Application Load Balancer

Elastic Load Balancing

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

Elastic Load Balancing: Application Load Balancer

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

Die Handelsmarken und 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 ein Application Load Balancer? ... 1
Application-Load-Balancer-Komponenten ... 1
Application Load Balancer – Übersicht ... 2
Vorteile der Migration von einem Classic Load Balancer ... 3
Zugehörige Services ... 4
Preisgestaltung ... 5
Erste Schritte ... 6
Bevor Sie beginnen ... 6
Schritt 1: Konfigurieren Ihrer Zielgruppe ... 6
Schritt 2: Wählen eines Load Balancer-Typs ... 7
Schritt 3: Konfigurieren Ihres Load Balancers und Listeners ... 8
Schritt 4: Testen Ihres Load Balancers ... 9
Schritt 5: Löschen Ihres Load Balancers (optional) ... 9
Erste Schritte mit dem AWS CLI ... 11
Bevor Sie beginnen ... 11
Erstellen Ihres Load Balancers ... 12
Hinzufügen eines HTTPS-Listeners ... 13
Hinzufügen von pfadbasierter Weiterleitung ... 14
Löschen des Load Balancers ... 15
Application Load Balancer ... 16
Subnetze für Ihren Load Balancer ... 17
Availability-Zone-Subnetze ... 17
Local-Zone-Subnetze ... 18
Outpost-Subnetze ... 18
Load-Balancer-Sicherheitsgruppen ... 20
Load Balancer-Status ... 20
Load Balancer-Attribute ... 21
IP-Adresstyp ... 23
IPAM-IP-Adresspools ... 24
Load Balancer-Verbindungen ... 25
Zonenübergreifendes Load Balancing ... 26
DNS-Name ... 26
Erstellen eines Load Balancers ... 27
Schritt 1: Konfigurieren einer Zielgruppe ... 6

Schritt 2: Registrieren von Zielen ... 29
Schritt 3: Konfigurieren von Load Balancer und Listener ... 30
Schritt 4: Testen des Load Balancers ... 9
Aktualisieren von Availability Zones ... 35
Aktualisieren von Sicherheitsgruppen ... 36
Empfohlene Regeln ... 36
Aktualisieren der zugeordneten Sicherheitsgruppen ... 39
Aktualisieren Sie den IP-Adresstyp ... 39
Aktualisieren Sie die IPAM-IP-Adresspools ... 40
Load Balancer-Integrationen ... 41
Amazon Application Recovery Controller (ARC) ... 41
Amazon CloudFront + AWS WAF ... 44
AWS Global Accelerator ... 45
AWS Config ... 45
AWS WAF ... 45
Bearbeiten Sie die Load Balancer-Attribute ... 46
Zeitlimit für Verbindungsleerlauf ... 46
Keepalive-Dauer des HTTP-Clients ... 47
Löschschutz ... 49
Desynchroner Mitigationsmodus ... 50
Beibehalten der Host-Header ... 52
Kennzeichnen Sie einen Load Balancer ... 54
Löschen eines -Load Balancers ... 56
Sehen Sie sich die Ressourcenübersicht an ... 57
Komponenten der Ressourcenübersicht ... 57
LCU-Reservierungen ... 58
Reservierung anfragen ... 60
Reservierung aktualisieren oder beenden ... 61
Überwachen Sie die Reservierung ... 62
Listener und Regeln ... 64
Listener-Konfiguration ... 64
Listener-Attribute ... 66
Listener-Regeln ... 68
Standardregeln ... 68
Priorität der Regel ... 68
Regelaktionen ... 68

Regelbedingungen ... 68
Regelaktionstypen ... 69
Aktionen mit feststehender Antwort ... 69
Weiterleitungsaktionen ... 70
Weiterleitungsaktionen ... 73
Regelbedingungstypen ... 77
HTTP-Header-Bedingungen ... 78
Bedingungen für HTTP-Anforderungsmethoden ... 79
Hostbedingungen ... 80
Pfadbedingungen ... 81
Abfragezeichenfolgebedingungen ... 82
Bedingungen für die Quell-IP-Adresse ... 83
X-Forwarded-Header ... 84
X-Forwarded-For ... 84
X-Forwarded-Proto ... 88
X-Forwarded-Port ... 88
Erstellen eines HTTP-Listeners ... 89
Voraussetzungen ... 89
Hinzufügen eines HTTP-Listeners ... 89
SSL-Zertifikate ... 90
Standardzertifikat ... 91
Zertifikatliste ... 92
Zertifikatserneuerung ... 92
Sicherheitsrichtlinien ... 93
TLS-Sicherheitsrichtlinien ... 95
FIPS-Sicherheitsrichtlinien ... 122
Von FS unterstützte Richtlinien ... 137
Erstellen eines HTTPS-Listeners ... 143
Voraussetzungen ... 144
Hinzufügen eines HTTPS-Listeners ... 144
Aktualisieren von Listener-Regeln ... 146
Voraussetzungen ... 147
Hinzufügen einer Regel ... 147
Bearbeiten einer Regel ... 150
Ändern der Reihenfolge von Regeln ... 151
Löschen einer Regel ... 152

Aktualisieren eines HTTPS-Listeners ... 152
Ersetzen des Standardzertifikats ... 153
Hinzufügen von Zertifikaten zu einer Zertifikatliste ... 153
Entfernen eines Zertifikats aus der Zertifikatliste ... 154
Aktualisieren der Sicherheitsrichtlinie ... 155
Änderung des HTTP-Headers ... 156
Gegenseitige TLS-Authentifizierung ... 156
Bevor Sie beginnen ... 157
HTTP-Header ... 160
Geben Sie den Namen des CA-Antragstellers bekannt ... 162
Verbindungsprotokolle. ... 163
Gegenseitiges TLS konfigurieren ... 163
Teilen Sie einen Trust Store ... 169
Konfigurieren der Benutzerauthentifizierung ... 174
Vorbereiten der Nutzung eines OIDC-konformen Identitätsanbieters ... 175
Vorbereitung für die Verwendung von Amazon Cognito ... 175
Bereiten Sie sich auf die Nutzung von Amazon vor CloudFront ... 178
Konfigurieren der Benutzerauthentifizierung ... 178
Authentifizierungsfluss ... 181
Codierung von Benutzeransprüchen und Signaturverifizierung ... 184
Zeitüberschreitung ... 186
Authentifizierung und Abmeldung ... 187
Kennzeichnen Sie einen Listener ... 188
Aktualisieren der Listener-Tags ... 188
Aktualisieren von Regel-Tags ... 189
Löschen eines Listeners ... 190
Änderung des Headers ... 191
mTLS/TLS Header umbenennen ... 191
Fügen Sie Antwort-Header hinzu ... 193
Header deaktivieren ... 195
Einschränkungen ... 195
Aktivieren Sie die Header-Änderung ... 196
Zielgruppen ... 199
Weiterleitungskonfiguration ... 200
Zieltyp ... 201
IP-Adresstyp ... 202

Protokollversion 203
Registrierte Ziele 205
Zielgruppenattribute 206
Routing-Algorithmen 208
Ändern Sie den Routing-Algorithmus einer Zielgruppe 209
Zustand der Zielgruppe 210
Maßnahmen bei fehlerhaftem Zustand 210
Anforderungen und Überlegungen 211
Überwachen 212
Beispiel 212
Verwenden des Route-53-DNS-Failover für Ihren Load Balancer 214
Erstellen einer Zielgruppe 215
Aktualisieren Sie die Gesundheitseinstellungen 217
Konfigurieren von Zustandsprüfungen 218
Zustandsprüfungseinstellungen 219
Zustandsstatus des Ziels 222
Ursachencodes für Zustandsprüfungen 224
Überprüfen Sie den Zustand Ihres Ziels 225
Aktualisieren Sie die Einstellungen für die Integritätsprüfung 226
Zielgruppenattribute bearbeiten 226
Verzögerung der Registrierungsaufhebung 227
Modus des langsamen Hochfahrens 228
Zonenübergreifendes Load Balancing 229
Automatische Zielgewichte (ATW) 232
Sticky Sessions 236
Ziele registrieren 243
Zielsicherheitsgruppen 244
Gemeinsam genutzte Subnetze 245
Registrieren oder Aufheben der Registrierung von Zielen 245
Verwenden Sie Lambda-Funktionen als Ziele 248
Vorbereiten der Lambda-Funktion 249
Erstellen Sie einer Zielgruppe für die Lambda-Funktion 247
Empfangen von Ereignissen vom Load Balancer 251
Antwort an den Load Balancer 252
Header mit mehreren Werten 253
Aktivieren von Zustandsprüfungen 256

Aufheben der Registrierung der Lambda-Funktion ... 257
Taggen Sie eine Zielgruppe ... 258
Löschen einer Zielgruppe ... 259
Überwachen Ihrer Load Balancers ... 260
CloudWatch Metriken ... 261
Application-Load-Balancer-Metriken ... 262
Metrik-Dimensionen für Application Load Balancer ... 285
Statistiken für Application-Load-Balancer-Metriken ... 285
CloudWatch Metriken für Ihren Load Balancer anzeigen ... 287
Zugriffsprotokolle ... 289
Zugriffsprotokolldateien ... 290
Zugriffsprotokolleinträge ... 292
Beispiel-Protokolleinträge ... 308
Verarbeiten von Zugriffsprotokolldateien ... 310
Aktivieren der Zugriffsprotokolle ... 311
Deaktivieren der Zugriffsprotokolle ... 322
Verbindungsprotokolle. ... 323
Verbindungsprotokolldateien ... 323
Verbindungsprotokolleinträge ... 325
Beispiel-Protokolleinträge ... 329
Verbindungsprotokolldateien werden verarbeitet ... 329
Aktivieren Sie Verbindungsprotokolle ... 330
Deaktivieren Sie die Verbindungsprotokolle ... 340
Anfragenachverfolgung ... 341
Syntax ... 341
Einschränkungen ... 342
Fehlerbehebung bei Ihren Load Balancern ... 343
Ein registriertes Ziel ist nicht in Betrieb ... 343
Clients können keine Verbindung zu einem mit dem Internet verbundenen Load Balancer herstellen ... 345
Anfragen, die an eine benutzerdefinierte Domain gesendet werden, werden vom Load Balancer nicht empfangen ... 345
An den Load Balancer gesendete HTTPS-Anfragen geben „NET::ERR_CERT_COMMON_NAME_INVALID“ zurück ... 346
Der Load Balancer zeigt erhöhte Verarbeitungszeiten an ... 346
Der Load Balancer sendet als Antwortcode „000“. ... 347

Der Load Balancer generiert einen HTTP-Fehler 347
HTTP 400: Schlechte Anfrage 348
HTTP 401: Unauthorized (Nicht autorisiert) 348
HTTP 403: Forbidden (Verboten) 348
HTTP 405: Methode nicht erlaubt 348
HTTP 408: Anfrage-Timeout 349
HTTP 413: Nutzlast zu hoch 349
HTTP 414: URI zu lang 349
HTTP 460 349
HTTP 463 349
HTTP 464 349
HTTP 500: Interner Serverfehler 350
HTTP 501: Nicht implementiert 350
HTTP 502: Schlechtes Gateway 350
HTTP 503: Service Unavailable 351
HTTP 504: Gateway-Timeout 351
HTTP 505: Version wird nicht unterstützt 352
HTTP 507: Nicht genügend Speicherplatz 352
HTTP 561: Unauthorized (Nicht autorisiert) 352
Ein Ziel generiert einen HTTP-Fehler 352
Ein AWS Certificate Manager Zertifikat steht nicht zur Verwendung zur Verfügung 353
Header mit mehreren Zeilen werden nicht unterstützt 353
Beheben Sie fehlerhafte Ziele mithilfe der Ressourcenübersicht 353
Kontingente 356
Load Balancers 356
Zielgruppen 357
Regeln 357
Vertraue Geschäften 358
Zertifikate 358
HTTP-Header 359
Load Balancer Balancer-Kapazitätseinheiten 359
Dokumentverlauf 360
..... ccclxviii

Was ist ein Application Load Balancer?

Elastic Load Balancing verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer oder mehreren Availability Zones. Es überwacht den Zustand der registrierten Ziele und leitet den Datenverkehr nur an die fehlerfreien Ziele weiter. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der eingehende Datenverkehr im Laufe der Zeit ändert. Es kann automatisch auf die meisten Workloads skaliert werden.

Elastic Load Balancing unterstützt die folgenden Load Balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers und Classic Load Balancers. Sie können den Typ des Load Balancers, der Ihren Anforderungen am besten entspricht, auswählen. In diesem Handbuch werden Application Load Balancer beschrieben. Weitere Informationen zu den anderen Load Balancers finden Sie im Benutzerhandbuch für Network Load Balancer, im Benutzerhandbuch für Gateway Load Balancer und im Benutzerhandbuch für Classic Load Balancer.

