liste der Ressourcentypen und ihrer ARNs sowie die Aktionen, mit denen Sie den ARN jeder Ressource für AWS Transform custom angeben können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform custom](#) in der Service Authorization Reference.

Beispiele für identitätsbasierte AWS Transform-Richtlinien finden Sie unter. [Identity-based Richtlinienbeispiele für AWS Transformieren](#)

Bedingungsschlüssel für Richtlinien für AWS Transformieren

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der AWS Transform-Bedingungsschlüssel und die Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform](#) in der Serviceautorisierungsreferenz.

Eine Liste mit Bedingungsschlüsseln und den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel für AWS Transform custom verwenden können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform custom](#) in der Service Authorization Reference.

Beispiele für identitätsbasierte AWS Transform-Richtlinien finden Sie unter. [Identity-based Richtlinienbeispiele für AWS Transformieren](#)

ACLs in AWS Transformieren

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Transformieren

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Attribute-based Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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 Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Definieren von Berechtigungen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS Transformieren

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Anmeldeinformationen in IAM](#) und [AWS-Services , die mit IAM funktionieren](#) im IAM-Benutzerhandbuch.

Cross-service Hauptberechtigungen für AWS Transformieren

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für AWS Transformieren

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern

und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

 Warning

Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Transform-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS Transform eine Anleitung dazu bietet.

Service-linked Rollen für AWS Transformieren

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen AWS Transform-Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS Transform](#).

Identity-based Richtlinienbeispiele für AWS Transformieren

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS Transform-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien \(Konsole\)](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS Transform definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transform](#) in der Referenz zur Serviceautorisierung.

Themen

- [Best Practices für Richtlinien](#)
- [Verwendung der AWS Transformieren Sie die Konsole](#)

- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Erlauben Sie Administratoren, eine Connectoranfrage vom Konto mit anzunehmen AWS Transformieren](#)
- [Erlauben Sie Administratoren, bestehende IAM Identity Center-Benutzer zuzuweisen und neue IAM Identity Center-Benutzer zu erstellen, denen diese zugewiesen werden können AWS Transformieren](#)
- [Erlauben Sie Administratoren die Aktivierung AWS Transformieren](#)
- [Erlauben Sie Benutzern den Zugriff AWS Transformieren Sie mit IAM-Anmeldeinformationen](#)

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand AWS Transform-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn du identitätsbasierte Richtlinien erstellst oder bearbeitest, befolge diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto 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 [Von AWS verwaltete Richtlinien](#) oder [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#) 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 für einen

bestimmten Zweck verwendet werden AWS-Service, z. 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 mit 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 System erfordert AWS-Konto, 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 [Sicherer API-Zugriff mit MFA](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Best Practices für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwendung der AWS Transformieren Sie die Konsole

Um auf die AWS Transform-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Transform-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für 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 API AWS CLI oder AWS .

```
{
  "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": "*"
    }
  ]
}
```

Erlauben Sie Administratoren, eine Connectoranfrage vom Konto mit anzunehmen

AWS Transformieren

JSON

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

```

    {
      "Effect": "Allow",
      "Action": [
        "transform:GetConnector",
        "transform:AssociateConnectorResource",
        "transform:RejectConnector"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/service-role/
AWSTransform-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "arn:aws:iam::111122223333:policy/service-role/
AWSTransform-*"
    }
  ]
}

```

Erlauben Sie Administratoren, bestehende IAM Identity Center-Benutzer zuzuweisen und neue IAM Identity Center-Benutzer zu erstellen, denen diese zugewiesen werden können AWS Transformieren

Die folgende Richtlinie gewährt die Berechtigungen, die ein Administrator benötigt, um IAM Identity Center-Benutzer und -Gruppen in der AWS Transform-Konsole zu verwalten. Mit dieser Richtlinie kann ein Administrator Benutzer und Gruppen zuweisen und entfernen, Anzeigenamen anzeigen, neue IAM Identity Center-Benutzer erstellen, Anwendungszuweisungen verwalten und Einstellungen für Anwendungssitzungen konfigurieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOApplicationAssignments",
      "Effect": "Allow",
      "Action": [
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:ListInstances",
        "sso:DescribeInstance",
        "sso:ListDirectoryAssociations",
        "sso:GetApplicationGrant",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationSessionConfiguration",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSODirectoryCreateUser",
      "Effect": "Allow",
      "Action": [
        "sso-directory:CreateUser"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IdentityStoreAccess",
      "Effect": "Allow",
      "Action": [
```

```

        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListUsers",
        "identitystore:ListGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowKmsAccessViaIdentityCenter",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "kms:EncryptionContext:aws:sso:instance-arn": "arn*:sso:::instance/*"
        },
        "StringLike": {
            "kms:ViaService": "sso.*.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowKmsAccessViaIdentityStore",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn*:identitystore:::identitystore/*"
        },
        "StringLike": {
            "kms:ViaService": "identitystore.*.amazonaws.com"
        }
    }
}
]
}

```

Erlauben Sie Administratoren die Aktivierung AWS Transformieren

Die folgende Richtlinie gewährt die Berechtigungen, die ein Administrator benötigt, um AWS Transform über die AWS Konsole zu aktivieren und zu verwalten. Dazu gehören die Verwaltung von Profilen, die Konfiguration von Agenten und die Verwaltung von Connectoren. Diese Richtlinie richtet sich nur an Administratoren und sollte auf vertrauenswürdige Prinzipale in Ihrem Konto beschränkt sein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOEnableTransform",
      "Effect": "Allow",
      "Action": [
        "sso:ListInstances",
        "sso:CreateInstance",
        "sso:CreateApplication",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:ListApplications",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:PutApplicationAccessScope",
        "sso:DescribeApplication",
        "sso>DeleteApplication",
        "sso:UpdateApplication",
        "sso:DescribeRegisteredRegions",
        "sso:GetSSOStatus"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSODirectoryActions",
      "Effect": "Allow",
      "Action": [
        "sso-directory:GetUserPoolInfo",
        "sso-directory:DescribeUsers",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso-directory:DescribeDirectory"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "KMSListAliases",
    "Effect": "Allow",
    "Action": [
      "kms:ListAliases"
    ],
    "Resource": "*"
  },
  {
    "Sid": "KMSActions",
    "Effect": "Allow",
    "Action": [
      "kms:CreateGrant",
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:GenerateDataKey*",
      "kms:RetireGrant",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "transform.*.amazonaws.com"
      }
    }
  },
  {
    "Sid": "IAMServiceLinkedRole",
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource": [
      "arn:*:iam::*:role/aws-service-role/transform.amazonaws.com/
AWSServiceRoleForAWSTransform"
    ]
  },
  {
    "Sid": "TransformConsoleActions",
    "Effect": "Allow",
    "Action": [

```



```

        "transform:GetAccountSettings",
        "transform:UpdateAccountSettings",
        "transform:CreateProfile",
        "transform:UpdateProfile",
        "transform:DeleteProfile",
        "transform:ListProfiles",
        "transform:GetConnector",
        "transform:ListConnectors",
        "transform:DeleteConnector",
        "transform:AssociateConnectorResource",
        "transform:RejectConnector",
        "transform:ListAgents",
        "transform:GetAgent",
        "transform:GetAgentRuntimeConfiguration",
        "transform:PutAgentRuntimeConfiguration",
        "transform:UpdateAgentAccess",
        "transform:TagResource",
        "transform:UntagResource",
        "transform:ListTagsForResource",
        "transform:GetWebAppUrl"
    ],
    "Resource": "*"
}
]
}

```

Erlauben Sie Benutzern den Zugriff AWS Transformieren Sie mit IAM-Anmeldeinformationen

Die folgende Richtlinie gewährt einem IAM-Prinzipal mithilfe von IAM-Anmeldeinformationen Zugriff auf die AWS Transform-Webanwendung und die APIs. Diese Richtlinie ist für den IAM-only Zugriff und für den IAM-Zugriff erforderlich, der zusammen mit einem Identitätsanbieter aktiviert wird.

Ersetzen Sie *regionaccount-id*, und *profile-id* durch Ihre Werte. Sie finden die Profil-ID in der AWS Transform-Konsole unter Einstellungen.

```

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

```

```
    "Action": "transform:AccessTransformProfile",
    "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
  }
]
```