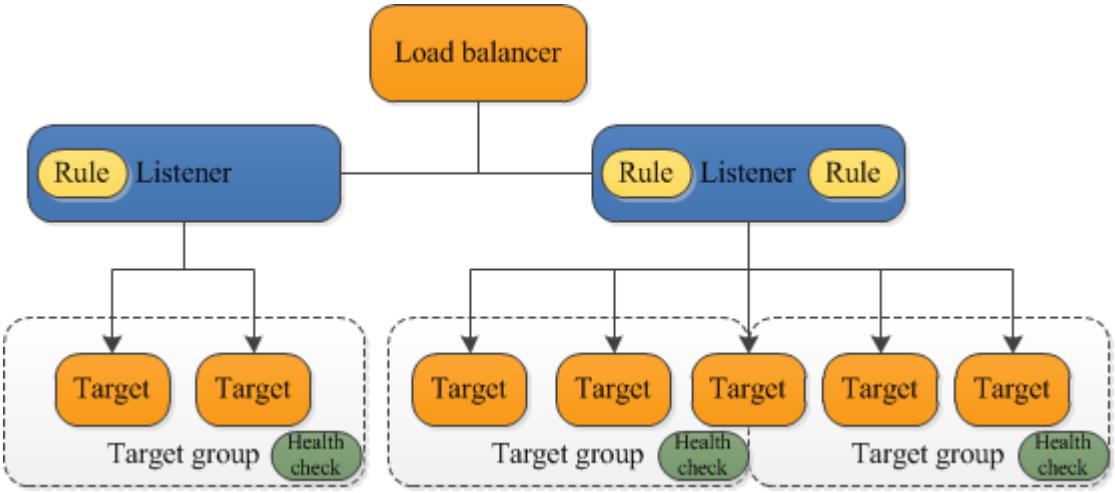
Application-Load-Balancer-Komponenten

Ein Load Balancer dient als zentraler Kontaktpunkt für Clients. Der Load Balancer verteilt den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. EC2 Instances, in mehreren Availability Zones. Dies erhöht die Verfügbarkeit Ihrer Anwendung. Sie fügen Ihrem Load Balancer einen oder mehrere Listener hinzu.

Ein Listener prüft Verbindungsanforderungen von Clients mit dem Protokoll und dem Port, das bzw. den Sie konfigurieren. Die für einen Listener definierten Regeln bestimmen, wie der Load Balancer Anforderungen an seine registrierten Ziele weiterleitet. Jede Rolle besteht aus einer Priorität, mindestens einer Aktion und mindestens einer Bedingung. Wenn die Bedingungen für eine Regel erfüllt sind, wird die dazugehörige Aktion durchgeführt. Sie müssen für jeden Listener eine Standardregel definieren und können optional zusätzliche Regeln definieren.

Jede Zielgruppe leitet Anfragen mithilfe des von Ihnen angegebenen Protokolls und der Portnummer an ein oder mehrere registrierte Ziele, z. B. EC2 Instanzen, weiter. Sie können ein Ziel bei mehreren Zielgruppen registrieren. Sie können Zustandsprüfungen pro Zielgruppe konfigurieren. Zustandsprüfungen werden auf allen Zielen ausgeführt, die bei einer Zielgruppe registriert sind, welche in einer Listener-Regel für Ihren Load Balancer abgegeben ist.

Das folgende Diagramm veranschaulicht die grundlegenden Komponenten. Beachten Sie, dass jeder Listener eine Standardregel enthält und ein Listener eine zweite Regel enthält, die Anforderungen an eine andere Zielgruppe weiterleitet. Ein Ziel ist bei zwei Zielgruppen registriert.



Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Load Balancers
- Listener
- Zielgruppen

Application Load Balancer – Übersicht

Ein Application Load Balancer funktioniert auf Anwendungsebene, der siebten Ebene der Open Systems Interconnection (OSI)-Modells. Nachdem der Load Balancer eine Anforderung empfangen hat, bewertet er die Listener-Regeln in der Reihenfolge ihrer Priorität, um zu ermitteln, welche Regel angewendet werden soll. Anschließend wählt er ein Ziel aus der Zielgruppe für die Regelaktion aus. Sie können Listener-Regeln zum Weiterleiten von Anforderungen an verschiedene Zielgruppen basierend auf dem Inhalt des Anwendungsdatenverkehrs konfigurieren. Die Weiterleitung erfolgt unabhängig für jede Zielgruppe, auch wenn ein Ziel bei mehreren Zielgruppen registriert ist. Sie können den Weiterleitungsalgorithmus konfigurieren, der auf der Ebene der Zielgruppe verwendet wird. Als standardmäßiger Routing-Algorithmus wird „Round Robin“ verwendet. Alternativ können Sie auch den Weiterleitungsalgorithmus „Am wenigsten ausstehende Anfragen“ angeben.

Sie können Ziele zu Ihrem Load Balancer hinzufügen und wieder entfernen, wenn sich Ihr Bedarf ändert, ohne den allgemeinen Fluss von Anfragen an Ihre Anwendung zu unterbrechen. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der Datenverkehr zu Ihrer Anwendung im Laufe der Zeit ändert. Elastic Load Balancing kann für die meisten Workloads automatisch skaliert werden.

Sie können Zustandsprüfungen konfigurieren, mit denen der Zustand der registrierten Ziele überwacht wird, sodass der Load Balancer nur an die fehlerfreien Ziele Anfragen senden kann.

Weitere Informationen finden Sie unter Funktionsweise von Elastic Load Balancing im Benutzerhandbuch für Elastic Load Balancing.

Vorteile der Migration von einem Classic Load Balancer

Die Verwendung eines Application Load Balancers anstelle eines Classic Load Balancers hat die folgenden Vorteile:

- Unterstützung für Pfadbedingungen. Sie können Regeln für Ihre Listener konfigurieren, die Anforderungen basierend auf der URL in der Anforderung weiterleiten. Auf diese Weise können Sie Ihre Anwendung als kleinere Services strukturieren und Anforderungen basierend auf dem Inhalt der URL an den richtigen Service weiterleiten.
- Unterstützung für Hostbedingungen. Sie können Regeln für Ihre Listener konfigurieren, die Anfragen basierend auf dem Hostfeld im HTTP-Header weiterleiten. Auf diese Weise können Sie mit einem einzigen Load Balancer Anfragen zu mehreren Domains weiterleiten.
- Unterstützung für Weiterleitung auf Grundlage von Feldern in der Anforderung, z. B. HTTP-Header-Bedingungen und Methoden, Abfrageparameter und IP-Adressen.
- Support für die Weiterleitung von Anfragen an mehrere Anwendungen auf einer einzigen EC2 Instanz. Sie können jede Instance oder IP-Adresse mit mehreren Zielgruppen registrieren, jede auf einem unterschiedlichen Port.
- Unterstützung für das Weiterleiten von Anforderungen von einer URL an eine andere.
- Unterstützung für das Zurückgeben einer benutzerdefinierten HTTP-Antwort.
- Unterstützung einer Registrierung von Zielen unter Verwendung von IP-Adressen, auch für Ziele, die außerhalb der VPC für den Load Balancer liegen.
- Unterstützung für die Registrierung von Lambda-Funktionen als Ziele.
- Unterstützung für das Authentifizieren von Benutzern Ihrer Anwendungen über deren Unternehmensidentitäten oder Social Identities vor dem Weiterleiten von Anfragen durch den Load Balancer.
- Unterstützung für Anwendungen in Containern. Amazon Elastic Container Service (Amazon ECS) kann beim Planen einer Aufgabe und Registrieren der Aufgabe bei einer Zielgruppe einen unbenutzten Port verwenden. Auf diese Weise können Sie Ihre Cluster effizient einsetzen.
- Support für die unabhängige Überwachung des Zustands der einzelnen Dienste, da Gesundheitschecks auf Zielgruppenebene definiert werden und viele CloudWatch Kennzahlen auf Zielgruppenebene gemeldet werden. Wenn Sie eine Zielgruppe einer Auto-Scaling-Gruppe zuweisen, können Sie jeden Service je nach Bedarf dynamisch skalieren.

- Zugriffsprotokolle enthalten weitere Informationen und werden in komprimiertem Format gespeichert.
- Verbesserte Load Balancer-Performance.

Weitere Informationen zu den Funktionen, die von den einzelnen Load Balancer-Typen unterstützt werden, finden Sie unter Elastic Load Balancing Balancing-Funktionen.

Zugehörige Services

Elastic Load Balancing arbeitet mit den folgenden Services, um die Verfügbarkeit und Skalierbarkeit Ihrer Anwendungen zu verbessern.

- Amazon EC2 — Virtuelle Server, auf denen Ihre Anwendungen in der Cloud ausgeführt werden. Sie können Ihren Load Balancer so konfigurieren, dass er den Datenverkehr an Ihre EC2 Instances weiterleitet.
- Amazon EC2 Auto Scaling — Stellt sicher, dass Sie die gewünschte Anzahl von Instances ausführen, auch wenn eine Instance ausfällt, und ermöglicht es Ihnen, die Anzahl der Instances automatisch zu erhöhen oder zu verringern, wenn sich die Nachfrage nach Ihren Instances ändert. Wenn Sie Auto Scaling mit Elastic Load Balancing aktivieren, werden Instances, die von Auto Scaling gestartet werden, automatisch bei der Zielgruppe registriert, und Instances, die durch Auto Scaling beendet wurden, werden automatisch von der Zielgruppe abgemeldet.
- AWS Certificate Manager – Wenn Sie einen HTTPS-Listener erstellen, können Sie von ACM bereitgestellte Zertifikate festlegen. Der Load Balancer verwendet Zertifikate, um Verbindungen zu beenden und Anfragen von Clients zu entschlüsseln. Weitere Informationen finden Sie unter SSL-Zertifikate für Ihren Application Load Balancer.
- Amazon CloudWatch — Ermöglicht es Ihnen, Ihren Load Balancer zu überwachen und bei Bedarf Maßnahmen zu ergreifen. Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Application Load Balancer.
- Amazon ECS — Ermöglicht das Ausführen, Stoppen und Verwalten von Docker-Containern in einem Cluster von EC2 Instances. Sie können Ihren Load Balancer so konfigurieren, dass der Datenverkehr an Ihre Container geleitet wird. Weitere Informationen finden Sie unter Service – Load Balancing im Amazon Elastic Container Service-Entwicklerhandbuch.
- AWS Global Accelerator – Verbessert die Verfügbarkeit und Leistung Ihrer Anwendung. Verwenden Sie einen Beschleuniger, um den Datenverkehr auf mehrere Load Balancer in einer oder mehreren

AWS Regionen zu verteilen. Weitere Informationen finden Sie im AWS Global Accelerator - Entwicklerhandbuch.

- Route 53 — Bietet eine zuverlässige und kostengünstige Möglichkeit, Besucher auf Websites weiterzuleiten, indem Domainnamen (z. B.`www.example.com`) in numerische IP-Adressen (z. B.`192.0.2.1`) übersetzt werden, die Computer verwenden, um sich miteinander zu verbinden. AWS weist Ihren Ressourcen URLs zu, z. B. Load Balancern. Sie können jedoch auch eine URL verwenden, die aussagekräftig und leicht zu merken ist. So können zum Beispiel Ihren Domainnamen einem Load Balancer zuordnen. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr an einen ELB Load Balancer im Entwicklerhandbuch von Amazon Route 53.
- AWS WAF— Sie können es AWS WAF zusammen mit Ihrem Application Load Balancer verwenden, um Anfragen auf der Grundlage der Regeln in einer Web-Zugriffskontrollliste (Web-ACL) zuzulassen oder zu blockieren. Weitere Informationen finden Sie unter AWS WAF.

Um Informationen über Dienste anzuzeigen, die in Ihren Load Balancer integriert sind, wählen Sie Ihren Load Balancer im AWS Management Console und dann den Tab Integrierte Dienste aus.

Preisgestaltung

Mit Ihrem Load Balancer zahlen Sie nur für das, was Sie auch tatsächlich nutzen. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing.

Erste Schritte mit Application Load Balancern

Dieses Tutorial bietet eine praktische Einführung in Application Load Balancers über eine webbasierte Oberfläche. AWS Management Console Führen Sie die folgenden Schritte aus, um Ihren ersten Application Load Balancer zu erstellen.

Inhalt

- Bevor Sie beginnen
- Schritt 1: Konfigurieren Ihrer Zielgruppe
- Schritt 2: Wählen eines Load Balancer-Typs
- Schritt 3: Konfigurieren Ihres Load Balancers und Listeners
- Schritt 4: Testen Ihres Load Balancers
- Schritt 5: Löschen Ihres Load Balancers (optional)

Demos häufiger Load-Balancer-Konfigurationen finden Sie unter Elastic-Load-Balancing-Demos.

Bevor Sie beginnen

- Entscheiden Sie, welche beiden Availability Zones Sie für Ihre EC2 Instances verwenden möchten. Konfigurieren Sie Ihre VPC (Virtual Private Cloud) in jeder dieser Availability Zones mit mindestens einem öffentlichen Subnetz. Diese öffentlichen Subnetze werden verwendet, um den Load Balancer zu konfigurieren. Sie können Ihre EC2 Instances stattdessen in anderen Subnetzen dieser Availability Zones starten.
- Starten Sie mindestens eine EC2 Instance in jeder Availability Zone. Stellen Sie sicher, dass Sie auf jeder EC2 Instanz einen Webserver wie Apache oder Internet Information Services (IIS) installieren. Stellen Sie sicher, dass die Sicherheitsgruppen für diese Instances den HTTP-Zugriff auf Port 80 erlauben.

Schritt 1: Konfigurieren Ihrer Zielgruppe

Erstellen Sie eine Zielgruppe, die bei der Weiterleitung von Anforderungen verwendet wird. Die Standardregel für Ihren Listener leitet Anforderungen an die registrierten Ziele in dieser Zielgruppe weiter. Der Load Balancer prüft anhand der Zustandsprüfungseinstellungen, die für die Zielgruppe definiert sind, den Zustand der Ziele in dieser Zielgruppe.

Um Ihre Zielgruppe mit der Konsole zu konfigurieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Behalten Sie unter Basiskonfiguration den Zieltyp als Instance bei.
5. Geben Sie unter Zielgruppenname einen Namen für die neue Zielgruppe ein.
6. Behalten Sie das Standardprotokoll (HTTP) und den Port (80) bei.
7. Wählen Sie die VPC aus, die Ihre Instances enthält. Behalten Sie die Protokollversion als bei HTTP1.
8. Behalten Sie für Zustandsprüfungen die Standardeinstellungen bei.
9. Wählen Sie Weiter.
10. Führen Sie auf der Seite Ziele registrieren die folgenden Schritte aus. Dies ist ein optionaler Schritt zum Erstellen des Load Balancers. Sie müssen dieses Ziel jedoch registrieren, wenn Sie Ihren Load Balancer testen und sicherstellen möchten, dass er den Datenverkehr zu diesem Ziel weiterleitet.
    a. Wählen Sie im Feld Verfügbare Instances eine oder mehrere Instances aus.
    b. Behalten Sie den Standardport 80 bei und wählen Sie Schließen Sie die unten angeführten als ausstehend ein aus.
11. Wählen Sie Zielgruppe erstellen aus.

Schritt 2: Wählen eines Load Balancer-Typs

Elastic Load Balancing unterstützt verschiedene Load-Balancer-Typen. In diesem Lernprogramm erstellen Sie einen Application Load Balancer.

So erstellen Sie einen Application Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste eine Region für Ihren Load Balancer aus. Achten Sie darauf, dieselbe Region auszuwählen, die Sie für Ihre EC2 Instances verwendet haben.
3. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
4. Klicken Sie auf Load Balancer erstellen.

5. Wählen Sie für Application Load Balancer Erstellen aus.

Schritt 3: Konfigurieren Ihres Load Balancers und Listeners

Um einen Application Load Balancer zu erstellen, müssen Sie zunächst grundlegende Konfigurationsinformationen für Ihren Load Balancer angeben, z. B. einen Namen, ein Schema und einen IP-Adresstyp. Geben Sie anschließend Informationen über Ihr Netzwerk und einen oder mehrere Listener an. Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Er wird mit einem Protokoll und einem Port für Verbindungen von Clients zum Load Balancer konfiguriert. Weitere Informationen zu unterstützten Protokollen und Ports finden Sie unter Listener-Konfiguration.

So konfigurieren Sie Load Balancer und Listener

1. Geben Sie im Feld Name des Load Balancers einen Namen für Ihren Load Balancer ein. Beispiel, `my-alb`.
2. Behalten Sie für Schema und IP-Adresstyp die Standardwerte.
3. Wählen Sie für Network Mapping die VPC aus, die Sie für Ihre EC2 Instances verwendet haben. Wählen Sie mindestens zwei Availability Zones und ein Subnetz pro Zone aus. Wählen Sie für jede Availability Zone, die Sie zum Starten Ihrer EC2 Instances verwendet haben, die Availability Zone und dann ein öffentliches Subnetz für diese Availability Zone aus.
4. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppe für die VPC aus, die Sie im vorherigen Schritt ausgewählt haben. Sie können stattdessen eine andere Sicherheitsgruppe wählen. Die Sicherheitsgruppe muss Regeln enthalten, die dem Load Balancer die Kommunikation mit registrierten Zielen sowohl auf dem Listener-Port als auch auf dem Zustandsprüfungs-Port ermöglichen. Weitere Informationen finden Sie unter Regeln zu Sicherheitsgruppen.
5. Behalten Sie für Listener und Routing das Standardprotokoll und den Standardport bei und wählen Sie die Zielgruppe aus der Liste aus. Dadurch wird ein Listener konfiguriert, der HTTP-Verkehr auf Port 80 akzeptiert und den Datenverkehr standardmäßig an die ausgewählte Zielgruppe weiterleitet. In diesem Tutorial erstellen Sie keinen HTTPS-Listener.
6. Wählen Sie für Standardaktion die Zielgruppe aus, die Sie in „Schritt 1: Konfigurieren Ihrer Zielgruppe“ erstellt und registriert haben.
7. (Optional) Sie können zwecks Kategorisierung Ihrem Load Balancer ein Tag hinzufügen. Tag-Schlüssel müssen für jeden Load Balancer eindeutig sein. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen (in UTF-8) sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen. Bei Tag-Werten muss die Groß- und Kleinschreibung beachtet werden.

8. Überprüfen Sie Ihre Konfiguration und wählen Sie Load Balancer erstellen aus. Bei der Erstellung werden einige Standardattribute auf Ihren Load Balancer angewendet. Sie können sie nach der Erstellung des Load Balancers anzeigen und bearbeiten. Weitere Informationen finden Sie unter Load Balancer-Attribute.

Schritt 4: Testen Ihres Load Balancers

Nachdem Sie den Load Balancer erstellt haben, stellen Sie sicher, dass er Traffic an Ihre EC2 Instances sendet.

Testen des Load Balancers

1. Nachdem Sie darüber informiert wurden, dass Ihr Load Balancer erfolgreich erstellt wurde, klicken Sie auf Schließen.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie die neu erstellte Zielgruppe aus.
4. Wählen Sie Targets und vergewissern Sie sich, dass die Instances bereit sind. Wenn der Status einer Instance `initial` lautet, liegt das wahrscheinlich daran, dass die Instance gerade registriert wird oder dass sie die Mindestanzahl von Zustandsprüfungen nicht bestanden hat, um als fehlerfrei zu gelten. Wenn der Status von mindestens einer Instance `healthy` lautet, können Sie Ihren Load Balancer testen.
5. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
6. Wählen Sie den neu erstellten Load Balancer aus.
7. Wählen Sie Beschreibung und kopieren Sie den DNS-Namen des Load Balancers (z. B. my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). Fügen Sie den DNS-Namen in das Adressfeld eines mit dem Internet verbundenen Webbrowsers ein. Wenn alles funktioniert, zeigt der Browser die Standardseite Ihres Servers an.
8. (Optional) Informationen zum Definieren von zusätzlichen Listener-Regeln finden Sie unter Hinzufügen einer Regel.

Schritt 5: Löschen Ihres Load Balancers (optional)

Sobald der Load Balancer verfügbar ist, wird Ihnen jede ganze oder angebrochene Stunde in Rechnung gestellt, in der er ausgeführt wird. Wenn Sie einen Load Balancer nicht mehr benötigen, können Sie ihn löschen. Sobald der Load Balancer gelöscht wurde, fallen keine weiteren Kosten

dafür mehr an. Beachten Sie, dass das Löschen eines Load Balancers keine Auswirkungen auf die beim Load Balancer registrierten Ziele hat. Ihre EC2 Instances laufen beispielsweise weiter, nachdem Sie den in diesem Handbuch erstellten Load Balancer gelöscht haben.

Um Ihren Load Balancer mithilfe der Konsole zu löschen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Aktivieren Sie das Kontrollkästchen für den Load Balancer und wählen Sie dann Aktionen und Löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja, löschen.

Erste Schritte mit Application Load Balancers mithilfe der AWS CLI

Dieses Tutorial bietet eine praktische Einführung in Application Load Balancers über die. AWS CLI

Inhalt

- Bevor Sie beginnen
- Erstellen Ihres Load Balancers
- Hinzufügen eines HTTPS-Listeners
- Hinzufügen von pfadbasierter Weiterleitung
- Löschen des Load Balancers

Bevor Sie beginnen

- Verwenden Sie den folgenden Befehl, um zu überprüfen, ob Sie eine Version der AWS CLI verwenden, die Application Load Balancer unterstützt.

  ```
  aws elbv2 help
  ```

  Wenn Sie die Fehlermeldung erhalten, dass elbv2 ungültig ist, aktualisieren Sie die AWS CLI. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Installation der AWS CLI neuesten Version von.
- Starten Sie Ihre EC2 Instances in einer Virtual Private Cloud (VPC). Stellen Sie sicher, dass die Sicherheitsgruppen für diese Instances den Zugriff auf den Listener-Port und die Port-Zustandsprüfung erlauben. Weitere Informationen finden Sie unter Zielsicherheitsgruppen.
- Entscheiden Sie, ob Sie einen Load Balancer IPv4 oder einen Dual-Stack-Load Balancer erstellen möchten. Verwenden Sie IPv4 diese Option, wenn Clients nur über Adressen mit dem Load Balancer kommunizieren sollen. IPv4 Verwenden Sie Dualstack, wenn Sie möchten, dass Clients mit dem Load Balancer über Adressen kommunizieren. IPv4 IPv6 Sie können Dualstack auch verwenden, um mit Backend-Zielen wie IPv6 Anwendungen oder Dual-Stack-Subnetzen zu kommunizieren. IPv6

- Stellen Sie sicher, dass Sie auf jeder Instanz einen Webserver wie Apache oder Internet Information Services (IIS) installieren. EC2 Stellen Sie sicher, dass die Sicherheitsgruppen für diese Instances den HTTP-Zugriff auf Port 80 erlauben.

Erstellen Ihres Load Balancers

Führen Sie die folgenden Schritte aus, um Ihren ersten Load Balancer zu erstellen.

Erstellen Sie einen Load Balancer wie folgt:

1. Verwenden Sie den create-load-balancerBefehl, um einen Load Balancer zu erstellen. Sie müssen zwei Subnetze angeben, die sich nicht in derselben Availability Zone befinden.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer  \
   --subnets subnet-0e3f5cac72EXAMPLE subnet-081ec835f3EXAMPLE --security-groups
    sg-07e8ffd50fEXAMPLE
   ```

   Verwenden Sie den create-load-balancerBefehl, um einen **dualstack** Load Balancer zu erstellen.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer  \
   --subnets subnet-0e3f5cac72EXAMPLE subnet-081ec835f3EXAMPLE --security-groups
    sg-07e8ffd50fEXAMPLE --ip-address-type dualstack
   ```

   Die Ausgabe enthält den Amazon Resource Name (ARN) des Load Balancers im folgenden Format:

   ```
   arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/app/my-load-
   balancer/1234567890123456
   ```

2. Verwenden Sie den create-target-groupBefehl, um eine Zielgruppe zu erstellen, indem Sie dieselbe VPC angeben, die Sie für Ihre EC2 Instances verwendet haben.

   Sie können Gruppen erstellen IPv4 und als IPv6 Zielgruppe festlegen, um sie mit Dual-Stack-Load Balancern zu verknüpfen. Der IP-Adresstyp der Zielgruppe bestimmt die IP-Version, die der Load Balancer verwendet, um sowohl mit Ihren Backend-Zielen zu kommunizieren als auch deren Zustand zu überprüfen.

   ```
   aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
   ```

```
--vpc-id vpc-0598c7d356EXAMPLE --ip-address-type [ipv4 or ipv6]
```

Die Ausgabe umfasst den ARN der Zielgruppe in diesem Format:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Verwenden Sie den Befehl register-targets, um Ihre Instances bei Ihrer Zielgruppe zu registrieren:

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-0abcdef1234567890 Id=i-1234567890abcdef0
```

4. Verwenden Sie den Befehl create-listener, um einen Listener für Ihren Load Balancer mit einer Standardregel zu erstellen, die Anforderungen an Ihre Zielgruppe weiterleitet:

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \
--protocol HTTP --port 80  \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Die Ausgabe enthält den ARN des Listeners im folgenden Format:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/app/my-load-
balancer/1234567890123456/1234567890123456
```

5. (Optional) Mit diesem Befehl können Sie den Zustand der registrierten Ziele für Ihre Zielgruppe überprüfen: describe-target-health

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Hinzufügen eines HTTPS-Listeners

Wenn Sie einen Load Balancer mit einem HTTP-Listener haben, können Sie wie folgt einen HTTP-Listener hinzufügen.

So fügen Sie einen HTTPS-Listener zu Ihrem Load Balancer hinzu

1. Erstellen Sie anhand einer der folgenden Methoden ein SSL-Zertifikat für die Verwendung mit Ihrem Load Balancer:

- Erstellen oder importieren Sie das Zertifikat mit AWS Certificate Manager (ACM). Weitere Informationen finden Sie unter Anfordern eines öffentlichen Zertifikats oder Importieren von Zertifikaten im AWS Certificate Manager Benutzerhandbuch.
- Laden Sie das Zertifikat mit AWS Identity and Access Management (IAM) hoch. Weitere Informationen finden Sie unter Arbeiten mit Serverzertifikaten im IAM-Benutzerhandbuch.

2. Verwenden Sie den Befehl create-listener, um den Listener mit einer Standardregel zu erstellen, die Anforderungen an Ihre Zielgruppe weiterleitet. Sie müssen ein SSL-Zertifikat angeben, wenn Sie einen HTTPS-Listener erstellen. Beachten Sie, dass Sie mithilfe der Option `--ssl-policy` eine andere SSL-Richtlinie als die Standardrichtlinie angeben können.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \
--protocol HTTPS --port 443  \
--certificates CertificateArn=certificate-arn \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Hinzufügen von pfadbasierter Weiterleitung

Wenn Sie einen Listener mit einer Standardregel haben, der Anforderungen an eine Zielgruppe weiterleitet, können Sie eine Regel hinzufügen, die Anforderungen an eine andere Zielgruppe auf der Grundlage von URL weiterleitet. Sie können beispielsweise allgemeine Anforderungen an die eine Zielgruppe und Anforderungen zur Anzeige von Bildern an eine andere Zielgruppe weiterleiten.