Um Zugriff auf alle Profile in einem Konto zu gewähren, verwenden Sie einen Platzhalter für die Profil-ID:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}
```

Note

Die `transform:AccessTransformProfile` Aktion gewährt nur Zugriff auf AWS Transform. Aktionen innerhalb von Workspaces werden durch AWS Transform-Workspace-Rollen (Administrator, Mitwirkender, Genehmiger Read-only) gesteuert, nicht durch IAM-Richtlinien. Workspace-Rollen bestimmen, was ein Benutzer tun kann, z. B. Jobs erstellen, Mitarbeiter verwalten oder Aufgaben genehmigen kann.

Fehlerbehebung AWS Transformieren Sie Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Transform und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Transformieren](#)

- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb meiner Umgebung zulassen AWS-Konto um auf meine zuzugreifen AWS Ressourcen transformieren](#)

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Transformieren

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *my-example-widget*-Ressource anzuzeigen, jedoch nicht über AWS Transform: *GetWidget*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS Transform: GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der AWS Transform: *GetWidget*-Aktion auf die *my-example-widget*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS Transform übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servic Rolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Transform auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servic Rolle 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 die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meiner Umgebung zulassen AWS-Konto um auf meine zuzugreifen AWS Ressourcen transformieren

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS Transform diese Funktionen unterstützt, finden Sie unter [Wie AWS Transform funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- 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.

Verwenden von serviceverknüpften Rollen für AWS Transform

AWS Transform verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Transform Service-linked Rollen sind von vordefiniert AWS Transform und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Verwenden von dienstbezogenen Rollen für AWS Transform

AWS Transform verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Transform Service-linked Rollen sind von vordefiniert AWS Transform und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Transform erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Transform definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Transform kann, sofern nicht anders definiert, nur ihre 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 AWS Transform Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter [AWS Dienste, die mit IAM funktionieren](#). Suchen Sie in der Rollenspalte nach den Diensten, für die Ja steht. Service-linked Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Service-linked Rollenberechtigungen für AWS Transform

AWS Transform verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen [AWSServiceRoleForAWSTransform](#)— Diese Service-Linked Rolle bietet AWS Transform die Möglichkeit, Nutzungsinformationen bereitzustellen.

Die AWSServiceRoleForAWSTransform dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `transform.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSServiceRoleForAWSTransform ermöglicht es AWS Transform , die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Cloudwatch: PutMetricData
 - Senden Sie benutzerdefinierte Metriken an CloudWatch für den Betrieb AWS Transform
 - Verfolgen Sie den Transformationsfortschritt, die Erfolgsquoten und die Leistungskennzahlen

- Ermöglichen Sie die Überwachung und Alarmierung von Transformationsworkflows
- sso: DescribeApplication
 - Details zu einer bestimmten Anwendung in Identity Center anzeigen
 - Rufen Sie Anwendungsmetadaten wie Name, Beschreibung, Status und Konfiguration ab
- sso: GetApplicationAssignmentConfiguration
 - Rufen Sie die Zuweisungskonfigurationseinstellungen für eine Anwendung ab
 - Erfahren Sie, wie users/groups sie konfiguriert sind, um der Anwendung zugewiesen zu werden
- sso: ListApplicationAssignmentsForPrincipal
 - Listet alle Anwendungen auf, die einem bestimmten Benutzer oder einer bestimmten Gruppe (Principal) zugewiesen sind
 - Sehen Sie sich an, auf welche Anwendungen eine bestimmte Identität Zugriff hat
- Ermöglicht die Entschlüsselung von KMS-encrypted Daten beim Zugriff über IAM Identity Center. Funktioniert nur, wenn der Verschlüsselungskontext einen gültigen ARN für die IAM Identity Center-Instanz enthält und über IAM Identity Center-Dienstendpunkte zugegriffen werden muss.
- Ermöglicht die Entschlüsselung von KMS-encrypted Daten beim Zugriff über Identity Store. Funktioniert nur, wenn der Verschlüsselungskontext einen gültigen Identity Store-ARN enthält und über Identity Store-Dienstendpunkte zugegriffen werden muss.
- Secretsmanager: GetSecretValue
 - Greifen Sie auf AWS Transform dienstbezogene Geheimnisse zu, die zum Speichern von Client-Geheimnissen für externe Identitätsanbieter verwendet werden
 - Ressource: arn:aws:secretsmanager:*:*:secret:transform-preprod! *
 - Bedingung: Muss Eigentum des Transform-Preprod-Dienstes sein und der Zugriff muss von demselben Konto aus erfolgen
- Unterstützung:CreateCase, Unterstützung:, Unterstützung:DescribeCases, Unterstützung:DescribeCommunications, Unterstützung: AddCommunicationToCase ResolveCase
 - Erstellen und verwalten Sie Premium-Supportanfragen über die AWS Transform Webanwendung
 - Falldetails und Mitteilungen anzeigen
 - Fügen Sie Mitteilungen hinzu und lösen Sie Supportfälle

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Service-linked Rollenberechtigungen](#).

Erstellen einer serviceverknüpften Rolle für AWS Transform

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Profil für AWS Transform in erstellen AWS Management Console, AWS Transform wird die serviceverknüpfte Rolle für Sie erstellt.

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 die Einstellungen aktualisieren, AWS Transform erstellt die dienstbezogene Rolle erneut für Sie.

Sie können auch die IAM-Konsole oder AWS CLI verwenden, um eine serviceverknüpfte Rolle mit dem `transform.amazonaws.com` Dienstnamen zu erstellen. Weitere Informationen finden Sie unter [Erstellen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für AWS Transform

AWS Transform erlaubt es Ihnen nicht, die `AWSServiceRoleForAWSTransform` serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften 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 AWS Transform

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn der AWS Transform Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForAWSTransform` dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für AWS Transform Serviceverknüpfte Rollen

AWS Transform unterstützt nicht die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Sie können die `AWSServiceRoleForAWSTransform` Rolle in den folgenden Regionen verwenden. Weitere Informationen erhalten Sie unter [AWS -Regionen und Endpunkte](#).

Name der Region	Regions-ID	Support in AWS Transform
USA Ost (Nord-Virginia)	us-east-1	Ja
Europa (Frankfurt)	eu-central-1	Ja

Verwenden von serviceverknüpften Rollen für AWS Benutzerdefiniert transformieren

AWS Transform Custom verwendet die angegebene dienstbezogene Rolle `AWSServiceRoleForAWSTransformCustom`, um in Ihrem Namen Metriken und Protokolle in Ihrem Konto zu veröffentlichen. Mit diesen Metriken können Sie die Anzahl der Transformationen, Latenzen und Statuscodes direkt in Ihren Dashboards überwachen. Protokolle bieten Einblick in Probleme, die bei Transformationen aufgetreten sind.

Diese [dienstbezogene Rolle](#) ist von AWS Transform Custom vordefiniert und umfasst nur die Berechtigungen, die der Dienst benötigt. Sie müssen keine Berechtigungen manuell hinzufügen, und die Rolle kann nur von AWS Transform Custom übernommen werden. Allgemeine Informationen zu serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen](#) im IAM-Benutzerhandbuch.

Service-linked Rollenberechtigungen für AWS Benutzerdefiniert transformieren

Die `AWSServiceRoleForAWSTransformCustom` dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `transform-custom.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AWSServiceRoleForAWSTransformCustom` ermöglicht es AWS Transform Custom, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- `cloudwatch:PutMetricData` auf allen AWS Ressourcen
 - Veröffentlichen Sie Betriebskennzahlen unter dem `AWS/TransformCustom` Namespace
 - Verfolgen Sie die Anzahl der Transformationen, Latenzen und Statuscodes
 - Über den Bedingungsschlüssel auf den `AWS/TransformCustom` Namespace beschränkt `cloudwatch:namespace`
- `logs:CreateLogGroup` und `logs:PutRetentionPolicy` der Protokollgruppe `/aws/TransformCustom`
 - Erstellen Sie die Protokollgruppe CloudWatch Logs für die Veröffentlichung von Transformationsprotokollen
 - Legen Sie Richtlinien zur Aufbewahrung von Protokollen für die Protokollgruppe fest
 - Gültig `aws:ResourceAccount` unter einer Bedingung, die `arn:aws:logs:*:*:log-group:/aws/TransformCustom` sicherstellt, dass der Zugriff nur innerhalb Ihres Kontos erfolgt
- `logs:CreateLogStream` und `logs:PutLogEvents` auf Protokollstreams innerhalb der `/aws/TransformCustom` Protokollgruppe
 - Erstellen Sie Protokollstreams und veröffentlichen Sie Protokollereignisse für Transformationsvorgänge
 - Gültig `aws:ResourceAccount` unter einer Bedingung, die `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*` sicherstellt, dass der Zugriff nur innerhalb Ihres Kontos erfolgt

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Service-linked Rollenberechtigungen](#).

Erstellen einer serviceverknüpften Rolle für AWS Benutzerdefiniert transformieren

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine Transformation mit der AWS Transform Custom CLI ausführen, erstellt AWS Transform Custom 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

Transformation mit der AWS Transform Custom CLI ausführen, erstellt AWS Transform Custom die serviceverknüpfte Rolle erneut für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem `AWSServiceRoleForAWSTransformCustomAnwendungsfall` zu erstellen. Erstellen Sie in der AWS CLI oder der AWS API eine dienstverknüpfte Rolle mit dem `transform-custom.amazonaws.com` Dienstnamen. Weitere Informationen finden Sie unter [Erstellen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für AWS Benutzerdefiniert transformieren

AWS Mit Transform Custom können Sie die `AWSServiceRoleForAWSTransformCustom` serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften 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 AWS Benutzerdefiniert transformieren

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

Die `AWSServiceRoleForAWSTransformCustom` serviceverknüpfte Rolle erstellt keine persistenten Ressourcen in Ihrem Konto. Sie können sie direkt löschen, ohne dass die Ressourcen bereinigt werden müssen.

Wenn Sie diese Rolle löschen und später eine Transformation mit der AWS Transform Custom CLI ausführen, wird die dienstverknüpfte Rolle automatisch neu erstellt.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die serviceverknüpfte Rolle zu löschen. `AWSServiceRoleForAWSTransformCustom` Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für AWS Transformieren Sie benutzerdefinierte dienstbezogene Rollen

AWS Transform Custom unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen AWS Transform Custom verfügbar ist. Eine Liste der unterstützten Regionen finden Sie unter [Unterstützte Regionen](#).

AWS verwaltete Richtlinien für AWS Transformieren

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 eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS Transformieren Sie Updates für AWS Verwaltete Richtlinien

Hier finden Sie Details zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Transform seit dem 1. März 2021.

Änderungen	Beschreibung	Date
AWSTransformInfrastructureExecutorAccessBatch – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die die Berechtigungen gewährt, die für die Ausführung von Assessments und Transformationen von AWS Transform Continuous Modernization mithilfe von AWS Batch erforderlich sind. Dazu gehören das Hochladen von Quellcode,	20. Juli 2026

Änderungen	Beschreibung	Date
	das Abrufen von Ergebnissen, die Überwachung des Batch-Jobstatus, das Lesen von Protokollen und die Verwaltung von Transformationsplänen.	
AWSTransformInfrastructureExecutorAccessEC2 – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die die Berechtigungen gewährt, die für die Durchführung von AWS Transform Continuous Modernization Assessments und Transformationen mit Amazon EC2 erforderlich sind, einschließlich des Hochladens von Quellcode, des Abrufs von Ergebnissen, der Überwachung des Jobstatus und der Verwaltung von Transformationsplänen.	20. Juli 2026
AWSTransformSecurityAgentExecutorAccess – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die AWS Transform Continuous Modernization die erforderlichen Berechtigungen gewährt, um den AWS Security Agent-Dienst für automatische Sicherheitsprüfungen und -behebungen, einschließlich des Hochladens von Scanartefakten und des Abrufs von Ergebnissen, aufzurufen.	30. Juni 2026

Änderungen	Beschreibung	Date
AWSServiceRoleForAWSTransformCustom – Richtlinie aktualisieren	Es wurden CloudWatch Logs-Berechtigungen hinzugefügt, damit AWS Transform custom Logs in der /aws/ TransformCustom Protokollgruppe in Ihrem Konto veröffentlichen kann.	5. Mai 2026
AWSTransformCustomExecuteTransformations – Richtlinie aktualisieren	Es wurde die Berechtigung hinzugefügt, die benutzerdefinierte serviceverknüpfte AWS Transform-Rolle (AWSServiceRoleForAWSTransformCustom) zu erstellen, um die Ausgabe von CloudWatch Kennzahlen an Kundenkonten zu ermöglichen.	27. April 2026
AWSTransformCustomManageTransformations – Richtlinie aktualisieren	Es wurde die Berechtigung hinzugefügt, die benutzerdefinierte serviceverknüpfte AWS Transform-Rolle (AWSServiceRoleForAWSTransformCustom) zu erstellen, um die Ausgabe von CloudWatch Kennzahlen an Kundenkonten zu ermöglichen.	27. April 2026

Änderungen	Beschreibung	Date
AWSTransformCustomFullAccess – Richtlinie aktualisieren	Es wurde die Berechtigung hinzugefügt, die benutzerdefinierte serviceverknüpfte AWS Transform-Rolle (AWSServiceRoleForAWSTransformCustom) zu erstellen, um die Ausgabe von CloudWatch Kennzahlen an Kundenkonten zu ermöglichen.	7. April 2026
AWSServiceRoleForAWSTransformCustom – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie für die benutzerdefinierte serviceverknüpfte AWS Transform-Rolle hinzugefügt. Diese Richtlinie ermöglicht es AWS Transform Custom, CloudWatch Metriken in Ihrem Konto zu veröffentlichen.	23. März 2026
DBModProvisioningAndMigration – Neue Richtlinie	Diese Richtlinie gewährt Funktionen zur Datenbank bereitstellung und Migration.	24. März 2026
DBModDiscoveryAndAssessment – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die umfassende Erkennung s- und Bewertungsfunktionen zur Datenbankmodernisierung bietet.	24. März 2026

Änderungen	Beschreibung	Date
AWSTransformCustomFullAccess – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die vollen Zugriff auf AWS Transform Custom bietet.	5. Dezember 2025
AWSTransformCustomExecuteTransformations – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die Zugriff auf die Ausführung von Transformationen in AWS Transform custom bietet.	5. Dezember 2025
AWSTransformCustomManageTransformations – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die Zugriff auf das Erstellen, Aktualisieren, Lesen und Löschen von Transformationsressourcen in AWS Transform custom sowie das Ausführen von Transformationen bietet.	5. Dezember 2025

Änderungen	Beschreibung	Date
AWSServiceRoleForAWSTransform – Richtlinie aktualisieren	Es wurden Berechtigungen für den Zugriff auf das mit dem AWS Transform-Service verknüpfte Geheimnis hinzugefügt, das zum Speichern des geheimen Client-Schlüssels für externe Identitätsanbieter verwendet wird. Es wurden Berechtigungen zum Erstellen eines Premium-Supportfalls über die AWS Transform-Web-App hinzugefügt.	1. Dezember 2025
AWSTransformApplicationECSDeploymentPolicy – Richtlinie aktualisieren	Es wurden IAM-Rolleninspektionsberechtigungen, die Erstellung von ECS-diensbezogenen Rollen und KMS-Berechtigungen für die Unterstützung der ECR-Verschlüsselung hinzugefügt.	22. November 2025
AWSTransformApplicationDeploymentPolicy – Richtlinie aktualisieren	EC2-Netzwerkberechtigungen, IAM-Rolleninspektionsberechtigungen, S3-Bucket-Listing-Berechtigungen und Unterstützung für KMS-Verschlüsselung für erweiterte Bereitstellungsfunktionen hinzugefügt.	22. November 2025
AWSServiceRoleForAWSTransform – Richtlinie aktualisieren	Unterstützung für vom Kunden verwaltete Schlüssel im IAM Identity Center hinzugefügt.	17. September 2025

Änderungen	Beschreibung	Date
AWSTransformApplicationDeploymentPolicy – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die es AWS Transform ermöglicht, transformierte.NET -Anwendungen bereitzustellen, indem Amazon EC2 EC2-Instances, CloudFormation Stacks und zugehörige Ressourcen erstellt und verwaltet werden.	28. August 2025
AWSServiceRoleForAWSTransform – Richtlinie aktualisieren	Eine neue Richtlinie wurde hinzugefügt.	15. Mai 2025

AWS verwaltete Richtlinie: AWSServiceRoleForAWSTransform

Diese Richtlinie ist der [AWSServiceRoleForAWSTransform](#) serviceverknüpften Rolle (SLR) zugeordnet.

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie [AWSServiceRoleForAWSTransform](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSServiceRoleForAWSTransformCustom

Diese Richtlinie ist der [AWSServiceRoleForAWSTransformCustom](#) serviceverknüpften Rolle (SLR) zugeordnet. Diese Rolle ermöglicht es AWS Transform Custom, in Ihrem CloudWatch Namen Metriken und Protokolle in Ihrem Konto zu veröffentlichen.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **Amazon CloudWatch** — Ermöglicht die Veröffentlichung von Metriken CloudWatch unter dem `AWS/TransformCustom` Namespace. Auf diese Weise können Sie die Anzahl der Transformationen, Latenzen und Statuscodes in Ihren CloudWatch Dashboards überwachen.
- **Amazon CloudWatch Logs** — Ermöglicht das Erstellen von Protokollgruppen und Protokollstreams, das Festlegen von Aufbewahrungsrichtlinien und das Veröffentlichen von Protokollereignissen in der `/aws/TransformCustom` Protokollgruppe. Dies bietet Einblick in Probleme, die bei Transformationen aufgetreten sind.

AWS verwaltete Richtlinie: `AWSTransformApplicationDeploymentPolicy`

Diese Richtlinie ermöglicht es AWS Transform, transformierte.NET-Anwendungen bereitzustellen, indem Amazon EC2 EC2-Instances, CloudFormation Stacks und zugehörige Ressourcen erstellt und verwaltet werden.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **CloudFormation**— Ermöglicht das Erstellen, Aktualisieren, Löschen und Beschreiben von CloudFormation Stacks, deren Namen mit `AWSTransform` beginnen. Stack-Operationen sind auf Ressourcen beschränkt, die mit `CreatedBy: awsTransform` gekennzeichnet sind, und auf dasselbe Konto beschränkt. AWS
- **Amazon EC2** — Ermöglicht die Beschreibung von VPCs, Subnetzen, Sicherheitsgruppen, Images, Instances, Routing-Tabellen und Internet-Gateways. Ermöglicht das Ausführen, Starten, Stoppen, Beenden und Ändern von EC2-Instances, jedoch nur, wenn sie aufgerufen werden. CloudFormation Die Tag-Erstellung ist auf bestimmte zulässige Tag-Schlüssel und nur während CloudFormation Operationen beschränkt.
- **AWS Identity and Access Management (IAM)** — Ermöglicht das Abrufen und Übergeben bestimmter IAM-Rollen für `AWSTransform`-Bereitstellungsinstanzen. Beinhaltet Berechtigungen zur Überprüfung von Rollenrichtlinien und Anhängen. Der Zugriff ist auf dasselbe AWS Konto beschränkt.
- **Amazon EC2 Systems Manager (SSM)** — Ermöglicht das Abrufen von Amazon AWS Linux-AMI-Parametern aus dem verwalteten Parameterspeicher und das Senden von Befehlen an Instances. `AWSTransform-tagged`
- **Amazon S3** — Ermöglicht die Verwaltung von Objekten in `AWSTransform`-Bereitstellungs-Buckets, einschließlich der Auflistung von Buckets und des Abrufs von Bucket-Standorten innerhalb desselben Kontos. AWS

- AWS Key Management Service (KMS) — Ermöglicht Verschlüsselungs- und Entschlüsselungsvorgänge mithilfe von KMS-Schlüsseln, die für AWSTransform gekennzeichnet sind, mit Einschränkungen bei der Nutzung von S3- und EC2-Services.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten durch Berechtigungen auf Ressourcenebene, tagbasierte Bedingungen, Einschränkungen der Nutzung von Diensten, Einschränkungen auf Kontoebene und explizite Ablehnungsbefehle `aws:CalledVia`, um unbefugte Tag-Änderungen außerhalb von Vorgängen zu verhindern. CloudFormation

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [AWSTransformApplicationDeploymentPolicy](#) AWS

AWS verwaltete Richtlinie: AWSTransformApplicationECSDeploymentPolicy

Diese Richtlinie ermöglicht es AWS Transform, transformierte Anwendungen in Amazon ECS bereitzustellen, indem ECS-Cluster, -Services, Aufgaben und zugehörige Ressourcen erstellt und verwaltet werden.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- CloudFormation— Ermöglicht das Erstellen, Aktualisieren, Löschen und Beschreiben von CloudFormation Stacks, deren Namen mit AWSTransform beginnen. Stack-Operationen sind auf Ressourcen beschränkt, die mit `CreatedBy: awsTransform` gekennzeichnet sind, und auf dasselbe Konto beschränkt. AWS
- Amazon ECS — Ermöglicht das Erstellen, Aktualisieren und Löschen von ECS-Clustern, -Services und Aufgabendefinitionen. Ermöglicht das Ausführen von Aufgaben, das Auflisten von Aufgaben und das Beschreiben des Aufgabenstatus. Alle Operationen sind auf Ressourcen beschränkt, deren Namen mit `awsTransform` beginnen und mit `CreatedBy: awsTransform` gekennzeichnet sind.
- AWS Identity and Access Management (IAM) — Ermöglicht das Abrufen und Weitergeben bestimmter IAM-Rollen für ECS-Aufgaben (und). `AWSTransform-Deploy-ECS-Task-Role` `AWSTransform-Deploy-ECS-Execution-Role` Beinhaltet Berechtigungen, um Rollenrichtlinien zu überprüfen und bei Bedarf die mit dem ECS-Dienst verknüpfte Rolle zu erstellen.

- Amazon CloudWatch Logs — Ermöglicht das Erstellen, Löschen und Verwalten von Protokollgruppen, deren Namen mit aws/ecs /awsTransform beginnen. Ermöglicht das Abrufen von Protokollereignissen zur Fehlerbehebung bei bereitgestellten Anwendungen.
- Amazon ECR — Ermöglicht die Erstellung von Container-Repositorys, deren Namen mit awstransform beginnen, zum Speichern von Anwendungscontainer-Images.
- AWS Key Management Service (KMS) — Ermöglicht die Erstellung von Zuschüssen und die Generierung von Datenschlüsseln für die ECR-Verschlüsselung, wenn vom Kunden verwaltete KMS-Schlüssel verwendet werden.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten durch Berechtigungen auf Ressourcenebene, tagbasierte Bedingungen und Einschränkungen auf Kontoebene, um sicherzustellen, dass der Betrieb auf Ressourcen innerhalb desselben Kontos beschränkt ist.

AWSTransform-managed AWS

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [AWSTransformApplicationECSDeploymentPolicy](#) AWS

AWS verwaltete Richtlinie: AWSTransformCustomFullAccess

Diese Richtlinie bietet vollen Zugriff auf AWS Transform custom.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- AWS Benutzerdefiniert transformieren — Ermöglicht alle Aktionen für alle benutzerdefinierten AWS Transform-Ressourcen. Dies bietet vollständigen administrativen Zugriff auf den Dienst.