Hinzufügen einer Regel zu einem Listener mit einem Pfadmuster

1. Verwenden Sie den create-target-groupBefehl, um eine Zielgruppe zu erstellen:

```
aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
--vpc-id vpc-0598c7d356EXAMPLE
```

2. Verwenden Sie den Befehl register-targets, um Ihre Instances bei Ihrer Zielgruppe zu registrieren:

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-0abcdef1234567890 Id=i-1234567890abcdef0
```

3. Verwenden Sie den Befehl create-rule, um zu Ihrem Listener eine Regel hinzuzufügen, die Anforderungen an die Zielgruppe weiterleitet, wenn die URL das angegebene Muster enthält:

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--conditions Field=path-pattern,Values='/img/*' \
--actions Type=forward,TargetGroupArn=targetgroup-arn
```

Löschen des Load Balancers

Wenn Sie Ihren Load Balancer und Ihre Zielgruppe nicht mehr benötigen, können Sie sie wie folgt löschen:

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Application Load Balancer

Ein Load Balancer dient als zentraler Kontaktpunkt für Clients. Clients senden Anfragen an den Load Balancer, und der Load Balancer sendet sie an Ziele wie EC2 Instances. Zur Konfiguration Ihres Load Balancers erstellen Sie Zielgruppen und registrieren anschließend Ziele bei den Zielgruppen. Außerdem erzeugen Sie Listener für Verbindungsanforderungen von Clients und Listener-Regeln zum Weiterleiten von Anforderungen von Clients an Ziele in einer oder mehreren Zielgruppen.

Weitere Informationen finden Sie unter Funktionsweise von Elastic Load Balancing im Benutzerhandbuch für Elastic Load Balancing.

Inhalt

- Subnetze für Ihren Load Balancer
- Load-Balancer-Sicherheitsgruppen
- Load Balancer-Status
- Load Balancer-Attribute
- IP-Adresstyp
- IPAM-IP-Adresspools
- Load Balancer-Verbindungen
- Zonenübergreifendes Load Balancing
- DNS-Name
- Erstellen eines Application Load Balancers
- Aktualisieren Sie die Availability Zones für Ihren Application Load Balancer
- Sicherheitsgruppen für Ihren Application Load Balancer
- Aktualisieren Sie die IP-Adresstypen für Ihren Application Load Balancer
- Aktualisieren Sie die IPAM-IP-Adresspools für Ihren Application Load Balancer
- Integrationen für Ihren Application Load Balancer
- Attribute für Ihren Application Load Balancer bearbeiten
- Einen Application Load Balancer taggen
- Löschen eines Application Load Balancers
- Sehen Sie sich die Application Load Balancer Balancer-Ressourcenübersicht an

- Kapazitätsreservierungen für Ihren Application Load Balancer

Subnetze für Ihren Load Balancer

Wenn Sie einen Application Load Balancer erstellen, müssen Sie die Zonen, die Ihre Ziele enthalten, aktivieren. Um eine Zone zu aktivieren, geben Sie ein Subnetz in der Zone an. Elastic Load Balancing erstellt in jeder Zone, die Sie angeben, einen Load-Balancer-Knoten.

Überlegungen

- Ihr Load Balancer ist am effektivsten, wenn Sie dafür sorgen, dass jede aktivierte Zone mindestens ein registriertes Ziel hat.
- Wenn Sie Ziele in einer Zone registrieren, aber die Zone nicht aktivieren, erhalten diese registrierten Ziele keinen Datenverkehr vom Load Balancer.
- Wenn Sie mehrere Zonen für Ihren Load Balancer aktivieren, müssen die Zonen vom gleichen Typ sein. Sie können beispielsweise nicht sowohl eine Availability Zone als auch eine Local Zone aktivieren.
- Sie können ein Subnetz angeben, das für Sie freigegeben wurde.

Application Load Balancer unterstützen die folgenden Arten von Subnetzen.

Subnetz-Typen

- Availability-Zone-Subnetze
- Local-Zone-Subnetze
- Outpost-Subnetze

Availability-Zone-Subnetze

Sie müssen mindestens zwei Availability-Zone-Subnetze auswählen. Beachten Sie die folgenden Einschränkungen:

- Jedes Subnetz muss einer anderen Availability Zone angehören.
- Damit Ihr Load Balancer ordnungsgemäß skaliert werden kann, stellen Sie sicher, dass jedes Availability-Zone-Subnetz für Ihren Load Balancer über einen CIDR-Block mit mindestens einer `/27`-Bitmaske (z. B. `10.0.0.0/27`) und über mindestens acht freie IP-Adressen pro Subnetz

verfügt. Diese acht IP-Adressen sind erforderlich, damit der Load Balancer bei Bedarf skalieren kann. Ihr Load Balancer verwendet diese IP-Adressen zum Einrichten von Verbindungen mit den Zielen. Ohne sie könnte Ihr Application Load Balancer Schwierigkeiten beim Versuch haben, Knoten zu ersetzen. Das könnte dazu führen, dass er in den Fehlerstatus übergeht.

Hinweis: Wenn einem Application-Load-Balancer-Subnetz beim Versuch der Skalierung die verwendbaren IP-Adressen ausgehen, wird der Application Load Balancer mit unzureichender Kapazität ausgeführt. Während dieser Zeit werden alte Knoten weiterhin Datenverkehr bereitstellen, aber der gescheiterte Skalierungsversuch kann zu 5xx-Fehlern oder Timeouts führen, wenn versucht wird, eine Verbindung herzustellen.

Local-Zone-Subnetze

Sie können ein oder mehrere Local-Zone-Subnetze angeben. Die folgenden -Features werden nicht unterstützt:

- Lambda-Funktionen als Ziele
- Gegenseitige TLS-Authentifizierung
- Sticky Sessions
- AWS WAF Integration

Outpost-Subnetze

Sie können ein einzelnes Outpost-Subnetz angeben. Beachten Sie die folgenden Einschränkungen:

- Sie müssen ein Outpost in Ihrem On-Premises-Rechenzentrum installiert und konfiguriert haben. Sie müssen über eine zuverlässige Netzwerkverbindung zwischen Ihrem Outpost und der entsprechenden AWS -Region verfügen. Weitere Informationen finden Sie im AWS Outposts - Benutzerhandbuch.
- Der Load Balancer benötigt zwei `large`-Instances auf dem Outpost für die Load-Balancer-Knoten. In der folgenden Tabelle sind die unterstützten Instance-Typen aufgeführt. Der Load Balancer skaliert nach Bedarf und ändert die Größe der Knoten jeweils um eine Größe (von `large` in `xlarge`, dann `xlarge` in `2xlarge` und dann `2xlarge` in `4xlarge`). Wenn Sie nach der Skalierung der Knoten in die größte Instance-Größe zusätzliche Kapazität benötigen, fügt der Load Balancer `4xlarge`-Instances als Load-Balancer-Knoten hinzu. Wenn Sie nicht genügend Instance-Kapazität oder verfügbare IP-Adressen haben, um den Load Balancer zu skalieren,

meldet der Load Balancer ein Ereignis an AWS Health Dashboard und der Load-Balancer-Status ist `active_impaired`.

- Sie können Ziele nach Instance-ID oder IP-Adresse registrieren. Wenn Sie Ziele in der AWS Region für den Außenposten registrieren, werden sie nicht verwendet.
- Die folgenden -Features werden nicht unterstützt:
  - AWS Global Accelerator Integration
  - Lambda-Funktionen als Ziele
  - Gegenseitige TLS-Authentifizierung
  - Sticky Sessions
  - Benutzerauthentifizierung
  - AWS WAF Integration

Ein Application Load Balancer kann in c5/c5d-, m5/m5d- oder r5/r5d-Instances auf einem Outpost bereitgestellt werden. Die folgende Tabelle enthält die Größe und das EBS-Volumen pro Instance-Typ, die der Load Balancer auf einem Outpost verwenden kann:

Instance-Typ und Größe	EBS-Volumen (GB)
c5/c5d	
large	50
xlarge	50
2xlarge	50
4xlarge	100
m5/m5d	
large	50
xlarge	50
2xlarge	100
4xlarge	100

Instance-Typ und Größe	EBS-Volumen (GB)	
r5/r5d		
large	50	
xlarge	100	
2xlarge	100	
4xlarge	100	

Load-Balancer-Sicherheitsgruppen

Eine Sicherheitsgruppe agiert als Firewall, die den Datenverkehr steuert, der in und aus Ihrem Load Balancer zulässig ist. Sie können Ports und Protokolle festlegen, um den ein- und ausgehenden Datenverkehr zu ermöglichen.

Die Regeln für die Sicherheitsgruppen, die Ihrem Load Balancer zugeordnet sind, müssen den Datenverkehr in beiden Richtungen auf den Listener- und Zustandsprüfungs-Ports zulassen. Wenn Sie einen Listener zu einem Load Balancer hinzufügen oder den Zustandsprüfungs-Port für eine Zielgruppe aktualisieren, müssen Sie Ihre Sicherheitsgruppenregeln überprüfen, um sicherzustellen, dass sie den Datenverkehr auf dem neuen Port in beiden Richtungen zulassen. Weitere Informationen finden Sie unter Empfohlene Regeln.

Load Balancer-Status

Ein Load Balancer kann einen der folgenden Status aufweisen:

`provisioning`

Der Load Balancer ist eingerichtet.

`active`

Der Load Balancer ist vollständig eingerichtet und kann den Datenverkehr weiterleiten.

`active_impaired`

Der Load Balancer leitet den Datenverkehr weiter, verfügt aber nicht über die notwendigen Ressourcen für die Skalierung.

`failed`

Der Load Balancer konnte nicht eingerichtet werden.

Load Balancer-Attribute

Sie können Ihren Application Load Balancer konfigurieren, indem Sie seine Attribute bearbeiten. Weitere Informationen finden Sie unter Bearbeiten Sie die Load Balancer-Attribute.

Dies sind die Load Balancer-Attribute:

`access_logs.s3.enabled`

Gibt an, ob in Amazon S3 gespeicherte Zugriffsprotokolle aktiviert sind. Der Standardwert ist `false`.

`access_logs.s3.bucket`

Der Name des Amazon-S3-Buckets für die Zugriffsprotokolle. Dieses Attribut ist erforderlich, wenn Zugriffsprotokolle aktiviert sind. Weitere Informationen finden Sie unter Aktivieren der Zugriffsprotokolle.

`access_logs.s3.prefix`

Das Präfix für den Speicherort im Amazon-S3-Bucket.

`client_keep_alive.seconds`

Der Keepalive-Wert des Clients in Sekunden. Die Standardeinstellung ist 3600 Sekunden.

`deletion_protection.enabled`

Gibt an, ob der Löschschutz aktiviert ist. Der Standardwert ist `false`.

`idle_timeout.timeout_seconds`

Der Timeoutwert für die Leerlaufzeit in Sekunden. Standardmäßig ist ein Zeitraum von 60 Sekunden festgelegt.

`ipv6.deny_all_igw_traffic`

Sperrt den Zugriff des Internet-Gateways (IGW) auf den Load Balancer und verhindert so unbeabsichtigten Zugriff auf Ihren internen Load Balancer über ein Internet-Gateway. Es ist auf für mit dem Internet verbundenen Load Balancers auf `false` und für interne Load Balancers auf

`true` eingestellt. Dieses Attribut verhindert nicht den Internetzugriff außerhalb von IGW (z. B. über Peering, Transit Gateway AWS Direct Connect, oder). AWS VPN

`routing.http.desync_mitigation_mode`

Legt fest, wie der Load Balancer Anforderungen verarbeitet, die ein Sicherheitsrisiko für Ihre Anwendung darstellen könnten. Die möglichen Werte sind `monitor`, `defensive` und `strictest`. Der Standardwert ist `defensive`.

`routing.http.drop_invalid_header_fields.enabled`

Gibt an, ob HTTP-Header mit ungültigen Header-Feldern vom Load Balancer entfernt (`true`) oder an Ziele weitergeleitet werden (`false`). Der Standardwert ist `false`. Elastic Load Balancing erfordert, dass gültige HTTP-Header-Namen dem regulären Ausdruck `[-A-Za-z0-9]+` entsprechen, wie in der HTTP Field Name Registry beschrieben. Jeder Name besteht aus alphanumerischen Zeichen oder Bindestrichen. Wählen Sie `true` aus, wenn Sie möchten, dass HTTP-Header, die diesem Muster nicht entsprechen, aus Anforderungen entfernt werden sollen.

`routing.http.preserve_host_header.enabled`

Gibt an, ob der Application Load Balancer den `Host`-Header in der HTTP-Anforderung beibehalten und unverändert an das Ziel senden soll. Die möglichen Werte sind `true` und `false`. Der Standardwert ist `false`.