- AWS Identity and Access Management (IAM) — Ermöglicht die Erstellung der benutzerdefinierten [serviceverknüpften AWS Transform-Rolle](#) (`AWSServiceRoleForAWSTransformCustom`). Diese Rolle ist erforderlich, damit AWS Transform custom CloudWatch Metriken und Protokolle an Ihr Konto sendet. Die Berechtigung ist so begrenzt, dass sie nur die Erstellung dieser speziellen dienstbezogenen Rolle erlaubt.

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie [AWSTransformCustomFullAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSTransformCustomExecuteTransformations

Diese Richtlinie bietet Zugriff auf die Ausführung von Transformationen in AWS Transform custom.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- AWS Benutzerdefiniert transformieren — Ermöglicht das Streamen von Konversationen, die Ausführung von Transformationen und die Verwaltung von Kampagnen. Beinhaltet Berechtigungen zum Abrufen von Kampagnendetails, zum Aktualisieren des Kampagnen-Repository-Status und zum Aktualisieren von Kampagnen.
- AWS Identity and Access Management (IAM) — Ermöglicht die Erstellung der benutzerdefinierten [serviceverknüpften AWS Transform-Rolle](#) (`AWSServiceRoleForAWSTransformCustom`). Diese Rolle ist erforderlich, damit AWS Transform custom CloudWatch Metriken und Protokolle an Ihr Konto sendet. Die Berechtigung ist so begrenzt, dass sie nur die Erstellung dieser speziellen dienstbezogenen Rolle erlaubt.

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie

[AWSTransformCustomExecuteTransformations](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSTransformCustomManageTransformations

Diese Richtlinie bietet Zugriff auf das Erstellen, Aktualisieren, Lesen und Löschen von Transformationsressourcen in AWS Transform custom sowie auf das Ausführen von Transformationen.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- AWS Benutzerdefiniert transformieren — Ermöglicht die umfassende Verwaltung von Transformationsressourcen, einschließlich Streaming-Konversationen, Ausführung von Transformationen und Verwaltung von Transformationspaketen. Ermöglicht das Erstellen, Abrufen und Löschen von Transformationspaket-URLs und das Abschließen von Paket-Uploads.
- Wissensmanagement — Ermöglicht das Auflisten, Abrufen, Löschen und Aktualisieren von Wissenselementen sowie deren Konfiguration und Status.

- Kampagnenverwaltung — Ermöglicht das Abrufen von Kampagnendetails, das Aktualisieren des Kampagnen-Repository-Status und das Aktualisieren von Kampagnen.
- Ressourcen-Tagging — Ermöglicht das Auflisten, Hinzufügen und Entfernen von Tags für benutzerdefinierte AWS Transform-Ressourcen.
- AWS Identity and Access Management (IAM) — Ermöglicht die Erstellung der benutzerdefinierten [serviceverknüpften AWS Transform-Rolle](#) (). `AWSServiceRoleForAWSTransformCustom` Diese Rolle ist erforderlich, damit AWS Transform custom CloudWatch Metriken und Protokolle an Ihr Konto sendet. Die Berechtigung ist so begrenzt, dass sie nur die Erstellung dieser speziellen dienstbezogenen Rolle erlaubt.

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie

[AWSTransformCustomManageTransformations](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: `AWSTransformInfrastructureExecutorAccessBatch`

Diese Richtlinie gewährt die erforderlichen Berechtigungen, um Assessments und Transformationen von AWS Transform Continuous Modernization mithilfe von AWS Batch durchzuführen. Ordnen Sie diese Richtlinie einer IAM-Rolle in Ihrem Konto zu. Die CLI und der Agent von AWS Transform Continuous Modernization übernehmen diese Rolle, um Quellcode hochzuladen, Ergebnisse abzurufen, den Batch-Jobstatus zu überwachen, Protokolle zu lesen und Transformationszeitpläne zu verwalten.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- AWS Lambda — Ermöglicht das Aufrufen und Abrufen der Konfiguration von Lambda-Funktionen mit `atx` Präfix, die den Transformationsworkflow orchestrieren.
- Amazon S3 — Ermöglicht das Hochladen von Quellcode in `atx-source-code-*` Buckets und das Herunterladen von Transformationsergebnissen aus `atx-custom-output-*` Buckets. `atx-ct-output-*`
- AWS Key Management Service (KMS) — Ermöglicht die Verschlüsselung und Entschlüsselung von Daten mithilfe des AWS Transform-Verschlüsselungsschlüssels (). `alias/atx-encryption-key`
- Amazon CloudWatch Logs — Ermöglicht das Lesen von Batch-Job- und Lambda-Ausführungsprotokollereignissen zur Transformationsüberwachung und zum Debuggen.

- Amazon CloudWatch — Ermöglicht das Abrufen und Auflisten des AWS Transform CLI-Dashboards für betriebliche Transparenz.
- AWS Batch — Ermöglicht die Beschreibung und Auflistung von Rechenumgebungen, Jobwarteschlangen, Jobdefinitionen und Jobstatus.
- CloudFormation— Ermöglicht die Beschreibung und Auflistung von AWS Transform-Infrastruktur-Stacks, um den Bereitstellungsstatus zu überprüfen.
- API zur Kennzeichnung von Resource Groups — Ermöglicht das Abrufen von markierten Ressourcen, um die AWS Transform-Infrastruktur in Ihrem Konto zu ermitteln.
- AWS Secrets Manager— Ermöglicht das Abrufen und Beschreiben von AWS Transform-Geheimnissen, die unter dem Präfix gespeichert sind. `atx/`
- Amazon EventBridge Scheduler — Ermöglicht die Verwaltung von geplanten Transformationsaufträgen innerhalb der `atx-ct` Zeitplangruppe.
- Amazon EC2 — Ermöglicht die Beschreibung der Konfiguration von VPC, Subnetz, Sicherheitsgruppe, Routing-Tabelle und NAT-Gateway für Netzwerke in Batch-Computing-Umgebungen.
- AWS Identity and Access Management (IAM) — Ermöglicht das Lesen von Rollenkonfigurationen mit ATX Präfix und mit `Atx` Präfix, um die Infrastruktureinrichtung zu validieren, und die Weitergabe `AtxSchedulerInvocationRole` an Amazon EventBridge Scheduler, damit dieser geplante Jobs aufrufen kann.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten durch Berechtigungen auf Ressourcenebene, tagbasierte Bedingungen, die `aws:ResourceAccount` Bedingung und Bedingungen im `iam:PassedToService` Servicebereich, um sicherzustellen, dass der Betrieb auf Transform-Ressourcen innerhalb desselben Kontos beschränkt ist. AWS AWS

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [AWSTransformInfrastructureExecutorAccessBatch](#) AWS

AWS verwaltete Richtlinie: AWSTransformInfrastructureExecutorAccessEC2

Diese Richtlinie gewährt die Berechtigungen, die für die Durchführung von AWS Transform Continuous Modernization Assessments und Transformationen mit Amazon EC2 erforderlich sind. Ordnen Sie diese Richtlinie einer IAM-Rolle in Ihrem Konto zu. Die CLI und der Agent von

AWS Transform Continuous Modernization übernehmen diese Rolle, um Quellcode hochzuladen, Ergebnisse abzurufen, den Jobstatus zu überwachen und Transformationspläne zu verwalten.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **CloudFormation**— Ermöglicht die Beschreibung von AWS Transform-Infrastruktur-Stacks, Stack-Ereignissen, Stack-Ressourcen und dem Status der Drift-Erkennung, das Auflisten von Stacks und die Validierung von CloudFormation Vorlagen vor der Bereitstellung.
- **Amazon EC2** — Ermöglicht die Beschreibung von Instances, AMIs, VPCs, Subnetzen, Sicherheitsgruppen, Schlüsselpaaren, Routing-Tabellen, NAT-Gateways und Internet-Gateways. Ermöglicht das Starten und Stoppen von EC2-Instances, die mit gekennzeichnet sind. `atx-remote-infra: true`
- **Amazon EC2 Systems Manager (SSM)** — Ermöglicht die Überwachung des Status der Befehlsausführung und die Ausführung von Befehlen und Sitzungen auf AWS Transform-tagged Instances, einschließlich der Ausführung des AWS-RunShellScript Dokuments.
- **Amazon S3** — Ermöglicht die Verwaltung von Quellcode und Ausgabeartefakten in AWS Transform-Buckets, einschließlich des Abrufs, Platzierens und Löschens von Objekten und des Auflistens von Buckets.
- **AWS Key Management Service (KMS)** — Ermöglicht die Verschlüsselung und Entschlüsselung von Daten mithilfe des AWS Transform-Verschlüsselungsschlüssels (). `alias/atx-encryption-key`
- **AWS Secrets Manager**— Ermöglicht das Abrufen und Beschreiben von Transformationsgeheimnissen, wie z. B. Repository-Anmeldeinformationen, die `atx/` unter dem Präfix gespeichert sind.
- **Amazon EventBridge Scheduler** — Ermöglicht die Verwaltung von geplanten Transformationsaufträgen innerhalb der `atx-ct` Zeitplangruppe.
- **API zur Kennzeichnung von Resource Groups** — Ermöglicht das Abrufen von markierten Ressourcen, um die AWS Transform-Infrastruktur in Ihrem Konto zu ermitteln.
- **AWS Identity and Access Management (IAM)** — Ermöglicht die Übergabe der `atx-transform-role*` Rolle an Amazon EC2 und den Amazon EventBridge Scheduler sowie das `AtxSchedulerInvocationRole` Lesen der Rollen- und Instance-Profilkonfiguration für EC2-Instances.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten durch Berechtigungen auf Ressourcenebene, tagbasierte Bedingungen, die `aws:ResourceAccount` Bedingung und Bedingungen im Servicebereich, um sicherzustellen, dass Operationen auf Transform-Ressourcen innerhalb desselben Kontos beschränkt sind `iam:PassedToService`. AWS AWS

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [AWSTransformInfrastructureExecutorAccessEC2](#) AWS

AWS verwaltete Richtlinie: AWSTransformSecurityAgentExecutorAccess

Diese Richtlinie gewährt AWS Transform Continuous Modernization die erforderlichen Berechtigungen, um den AWS Security Agent-Dienst zur automatisierten Überprüfung und Behebung der Codesicherheit aufzurufen. Fügen Sie diese Richtlinie einer IAM-Rolle in Ihrem Konto hinzu, von der die CLI und der Agent von AWS Transform Continuous Modernization annehmen, dass sie Scan-Artefakte hochlädt und Ergebnisse abrufen.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **AWS Security Agent** — Ermöglicht das Auflisten von Agentenbereichen, das Erstellen von Code-Reviews, das Starten von Code-Review-Jobs, das Auflisten und Abrufen von Ergebnissen sowie das Starten der Codekorrektur. Diese Aktionen sind auf Agentenbereiche in Ihrem Konto beschränkt.
- **Amazon S3** — Ermöglicht das Herunterladen von Scanergebnissen und Ergebnissen aus dem `kct-security-agent-*` Bucket sowie das Hochladen von Quellcode für Sicherheitsscans in das `security-scans/*` Präfix innerhalb dieses Buckets.
- **AWS Identity and Access Management (IAM)** — Ermöglicht die Übergabe der `security-agent-*` Rolle an den AWS Security Agent-Dienst, damit dieser den Scan durchführen kann.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten über Berechtigungen auf Ressourcenebene, S3-Bucket- und Schlüsselpräfixe, die `s3:ResourceAccount` Bedingungen `aws:ResourceAccount` und sowie eine dienstbezogene `iam:PassedToService` Bedingung, um sicherzustellen, dass Operationen auf Security Agent-Ressourcen innerhalb desselben Kontos beschränkt sind. AWS AWS

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [AWSTransformSecurityAgentExecutorAccess](#) AWS

AWS verwaltete Richtlinie: DBModDiscoveryAndAssessment

Diese Richtlinie bietet umfassende Erkennungs- und Bewertungsfunktionen zur Datenbankmodernisierung für AWS Transform.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- Amazon EC2 — Ermöglicht die Beschreibung von Infrastrukturkomponenten wie Instances, VPCs, Subnetzen, Sicherheitsgruppen, Verfügbarkeitszonen, VPC-Endpunkten und Internet-Gateways.
- Amazon RDS — Ermöglicht die Beschreibung von Datenbank-Instances, Clustern und Subnetzgruppen. Ermöglicht das Ändern von DB-Subnetzgruppen innerhalb desselben AWS Kontos zur Vorbereitung der Migration.
- Amazon RDS Data API — Ermöglicht die Aktivierung und Deaktivierung von HTTP-Endpunkten und die Ausführung von SQL-Anweisungen auf Datenbankclustern, die für das Datenbankmodernisierungsprojekt gekennzeichnet sind.
- AWS DMS— Ermöglicht die Beschreibung von Endpunkten, Replikationsinstanzen, Aufgaben, Subnetzgruppen und bestellbaren Instances. Ermöglicht das Auflisten von Datenanbietern, Instanzprofilen und Migrationsprojekten. Ermöglicht die Beschreibung von Tabellenstatistiken, Bewertungsläufen und Metadatenmodelloperationen. Ausführliche Beschreibungs- und Metadatenoperationen sind auf Ressourcen beschränkt, die für das Projekt zur Datenbankmodernisierung gekennzeichnet sind.
- — Ermöglicht das Auflisten von Geheimnissen zum Auffinden von Datenbankanmeldedaten.
- AWS Identity and Access Management (IAM) — Ermöglicht die Überprüfung bestimmter AWS DMS Servicerollen und der damit verbundenen Richtlinien. Beinhaltet den Zugriff auf Richtlinien mit AWS Leseverwaltung AWS DMS .
- AWS Key Management Service (KMS) — Ermöglicht das Auflisten von Schlüsselaliasen und das Beschreiben von Schlüsseln. Ermöglicht die Entschlüsselung von Geheimnissen durch Integration, beschränkt auf dasselbe AWS Konto.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten durch Berechtigungen auf Ressourcenebene, tagbasierte Bedingungen und Einschränkungen auf Kontoebene, um

sicherzustellen, dass der Betrieb auf Projektressourcen zur Datenbankmodernisierung innerhalb desselben Kontos beschränkt ist. AWS

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [DBModDiscoveryAndAssessment](#) AWS

AWS verwaltete Richtlinie: DBModProvisioningAndMigration

Diese Richtlinie bietet Funktionen zur Datenbankbereitstellung und Migration für AWS Transform-Datenbankmodernisierungsprojekte. Sie umfasst Berechtigungen zum Erstellen und Verwalten der Migrationsinfrastruktur, zur Bereitstellung von Zieldatenbanken und zum Speichern von Migrationsdaten.

Beschreibung

Diese Richtlinie umfasst die folgenden Berechtigungen:

- AWS DMS— Ermöglicht die Erstellung und Verwaltung von Replikationssubnetzgruppen, Instanzprofilen, Datenanbietern, Migrationsprojekten, Endpunkten, Replikationsinstanzen und Replikationsaufgaben. Beinhaltet Schemakonvertierungsvorgänge wie Import, Konvertierung, Export und Bewertung von Metadatenmodellen. Ermöglicht das Lebenszyklusmanagement von Replikationsinstanzen (Erstellen, Löschen, Ändern, Neustarten) und Replikationsaufgaben (Löschen, Starten, Stoppen, Bewerten). Alle Schreibvorgänge sind auf Ressourcen beschränkt, die für das Projekt zur Datenbankmodernisierung gekennzeichnet sind.
- Amazon RDS — Ermöglicht die Erstellung von Datenbank-Subnetzgruppen, Datenbankclustern und Datenbank-Instances. Alle Ressourcen müssen für das Projekt zur Datenbankmodernisierung mit Tags versehen werden.
- — Ermöglicht das Erstellen, Aktualisieren und Markieren von Geheimnissen mit dem Namenspräfix für die Datenbankmodernisierung. Ermöglicht das Abrufen geheimer Werte und das Beschreiben von Geheimnissen für markierte Ressourcen.
- Amazon S3 — Ermöglicht die Erstellung und Verwaltung von S3-Buckets und Objekten für die Speicherung von Migrationsdaten. Beinhaltet Bucket-Tagging, Versionierung und Objektlebenszyklus-Operationen. Beschränkt auf Buckets mit dem Namenspräfix für die Datenbankmodernisierung.
- AWS Identity and Access Management (IAM) — Ermöglicht die Übergabe bestimmter AWS DMS Dienstrollen an Dienste AWS DMS und die Schemakonvertierung. Ermöglicht die Erstellung der serviceverknüpften Amazon RDS-Rolle, die für Datenbankoperationen erforderlich ist.

Die Richtlinie implementiert den Zugriff mit den geringsten Rechten durch Berechtigungen auf Ressourcenebene, tagbasierte Bedingungen und Einschränkungen auf Kontoebene, um sicherzustellen, dass der Betrieb auf Projektressourcen zur Datenbankmodernisierung innerhalb desselben Kontos beschränkt ist. AWS

Details zu Berechtigungen

Einzelheiten zu den Richtlinienberechtigungen finden Sie im Referenzhandbuch für verwaltete Richtlinien. [DBModProvisioningAndMigration](#) AWS

AWS Referenz zu Transformationsberechtigungen

Dieser Abschnitt enthält Informationen zu den von AWS Transform verwendeten APIs und deren Funktionsweise.

Topics

- [AWS Transformieren Sie APIs](#)

AWS Transformieren Sie APIs

- transformieren: BatchGetMessage
- transformieren: BatchGetUserDetails
- transformieren: CompleteArtifactUpload
- transformieren: CreateArtifactDownloadUrl
- transformieren: CreateArtifactUploadUrl
- transformieren: CreateAssetDownloadUrl
- transformieren: CreateConnector
- transformieren: CreateFeedback
- transformieren: CreateJob
- transformieren: CreateSession
- transformieren: CreateWorkspace
- transformieren: DeleteConnector
- transformieren: DeleteJob
- transformieren: DeleteSelfRoleMappings

- transformieren: DeleteUserRoleMappings
- transformieren: DeleteWorkspace
- transformieren: DetectIsAllowedForOperation
- transformieren: GetConnector
- transformieren: GetFeedbackQuestions
- transformieren: GetHitITask
- transformieren: GetJob
- transformieren: GetLoginRedirectUri
- transformieren: GetUserDetails
- transformieren: GetUserPreferences
- transformieren: GetWebAppUrl
- transformieren: GetWorkspace
- transformieren: ListArtifacts
- transformieren: ListConnectors
- transformieren: ListHitITasks
- transformieren: ListJobPlanSteps
- transformieren: ListJobs
- transformieren: ListMessages
- transformieren: ListPlanUpdates
- transformieren: ListUserRoleMappings
- transformieren: ListWorklogs
- transformieren: ListWorkspaces
- transformieren: PutUserPreferences
- transformieren: PutUserRoleMappings
- transformieren: RevokeSession
- transformieren: SearchUsers
- transformieren: SearchUsersTypeahead
- transformieren: SendMessage
- transformieren: StartJob
- transformieren: StopJob

- transformieren: SubmitCriticalHitITask
- transformieren: SubmitStandardHitITask
- transformieren: TestReleaseTraitPreProd
- transformieren: TestReleaseTraitProd
- transformieren: UpdateHitITask
- transformieren: UpdateJob
- transformieren: UpdateWorkspace
- transformieren: VerifySession

Konformitätsvalidierung für AWS Transformieren

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

Resilienz in AWS Transformieren

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen 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 Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Zusätzlich zur AWS globalen Infrastruktur bietet AWS Transform mehrere Funktionen, die Sie bei der Erfüllung Ihrer Datenausfallsicherheit und Ihrer Backup-Anforderungen unterstützen.

AWS Transform und Schnittstellenendpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC herstellen und AWS Transform einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellen-Endpunkte werden mit einer Technologie betrieben [AWS PrivateLink](#), mit der Sie privat auf die AWS Transform Konsole zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung erforderlich ist. Direct Connect Datenverkehr zwischen Ihrer VPC und AWS Transform verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere [Elastic-Netzwerk-Schnittstellen](#) in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter [Schnittstellen-VPC-Endpunkte \(AWS PrivateLink\)](#) im Amazon-VPC-Benutzerhandbuch.

Note

Eine AWS Transform benutzerdefinierte PrivateLink Dokumentation finden Sie unter [AWS Transform benutzerdefinierte Endpunkte und Schnittstellenendpunkte \(AWS PrivateLink\)](#).

Überlegungen zu AWS Transform VPC-Endpunkte

Bevor Sie einen Schnittstellen-VPC-Endpunkt für einrichten, stellen Sie sicher AWS Transform, dass Sie die [Eigenschaften und Einschränkungen der Schnittstellen-Endpunkte](#) im Amazon VPC-Benutzerhandbuch lesen.

Voraussetzungen

Beginnen Sie mit den nachstehenden Schritten erst, wenn Folgendes vorliegt:

- Ein AWS Konto mit den entsprechenden Berechtigungen zum Erstellen und Konfigurieren von Ressourcen.
- Eine VPC wurde bereits in Ihrem AWS Konto erstellt.
- Vertrautheit mit AWS Diensten, insbesondere Amazon VPC und. AWS Transform

Erstellen eines Schnittstellen-VPC-Endpunkts für AWS Transform

Sie können einen VPC-Endpunkt für den AWS Transform Service entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter [Erstellung eines Schnittstellenendpunkts](#) im Benutzerhandbuch für Amazon VPC.

AWS Transform unterstützt die folgenden VPC-Endpunktdienste:

Service-Name	Endpoint	Hinweis
Steuerebene	<code>com.amazonaws.<i>region</i>.transform</code>	
Agenten-API	<code>com.amazonaws.<i>region</i>.transform-agents</code>	
Webanwendung	<code>com.amazonaws.<i>region</i>.api.transform</code>	Für die AWS Transform Webanwendung erforderlich. Für diesen Endpunkt muss privates DNS aktiviert sein (die Option DNS-Name aktivieren), damit es zu einer privaten IP-Adresse in Ihrer VPC <code>api.transform.<i>region</i>.on.aws</code> aufgelöst wird.

region Ersetzen Sie es durch die AWS Region, in der Ihr AWS Transform Profil installiert ist, z. B. `com.amazonaws.us-east-1.transform`.

Note

Wenn Sie die Webanwendung verwenden, ist der Endpunkt erforderlich `api.transform`. Die vollständige Anleitung zur Einrichtung finden Sie unter [Zugriff auf AWS Transform Webanwendung aus einer VPC](#).

Weitere Informationen finden Sie unter [Unterstützte Regionen für AWS Transform](#) und [Zugreifen auf einen Service über einen Schnittstellenendpunkt](#) im Amazon VPC-Benutzerhandbuch.

Verwenden Sie einen lokalen Computer, um eine Verbindung zu einem herzustellen AWS Transform Endpunkt

In diesem Abschnitt wird beschrieben, wie Sie mithilfe eines lokalen Computers eine Verbindung AWS Transform über einen AWS PrivateLink Endpunkt in Ihrer AWS VPC herstellen.

1. [Stellen Sie eine VPN-Verbindung zwischen Ihrem lokalen Gerät und Ihrer VPC her.](#)
2. [Erstellen Sie einen VPC-Schnittstellen-Endpunkt für AWS Transform.](#)
3. [Richten Sie einen eingehenden Endpunkt von Amazon Route 53 ein.](#) Auf diese Weise können Sie den DNS-Namen Ihres AWS Transform Endpunkts von Ihrem lokalen Gerät aus verwenden.

Zugriff auf AWS Transform Webanwendung aus einer VPC

Wenn Sie AWS PrivateLink privat von Ihrer VPC aus auf die AWS Transform API zugreifen, erfordert die Webanwendung eine zusätzliche Netzwerkkonfiguration. Sie stellt statische Inhalte (HTML, JavaScript, CSS) bereit CloudFront, wofür eine Internetverbindung erforderlich ist. API-Aufrufe von der Webanwendung gehen über Ihren VPC-Endpunkt und bleiben vollständig privat.

In diesem Handbuch erfahren Sie, wie Sie den kontrollierten Internetausgang von Ihrer VPC aus so konfigurieren, dass die Webanwendung geladen werden kann, während Ihre VPC nur auf die erforderlichen Domänen beschränkt bleibt.

Funktionsweise

Die AWS Transform Webanwendung verwendet zwei Netzwerkpfade:

- API-Aufrufe — Wenn Sie mit der Webanwendung interagieren (Jobs starten, Arbeitsbereiche anzeigen usw.), sendet der Browser API-Anfragen `anapi.transform.region.on.aws`. Wenn der `com.amazonaws.region.api.transform` VPC-Endpunkt und das private DNS aktiviert sind, werden diese Anfragen zu einer privaten IP-Adresse in Ihrer VPC aufgelöst und verlassen niemals das AWS Netzwerk.
- Statischer Inhalt — Die HTML- und CSS-Dateien der Webanwendung werden über CloudFront bereitgestellt. JavaScript `tenant-id.transform.region.on.aws` Für das Laden dieser

Dateien ist eine Internetverbindung erforderlich, da die Bereitstellung von CloudFront Inhalten nur über das öffentliche Internet möglich ist.

- Authentifizierung — Es werden AWS IAM Identity Center-Anmeldeabläufe verwendet `<region>.signin.aws`, für die auch eine Internetverbindung erforderlich ist.

Um die Webanwendung zu aktivieren und gleichzeitig die Sicherheit aufrechtzuerhalten, erstellen Sie mithilfe der AWS Network Firewall mit domänenbasierter Filterung einen kontrollierten Ausgangspfad. Auf diese Weise kann Ihre VPC nur die spezifischen Domänen erreichen, die von der Webanwendung benötigt werden, während der gesamte andere Internetverkehr blockiert wird.

Architektur

Das folgende Diagramm zeigt den Netzwerkpfad für den Datenverkehr von Webanwendungen:

```
EC2 Instance / Workspace (Private Subnet)
|
| Route: 0.0.0.0/0 # Network Firewall Endpoint
v
AWS Network Firewall (Firewall Subnet)
| Allows: *.cloudfront.net, *.transform.<region>.on.aws,
|         <region>.signin.aws, SSO domains, S3 presigned URLs
| Blocks: everything else (TLS SNI inspection)
|
| Route: 0.0.0.0/0 # NAT Gateway
v
NAT Gateway (Public Subnet)
|
| Route: 0.0.0.0/0 # Internet Gateway
v
Internet Gateway # CloudFront Edge Locations
```

Important

Die Network Firewall muss beide Verkehrsrichtungen erkennen (symmetrisches Routing), um die TLS-SNI-Inspektion durchführen zu können. Sie müssen im NAT-Gateway-Subnetz eine Rückroute konfigurieren, die den für das private Subnetz bestimmten Datenverkehr durch die Firewall zurücksendet. Ohne dies funktionieren domänenbasierte Filterregeln nicht.

Voraussetzungen

Stellen Sie vor Beginn sicher, dass Sie über Folgendes verfügen:

- Ein AWS Konto mit Berechtigungen zum Erstellen von VPC-Ressourcen, Network Firewall und NAT-Gateways.
- Eine VPC mit einem privaten Subnetz, in dem Ihre Instances oder Workloads ausgeführt werden.
- Ein an die VPC angeschlossenes Internet-Gateway (oder Berechtigungen zum Erstellen eines solchen).
- Ein AWS Transform VPC-Endpunkt für `com.amazonaws.region.api.transform` mit aktiviertem privaten DNS. Dies ist der Endpunkt, der vom Browser-Client für Webanwendungen verwendet wird. Anweisungen zum Erstellen von Endpunkten finden Sie unter [AWS Transform und Schnittstellenendpunkte \(AWS PrivateLink\)](#).

Konfiguration der VPC-Endpunktrichtlinie

Wenn Ihr `com.amazonaws.region.api.transform` VPC-Endpunkt über eine benutzerdefinierte Endpunktrichtlinie verfügt, müssen Sie eine Anweisung hinzufügen, die AWS Transform Operationen zulässt. Andernfalls kann die Webanwendung keine API-Aufrufe über den Endpunkt tätigen.

Fügen Sie Ihrer VPC-Endpunktrichtlinie die folgende Aussage hinzu.

`AWS_TRANSFORM_PROFILE_ARN` Ersetzen Sie es durch Ihr AWS Transform Dienstprofil ARN, das Sie in der AWS Transform Konsole auf der Seite Einstellungen finden.