`routing.http.x_amzn_tls_version_and_cipher_suite.enabled`

Gibt an, ob die beiden Header (`x-amzn-tls-version` und `x-amzn-tls-cipher-suite`), die Informationen über die ausgehandelte TLS-Version und die Verschlüsselungssammlung enthalten, der Client-Anforderung hinzugefügt werden, bevor sie an das Ziel gesendet wird. Der `x-amzn-tls-version`-Header enthält Informationen über die mit dem Client ausgehandelte TLS-Protokollversion und der `x-amzn-tls-cipher-suite`-Header enthält Informationen über die mit dem Client ausgehandelte Verschlüsselungssammlung. Beide Header sind im OpenSSL-Format. Die möglichen Werte für dieses Attribut sind `true` und `false`. Der Standardwert ist `false`.

`routing.http.xff_client_port.enabled`

Zeigt an, ob der `X-Forwarded-For`-Header den Quellport beibehalten sollte, den der Client für die Verbindung mit dem Load Balancer verwendet hat. Die möglichen Werte sind `true` und `false`. Der Standardwert ist `false`.

`routing.http.xff_header_processing.mode`

Ermöglicht das Ändern, Beibehalten oder Entfernen der `X-Forwarded-For`-Header in der HTTP-Anforderung, bevor der Application Load Balancer die Anforderung an das Ziel sendet. Die möglichen Werte sind `append`, `preserve` und `remove`. Der Standardwert ist `append`.

- Wenn der Wert `append` ist, fügt der Application Load Balancer die Client-IP-Adresse (des letzten Hop) zum `X-Forwarded-For`-Header in der HTTP-Anforderung hinzu, bevor sie an Ziele gesendet wird.
- Wenn der Wert `preserve` ist, behält Application Load Balancer den `X-Forwarded-For`-Header in der HTTP-Anforderung und sendet sie ohne Änderung an Ziele.
- Wenn der Wert `remove` ist, entfernt Application Load Balancer den `X-Forwarded-For`-Header in der HTTP-Anforderung, bevor sie an Ziele gesendet wird.

`routing.http2.enabled`

Gibt an, ob HTTP/2 aktiviert ist. Der Standardwert ist `true`.

`waf.fail_open.enabled`

Gibt an, ob ein Load Balancer mit AWS WAF aktiviertem Load Balancer Anfragen an Ziele weiterleiten darf, wenn er die Anfrage nicht weiterleiten kann. AWS WAF Die möglichen Werte sind `true` und `false`. Der Standardwert ist `false`.

> **Note**
>
> Das `routing.http.drop_invalid_header_fields.enabled`-Attribut wurde eingeführt, um einen Schutz vor HTTP-Desync-Angriffen zu bieten. Das `routing.http.desync_mitigation_mode`-Attribut wurde hinzugefügt, um Ihren Anwendungen einen umfassenderen Schutz vor HTTP-Desync-Angriffen zu bieten. Sie müssen nicht beide Attribute verwenden und können je nach den Anforderungen Ihrer Anwendung auch nur eines der beiden auswählen.

IP-Adresstyp

Sie können die IP-Adresstypen festlegen, die Clients verwenden können, um auf Ihre Load Balancer, die mit dem Internet verbunden sind, und Ihre internen Load Balancer zuzugreifen.

Application Load Balancers unterstützen die folgenden IP-Adresstypen:

`ipv4`

Clients müssen über IPv4 Adressen (z. B. 192.0.2.1) eine Verbindung zum Load Balancer herstellen.

`dualstack`

Clients können eine Verbindung zum Load Balancer herstellen, indem sie sowohl IPv4 Adressen (z. B. 192.0.2.1) als auch Adressen (z. B. 2001:0 db 8:85 a IPv6 3:0:0:0:8 a2e: 0370:7334) verwenden.

`dualstack-without-public-ipv4`

Clients müssen über Adressen (z. B. 2001:0 db 8:85 a 3:0:0:0:8 a2e: 0370:7334) eine Verbindung zum Load Balancer herstellen. IPv6

Überlegungen

- Der Load Balancer kommuniziert mit Zielen auf der Grundlage des IP-Adresstyps der Zielgruppe.
- Wenn Sie den Dualstack-Modus für den Load Balancer aktivieren, stellt Elastic Load Balancing einen AAAA-DNS-Eintrag für den Load Balancer bereit. Clients, die über Adressen mit dem Load Balancer kommunizieren, lösen den A-DNS-Eintrag auf. IPv4 Clients, die über IPv6 Adressen mit dem Load Balancer kommunizieren, lösen den AAAA-DNS-Eintrag auf.
- Der Zugriff auf Ihre internen Dualstack-Load-Balancers über das Internet-Gateway ist blockiert, um einen unbeabsichtigten Internetzugriff zu verhindern. Dies verhindert jedoch nicht den Internetzugang, der nicht von IGW stammt (z. B. über Peering, Transit Gateway AWS Direct Connect, oder). AWS VPN
- Die Application Load Balancer Balancer-Authentifizierung wird nur unterstützt IPv4 , wenn eine Verbindung zu einem Identity Provider (IdP) oder Amazon Cognito Cognito-Endpunkt hergestellt wird. Ohne eine öffentliche IPv4 Adresse kann der Load Balancer den Authentifizierungsprozess nicht abschließen, was zu HTTP 500-Fehlern führt.

Weitere Informationen finden Sie unter Aktualisieren Sie die IP-Adresstypen für Ihren Application Load Balancer.

IPAM-IP-Adresspools

Ein IPAM-IP-Adresspool ist eine Sammlung zusammenhängender IP-Adressbereiche (oder CIDRs) innerhalb von Amazon VPC IP Address Manager (IPAM). Durch die Verwendung von IPAM-IP-

Adresspools mit Ihrem Application Load Balancer können Sie Ihre IPv4 Adressen entsprechend Ihren Routing- und Sicherheitsanforderungen organisieren. IPAM-IP-Adresspools müssen zuerst in IPAM erstellt werden, bevor sie von Ihrem Application Load Balancer verwendet werden können. Weitere Informationen finden Sie unter Bringen Sie Ihre IP-Adressen zu IPAM.

Überlegungen

- IPAM-IP-Adresspools sind nicht mit internen Load Balancern oder dem Dualstack ohne öffentlichen IP-Adresstyp kompatibel. IPv4
- Sie können eine IP-Adresse in einem IPAM-IP-Adresspool nicht löschen, wenn sie derzeit von einem Load Balancer verwendet wird.
- Während des Übergangs zu einem anderen IPAM-IP-Adresspool werden bestehende Verbindungen entsprechend der Keepalive-Dauer des HTTP-Clients des Load Balancers beendet.
- IPAM-IP-Adresspools können von mehreren Konten gemeinsam genutzt werden. Weitere Informationen finden Sie unter Integrationsoptionen für Ihr IPAM konfigurieren

IPAM-IP-Adresspools bieten Ihnen die Wahl, einige oder alle Ihrer öffentlichen IPv4 Adressbereiche in Ihre Application Load Balancers zu übertragen AWS und sie mit ihnen zu verwenden. Durch eine bessere Kontrolle der IP-Adresszuweisung können Sie Sicherheitsrichtlinien und -kontrollen effektiver verwalten und durchsetzen und gleichzeitig von niedrigeren Kosten profitieren. Für die Verwendung von IPAM-IP-Adresspools mit Ihren Application Load Balancers fallen keine zusätzlichen Gebühren an. Je nach verwendeter Stufe können jedoch Gebühren für IPAM anfallen. Weitere Informationen finden Sie unter Amazon VPC-Preise

Ihr IPAM-IP-Adresspool hat beim Starten von EC2 Instances und Application Load Balancers immer Priorität. Wenn Ihre IP-Adressen nicht mehr verwendet werden, sind sie sofort wieder verfügbar. Wenn es in Ihrem IPAM-IP-Adresspool keine zuweisbaren IP-Adressen mehr gibt, werden AWS verwaltete IP-Adressen zugewiesen. AWS Für verwaltete IP-Adressen fallen zusätzliche Kosten an. Um zusätzliche IP-Adressen hinzuzufügen, können Sie einem vorhandenen IPAM-IP-Adresspool neue IP-Adressbereiche hinzufügen.

Load Balancer-Verbindungen

Bei der Verarbeitung einer Anfrage unterhält der Load Balancer zwei Verbindungen: eine Verbindung mit dem Client und eine Verbindung mit einem Ziel. Die Verbindung zwischen dem Load Balancer und dem Client wird auch als Front-End-Verbindung bezeichnet. Die Verbindung zwischen dem Load Balancer und dem Ziel wird auch als Back-End-Verbindung bezeichnet.

Zonenübergreifendes Load Balancing

Bei Application Load Balancern ist zonenübergreifendes Load Balancing standardmäßig aktiviert und kann nicht auf Load-Balancer-Ebene geändert werden. Weitere Informationen finden Sie im Abschnitt ZonenübergreifenderLoad Balancing im Benutzerhandbuch für Elastic Load Balancing.

Das Deaktivieren des zonenübergreifenden Load Balancings ist auf Zielgruppenebene möglich. Weitere Informationen finden Sie unter the section called “Wenn zonenübergreifendes Load Balancing deaktivieren”.

DNS-Name

Jeder Application Load Balancer erhält einen Standard-DNS-Namen (Domain Name System) mit der folgenden Syntax: *name* - *id* .elb. *region*.amazonaws.com. Zum Beispiel my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com.

Wenn Sie lieber einen DNS-Namen verwenden möchten, den Sie sich leichter merken können, können Sie einen benutzerdefinierten Domainnamen erstellen und ihn mit dem DNS-Namen für Ihren Application Load Balancer verknüpfen. Wenn ein Client eine Anfrage mit diesem benutzerdefinierten Domänennamen stellt, löst der DNS-Server sie in den DNS-Namen für Ihren Application Load Balancer auf.

Registrieren Sie zunächst einen Domainnamen bei einer akkreditierten Domainnamenvergabestelle. Verwenden Sie als Nächstes Ihren DNS-Dienst, z. B. Ihren Domain-Registrar, um einen DNS-Eintrag zu erstellen, um Anfragen an Ihren Application Load Balancer weiterzuleiten. Weitere Informationen finden Sie in der Dokumentation zu Ihrem DNS-Service. Wenn Sie beispielsweise Amazon Route 53 als Ihren DNS-Service verwenden, erstellen Sie einen Aliaseintrag, der auf Ihren Application Load Balancer verweist. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr an einen ELB Load Balancer im Entwicklerhandbuch von Amazon Route 53.

Der Application Load Balancer hat eine IP-Adresse pro aktivierter Availability Zone. Dies sind die IP-Adressen der Application Load Balancer Balancer-Knoten. Der DNS-Name des Application Load Balancer wird in diese Adressen aufgelöst. Nehmen wir zum Beispiel an, der benutzerdefinierte Domainname für Ihren Application Load Balancer lautet`example.applicationloadbalancer.com`. Verwenden Sie den folgenden nslookup Befehl dig oder, um die IP-Adressen der Application Load Balancer Balancer-Knoten zu ermitteln.

Linux oder Mac

```
$ dig +short example.applicationloadbalancer.com
```

Windows

```
C:\> nslookup example.applicationloadbalancer.com
```

Der Application Load Balancer hat DNS-Einträge für seine Knoten. Sie können DNS-Namen mit der folgenden Syntax verwenden, um die IP-Adressen der Application Load Balancer Balancer-Knoten zu ermitteln:*az*. *name*- *id* .elb. *region*.amazonaws.com.

Linux oder Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Erstellen eines Application Load Balancers

Ein Load Balancer empfängt Anfragen von Clients und leitet sie über Ziele in einer Zielgruppe weiter.

Bevor Sie beginnen, stellen Sie sicher, dass Sie über eine Virtual Private Cloud (VPC) mit mindestens einem öffentlichen Subnetz in jeder der Zonen verfügen, die von Ihren Zielen verwendet werden. Weitere Informationen finden Sie unter the section called “Subnetze für Ihren Load Balancer”.

Informationen zum Erstellen eines Load Balancers mit dem finden Sie unter. AWS CLIErste Schritte mit Application Load Balancers mithilfe der AWS CLI

Um einen Load Balancer mit dem zu erstellen AWS Management Console, führen Sie die folgenden Aufgaben aus.

Aufgaben

- Schritt 1: Konfigurieren einer Zielgruppe
- Schritt 2: Registrieren von Zielen
- Schritt 3: Konfigurieren von Load Balancer und Listener
- Schritt 4: Testen des Load Balancers

Schritt 1: Konfigurieren einer Zielgruppe

Durch die Konfiguration einer Zielgruppe können Sie Ziele wie EC2 Instances registrieren. Die Zielgruppe, die Sie in diesem Schritt konfigurieren, wird als Zielgruppe in der Listener-Regel verwendet, wenn Sie Ihren Load Balancer konfigurieren. Weitere Informationen finden Sie unter Zielgruppen für Ihre Application Load Balancer.

Um Ihre Zielgruppe mit der Konsole zu konfigurieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Target Groups aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Legen Sie im Abschnitt Grundlegende Konfiguration die folgenden Parameter fest:

   a. Wählen Sie unter Zieltyp wählen die Option Instances aus, um Ziele nach Instance-ID anzugeben, oder wählen Sie IP-Adressen aus, um Ziele nur nach IP-Adresse anzugeben. Wenn der Zieltyp eine Lambda-Funktion ist, können Sie Zustandsprüfungen aktivieren, indem Sie im Abschnitt Zustandsprüfungen die Option Aktivieren auswählen.

   b. Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein.

   c. Ändern Sie Port und Protokoll nach Bedarf.

   d. Wenn der Zieltyp Instances oder IP-Adressen ist, wählen Sie IPv4oder IPv6als IP-Adresstyp, andernfalls fahren Sie mit dem nächsten Schritt fort.

      Beachten Sie, dass nur Ziele, die den ausgewählten IP-Adresstyp haben, in diese Zielgruppe eingefügt werden können. Der IP-Adresstyp kann nicht geändert werden, nachdem die Zielgruppe erstellt wurde.

   e. Wählen Sie für VPC eine Virtual Private Cloud (VPC) mit den Zielen aus, die Sie Ihrer Zielgruppe hinzufügen möchten.

   f. Wählen Sie für Protokollversion aus, HTTP1wann das Anforderungsprotokoll HTTP/1.1 oder HTTP/2 ist; wählen Sie aus HTTP2, wann das Anforderungsprotokoll HTTP/2 oder gRPC ist; und wählen Sie gRPC, wenn das Anforderungsprotokoll gRPC ist.

5. Behalten Sie im Abschnitt Zustandsprüfungen die Standardeinstellungen bei. Wählen Sie unter Erweiterte Zustandsprüfungseinstellungen den Port, die Anzahl, das Timeout und das Intervall für die Zustandsprüfung aus und geben Sie die Erfolgscodes an. Überschreitet die Anzahl der Zustandsprüfungen nacheinander den Schwellenwert für fehlerhaften Zustand, nimmt der Load Balancer das Ziel außer Betrieb. Überschreitet die Anzahl der Zustandsprüfungen nacheinander

den Schwellenwert für fehlerfreien Zustand, nimmt der Load Balancer das Ziel wieder in Betrieb. Weitere Informationen finden Sie unter Gesundheitschecks für Application Load Balancer Balancer-Zielgruppen.

6. (Optional) Fügen Sie einen oder mehrere Tags wie folgt hinzu:

   a. Erweitern Sie den Abschnitt Tags.

   b. Wählen Sie Add tag.

   c. Geben Sie den Schlüssel und den Wert für das Tag ein. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen (in UTF-8) sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen. Bei Tag-Werten muss die Groß- und Kleinschreibung beachtet werden.

7. Wählen Sie Weiter aus.

Schritt 2: Registrieren von Zielen

Sie können EC2 Instances, IP-Adressen oder Lambda-Funktionen als Ziele in einer Zielgruppe registrieren. Dies ist ein optionaler Schritt zum Erstellen eines Load Balancers. Sie müssen Ihre Ziele jedoch registrieren, um sicherzustellen, dass Ihr Load Balancer den Datenverkehr an sie weiterleitet.

1. Auf der Seite Ziele registrieren fügen Sie ein oder mehrere Ziele wie folgt hinzu:

   - Wenn der Zieltyp Instances ist, wählen Sie eine oder mehrere Instances aus, geben Sie einen oder mehrere Ports ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus.
   - Wenn der Zieltyp IP-Adressen lautet, gehen Sie wie folgt vor:

     a. Wählen Sie eine Netzwerk-VPC in der Liste aus oder wählen Sie Andere private IP-Adresse aus.

     b. Geben Sie die IP-Adresse manuell ein oder suchen Sie die IP-Adresse anhand der Instance-Details. Sie können bis zu fünf IP-Adressen gleichzeitig eingeben.

     c. Geben Sie die Ports für die Weiterleitung des Datenverkehrs an die angegebenen IP-Adressen ein.

     d. Wählen Sie Schließen Sie die unten angeführten als ausstehend ein aus.

   - Wenn der Zieltyp Lambda ist, wählen Sie eine Lambda-Funktion aus oder geben Sie einen Lambda-Funktions-ARN ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus.

2. Wählen Sie Zielgruppe erstellen aus.

Schritt 3: Konfigurieren von Load Balancer und Listener

Um einen Application Load Balancer zu erstellen, müssen Sie zunächst grundlegende Konfigurationsinformationen für Ihren Load Balancer angeben, z. B. einen Namen, ein Schema und einen IP-Adresstyp. Geben Sie anschließend Informationen über Ihr Netzwerk und einen oder mehrere Listener an. Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Er wird mit einem Protokoll und einem Port für Verbindungen von Clients zum Load Balancer konfiguriert. Weitere Informationen zu unterstützten Protokollen und Ports finden Sie unter Listener-Konfiguration.

So konfigurieren Sie Ihren Load Balancer und Listener mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Klicken Sie auf Load Balancer erstellen.
4. Wählen Sie unter Application Load Balancer Create (Erstellen) aus.
5. Basiskonfiguration

    a. Geben Sie im Feld Name des Load Balancers einen Namen für Ihren Load Balancer ein. Beispiel, **`my-alb`**. Der Name Ihres Application Load Balancers muss innerhalb Ihrer Gruppe von Application Load Balancers und Network Load Balancers für die Region eindeutig sein. Namen dürfen maximal 32 Zeichen lang sein und dürfen nur alphanumerische Zeichen und Bindestriche enthalten. Sie dürfen nicht mit einem Bindestrich oder mit `internal-` beginnen oder enden. Der Name Ihres Application Load Balancers kann nicht mehr geändert werden, sobald er erstellt wurde.

    b. Wählen Sie für Scheme (Schema) entweder Internet-facing (Mit dem Internet verbunden) oder Internal (Intern) aus. Ein mit dem Internet verbundener Load Balancer leitet Anfragen von Clients über das Internet an Ziele weiter. Ein interner Load Balancer leitet Anforderungen an Ziele unter Verwendung privater IP-Adressen weiter.

    c. Wählen Sie IPv4als IP-Adresstyp Dualstack oder Dualstack without public. IPv4 Wählen Sie aus IPv4, ob Ihre Clients IPv4 Adressen für die Kommunikation mit dem Load Balancer verwenden. Wählen Sie Dualstack, wenn Ihre Clients IPv4 sowohl als auch IPv6 Adressen für die Kommunikation mit dem Load Balancer verwenden. Wählen Sie Dualstack ohne public, IPv4 wenn Ihre Clients nur IPv6 Adressen für die Kommunikation mit dem Load Balancer verwenden.

6. Netzwerkzuordnung

   a. Wählen Sie für VPC die VPC aus, die Sie für Ihre EC2 Instances verwendet haben. Wenn Sie Internet-facing für Scheme ausgewählt haben, steht nur die Option VPCs mit Internet-Gateway zur Auswahl.

   b. Für IPAM-IP-Adresspools können Sie wählen, ob Sie den IPAM-Pool für öffentliche Adressen verwenden möchten. IPv4 Weitere Informationen finden Sie unter IPAM-IP-Adresspools

   c. Aktivieren Sie für Availability Zones und Subnetze Zonen für Ihren Load Balancer, indem Sie Subnetze wie folgt auswählen:

      - Subnetze aus zwei oder mehr Availability Zones
      - Subnetze aus einer oder mehreren Local Zones
      - Outpost-Subnetz

      Weitere Informationen finden Sie unter the section called “Subnetze für Ihren Load Balancer”.

      Für interne Load Balancer werden die IPv6 Adressen IPv4 und aus dem Subnetz CIDR zugewiesen.

      Wenn Sie den Dualstack-Modus für den Load Balancer aktiviert haben, wählen Sie Subnetze mit beiden Blöcken und CIDR-Blöcken aus. IPv4 IPv6

7. Für die Security groups (Sicherheitsgruppen) können Sie eine vorhandene Sicherheitsgruppe auswählen oder eine neue erstellen.

   Die Sicherheitsgruppe für Ihren Load Balancer ermöglicht die Kommunikation mit registrierten Zielen sowohl auf dem Listener-Port als auch auf dem Zustandsprüfungs-Port. Die Konsole kann eine Sicherheitsgruppe für Ihren Load Balancer mit Regeln erstellen, die diese Kommunikation zulassen. Sie können auch eine Sicherheitsgruppe erstellen und diese stattdessen auswählen. Weitere Informationen finden Sie unter Empfohlene Regeln.

   (Optional) Um eine neue Sicherheitsgruppe für Ihren Load Balancer zu erstellen, wählen Sie Create a new security group (Neue Sicherheitsgruppe erstellen) aus.

8. Bei Listener und Routing ist standardmäßig ein Listener eingestellt, der über Port 80 HTTP-Datenverkehr annimmt. Sie können das Standardprotokoll und den Standardport beibehalten oder andere auswählen. Wählen Sie für Default action (Standardaktion) die von Ihnen erstellte

Zielgruppe aus. Sie können optional Add listener (Listener hinzufügen) auswählen, um einen weiteren Listener hinzuzufügen (z. B. einen HTTPS-Listener).

9. (Optional) Wenn Sie einen HTTPS-Listener verwenden

   Wir empfehlen, dass Sie für Sicherheitsrichtlinie immer die neueste vordefinierte Sicherheitsrichtlinie verwenden.

   a. Für das SSL/TLS Standardzertifikat sind die folgenden Optionen verfügbar:

      - Wenn Sie ein Zertifikat mit erstellt oder importiert haben AWS Certificate Manager, wählen Sie Aus ACM und dann das Zertifikat unter Zertifikat auswählen aus.
      - Wenn Sie ein Zertifikat mit IAM importiert haben, wählen Sie Von ACM aus und wählen Sie dann das Zertifikat unter Zertifikat auswählen aus.
      - Wenn Sie ein Zertifikat importieren, aber ACM in Ihrer Region nicht verfügbar ist, wählen Sie Importieren und dann An IAM aus. Geben Sie im Feld Zertifikatname den Namen des Zertifikats ein. Kopieren Sie den Inhalt der privaten Schlüsseldatei (PEM-kodiert) und fügen Sie ihn in das Feld Privater Zertifikatsschlüssel ein. Kopieren Sie den Inhalt der öffentlichen Schlüsselzertifikatdatei (PEM-kodiert) und fügen Sie ihn in das Feld Zertifikatstext ein. Kopieren Sie den Inhalt der Zertifikatskettendatei (PEM-kodiert) und fügen Sie ihn in das Feld Certificate Chain (Zertifikats-Kette) ein, es sei denn, Sie verwenden ein selbst signiertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.

   b. (Optional) Um die gegenseitige Authentifizierung zu aktivieren, aktivieren Sie unter Verwaltung von Client-Zertifikaten die Option Gegenseitige Authentifizierung (mTLS).

      Wenn diese Option aktiviert ist, ist der standardmäßige Modus für gegenseitiges TLS Passthrough.

      Wenn Sie „Mit Trust Store verifizieren“ auswählen:

      - Standardmäßig werden Verbindungen mit abgelaufenen Client-Zertifikaten abgelehnt. Um dieses Verhalten zu ändern, erweitern Sie die erweiterten mTLS-Einstellungen und wählen Sie dann unter Ablauf des Client-Zertifikats die Option Abgelaufene Client-Zertifikate zulassen aus.
      - Wählen Sie unter Trust Store einen vorhandenen Trust Store aus, oder wählen Sie Neuer Trust Store aus.

- Wenn Sie Neuer Vertrauensspeicher ausgewählt haben, geben Sie einen Namen für den Vertrauensspeicher, den Speicherort der S3-URI-Zertifizierungsstelle und optional einen Speicherort für die Sperrliste für S3-URI-Zertifikate an.
- (Optional) Wählen Sie aus, ob Sie Advertise TrustStore CA Subject Names aktivieren möchten.

10. (Optional) Sie können während der Erstellung unter Mit Serviceintegrationen optimieren andere Dienste in Ihren Load Balancer integrieren.

    - Sie können wählen, ob Sie AWS WAFSicherheitsvorkehrungen für Ihren Load Balancer mit einer vorhandenen oder automatisch erstellten Web-ACL einbeziehen möchten. Nach der Erstellung ACLs kann das Web in der AWS WAF Konsole verwaltet werden. Weitere Informationen finden Sie im Entwicklerhandbuch unter Web-ACL mit einer AWS Ressource verknüpfen oder deren Zuordnung aufheben.AWS WAF
    - Sie können wählen, ob Sie einen Accelerator für Sie AWS Global Acceleratorerstellen und Ihren Load Balancer mit dem Accelerator verknüpfen möchten. Der Name des Beschleunigers kann die folgenden Zeichen (bis zu 64 Zeichen) enthalten: a-z, A-Z, 0-9,. (Punkt) und - (Bindestrich). Nachdem der Accelerator erstellt wurde, können Sie ihn in der AWS Global Accelerator Konsole verwalten. Weitere Informationen finden Sie im AWS Global Accelerator Entwicklerhandbuch unter Hinzufügen eines Accelerators beim Erstellen eines Load Balancers.

11. Hinzufügen von Tags und Erstellen

    a. (Optional) Sie können zwecks Kategorisierung Ihrem Load Balancer ein Tag hinzufügen. Tag-Schlüssel müssen für jeden Load Balancer eindeutig sein. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen (in UTF-8) sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen. Bei Tag-Werten muss die Groß- und Kleinschreibung beachtet werden.

    b. Überprüfen Sie Ihre Konfiguration und wählen Sie Load Balancer erstellen aus. Bei der Erstellung werden einige Standardattribute auf Ihren Load Balancer angewendet. Sie können sie nach der Erstellung des Load Balancers anzeigen und bearbeiten. Weitere Informationen finden Sie unter Load Balancer-Attribute.

Schritt 4: Testen des Load Balancers

Nachdem Sie Ihren Load Balancer erstellt haben, können Sie überprüfen, ob Ihre EC2 Instances die erste Zustandsprüfung bestehen. Anschließend können Sie überprüfen, ob der Load Balancer

Traffic an Ihre EC2 Instance sendet. Informationen zum Löschen des Load Balancers finden Sie unter Löschen eines Application Load Balancers.