```
{
  "Statement": [
    {
      "Sid": "AllowAWSTransform",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalArn": [
            "AWS_TRANSFORM_PROFILE_ARN"
          ]
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Note

Wenn Ihr VPC-Endpoint die Standardrichtlinie (Vollzugriff) verwendet, sind keine Änderungen erforderlich und Sie können diesen Schritt überspringen.

Einrichtung eines kontrollierten Internetausgangs

Gehen Sie wie folgt vor, um die Network Firewall mit domänenbasierter Filterung für die AWS Transform Webanwendung zu konfigurieren.

Schritt 1: Erstellen Sie das Firewall-Subnetz

Erstellen Sie ein kleines /28-Subnetz, das dem Netzwerk-Firewall-Endpoint gewidmet ist. Dieses Subnetz muss sich in derselben Availability Zone wie Ihr privates Subnetz befinden.

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block firewall-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Schritt 2: Erstellen Sie ein öffentliches Subnetz für das NAT-Gateway

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block public-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Schritt 3: Konfigurieren Sie die Routing-Tabelle für öffentliche Subnetze

Erstellen Sie eine Routentabelle für das öffentliche Subnetz, das den Internetverkehr an das Internet-Gateway weiterleitet.

```
# Create route table
PUB_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

# Add default route to internet gateway
aws ec2 create-route \
  --route-table-id $PUB_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --gateway-id your-igw-id \
  --region region

# Associate with public subnet
aws ec2 associate-route-table \
  --route-table-id $PUB_RTB \
  --subnet-id public-subnet-id \
  --region region
```

Schritt 4: Erstellen Sie das NAT-Gateway

```
# Allocate an Elastic IP
EIP=$(aws ec2 allocate-address --domain vpc \
  --region region --query 'AllocationId' --output text)

# Create NAT Gateway in the public subnet
NAT_ID=$(aws ec2 create-nat-gateway \
  --subnet-id public-subnet-id \
  --allocation-id $EIP \
  --region region \
  --query 'NatGateway.NatGatewayId' --output text)

# Wait for NAT Gateway to become available (~2 minutes)
aws ec2 wait nat-gateway-available \
```

```
--nat-gateway-ids $NAT_ID --region region
```

Schritt 5: Erstellen Sie die Netzwerk-Firewall-Regelgruppe

Erstellen Sie eine statusbehaftete Regelgruppe, die nur Datenverkehr zu den Domänen zulässt, die für die AWS Transform Webanwendung erforderlich sind.

```
aws network-firewall create-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL \
  --capacity 100 \
  --rule-group '{
    "StatefulRuleOptions": {
      "RuleOrder": "STRICT_ORDER"
    },
    "RulesSource": {
      "RulesSourceList": {
        "Targets": [
          ".cloudfront.net",
          ".transform.region.on.aws",
          "region.signin.aws",
          ".s3.region.amazonaws.com",
          "oidc.region.amazonaws.com",
          "portal.sso.region.amazonaws.com",
          "assets.sso-portal.region.amazonaws.com",
          "directory-id.awsapps.com"
        ],
        "TargetTypes": ["TLS_SNI", "HTTP_HOST"],
        "GeneratedRulesType": "ALLOWLIST"
      }
    }
  }' \
  --region region
```

region Ersetzen Sie es durch die AWS Region, in der Ihr AWS Transform Profil installiert ist (z. B. us-east-1). *directory-id* Ersetzen Sie es durch Ihre IAM Identity Center-Verzeichnis-ID (z. B. d-1234567890). Sie finden Ihre Verzeichnis-ID in der IAM Identity Center-Konsole.

In der folgenden Tabelle werden die zulässigen Domänen erklärt.

Domain	Zweck
<code>.cloudfront.net</code>	CloudFront CDN — stellt statische Ressourcen (CSSJavaScript, Bilder) für Webanwendungen bereit
<code>.transform. <i>region</i>.on.aws</code>	Mandanten-URL der Webanwendung — der Browser lädt die erste Seite von dieser Domain über CloudFront
<code><i>region</i>.signin.aws</code>	Umleitungsseite für die SSO-Anmeldung
<code>.s3.<i>region</i>.amazonaws.com</code>	Vorsignierte S3-URLs — Uploads und Downloads von Artefakten
<code>oidc.<i>region</i>.amazonaws.com</code>	Austausch von OIDC-Tokens für die SSO-Authentifizierung
<code>portal.sso. <i>region</i>.amazonaws.com</code>	Anmeldeseite für das SSO-Portal
<code>assets.sso-portal. <i>region</i>.amazonaws.com</code>	Statische Ressourcen des SSO-Portals (CSS, JavaScript)
<code><i>directory-id</i> .awsapps.com</code>	IAM Identity Center-Portal für Ihre Organisation

Note

Der `.cloudfront.net` Platzhalter ermöglicht den Datenverkehr zu jeder CloudFront Distribution, nicht nur zu der der AWS Transform Webanwendung. Ein schmalere Domänenfilter ist nicht möglich, da CloudFront Edge-IPs von allen Distributionen gemeinsam genutzt werden und die TLS-SNI-Inspektion nicht zwischen einzelnen Distributionen hinter derselben Domain unterscheiden kann.

Note

API-Aufrufe müssen weitergeleitet werden `api.transform.region.on.aws` AWS PrivateLink und erfordern keinen ausgehenden Internetzugriff. Sie sind von der Firewall nicht betroffen.

Schritt 6: Erstellen Sie die Firewall-Richtlinie

Die Richtlinie muss die `STRICT_ORDER` Regelauswertung mit `drop_established` als Standardaktion verwenden. Dadurch wird sichergestellt, dass jeglicher Datenverkehr, der nicht der Zulassungsliste entspricht, gelöscht wird.

```
# Get the rule group ARN
RG_ARN=$(aws network-firewall describe-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region \
  --query 'RuleGroupResponse.RuleGroupArn' --output text)

# Create the firewall policy
aws network-firewall create-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --firewall-policy "{
    \"StatelessDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatelessFragmentDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatefulRuleGroupReferences\": [
      {
        \"ResourceArn\": \"$RG_ARN\",
        \"Priority\": 1
      }
    ],
    \"StatefulEngineOptions\": {
      \"RuleOrder\": \"STRICT_ORDER\"
    },
    \"StatefulDefaultActions\": [\"aws:drop_established\", \"aws:alert_established\"]
  }" \
  --region region
```


Schritt 7: Erstellen Sie die Network Firewall

```
# Get the policy ARN
FW_POLICY_ARN=$(aws network-firewall describe-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region \
  --query 'FirewallPolicyResponse.FirewallPolicyArn' --output text)

# Create the firewall
aws network-firewall create-firewall \
  --firewall-name transform-webapp-firewall \
  --firewall-policy-arn $FW_POLICY_ARN \
  --vpc-id your-vpc-id \
  --subnet-mappings SubnetId=firewall-subnet-id \
  --region region

# Wait for the firewall to become READY (3-5 minutes)
while true; do
  STATUS=$(aws network-firewall describe-firewall \
    --firewall-name transform-webapp-firewall \
    --region region \
    --query 'FirewallStatus.Status' --output text)
  echo "Status: $STATUS"
  if [ "$STATUS" = "READY" ]; then break; fi
  sleep 15
done
```

Schritt 8: Holen Sie sich die Firewall-Endpoint-ID

```
FW_ENDPOINT=$(aws network-firewall describe-firewall \
  --firewall-name transform-webapp-firewall \
  --region region \
  --query "FirewallStatus.SyncStates.\"your-az\".Attachment.EndpointId" \
  --output text)
echo "Firewall endpoint: $FW_ENDPOINT"
```

Schritt 9: Konfigurieren Sie die Routentabelle des Firewall-Subnetzes

Leiten Sie den internetgebundenen Verkehr vom Firewall-Subnetz zum NAT-Gateway weiter.

```
FW_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

aws ec2 create-route \
  --route-table-id $FW_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_ID \
  --region region

aws ec2 associate-route-table \
  --route-table-id $FW_RTB \
  --subnet-id firewall-subnet-id \
  --region region
```

Schritt 10: Aktualisieren Sie die Routentabelle für private Subnetze

Leiten Sie den gesamten internetgebundenen Verkehr vom privaten Subnetz durch die Firewall.

```
aws ec2 create-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

Wenn bereits eine Standardroute vorhanden ist, verwenden Sie anstelle von `replace-route`.
`create-route`

Schritt 11: Fügen Sie die symmetrische Rückroute hinzu (erforderlich)

Important

Dieser Schritt ist entscheidend. Die Network Firewall verwendet die TLS-SNI-Inspektion und muss beide Richtungen einer TCP-Verbindung erkennen. Fügen Sie der Routentabelle des NAT-Gateway-Subnetzes eine Route hinzu, die den für das private Subnetz bestimmten Rückverkehr durch die Firewall zurücksendet.

```
aws ec2 create-route \  
  --route-table-id $PUB_RTB \  
  --destination-cidr-block private-subnet-cidr \  
  --vpc-endpoint-id $FW_ENDPOINT \  
  --region region
```

private-subnet-cidr Ersetzen Sie ihn durch den CIDR-Block Ihres privaten Subnetzes (z. B.).
10.0.144.0/20

Ohne symmetrisches Routing erkennt die Firewall nur eine Richtung des Datenverkehrs. Die TLS Inspection Engine kann die Server Name Indication (SNI) nicht aus dem TLS-Handshake extrahieren, und alle domänenbasierten Regeln schlagen automatisch fehl.

Schritt 12: Entfernen Sie die IPv6-Standardroute (falls vorhanden)

Wenn die Routentabelle für private Subnetze eine IPv6-Standardroute (:::/0) enthält, die direkt auf ein Internet-Gateway verweist, wird die Firewall für Ziele umgangen. IPv6-capable Entferne sie:

```
aws ec2 delete-route \  
  --route-table-id private-subnet-route-table-id \  
  --destination-ipv6-cidr-block ::/0 \  
  --region region
```

Verifizierung

Überprüfen Sie die Konfiguration von einer Instanz im privaten Subnetz aus:

```
# Should SUCCEED - web application content via CloudFront (allowed)
curl -vL --connect-timeout 15 \
  'https://tenant-id.transform.region.on.aws'

# Should SUCCEED - API via PrivateLink (does not use firewall)
curl -v --connect-timeout 15 \
  'https://api.transform.region.on.aws/'

# Should FAIL - non-allowlisted domain (blocked by firewall)
curl -v --connect-timeout 15 'https://www.example.com'
# Expected: TLS connection error (firewall drops after SNI inspection)
```

Fehlerbehebung

API-Aufrufe von api.transform werden von Ihrer Firewall blockiert

Die Domain api.transform.region.on.aws sollte über den VPC-Endpunkt zu einer privaten IP-Adresse aufgelöst werden und Ihre Internet-Firewall nicht erreichen.

- Stellen Sie sicher, dass Sie den com.amazonaws.region.api.transform Endpunkt erstellt haben.
- Stellen Sie sicher, dass privates DNS auf dem Endpunkt aktiviert ist:

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

Erwartete Ausgabe: available | True

Die Webanwendung wird nicht geladen (Verbindungs-Timeout)

- Stellen Sie sicher, dass die Routentabelle des privaten Subnetzes eine 0.0.0.0/0 Route enthält, die auf den Firewall-Endpunkt verweist.
- Stellen Sie sicher, dass die Routentabelle des Firewall-Subnetzes eine 0.0.0.0/0 Route enthält, die auf das NAT-Gateway verweist.

- Stellen Sie sicher, dass sich das NAT-Gateway in einem bestimmten available Zustand befindet.

Non-allowlisted Domänen sind nicht blockiert

- Suchen Sie nach einer `::/0` IPv6-Route, die auf das Internet-Gateway verweist. Dadurch wird die Firewall umgangen. Entfernen Sie es (Schritt 12).
- Stellen Sie sicher, dass symmetrisches Routing konfiguriert ist. Die NAT-Gateway-Subnetz-Routentabelle muss eine Rückroute durch die Firewall für das private Subnetz CIDR haben (Schritt 11).
- Vergewissern Sie sich, dass die Firewall-Richtlinie die Aktionen `STRICT_ORDER` mit `drop_established` und `alert_established` als Standardaktionen verwendet.

Kostenüberlegungen

Ressource	Ungefähre Kosten
Network Firewall	~0 \$. 395/hr (~\$288/month) pro Availability Zone
NAT-Gateway	~0 \$. 045/hr (~\$33/month) + Datenverarbeitungsgebühren
Elastic IP (öffentliches IPv4)	~0 \$. 005/hr (~3 \$). 60/month)
Datenverarbeitung durch Network Firewall	0\$. 065/GB
NAT-Gateway-Datenverarbeitung	0\$. 045/GB

Die geschätzten Grundkosten 325/month für eine einzelne Availability Zone-Bereitstellung belaufen sich auf ungefähr \$. Stellen Sie für Produktionsbereitstellungen die Firewall, das NAT-Gateway und die zugehörigen Subnetze in jeder Availability Zone bereit, in der private Subnetze existieren.

Bereinigen

Um alle in diesem Handbuch erstellten Ressourcen zu entfernen, führen Sie die folgenden Befehle in umgekehrter Reihenfolge aus. Ersetzen Sie die Platzhalter durch die Ressourcen-IDs aus Ihrer

Bereitstellung. Sie finden diese Werte in der AWS Management Console oder mithilfe der `describe` Befehle aus den Einrichtungsschritten.

```
# Remove return route from NAT Gateway subnet
aws ec2 delete-route --route-table-id pub-rtb-id \
  --destination-cidr-block private-subnet-cidr \
  --region region

# Remove route from private subnet
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 --region region

# Delete Network Firewall (takes ~5 minutes)
aws network-firewall delete-firewall \
  --firewall-name transform-webapp-firewall \
  --region region

# Delete firewall policy and rule group
aws network-firewall delete-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region
aws network-firewall delete-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region

# Delete NAT Gateway (wait ~5 minutes for full deletion)
aws ec2 delete-nat-gateway --nat-gateway-id nat-gateway-id \
  --region region

# Release Elastic IP
aws ec2 release-address --allocation-id eip-allocation-id \
  --region region

# Delete subnets
aws ec2 delete-subnet --subnet-id firewall-subnet-id \
  --region region
aws ec2 delete-subnet --subnet-id public-subnet-id \
  --region region
```

Überwachen AWS Transformieren

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Transform und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um AWS Transform zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarmer festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im [Amazon CloudWatch Logs-Benutzerhandbuch](#).
- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse aus AWS Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im [EventBridge Amazon-Benutzerhandbuch](#).
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im [AWS CloudTrail -Benutzerhandbuch](#).

Protokollierung AWS Transformieren Sie API-Aufrufe mit AWS CloudTrail

AWS Transform ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in AWS Transform ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für AWS Transform als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Transform-Konsole und Codeaufrufen für die AWS Transform-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Transform. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an AWS Transform gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

AWS Verwandeln Sie Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in AWS Transform eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter [Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für AWS Transform, 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 anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen 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 den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [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](#)

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Verständnis AWS Logdateieinträge transformieren

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 Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Benachrichtigungen

AWS Transform bietet E-Mail-Benachrichtigungen, um dich über Änderungen des Workspace-Zugriffs, Aktualisierungen des Jobstatus und ausstehende Anfragen von Mitarbeitern auf dem Laufenden zu halten.

E-Mail-Benachrichtigungen

E-Mail-Benachrichtigungen sind standardmäßig aktiviert und werden an Benutzer gesendet, die nur über Leseberechtigungen oder höhere Berechtigungen für einen Job verfügen. Benutzer können ihre Benachrichtigungseinstellungen ändern. Es gibt drei Kategorien von E-Mail-Benachrichtigungen:

- Updates für den Workspace-Zugriff

Du erhältst eine Benachrichtigung, wenn du zu einem neuen Workspace hinzugefügt wirst und wenn deine Rolle innerhalb eines Workspace geändert wird.

- Tägliche Übersichts-E-Mails

Sie erhalten täglich um 9:00 Uhr MEZ eine Zusammenfassung Ihrer aktuellen Jobs, sofern Sie aktive Jobs mit einer oder mehreren offenen Anfragen von Mitarbeitern haben. Die E-Mail enthält eine Tabelle mit Workspace-Namen, Jobname, Jobstatus, Details zu Mitarbeiteranfragen und erforderlichen Aktionen (begrenzt auf 10 Zeilen)

 Note

Tägliche Übersichts-E-Mails werden nur für Jobs gesendet, für die Anfragen von Mitarbeitern erforderlich sind. Optionale Anfragen von Mitarbeitern lösen keine Übersichts-E-Mails aus.

- Aktualisierungen des Jobstatus

Sie erhalten eine E-Mail, wenn ein Job, auf den Sie Zugriff haben, abgeschlossen ist oder fehlschlägt.

- Mitarbeiter fordern Updates an

Sie erhalten eine E-Mail, wenn eine Aufgabe Ihre Eingabe, Überprüfung oder Genehmigung erfordert.

E-Mail-Benachrichtigungen verwalten

Sie können Ihre Einstellungen für E-Mail-Benachrichtigungen in der Webanwendung ändern, indem Sie in der oberen rechten Ecke der Anwendung auf das Einstellungen-Zahnrad klicken und Benachrichtigungseinstellungen auswählen.

Die Seite mit den Benachrichtigungseinstellungen bietet die folgenden Steuerelemente:

Art der Benachrichtigung	Description	Standardeinstellung
Aktualisierungen für Workspace Access	Erhalte E-Mails, wenn du zu einem Workspace hinzugefügt wirst oder wenn deine Rolle innerhalb eines Workspace geändert wird	Aktiviert
Täglicher Überblick über Anfragen von Mitarbeitern	Erhalten Sie täglich eine Zusammenfassung offener Anfragen von Mitarbeitern für Jobs in barrierefreien Arbeitsbereichen	Aktiviert
Aktualisierungen zum Abschluss von Aufträgen	Erhalten Sie E-Mails, wenn ein Job abgeschlossen ist oder fehlschlägt	Aktiviert
Mitarbeiter fordern Updates an	Erhalten Sie E-Mails, wenn eine Eingabe oder Genehmigung von Ihnen erforderlich ist	Disabled

Sie können eine allgemeine Einstellung verwenden, um alle Benachrichtigungen zu aktivieren oder zu deaktivieren, oder einzelne Benachrichtigungstypen separat konfigurieren.

Kontingente für AWS Transformieren

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. Sofern nicht anders angegeben, gilt für jedes Kontingent Region-specific. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für AWS Transform anzuzeigen, öffnen Sie die [Service Quotas Quotas-Konsole](#). Wählen Sie im Navigationsbereich AWS Dienste und dann AWS Transform aus.

Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent noch nicht unter Service Quotas verfügbar ist, verwenden Sie das [Formular zur Erhöhung des Limits](#).

Ihr AWS Konto hat die folgenden Kontingente für AWS Transform.

Workload	Dimension	Kontingent	Anpassbar	Description
Plattform	Arbeitsbereiche AWS-Region pro AWS Transform aktiviertem Konto	100 Arbeitsbe reiche für jeden unterstützten AWS-Region	Ja	Die maximale Anzahl von Workspaces pro AWS Transform aktiviertem Konto pro AWS- Region
VMware-Mi gration	Anzahl der Server für jede Welle	Jede Welle: 150 Server	Nein	Die maximale Anzahl von Servern in einer Welle
Mainframe	Gleichzeitige Jobs für jedes IAM Identity Center-Konto	10 Jobs für jede unterstützte Region	Ja	Die maximale Anzahl gleichzei tiger Mainframe -Jobs in einem IAM Identity Center-Konto

Workload	Dimension	Kontingent	Anpassbar	Description
	Codezeilen für jeden Job	3.000.000 Codezeilen für jede unterstützte Region	Nein	Die maximale Anzahl von Codezeilen für jeden Job.
	Analysieren Sie die monatlichen Codezeilen	100.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen für das Jobziel „Code analysieren“ in einem Kalendermonat
	Monatliche Codezeilen zur Generierung von Geschäftsdokumenten	50.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen für das Jobziel „Erstellung von Geschäftsdokumenten“ in einem Kalendermonat
	Monatliche Codezeilen für die Erstellung technischer Dokumente	50.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen für das Jobziel „Generierung technischer Dokumentation“ in einem Kalendermonat

Workload	Dimension	Kontingent	Anpassbar	Description
	Transformation von Codezeilen	10.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen, die in einem Kalendermonat transformiert wurden
	Zerlegung monatlicher Codezeilen	50.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen für das Jobziel „Zerlegung“ in einem Kalendermonat
	Forge die monatlichen Codezeilen neu	50.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen für das Reforge-Jobziel in einem Kalendermonat
	Extrahierte monatliche Codezeilen für Geschäftslogik	50.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl von Codezeilen für das Jobziel Extracted Business Logic in einem Kalendermonat

Workload	Dimension	Kontingent	Anpassbar	Description
.NET	.NET-Codezeilen pro Monat (Web und IDE)	1.000.000 Codezeilen für jede unterstützte Region	Ja	Die maximale Anzahl an Zeilen an .NET-Anwendungscode, die in einem Kalendermonat in jedem unterstützten IAM Identity Center-Konto umgewandelt werden können
	Gleichzeitige .NET-Jobs mit der Microsoft Visual Studio-Erweiterung für jedes IAM Identity Center-Konto	10 Jobs für jede unterstützte Region	Ja	Die maximale Anzahl gleichzeitiger .NET-Transformationsaufträge in jedem unterstützten AWS-Region IAM Identity Center-Konto bei Verwendung der Microsoft Visual Studio-Erweiterung.

Workload	Dimension	Kontingent	Anpassbar	Description
	Gleichzeitige .NET-Webjobs für jedes IAM Identity Center-Konto	5 Jobs für jede unterstützte Region	Ja	Die maximale Anzahl gleichzeitiger .NET-Transformationsjobs in jedem unterstützten AWS-Region IAM Identity Center-Konto bei Verwendung der AWS Transform-Web-App.
Benutzerdefinierte Transformationen	Benutzerdefinierte Transformationsdefinitionen	1.000	Ja	Die maximale Anzahl von benutzerdefinierten Transformationsdefinitionen
	Größe der benutzerdefinierten Transformationsdefinition	10 MB	Nein	Die maximale Gesamtgröße aller in der Transformationsdefinition enthaltenen Dateien, einschließlich Dokumentverweise.

Workload	Dimension	Kontingent	Anpassbar	Description
	Monatliche CLI-Konversationsanfragen für benutzerdefinierte Transformation	1 000 000	Ja	Die maximale Anzahl benutzerdefinierter Transformationskonversationsanfragen, die in der CLI gestellt werden, die in einem Kalendermonat zulässig sind
Bewertung	Limit für die Anzahl der Server für jede Bewertung	Jede Bewertung: 30.000 Server	Nein	Die maximale Anzahl von Servern in einem einzelnen Bewertungsauftrag

Unterstützte Regionen für AWS Transform

Note

Wenn Sie eine Anfrage stellen, die AWS Transform den Abruf von Informationen aus einer Region erfordert, die nicht auf dieser Seite aufgeführt ist, AWS Transform können Sie Anrufe in diese Region tätigen. Informationen zur Verwaltung des Zugriffs auf Regionen, in die Sie Anrufe tätigen AWS Transform können, finden Sie unter [Sicherheit bei AWS Transformieren](#).

In diesem Thema wird beschrieben AWS-Regionen , wo Sie Folgendes verwenden können AWS Transform. Weitere Informationen AWS-Regionen dazu finden Sie im AWS -Kontenverwaltung Referenzhandbuch unter [Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann](#).

Ihre Daten werden möglicherweise in einer anderen Region als der Region verarbeitet, in der Sie sie verwenden AWS Transform. Informationen zur regionsübergreifenden Verarbeitung in finden Sie AWS Transform unter [Cross-region Verarbeitung](#). Informationen darüber, wo Daten während der Verarbeitung gespeichert werden, finden Sie unter [Datenschutz](#).

Unterstützt AWS-Regionen (standardmäßig aktiviert)

Im Folgenden AWS-Regionen können Sie AWS Transform Arbeitsbereiche erstellen. Diese Regionen sind standardmäßig aktiviert. Sie müssen sie vor der Verwendung nicht aktivieren. Weitere Informationen erhalten Sie unter [Regionen, die standardmäßig aktiviert sind](#).

- USA Ost (Nord-Virginia)
- Europa (Frankfurt)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Europa (London)
- Asien-Pazifik (Seoul)
- Kanada (Zentral)
- Südamerika (São Paulo) — Nur für Mainframe-Modernisierungsagenten

Der Workspace, in dem Sie einen Job erstellen, bestimmt den AWS-Region Typ des Jobs. Um einen Job in einer anderen Region zu erstellen, müssen Sie einen anderen Workspace verwenden, der sich in Ihrer gewünschten Region befindet.

Bei VMware-Projekten wird die Region des Workspace für die Suche verwendet. Sie können jedoch eine andere Region als Migrationsziel angeben. In dieser Zielregion werden Ihre Workloads gehostet, wenn die Migration abgeschlossen ist. Weitere Informationen zu AWS-Region Überlegungen bei VMware-Migrationen, einschließlich der Liste möglicher Zielregionen, finden Sie unter [the section called “Unterstützte Zielregionen”](#)

AWS Unterstützung für AWS Transform

AWS Transform ermöglicht es Ihnen, AWS Supportanfragen über den Chat zu erstellen und zu verwalten, falls Sie während Ihrer Transformationsjobs auf Probleme stoßen. Ihre Anfragen werden automatisch mit dem Jobkontext angereichert und an das entsprechende Support-Team weitergeleitet. Wenn Sie ein aktiver Countdown Premium-Kunde sind, wird sich Ihr designierter Techniker mit Ihnen in Verbindung setzen, um das Problem zu lösen. Erfahren Sie mehr [AWS unter Countdown Premium](#). Andernfalls wird Ihr Fall vom AWS Transform Support-Team in der Support-Warteschlange untersucht.

Voraussetzungen

Bevor Sie das Support Case Management nutzen können, benötigen Sie:

- Ein aktiver AWS Support-Plan — Business On-Ramp, Enterprise oder Enterprise
- Eine bestehende AWS Transform Anwendung

Support Case Management aktivieren

1. Öffnen Sie die AWS Transform Konsole.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter Support die Option Support-Fallmanagement aktivieren aus.
4. Wählen Sie Änderungen speichern aus.

AWS Transform verwendet eine serviceverknüpfte Rolle (SLR), um Supportfälle in Ihrem Namen zu erstellen und zu verwalten. Es sind keine zusätzlichen IAM-Berechtigungen erforderlich.

Einen Support-Fall erstellen

Verwenden Sie die Chat-Oberfläche, um einen Support-Fall zu erstellen:

1. Bitten Sie darum, einen Support-Fall zu erstellen. Beispiel:
 - „Einen Support-Fall für meinen fehlgeschlagenen Transformationsjob erstellen“
 - „Ich benötige Hilfe bei Jobfehlern, erstellen Sie einen Fall“

2. Im Chat werden Sie zur Eingabe der erforderlichen Informationen aufgefordert:
 - Eine kurze Beschreibung Ihres Problems
 - Eine ausführliche Beschreibung
3. Bestätigen Sie die Erstellung des Falls, wenn Sie dazu aufgefordert werden.

Der Fall wird automatisch mit dem Kontext aus Ihrem Transformationsjob gefüllt, einschließlich:

- Job-ID und Status
- Job-Metadaten
- Protokolle zur Auftragsausführung (Arbeitsprotokolle)
- Stellenplan

Der Fall wird automatisch auf der Grundlage Ihres Jobtyps und Ihrer Problemkategorie zugewiesen.

Supportfälle anzeigen

Rufen Sie den Chat auf, um Ihre Supportfälle einzusehen:

- „Meine Supportfälle auflisten“
- „Zeige mir offene Support-Fälle“
- „Was ist der Status meiner Fälle?“

Im Chat wird Folgendes angezeigt:

- Fall-ID
- Betreff
- Status, z. B. „Offen“, „Ausstehend“, „Gelöst“ oder „Geschlossen“
- Datum der letzten Aktualisierung
- Zugeordnete Job-ID

Um Details zu einem bestimmten Fall einzusehen:

- „Zeige mir Details für den Fall [Case-ID]“
- „Was ist das neueste Update zu Fall [Case-ID]?“

Kommunikation zu einem Fall hinzufügen

Um eine Nachricht zu einem bestehenden Fall hinzuzufügen:

1. Frage an den Chat: „Füge dem Fall [Case-ID] eine Nachricht hinzu“
2. Geben Sie Ihre Nachricht ein, wenn Sie dazu aufgefordert werden.
3. Der Chat bestätigt, dass die Nachricht hinzugefügt wurde.

Sie erhalten Benachrichtigungen, wenn der AWS Support auf Ihren Fall reagiert.

Einen Fall lösen

Um einen Support-Fall zu lösen:

1. Fragen Sie im Chat: „Fall lösen [Fallnummer]“
2. Bestätigen Sie die Lösung, wenn Sie dazu aufgefordert werden.

Note

Sie können nur Fälle lösen, die vom AWS Support bearbeitet wurden.

Support Case Management deaktivieren