So testen Sie den Load Balancer

1. Nachdem der Load Balancer erstellt wurde, klicken Sie auf Close (Schließen).
2. Wählen Sie im Navigationsbereich Target Groups aus.
3. Wählen Sie die neu erstellte Zielgruppe aus.
4. Wählen Sie Targets und vergewissern Sie sich, dass die Instances bereit sind. Wenn der Status einer Instance `initial` lautet, liegt das in der Regel daran, dass sich die Instance noch im Registrierungsprozess befindet. Dieser Status kann auch darauf hindeuten, dass die Instance nicht die Mindestanzahl an Zustandsprüfungen nicht bestanden hat, um als fehlerfrei angesehen zu werden. Wenn der Status von mindestens einer Instance fehlerfrei ist, können Sie Ihren Load Balancer testen. Weitere Informationen finden Sie unter Zustandsstatus des Ziels.
5. Klicken Sie im Navigationsbereich auf Load Balancers.
6. Wählen Sie den neu erstellten Load Balancer aus.
7. Wählen Sie Beschreibung und kopieren Sie den DNS-Namen des mit dem Internet verbundenen oder internen Load Balancers (z. B. my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com).

   - Fügen Sie für mit dem Internet verbundene Load Balancer den DNS-Namen in das Adressfeld eines mit dem Internet verbundenen Webbrowsers ein.
   - Fügen Sie für interne Load Balancer den DNS-Namen in das Adressfeld eines Webbrowsers ein, der über private Konnektivität mit der VPC verbunden ist.

   Wenn alles korrekt konfiguriert ist, zeigt der Browser die Standardseite Ihres Servers an.
8. Wenn die Webseite nicht angezeigt wird, finden Sie in den folgenden Dokumenten zusätzliche Hilfe für die Konfiguration und Schritte zur Fehlerbehebung.

   - Informationen zu Problemen in Bezug auf DNS finden Sie unter Weiterleiten von Datenverkehr an einen ELB Load Balancer im Entwicklerhandbuch von Amazon Route 53.
   - Informationen zu Problemen im Zusammenhang mit Load Balancer finden Sie unter Fehlerbehebung bei Ihren Application Load Balancern.

Aktualisieren Sie die Availability Zones für Ihren Application Load Balancer

Sie können die Availability Zones für Ihren Load Balancer jederzeit aktivieren oder deaktivieren. Nachdem Sie eine Availability Zone aktiviert haben, beginnt der Load Balancer, Anforderungen an die registrierten Ziele in der Availability Zone weiterzuleiten. Bei Application Load Balancers ist standardmäßig der zonenübergreifende Load Balancing aktiviert, was dazu führt, dass Anfragen an alle registrierten Ziele in allen Availability Zones weitergeleitet werden. Wenn der zonenübergreifende Load Balancing deaktiviert ist, leitet der Load Balancer Anfragen nur an Ziele in derselben Availability Zone weiter. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing. Ihr Load Balancer ist am effektivsten, wenn Sie dafür sorgen, dass jede aktivierte Availability Zone mindestens ein registriertes Ziel hat.

Nachdem Sie eine Availability Zone deaktivieren, bleiben die Ziele in der Availability Zone beim Load Balancer registriert, aber der Load Balancer leitet keine Anforderungen an sie weiter.

So aktualisieren Sie Availability Zones mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Netzwerkzuordnung die Option Subnetze bearbeiten aus.
5. Um eine Availability Zone zu aktivieren, aktivieren Sie das entsprechende Kontrollkästchen und wählen Sie ein Subnetz aus. Wenn nur ein Subnetz verfügbar ist, ist es bereits für Sie ausgewählt.
6. Um das Subnetz für eine aktivierte Availability Zone zu ändern, wählen Sie eines der anderen Subnetze in der Liste aus.
7. Um eine Availability Zone zu deaktivieren, deaktivieren Sie das entsprechende Kontrollkästchen.
8. Wählen Sie Änderungen speichern aus.

Um Availability Zones mit dem zu aktualisieren AWS CLI

Verwenden Sie den Befehl set-subnets.

Sicherheitsgruppen für Ihren Application Load Balancer

Die Sicherheitsgruppe für Ihren Application Load Balancer steuert den Datenverkehr, der den Load Balancer erreichen und verlassen darf. Sie müssen sicherstellen, dass der Load Balancer mit den registrierten Zielen sowohl auf dem Listener-Port als auch auf dem Zustandsprüfungs-Port kommunizieren kann. Wenn Sie einen Listener zum Load Balancer hinzufügen oder den Zustandsprüfungs-Port für eine Zielgruppe, die vom Load Balancer zum Weiterleiten von Anforderungen verwendet wird, aktualisieren, müssen Sie überprüfen, ob die Sicherheitsgruppen für den Load Balancer den Datenverkehr auf dem neuen Port in beide Richtungen zulassen. Falls nicht, können Sie die Regeln für die derzeit zugeordneten Sicherheitsgruppen ändern oder dem Load Balancer andere Sicherheitsgruppen zuordnen. Sie können die Ports und Protokolle auswählen, die zugelassen werden sollen. Sie können beispielsweise ICMP-Verbindungen (Internet Control Message Protocol) für den Load Balancer öffnen, um auf Ping-Anforderungen zu antworten (Ping-Anforderungen werden jedoch nicht an alle Instances übermittelt).

Empfohlene Regeln

Die folgenden Regeln werden für einen Load Balancer empfohlen, der mit dem Internet verbunden ist.

Inbound		
Source	Port Range	Comment
0.0.0.0/0	*listener*	Allen eingehenden Datenverkehr auf dem Load Balancer Listener-Port erlauben
Outbound		
Destination	Port Range	Comment
instance security group	*instance listener*	Ausgehenden Datenverkehr an Instances auf dem Instance-Listener-Port erlauben
instance security group	*health check*	Ausgehenden Datenverkehr an Instances auf dem

		Zustandsprüfungsport erlauben

Die folgenden Regeln werden für einen internen Load Balancer empfohlen.

Inbound

Source	Port Range	Comment
VPC CIDR	*listener*	Eingehenden Datenverkehr aus dem VPC CIDR auf dem Load Balancer-Listener-Port erlauben

Outbound

Destination	Port Range	Comment
instance security group	*instance listener*	Ausgehenden Datenverkehr an Instances auf dem Instance-Listener-Port erlauben
instance security group	*health check*	Ausgehenden Datenverkehr an Instances auf dem Zustandsprüfungsport erlauben

Die folgenden Regeln werden für einen Application Load Balancer empfohlen, der als Ziel für einen Network Load Balancer verwendet wird.

Inbound

Source	Port Range	Comment

client IP addresses/ CIDR	*alb listener*	Eingehenden Client-Datenverkehr am Load-Balancer-Listener-Port erlauben.
VPC CIDR	*alb listener*	Lassen Sie eingehenden Client-Verkehr über AWS PrivateLink den Load Balancer-Listener-Port zu
VPC CIDR	*alb listener*	Eingehenden Zustandsdatenverkehr vom Network Load Balancer erlauben

Outbound

Destination	Port Range	Comment
instance security group	*instance listener*	Ausgehenden Datenverkehr an Instances auf dem Instance-Listener-Port erlauben
instance security group	*health check*	Ausgehenden Datenverkehr an Instances auf dem Zustandsprüfungsport erlauben

Beachten Sie, dass die Sicherheitsgruppen für Ihren Application Load Balancer die Verbindungsverfolgung verwenden, um Informationen über den vom Network Load Balancer kommenden Datenverkehr zu verfolgen. Das geschieht unabhängig von den Sicherheitsgruppenregeln, die für Ihren Application Load Balancer festgelegt wurden. Weitere Informationen zur EC2 Amazon-Verbindungsverfolgung finden Sie unter Verbindungsverfolgung für Sicherheitsgruppen im EC2 Amazon-Benutzerhandbuch.

Um sicherzustellen, dass Ihre Ziele ausschließlich Traffic vom Load Balancer erhalten, beschränken Sie die mit Ihren Zielen verknüpften Sicherheitsgruppen so, dass sie ausschließlich Traffic vom Load Balancer akzeptieren. Dies kann erreicht werden, indem Sie die Sicherheitsgruppe des Load Balancers als Quelle in der Eingangsregel der Sicherheitsgruppe des Ziels festlegen.

Außerdem sollten Sie eingehenden ICMP-Datenverkehr zur Unterstützung von Path MTU Discovery erlauben. Weitere Informationen finden Sie unter Path MTU Discovery im EC2 Amazon-Benutzerhandbuch.

Aktualisieren der zugeordneten Sicherheitsgruppen

Sie können die dem Load Balancer zugeordneten Sicherheitsgruppen jederzeit ändern.

So aktualisieren Sie Sicherheitsgruppen mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Sicherheit die Option Bearbeiten aus.
5. Um eine Sicherheitsgruppe mit Ihrem Load Balancer zu verknüpfen, wählen Sie sie aus. Um eine Sicherheitsgruppenverknüpfung zu entfernen, wählen Sie das X-Symbol für die Sicherheitsgruppe.
6. Wählen Sie Änderungen speichern aus.

Um Sicherheitsgruppen mit dem zu aktualisieren AWS CLI

Verwenden Sie den set-security-groups-Befehl.

Aktualisieren Sie die IP-Adresstypen für Ihren Application Load Balancer

Sie können Ihren Application Load Balancer so konfigurieren, dass Clients mit dem Load Balancer nur über IPv4 Adressen oder über beide IPv4 Adressen kommunizieren können (IPv6 Dualstack). Der Load Balancer kommuniziert mit Zielen auf der Grundlage des IP-Adresstyps der Zielgruppe. Weitere Informationen finden Sie unter IP-Adresstyp.

Dualstack-Anforderungen

- Sie können den IP-Adressentyp bei der Erstellung des Load Balancers festlegen und jederzeit aktualisieren.

- Der Virtual Private Cloud (VPC) und den Subnetzen, die Sie für den Load Balancer angeben, müssen zugeordnete IPv6 CIDR-Blöcke haben. Weitere Informationen finden Sie unter IPv6Adressen im EC2 Amazon-Benutzerhandbuch.
- Die Routing-Tabellen für die Load Balancer-Subnetze müssen den Verkehr weiterleiten IPv6 .
- Die Sicherheitsgruppen für den Load Balancer müssen Datenverkehr zulassen. IPv6
- Das Netzwerk ACLs für die Load Balancer-Subnetze muss Datenverkehr zulassen. IPv6

So legen Sie den IP-Adresstyp bei der Erstellung fest

Konfigurieren Sie die Einstellungen wie unter Erstellen eines Load Balancers beschrieben.

So aktualisieren Sie den IP-Adresstyp mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Netzwerkzuordnung die Option IP-Adressentyp bearbeiten aus.
5. Wählen Sie für den IP-Adresstyp, ob IPv4nur IPv4 Adressen unterstützt werden sollen, Dualstack, um beide IPv4 IPv6 Adressen zu unterstützen, oder Dualstack without public, um nur Adressen IPv4 zu unterstützen. IPv6
6. Wählen Sie Änderungen speichern aus.

Um den IP-Adresstyp mit dem zu aktualisieren AWS CLI

Verwenden Sie den set-ip-address-type-Befehl.

Aktualisieren Sie die IPAM-IP-Adresspools für Ihren Application Load Balancer

IPAM-IP-Adresspools müssen zuerst in IPAM erstellt werden, bevor sie von Ihrem Application Load Balancer verwendet werden können. Weitere Informationen finden Sie unter Bringen Sie Ihre IP-Adressen zu IPAM.

So richten Sie die IPAM-IP-Adresspools bei der Erstellung ein

Konfigurieren Sie die Einstellungen wie unter Erstellen eines Load Balancers beschrieben.

Um die IPAM-IP-Adresspools mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Netzwerkzuordnung die Option IP-Pools bearbeiten aus.
5. Aktivieren Sie unter IP-Pools die Option IPAM-Pool für öffentliche IPv4 Adressen verwenden.
6. Wählen Sie unter Öffentlicher IPv4 IPAM-Pool den IPAM-Pool aus, den Sie verwenden möchten.
7. Wählen Sie Änderungen speichern aus.

Um die IPAM-IP-Adresspools mit dem zu aktualisieren AWS CLI

Verwenden Sie den modify-ip-pools-Befehl.

Integrationen für Ihren Application Load Balancer

Sie können Ihre Application Load Balancer Balancer-Architektur optimieren, indem Sie sie in mehrere andere AWS Dienste integrieren, um die Leistung, Sicherheit und Verfügbarkeit Ihrer Anwendung zu verbessern.

Load Balancer-Integrationen

- Amazon Application Recovery Controller (ARC)
- Amazon CloudFront + AWS WAF
- AWS Global Accelerator
- AWS Config
- AWS WAF

Amazon Application Recovery Controller (ARC)

Amazon Application Recovery Controller (ARC) unterstützt Sie bei der Vorbereitung und Durchführung schnellerer Wiederherstellungsvorgänge für Anwendungen, die auf ausgeführt AWS werden. Zonal Shift und Zonal Autoshift sind Funktionen von Amazon Application Recovery Controller (ARC).