1. Öffnen Sie die AWS Transform Konsole.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter Support die Option Support-Fallverwaltung deaktivieren aus.
4. Wählen Sie Änderungen speichern aus.

Note

Durch die Deaktivierung der Support-Fallverwaltung wird die Chat-basierte Oberfläche für die Fallverwaltung entfernt, bestehende Fälle werden jedoch nicht geschlossen. Sie können weiterhin über das AWS Support Center auf Ihre Fälle zugreifen.

Nutzung Telemetrie

Das AWS Transform IDE-Plugin, AWS Transform Agent Skill und AWS Transform Kiro Power erfassen während der Ausführung der Transformation standardmäßig Nutzungstelemetrie. Die Telemetrie besteht aus verschiedenen Datenpunkten, wie dem IDE-Namen (zum Beispiel VS Code oder Kiro), dem Namen des AI-Agenten (zum Beispiel Claude Code oder OpenAI Codex) und dem Ausführungsmodus (lokal oder remote). Diese Daten werden von AWS Transform verwendet, um Kompatibilitätstests sowie Latenz und Zuverlässigkeit zu priorisieren.

Um die Telemetrie zu deaktivieren, teilen Sie dem Agenten während Ihrer Chat-Sitzung mit, dass keine Telemetrie gesendet werden soll. Diese Abmeldung gilt nur für die aktuelle Chat-Sitzung und muss für jede neue Sitzung wiederholt werden. Wenn Sie die AWS Transform-CLI direkt ausführen, legen Sie die `ATX_DISABLE_TELEMETRY=true` Umgebungsvariable fest.

Operative Daten

Wir können betriebliche Signale in Bezug auf Ihre Nutzung von AWS Transform erheben, z. B. welche Funktionen Sie verwenden, Fehlerprotokolle und Kennzahlen auf der Grundlage Ihres Feedbacks in natürlicher Sprache (z. B. ob Sie der Fortführung eines Transformationsplans zugestimmt oder Anweisungen zur Iteration eines vorgeschlagenen Plans gegeben haben), um den Service bereitzustellen und die Serviceleistung zu bewerten.

Änderungsprotokoll

In der folgenden Tabelle werden wichtige Versionen und Updates für AWS Transform beschrieben.

Date	Title	Description	Links
2026-07-16	AWS Transform for Migrations fügt einen herunterladbaren Workspace-Übersichtsbericht hinzu	AWS Mit Transform for Migrations können Sie jetzt einen Workspace-Übersichtsbericht als herunterladbares PDF erstellen . Der Bericht konsolidiert Daten aus allen Migrationsaufträgen in Ihrem Workspace , einschließlich Jobstatus, Fortschritt der Workflow-Schritte, Wellenplanung, Netzwerkmigration, Landezonenkonfiguration, Rehost-Fortschritt und erzeugte Artefakte.	Einen zusammenfassenden Workspace-Bericht wird heruntergeladen
2026-07-03	AWS Das Transform Discovery-Tool fügt Unterstützung für Oracle Database hinzu	Das AWS Transform Discovery Tool sammelt jetzt detaillierte Oracle-Metadaten direkt aus Ihren Datenbanken auf VMware Hyper-V - und Bare-Metal-Servern. Sie können Oracle-Instanzen	Oracle-Datenbankerkennung

Date	Title	Description	Links
		über direkte SQL-Verbindungen erkennen. Das Tool erfasst die Aufzählung der Database/Pluggable Container-Datenbank (CDB/PDB), das Komponenteninventar und die Größenbestimmung von Datendateien. Es erfasst auch Topologie-Flags für Real Application Clusters (RAC), Data Guard und Multitenant-Architekturen. Wenn Sie keine Datenbankanmeldedaten konfiguriert haben, greift das Tool auf OS-level Erkennung zurück. Alle Oracle-Versionen werden unterstützt.	

Date	Title	Description	Links
2026-06-22	Unterstützung für Mainframe-Modernisierungsagenten in der Region Südamerika (São Paulo)	AWS Transform for Mainframe-Modernisierungsagenten ist jetzt in der Region Südamerika (São Paulo) (sa-east-1) verfügbar. sa-east-1 wurde zu unterstützten Regionen und regionsübergreifenden Inferenztabellen hinzugefügt.	Unterstützte Regionen, Inferenz Cross-region
2026-06-22	AWS Transform for VMware-Migrationen unterstützt die Lokalisierung	AWS Transform for VMware-Migrationen unterstützt jetzt Lokalisierung. Sie können die Anzeigesprache der Webanwendung ändern, wenn Sie mit VMware-Migrationsworkflows arbeiten, indem Sie auf das Einstellungssymbol klicken und Ihre bevorzugte Sprache auswählen.	Lokalisierungseinstellungen

Date	Title	Description	Links
2026-06-18	AWS Transform for Migrations unterstützt alle Handelsregionen als Migrationsziele AWS	AWS Transform for VMware-Migrations unterstützt alle AWS Handelsregionen als Migrationsziele, mit Ausnahme des Nahen Ostens (Bahrain) und des Mittleren Ostens (VAE). Eine Migration szielregion ist die AWS Region, in der migrierte Ressourcen bereitgestellt werden, einschließlich Landing Zones, Netzwerkinfrastruktur und Server-Rehosting.	Unterstützte Migration szielregionen

Date	Title	Description	Links
2026-06-18	AWS Mit Transform for Migrations können Sie bestehende ENIs an Ihre Startvorlage anhängen	AWS Mit Transform können Sie bestehende Elastic Network Interfaces (ENIs) an Ihre Startvorlage für Ihre Migration anhängen. AWS Transform zeigt alle vorhandenen ENIs an, die in Ihrem Zielkonto gefunden wurden. Sie können sie taggen, sodass sie beim Start von Instances über die Startkonfiguration verwendet werden können.	ENI-Ressourcen-Tagging für die Migration
2026-06-18	AWS Mit Transform for Migrations können Sie die Replikations- und Starteinstellungen konfigurieren	AWS Mit Transform können Sie Ihre Replikationseinstellungen und Starteinstellungen für Ihre Migration konfigurieren. Sie können die Konfiguration für Ihr Zielkonto oder für bestimmte Quellserv er festlegen.	Einstellungen für Replikation und Start

Date	Title	Description	Links
2026-06-17	Model-to-model Migrationsbewertung für generative KI-Workloads	AWS Transform bietet jetzt eine benutzerdefinierte Transformation für die Migration von Modell zu Modell. Bei der Transformation werden Ihre generativen KI-Workloads bewertet. Es erstellt einen Migrationsplan für den Umstieg von Drittanbietern zu Amazon Bedrock. Der AI-powered Agent scannt Ihre Codebasis, um alle verwendeten KI-SDKs und -Modelle zu identifizieren. Der Agent erfasst die Migrationanforderungen anhand interaktiver Fragen. Anschließend ordnet es Modelle Amazon Bedrock-Äquivalenten zu und bietet transparente Kostenvergleiche und produktionsreife Codeänderungen. Unterstützt Migrationen von OpenAI, Google Gemini,	Was ist neu im Beitrag, Benutzerdefinierte Transformationen

Date	Title	Description	Links
		direkte Nutzung des Anthropic SDK und Open-Source-Modelle über LiteLLM oder Ollama. Verwaltet direkte SDK-Integrationen und Framework-Pattern, einschließlich CrewAI und Routing-Ebenen mit mehreren Anbietern. LangChain LlamaIndex LangGraph Erhältlich ohne zusätzliche Kosten, die über die Standardpreise von Transform hinausgehen. AWS	

Date	Title	Description	Links
2026-06-16	AWS Transform for Mainframe bietet einen nachvollziehbaren, neu konzipierten Arbeitsablauf	AWS Transform for Mainframe bietet jetzt ein vernetztes, rückverfolgbares Neuimagine-Erlebnis von der Bewertung bis zur Codegenerierung. Unternehmen, die z/OS COBOL und PL/I Workloads einsetzen, können ihr Portfolio bewerten, um einzelne Geschäftsfunktionen zu identifizieren, Geschäftsregeln zu extrahieren, entwicklungsreife Anforderungen zu generieren und rückverfolgbaren Cloud-nativen Code in einem einzigen verbundenen Workflow zu erstellen. Jede Anforderung lässt sich auf den Quellcode zurückführen, sodass eine vollständige Überprüfbarkeit gewährleistet ist.	Was ist neu im Beitrag, Dokumentation

Date	Title	Description	Links
2026-06-16	AWS Transform unterstützt jetzt Amazon FSx for NetApp ONTAP als Zielspeicher (Public Preview)	Im Rahmen des Compute-Rehostings können Sie jetzt Blockspeicher-Workloads zusätzlich zu Amazon EBS zu Amazon FSx for NetApp ONTAP migrieren. AWS Transform repliziert Blockspeicherdaten direkt auf FSx für ONTAP-Volumes innerhalb derselben Migrationswelle, die Datenverarbeitung und Netzwerk verarbeitet.	Was ist neu im Beitrag, Dokumentation

Date	Title	Description	Links
2026-06-05	Unterstützung bei der Bewertung der Gesamtbetriebskosten von Amazon RDS for SQL Server	Sie können jetzt die Kosten für die Migration von lokalen SQL Server-Datenbanken zu Amazon RDS for SQL Server abschätzen. Verwenden Sie die AI-powered TCO-Bewertung in AWS Transform, um Ihre Umgebung zu analysieren und Empfehlungen für optimale Datenbank-Instances zu erhalten. Die Bewertung unterstützt die Optionen Bring Your Own Media (BYOM) und License Included (LI) mit Datenbank-Sparplänen für Einsparungen von bis zu 20%	Was ist neu im Beitrag, Dokumentation

Date	Title	Description	Links
2026-06-04	AWS Das Transform Discovery Tool wird jetzt als Eingabequelle für die Netzwerkmigration unterstützt	Sie können das AWS Transform Discovery Tool jetzt zusammen mit ModelizeIT als Quelle für die Netzwerkmigration verwenden und so hybride Netzwerkmigrationen für Umgebungen ermöglichen, in denen sowohl VMware- als auch Nicht-VMware-Workloads ausgeführt werden.	Benutzerhandbuch
2026-05-27	AWS Transformieren Sie die benutzerdefinierte Dokumentation und fügt Beispiele für Fähigkeiten und bewährte Verfahren auf Kundenseite hinzu	Die Dokumentation zu den Fähigkeiten auf Kundenseite enthält jetzt praktische Beispiele für Dockerfile-Compliance, Sicherheit bei der Datenbankmigration, Durchsetzung von Terraform-Richtlinien und API-Deprecation-Helfern sowie bewährte Methoden für den Aufbau und die gemeinsame Nutzung von Fähigkeiten.	Dokumentation

Date	Title	Description	Links
2026-05-22	Neue Funktionen zur Bewertung der Migration durch Agenturen sind jetzt mit Transform verfügbar AWS	AWS Transform bietet jetzt erweiterte Funktionen zur Migrationsbewertung, darunter Was-wäre-wenn-Szenarien, anpassbare Annahmen, flexible Dateiformatunterstützung und mehrere neue Funktionen zur Bewertung der Gesamtbetriebskosten (TCO).	Was ist neu im Beitrag, Dokumentation
2026-05-20	AWS Transform erkennt bestehende VPCs bei der Überprüfung der Netzwerkmigration	AWS Transform erkennt jetzt bei der Überprüfung der Netzwerkmigration vorhandene VPCs in Ihrem Zielkonto. Sie können vorhandene VPCs neben Ihren zugewiesenen VPCs sehen, CIDR-Konflikte identifizieren und diese vor der Bereitstellung lösen.	Dokumentation

Date	Title	Description	Links
2026-05-14	AWS Transformationsagenten sind jetzt in Kiro, Claude, Cursor und Codex verfügbar	AWS Transformationsagenten sind jetzt über eine Kiro Power, Agent-Plugins und den AWS Transform MCP-Server zugänglich, sodass Entwickler Transformationsfunktionen direkt von ihrer bevorzugten Entwicklungsumgebung aus nutzen können.	Was ist ein neuer Beitrag
2026-05-14	AWS Transform führt das Agent Builder-Toolkit zum Erstellen maßgeschneiderter Transformationsagenten ein	Partner und Kunden können jetzt mithilfe des Agent Builder-Toolkits Kiro Power spezialisierte Transformationsagenten erstellen, gemeinsam nutzen und registrieren. Dabei werden benutzerdefinierte Tools und Workflows in Transform integriert. AWS	Was ist ein neuer Beitrag

Date	Title	Description	Links
2026-05-14	AWS Transform erweitert das AWS Toolkit for Visual Studio um einen agentischen KI-Assistenten	.NET-Entwickler können Anwendungen jetzt direkt in Visual Studio mithilfe einer Konversation, die Schritt für Schritt geführt wird, modernisieren, wobei der gesamte Kontext in IDE und Webkonsole erhalten bleibt.	Was ist ein neuer Beitrag
2026-05-14	AWS Transform unterstützt jetzt kundeneigene Artefaktläden	Sie können Ihren eigenen Amazon S3 S3-Bucket konfigurieren und optional Artefakte mit Ihrem eigenen AWS KMS-Schlüssel verschlüsseln, sodass Sie die volle Kontrolle darüber haben, wo Transformationsartefakte gespeichert werden.	Was ist neu im Beitrag , Benutzerhandbuch

Date	Title	Description	Links
2026-05-14	AWS Transform fügt Empfehlungen zur Migrationsstrategie (7Rs) hinzu	Mit AWS Transform können Sie jetzt Ihr entdecktes Inventar analysieren und eine Empfehlung zur Migrationsstrategie für jeden Server und jede Anwendung erhalten. Die Empfehlungen folgen den sieben branchenüblichen Migrationsstrategien (7Rs). Jede Empfehlung beinhaltet eine vorgeschlagene AWS Zieldienstleistung, einen Vertrauenswert und die Begründung dafür. Sie können ein interaktives HTML-Dashboard, eine PDF- oder PowerPoint Microsoft-Ausgabe generieren.	Empfehlungen von 7R

Date	Title	Description	Links
2026-05-11	AWS Transform fügt Containerisierungsfunktionen bei Migrationen hinzu	AWS Transform unterstützt jetzt die Umstellung von Anwendungen auf Container während der Migration, die Automatisierung der Dockerfile-Generierung, die Erstellung von Container-Images mit CVE-Scanning und die Bereitstellung auf Amazon ECS oder Amazon EKS.	Beitrag „Was ist neu“, Benutzerhandbuch
2026-05-01	AWS Transform bietet jetzt BI-Migrationsagenten für Power BI und Tableau to Quick	Partner-built Agenten von Wavicle Data Solutions konvertieren Power BI- und Tableau-Dashboards innerhalb des AWS Transform-Workflows in Quick-Assets.	Was ist ein neuer Beitrag
2026-04-21	AWS Transform Custom ist jetzt in sechs weiteren Regionen verfügbar AWS	AWS Transform Custom expandiert nach Asien-Pazifik, Kanada und Europa (London) und erreicht insgesamt acht AWS Regionen.	Was ist ein neuer Beitrag

Date	Title	Description	Links
2026-04-15	AWS Transform fügt die Erstellung von landing zone in Migrationsworkflows hinzu	Die Erstellung von Landezonen wurde direkt in den Migrationsworkflows hinzugefügt. AWS Transform prüft auf eine bestehende Grundlage, empfiehlt Strukturen und Zielkonten von Organisationseinheiten (OU) und bietet vollautomatische Bereitstellung oder IaC-Ausgabe (Infrastructure as Code) (CloudFormation, AWS CDK- oder Landing Zone Accelerator (LZA) - Formate).	Was ist neu im Beitrag, Dokumentation

Date	Title	Description	Links
2026-04-15	AWS Transform fügt Diagramme und Berichte zur Migrationssplanunng hinzu	Sie können jetzt während der Migrationssplanunng interaktive Diagramme und Analyseberichte erstellen. Zu den Diagrammtypen gehören Netzwerktopologiekarten, Anwendungsabhängigkeitsdiagramme, Wellen-Gantt-Diagramme und allgemeine Diagramme. Zu den Berichtstypen gehören Risikobewertungen, 7R-Empfehlungen und benutzerdefinierte Analyseberichte. Die Ausgaben sind als interaktive HTML-, PDF- oder Microsoft-Dateien PowerPoint (.pptx) verfügbar.	Diagrammerstellung und Berichterstattung

Date	Title	Description	Links
2026-04-14	AWS Transform ist jetzt in Kiro und VS Code verfügbar	AWS Benutzerdefinierte Transformationen sind jetzt von Kiro und VS Code aus zugänglich, wobei der Jobstatus von IDE-, CLI- und Webkonsolenoberflächen gemeinsam genutzt wird.	Was ist ein neuer Beitrag
2026-04-10	AWS Transform fügt DHCP mit Sicherheitsgruppenzuweisung für die Netzwerkmigration hinzu	Unterstützung für DHCP mit Sicherheitsgruppenzuweisung während der Netzwerkmigration hinzugefügt. Wenn Sie DHCP-enabled Migrations-Workloads haben, können Sie jetzt sicherstellen, dass Ihre Sicherheitsregeln auch nach der Migration gültig bleiben. Dies gilt sowohl für interne VPC-Sicherheitsgruppenreferenzen als auch für vPC- und kontoübergreifende Regeln für ausgehenden Datenverkehr über Transit Gateway.	Dokumentation

Date	Title	Description	Links
2026-03-31	AWS Transform Custom kündigt die allgemeine Verfügbarkeit der automatisierten Codebase-Analyse an	Die umfassende Transformation der Codebase-Analyse erreicht allgemeine Verfügbarkeit und generiert Architekturdokumente, technische Schuldenberichte und Modernisierungsempfehlungen in allen Sprachen.	Was ist ein neuer Beitrag
2026-03-31	AWS Transform Custom führt neue verwaltete Transformationen ein, um Code in großem Maßstab zu modernisieren	Sieben neue verwaltete Transformationen wurden hinzugefügt, darunter Node.js Upgrades (allgemeine Verfügbarkeit), Java-Optimierung, Log4j-Migration Angular-to-React, Angular Upgrades und Vue Upgrades (Early Access).	Was ist ein neuer Beitrag
2026-03-20	AWS Transform fügt öffentliche APIs für die Netzwerkmigration hinzu	Öffentliche APIs für die Netzwerkmigration wurden hinzugefügt, sodass Partner- und programmatischen Zugriff auf Netzwerk migrationsfunktionen erhalten.	API Reference

Date	Title	Description	Links
2026-01-14	AWS Transform Custom fügt AWS PrivateLink Unterstützung hinzu und expandiert nach Europa (Frankfurt)	AWS Transform Custom unterstützt jetzt privaten VPC-Zugriff über AWS PrivateLink und ist in Europa (Frankfurt) sowie in USA Ost (Nord-Virginia) verfügbar.	Was ist ein neuer Beitrag
2025-12-23	AWS Transform ermöglicht Netzwerkkonvertierung für Migrationen hybrider Rechenzentren	AWS Transform for VMware konvertiert automatisch Netzwerkkonfigurationen (VLANs, IP-Bereiche) in Hybrid-Rechenzentren in AWS VPCs, Subnetze und Sicherheitsgruppen ohne manuelle Zuordnung.	Was ist ein neuer Beitrag
2025-12-01	AWS führt AWS Transform Custom ein, um die unternehmensweite Modernisierung zu beschleunigen	AWS Transform Custom ist jetzt allgemein verfügbar und ermöglicht es Unternehmen, wiederholbare Codetransformationen in großem Umfang über einen einzigen CLI-Befehl zu automatisieren.	Was ist ein neuer Beitrag

Date	Title	Description	Links
2025-12-01	AWS Transform fügt neue agentische KI-Funktionen für VMware-Migrationen in Unternehmen hinzu	AWS Der VMware-Agent von Transform kann jetzt lokale Umgebungen erkennen, Abhängigkeiten zuordnen, Migrationswellenpläne erstellen und zwischen HyperV-, Nutanix-, KVM- und Bare-Metal-Zielen migrieren.	Was ist ein neuer Beitrag
2025-12-01	AWS Transform bringt einen KI-Agenten für die vollständige Windows-Modernisierung auf den Markt	Ein neuer Full-Stack-Windows-Agent automatisiert die Transformation von .NET-Apps und SQL Server-Datenbanken nach Aurora PostgreSQL und wird in Containern auf Amazon ECS oder EC2 Linux bereitgestellt.	Was ist ein neuer Beitrag
2025-12-01	AWS Transform erweitert die Möglichkeiten der .NET-Transformation und verbessert das Entwicklererlebnis	AWS Transform fügt Unterstützung für .NET 10, ASP.NET Web Forms zur Blazor-Portierung und ein verbessertes interaktives IDE-Erlebnis über AWS Toolkit for Visual Studio hinzu.	Was ist ein neuer Beitrag

Date	Title	Description	Links
2025-12-01	AWS Transform for Mainframe bietet neue Funktionen zur Testautomatisierung	AWS Transform for Mainframe führt automatisierte Testplangenerierung, Testdatenerfassung sskripts und Testfalla utomatisierung ein, um das Testen der Mainframe-Modernis ierung zu beschleun igen.	Was ist ein neuer Beitrag
2025-12-01	AWS Transform for Mainframe unterstüt zt jetzt die Neugestalt ung von Anwendung en	Neue Daten- und Aktivitätsanalysen sowie Funktione n zur Extraktion von Geschäftslogik ermöglichen die Zerlegung älterer Mainframe-Anwendun gen in cloudnative Architekturen.	Was ist ein neuer Beitrag
2025-11-13	AWS Transform automatisiert die Netzwerkkonfiguratio n von Landing Zone Accelerator	AWS Transform for VMware generiert automatisch LZA-compatible Netzwerk-YAML-Dateien und optimiert so die Einrichtung der Cloud-Infrastruktur für mehrere Konten in VMware-Um gebungen.	Was ist ein neuer Beitrag

Date	Title	Description	Links
2025-07-16	AWS Transform for Mainframe bietet erweiterte Funktionen für Code-Refactoring und Geschäftslogik	AWS Transform for Mainframe bietet die allgemeine Verfügbarkeit von Reforge (Code-Restrukturierung) und erweitert die Extraktion von Geschäftslogik auf Anwendungsebene, um die Codequalität zu verbessern.	Was ist ein neuer Beitrag
15.05.2025	AWS Transform for VMware ist jetzt allgemein verfügbar	AWS Transform for VMware, ein agentischer KI-Service, der den gesamten Modernisierungszyklus von VMware von der Entdeckung bis zur Bereitstellung automatisiert, ist jetzt allgemein verfügbar.	Was ist ein neuer Beitrag

Date	Title	Description	Links
15.05.2025	AWS Transform for Mainframe ist jetzt allgemein verfügbar	AWS Transform for Mainframe, der erste agentische KI-Service für die Modernisierung von IBM z/OS Anwendungen im großen Maßstab, ist jetzt mit neuen Funktionen für Analyse, Zerlegung und Auftragsverwaltung allgemein verfügbar.	Was ist ein neuer Beitrag

[Laden Sie diese Daten](#) herunter.

Dokumentenhistorie für die AWS Transform-Benutzerhandbuch

In der folgenden Tabelle wird der Dokumentverlauf für das AWS Transform-Benutzerhandbuch beschrieben.

Änderung	Beschreibung	Datum
Kontinuierliche Modernisierung, Portfolioanalyse und Problembehebung	Es wurde ein neues Kapitel hinzugefügt, das die Funktion „Kontinuierliche Modernisierung AWS transformieren“ (atx ctUnterbefehle) zur automatisierten Codeanalyse und -behebung dokumentiert. Siehe Kontinuierliche Modernisierung.	3. Juni 2026
Brownfield-Netzwerk: Sichtbarkeit vorhandener VPCs	Bestehende VPC-Erkennung während der Überprüfung der Netzwerkmigration hinzugefügt. AWS Transform erkennt automatisch VPCs, die bereits in Ihrem Zielkonto bereitgestellt sind, und kennzeichnet CIDR-Konflikte mit Ihren zugewiesenen VPCs. Sehen Sie sich Vorhandene VPCs in Ihrem Zielkonto an.	18. Mai 2026
Das Skills-Format, clientseitige Skills und Subagent-Logs für Transform Custom wurden hinzugefügt AWS	Transformationsdefinitionen verwenden jetzt das Skills-Format (SKILL.md mit YAML-Frontmatter und optionalem Ordner). <code>reference</code> s/ Es wurden clientseitige	11. Mai 2026

Fähigkeiten hinzugefügt, um den Agenten um zusätzliche Funktionen zu erweitern, und Subagent-Logs für ein verbessertes Debugging. Erfordert CLI Version 2.0 oder höher. Weitere Informationen finden Sie unter [Definitionen und Client-Side Fähigkeiten zur Transformation](#).

[Containerisierung des Quellcodes hinzugefügt](#)

AWS Transform kann Ihre Anwendungen jetzt mithilfe generativer KI containerisieren. Stellen Sie Ihren Quellcode aus Git-Repositories oder Zip-Uploads bereit, und AWS Transform analysiert ihn, generiert Docker-Artefakte, veröffentlicht Container-Images in Amazon ECR, generiert Infrastruktur als Code und stellt ihn auf Amazon Elastic Container Service oder Amazon Elastic Kubernetes Service bereit. Siehe [Containerisierung des Quellcodes](#).

7. Mai 2026

[Es wurden Netzwerkoptimierungsoperationen und Empfehlungen hinzugefügt](#)

Schritt 5 hinzugefügt: Überprüfung und Optimierung des Netzwerks mit VPC- und Subnetzoperationen (Löschen, Ausschließen, Zusammenführen, Teilen, Ändern der Größe, Umbenennen, IP-Adresse ändern) und Empfehlungen für Benennungssstandardisierung, Überprüfung des Umfangs, Anpassung der Kapazität, Sicherheitsüberprüfung und VPC-Konsolidierung. [Weitere Informationen finden Sie unter Überprüfen und Optimieren des Netzwerks.](#)

27. April 2026

[AWS Transform Custom ist in 6 neuen Regionen verfügbar](#)

[Unterstützung für ca-central-1, eu-west-2, ap-northeast-1, ap-northeast-2, ap-southeast-2 und ap-south-1 in Transform custom hinzugefügt.](#)[AWS](#)

21. April 2026

[Die Dokumentation zu Konnektorberechtigungen wurde aktualisiert](#)

Es wurde eine detaillierte Aufschlüsselung der Berechtigungen für den AWS-Konto Ziel-Connector hinzugefügt, die S3-, MGN-, Migration Hub Hub-Berechtigungen, Workload-Migration und Bereitstellung der Landingzone-Infrastruktur abdeckt. Siehe [Ziele AWS-Konto Connect.](#)

19. April 2026

Die Jobtypen für die VMware-Migration wurden aktualisiert

Die Jobtypen Discovery und Migrationsplanung, Landing Zone und Landing Zone, Netzwerk und Servermigration wurden hinzugefügt. Umbenannt in „Nur Netzwerkmigration“ in „Netzwerkmigration und Migrationsplanung“ in „Migrationsplan erstellen“. Weitere Informationen finden Sie unter [Jobtypen für die VMware-Migration](#).

19. April 2026

Restrukturiertes Connect-Ziels AWS-Konto

Das Connector-Setup wurde in drei Schritte umstrukturiert: Auswahl des Migrationstyps, MAP-Vereinbarung und Connector-Konfiguration, einschließlich unterstützter Zielregionen, Kontorollen, delegierter Administratorführung und IAM-Rollen. Siehe [Ziele AWS-Konto Connect](#).

19. April 2026

Es wurden zusätzliche Zielregionen hinzugefügt, die nur für Servermigrationen bestimmt sind

Es wurden 14 weitere kommerzielle Regionen dokumentiert, die für Servermigrationsaufträge ohne Netzwerkmigration verfügbar sind, wobei bis zum 3. Quartal 2026 eine Zulassungsliste erforderlich ist. [Siehe Unterstützte Zielregionen](#).

19. April 2026

<u>Das Kapitel Server migrieren wurde hinzugefügt</u>	Es wurde ein neues Kapitel mit <u>Migrate-Servern</u> hinzugefügt, das den vollständigen Rehost-Workflow behandelt, einschließlich Kontostruktur, IAM-Rollen, Einrichtung delegierter Administratoren, Bereitstellung, Testen und Umstellung von Replikationsagenten.	19. April 2026
<u>Kapitel landing zone bauen hinzugefügt</u>	Es wurde ein neues Kapitel „ <u>landing zone erstellen</u> “ mit Details zu den Connector-Berechtigungen für die Bereitstellung von landing zone hinzugefügt.	19. April 2026
<u>Zuordnung und Referenzierung von Sicherheitsgruppen</u>	<u>Strategien zur Zuordnung von Sicherheitsgruppen (MAP, MAP_DHCP, SKIP) und Dokumentation zur Referenzierung von Sicherheitsgruppen wurden dem Migrate-Netzwerk hinzugefügt.</u>	13. April 2026
<u>Auto-conversion für nicht unterstützte Netzwerkdateitypen</u>	Unterstützung für die automatische Konvertierung von nicht unterstützten Netzwerkkonfigurationsdateitypen im <u>Migrate-Netzwerk</u> hinzugefügt.	6. April 2026
<u>KMS-Schlüsselrichtlinie für die Datenbankmigration hinzugefügt</u>	Der Abschnitt <u>Verschlüsselung für die Datenbankmigration</u> wurde hinzugefügt.	26. März 2026

Dokumentierte neue AWS verwaltete Richtlinie	DBModProvisioningAndMigration Abschnitt hinzugefügt.	24. März 2026
Dokumentierte neue AWS verwaltete Richtlinie	DBModDiscoveryAndAssessment Abschnitt hinzugefügt.	24. März 2026
Generierung von Netzwerkdiagrammen	Optionale Generierung von Netzwerkdiagrammen (Meerjungfrau- und PNG-Formate) zum Migrate-Netzwerk hinzugefügt.	18. März 2026
Unterstützung für Firewall- und SDN-Konfigurationsdateien	Unterstützung für Palo Alto Networks-, Fortinet FortiGate - und Cisco ACI-Konfigurationsdateien für die Netzwerkmigration im Migrate-Netzwerk hinzugefügt.	11. Februar 2026
Benutzerdefiniertes Tagging für Netzwerkressourcen	Unterstützung für Tagging auf Jobebene und VPC-level benutzerdefiniertes Tagging für die Netzwerkmigration im Migrate-Netzwerk hinzugefügt.	28. Januar 2026
Support-Dokumentation hinzugefügt	AWS Unterstützung für Abschnitt hinzugefügt.	23. Dezember 2025
Dokumentierte neue AWS verwaltete Richtlinien	AWSTransformCustomManageTransformations Abschnitte AWSTransformCustomFullAccess AWSTransformCustomExecuteTransformations , und hinzugefügt.	7. Dezember 2025

VMware-Migration	Der Abschnitt zur VMware-Migration wurde aktualisiert.	1. Dezember 2025
Die AWS verwaltete Richtlinie wurde aktualisiert	Die AWSServiceRoleForAWSTransform Dokumentation wurde aktualisiert, um die hinzugefügten Berechtigungen widerzuspiegeln.	1. Dezember 2025
Unterstützte Regionen	Das Thema Unterstützte Regionen wurde aktualisiert.	1. Dezember 2025
Mainframe-Modernisierung	Der Abschnitt zur Mainframe-Modernisierung wurde aktualisiert.	1. Dezember 2025
Erste Schritte	Das Thema Erste Schritte wurde aktualisiert.	1. Dezember 2025
Full-stack Windows-Modernisierung	Das Thema Full-stack Windows-Modernisierung wurde hinzugefügt, das den aktualisierten.NET-Abschnitt und den neuen Abschnitt zur SQL Server-Modernisierung umfasst.	1. Dezember 2025
Tool zur Entdeckung	Der Abschnitt mit dem Discovery-Tool wurde hinzugefügt.	1. Dezember 2025

Die AWS verwaltete Richtlinie wurde aktualisiert	Die wurde AWSTransformApplicationECSEmploymentPolicy mit erweiterten IAM-Rolleninspektionsberechtigungen, der Erstellung von ECS-serververknüpften Rollen und KMS-Berechtigungen für die Unterstützung der ECR-Verschlüsselung aktualisiert.	22. November 2025
Die AWS verwaltete Richtlinie wurde aktualisiert	Das wurde AWSTransformApplicationDeploymentPolicy mit zusätzlichen EC2-Netzwerken, IAM-Rolleninspektion, S3-Bucket-Verwaltung und KMS-Verschlüsselungsberechtigungen aktualisiert.	22. November 2025
Entdeckungssammler	Die Dokumentation zum AWS Transform Discovery Tool wurde hinzugefügt.	31. Oktober 2025
Diagramm zur VMware-Migrationsarchitektur hinzugefügt	Ein Diagramm der VMware-Migrationsarchitektur wurde im Migrate-Netzwerk hinzugefügt.	23. Oktober 2025
Aktualisierung der VMware-Migrationsergebnisse	Die Informationen zu den Migrationsergebnissen wurden im Migrate-Netzwerk aktualisiert.	12. Oktober 2025
Aktualisierung der VMware-Migrationsergebnisse	Die Informationen zu den Migrationsergebnissen wurden im Migrate-Netzwerk aktualisiert.	12. Oktober 2025

Dokumentation zum S3-Anschluss	Die Dokumentation zum S3-Connector für die .NET-Web-App wurde hinzugefügt.	8. Oktober 2025
Neues Thema für Benutzerkonnektoren	Thema Benutzerkonnektoren hinzugefügt.	21. September 2025
Die AWS verwaltete Richtlinie wurde aktualisiert	Die AWSServiceRoleForAWSTransform Dokumentation wurde aktualisiert.	17. September 2025
Unterstützung bei der Speicherbewertung	Unterstützung für NetApp Data Infrastructure Insights (DII) -Dateien für Speicherbewertungen hinzugefügt.	2. September 2025
Aktualisierung der Zielregionen	Drei unterstützte Zielregionen wurden hinzugefügt.	31. August 2025
Aktualisierung der verwalteten Richtlinien	Es wurden Leseberechtigungen für IAM Identity Center hinzugefügt, die von AWSServiceRoleForAWSTransform	29. August 2025
Dokumentierte neue AWS verwaltete Richtlinie	AWSTransformApplicationDeploymentPolicy Abschnitt hinzugefügt.	28. August 2025
Schnittstellen-Endpunkte	Das Thema Schnittstellenendpunkte wurde hinzugefügt.	9. Juli 2025
Erstversion	Erste Version des AWS Transform-Benutzerhandbuchs.	15. Mai 2025

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.