Mit Zonal Shift können Sie den Verkehr mit einer einzigen Aktion von einer beeinträchtigten Availability Zone wegverlagern. Auf diese Weise können Sie den Betrieb von anderen fehlerfreien Availability Zones in einer AWS-Region fortsetzen.

Mit Zonal Autoshift autorisieren AWS Sie, den Ressourcenverkehr für eine Anwendung bei Ereignissen in Ihrem Namen aus einer Availability Zone zu verlagern, um die Zeit bis zur Wiederherstellung zu verkürzen. AWS startet eine automatische Verschiebung, wenn die interne Überwachung darauf hindeutet, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Wenn ein Autoshift gestartet wird, AWS beginnt der Anwendungsdatenverkehr zu Ressourcen, die Sie für zonales Autoshift konfiguriert haben, von der Availability Zone weg zu verlagern.

Wenn Sie eine Zonenverschiebung starten, sendet Ihr Load Balancer keinen neuen Datenverkehr für die Ressource mehr an die betroffene Availability Zone. ARC erstellt die Zonenverschiebung sofort. Es kann jedoch eine kurze Zeit dauern, bis bestehende, laufende Verbindungen in der Availability Zone abgeschlossen sind. Dies hängt vom Verhalten des Clients und der Wiederverwendung der Verbindung ab. Abhängig von Ihren DNS-Einstellungen und anderen Faktoren können bestehende Verbindungen in nur wenigen Minuten abgeschlossen werden oder länger dauern. Weitere Informationen finden Sie unter Beschränken der Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben, im Amazon Application Recovery Controller (ARC) Developer Guide.

Um Zonal Shift-Funktionen auf Application Load Balancers verwenden zu können, muss das ARC-Integrationsattribut für Zonal Shift auf Aktiviert gesetzt sein.

Bevor Sie die Amazon Application Recovery Controller (ARC) -Integration aktivieren und mit der Nutzung von Zonal Shift beginnen, sollten Sie Folgendes überprüfen:

- Sie können eine Zonenverschiebung für einen bestimmten Load Balancer nur für eine Availability Zone starten. Eine Zonenverschiebung lässt sich nicht für mehrere Availability Zones starten.
- AWS entfernt proaktiv IP-Adressen von zonalen Load Balancer-Diensten aus DNS, wenn mehrere Infrastrukturprobleme die Dienste beeinträchtigen. Prüfen Sie immer die aktuelle Kapazität der Availability Zone, bevor Sie mit einer Zonenverschiebung beginnen. Wenn bei Ihren Load Balancern das zonenübergreifende Load Balancing deaktiviert ist und Sie eine Zonenverschiebung verwenden, um eine zonale Load-Balancer-IP-Adresse zu entfernen, verliert die Availability Zone, die von der Zonenverschiebung betroffen ist, auch die Zielkapazität.

Weitere Informationen finden Sie unter Bewährte Methoden für Zonenverschiebungen in ARC im Amazon Application Recovery Controller (ARC) Developer Guide.

Zonenübergreifende, aktivierte Application Load Balancers

Wenn eine Zonenverschiebung auf einem Application Load Balancer mit aktiviertem zonenübergreifendem Load Balancing gestartet wird, wird der gesamte Datenverkehr zu Zielen in der betroffenen Availability Zone blockiert, und zonale IP-Adressen werden aus DNS entfernt.

Vorteile:

- Schnellere Wiederherstellung nach Ausfällen in der Availability Zone.
- Die Möglichkeit, den Datenverkehr in eine fehlerfreie Availability Zone zu verlagern, falls in einer Availability Zone Fehler festgestellt werden.
- Sie können die Anwendungsintegrität testen, indem Sie Fehler simulieren und identifizieren, um ungeplante Ausfallzeiten zu verhindern.

Verwaltungsüberschreibung bei zonaler Schicht

Ziele, die zu einem Application Load Balancer gehören, erhalten einen neuen Status`AdministrativeOverride`, der unabhängig vom `TargetHealth` Status ist.

Wenn eine Zonenverschiebung für einen Application Load Balancer gestartet wird, gelten alle Ziele innerhalb der Zone, aus der verschoben wird, als vom Administrator überschrieben. Der Application Load Balancer beendet die Weiterleitung von neuem Datenverkehr an die vom Administrator überschriebenen Ziele, bestehende Verbindungen bleiben jedoch intakt, bis sie organisch geschlossen werden.

Die möglichen Zustände sind: `AdministrativeOverride`

unbekannt

Der Status kann aufgrund eines internen Fehlers nicht weitergegeben werden

no_override

Auf dem Ziel ist derzeit kein Override aktiv

zonal_shift_active

Zonal Shift ist in der Ziel-Availability Zone aktiv

Amazon CloudFront + AWS WAF

Amazon CloudFront ist ein Webservice, der dazu beiträgt, die Leistung, Verfügbarkeit und Sicherheit Ihrer Anwendungen zu verbessern, die Sie verwenden AWS. CloudFront fungiert als verteilter, zentraler Zugangspunkt für Ihre Webanwendungen, die Application Load Balancers verwenden. Es erweitert die globale Reichweite Ihres Application Load Balancers und ermöglicht es ihm, Benutzer effizient von nahegelegenen Edge-Standorten aus zu bedienen, die Inhaltsbereitstellung zu optimieren und die Latenz für Benutzer weltweit zu reduzieren. Das automatische Zwischenspeichern von Inhalten an diesen Edge-Standorten reduziert die Belastung Ihres Application Load Balancer erheblich und verbessert so dessen Leistung und Skalierbarkeit.

Die in der Elastic Load Balancing Balancing-Konsole verfügbare Ein-Klick-Integration erstellt eine CloudFront Distribution mit den empfohlenen AWS WAF Sicherheitsvorkehrungen und ordnet sie Ihrem Application Load Balancer zu. Die AWS WAF Schutzmaßnahmen blockieren vor gängigen Web-Exploits, bevor sie Ihren Load Balancer erreichen. Sie können auf die CloudFront Distribution und das entsprechende Sicherheits-Dashboard über den Tab Integrationen des Load Balancers in der Konsole zugreifen. Weitere Informationen finden Sie unter Sicherheitsvorkehrungen im AWS WAF Sicherheits-Dashboard verwalten im CloudFront Amazon CloudFront Developer Guide und Introducing CloudFront Security Dashboard, a Unified CDN and Security Experience auf aws.amazon.com/blogs.

Aus Sicherheitsgründen sollten Sie die Sicherheitsgruppen Ihres mit dem Internet verbundenen Application Load Balancers so konfigurieren, dass eingehender Datenverkehr nur aus der Liste mit AWS verwalteten Präfixen zugelassen wird, und alle anderen Regeln für eingehenden Datenverkehr entfernen. CloudFront Weitere Informationen finden Sie unter Verwenden der CloudFront verwalteten Präfixliste, Konfigurieren, CloudFront um Anfragen einen benutzerdefinierten HTTP-Header hinzuzufügen und Einen Application Load Balancer so konfigurieren, dass er nur Anfragen weiterleitet, die einen bestimmten Header enthalten im Amazon CloudFront Developer Guide >.

> **Note**
>
> CloudFront unterstützt nur ACM-Zertifikate in der Region USA Ost (Nord-Virginia) us-east-1. Wenn Ihr Application Load Balancer über einen HTTPS-Listener verfügt, der mit einem ACM-Zertifikat in einer anderen Region als us-east-1 konfiguriert ist, müssen Sie entweder die CloudFront Ursprungsverbindung von HTTPS auf HTTP ändern oder ein ACM-Zertifikat in der Region USA Ost (Nord-Virginia) bereitstellen und es an Ihre Distribution anhängen. CloudFront

AWS Global Accelerator

Um die Verfügbarkeit, Leistung und Sicherheit von Anwendungen zu optimieren, erstellen Sie einen Beschleuniger für Ihren Load Balancer. Der Accelerator leitet den Datenverkehr über das AWS globale Netzwerk an statische IP-Adressen weiter, die als feste Endpunkte in der Region dienen, die dem Client am nächsten ist. AWS Global Accelerator ist durch Shield Standard geschützt, wodurch Anwendungsausfälle und Latenz aufgrund von DDo S-Angriffen minimiert werden.

Weitere Informationen finden Sie im AWS Global Accelerator Entwicklerhandbuch unter Hinzufügen eines Accelerators bei der Erstellung eines Load Balancers.

AWS Config

Um die Überwachung und Einhaltung von Vorschriften für Ihren Load Balancer zu optimieren, richten Sie ihn ein. AWS Config AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS Ressourcen in Ihrem AWS Konto. Dazu gehört auch, wie die Ressourcen miteinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, sodass Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit ändern. AWS Config optimiert Audits, Einhaltung von Vorschriften und Problembehebung.

Weitere Informationen finden Sie unter Was ist AWS Config? im AWS Config Entwicklerhandbuch.

AWS WAF

Sie können es AWS WAF zusammen mit Ihrem Application Load Balancer verwenden, um Anfragen auf der Grundlage der Regeln in einer Web-Zugriffskontrollliste (Web-ACL) zuzulassen oder zu blockieren.

Wenn der Load Balancer keine Antwort von erhalten kann AWS WAF, gibt er standardmäßig einen HTTP 500-Fehler zurück und leitet die Anfrage nicht weiter. Wenn Sie möchten, dass Ihr Load Balancer Anfragen an Ziele weiterleitet, auch wenn er keinen Kontakt herstellen kann AWS WAF, können Sie AWS WAF Fail Open aktivieren.

Vordefiniertes Web ACLs

Wenn Sie die AWS WAF Integration aktivieren, können Sie wählen, ob automatisch eine neue Web-ACL mit vordefinierten Regeln erstellt werden soll. Die vordefinierte Web-ACL umfasst drei AWS verwaltete Regeln, die Schutz vor den häufigsten Sicherheitsbedrohungen bieten.

- `AWSManagedRulesAmazonIpReputationList`- Die Regelgruppe der Amazon IP-Reputationsliste blockiert IP-Adressen, die typischerweise mit Bots oder anderen Bedrohungen in Verbindung stehen. Weitere Informationen finden Sie unter verwaltete Regelgruppe der Amazon IP-Reputationsliste im AWS WAF Entwicklerhandbuch.
- `AWSManagedRulesCommonRuleSet`- Die Regelgruppe Core Rule Set (CRS) bietet Schutz vor der Ausnutzung einer Vielzahl von Sicherheitslücken, darunter einige der risikoreichen und häufig auftretenden Sicherheitslücken, die in OWASP-Publikationen wie OWASP Top 10 beschrieben werden. Weitere Informationen finden Sie unter verwaltete Regelgruppe Core Rule Set (CRS) im Entwicklerhandbuch.AWS WAF
- `AWSManagedRulesKnownBadInputsRuleSet`- Die Regelgruppe Bekannte fehlerhafte Eingaben blockiert Anforderungsmuster, die bekanntermaßen ungültig sind und mit der Ausnutzung oder Entdeckung von Sicherheitslücken in Verbindung stehen. Weitere Informationen finden Sie unter Verwaltete Regelgruppe „Bekannte fehlerhafte Eingaben“ im AWS WAF Entwicklerhandbuch.

Weitere Informationen finden Sie unter Verwenden des ACLs Webs AWS WAF im AWS WAF Entwicklerhandbuch.

Attribute für Ihren Application Load Balancer bearbeiten

Nachdem Sie einen Application Load Balancer erstellt haben, können Sie seine Attribute bearbeiten.

Load Balancer-Attribute

- Zeitlimit für Verbindungsleerlauf
- Keepalive-Dauer des HTTP-Clients
- Löschschutz
- Desynchroner Mitigationsmodus
- Beibehalten der Host-Header

Zeitlimit für Verbindungsleerlauf

Das Timeout bei der Verbindungsinaktivität ist der Zeitraum, für den eine bestehende Client- oder Zielverbindung inaktiv bleiben kann, ohne dass Daten gesendet oder empfangen werden, bevor der Load Balancer die Verbindung schließt.

Um sicherzustellen, dass langwierige Vorgänge wie Datei-Uploads rechtzeitig abgeschlossen werden können, senden Sie vor Ablauf jedes Leerlauf-Timeouts mindestens 1 Byte an Daten und erhöhen Sie die Dauer des Leerlauf-Timeouts nach Bedarf. Wir empfehlen außerdem, das Leerlaufzeitlimit für Ihre Anwendung auf einen höheren Wert als das Leerlaufzeitlimit für den Load Balancer festzulegen. Andernfalls könnte der Load Balancer, wenn die Anwendung die TCP-Verbindung zum Load Balancer nicht ordnungsgemäß schließt, eine Anforderung an die Anwendung senden, bevor er das Paket empfängt, um anzugeben, dass die Verbindung geschlossen ist. Wenn dies der Fall ist, sendet der Load Balancer einen HTTP-502-Bad-Gateway-Fehler an den Client.

Application Load Balancer unterstützen keine HTTP/2-PING-Frames. Diese setzen das Timeout der Verbindung im Leerlauf nicht zurück.

Standardmäßig legt Elastic Load Balancing den Leerlauf-Timeout-Wert für Ihren Load Balancer auf 60 Sekunden oder 1 Minute fest. Gehen Sie folgendermaßen vor, um einen anderen Leerlauf-Timeoutwert festzulegen.

Um den Wert für das Leerlauf-Timeout der Verbindung mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Geben Sie unter Verkehrskonfiguration einen Wert für das Timeout bei Verbindungsinaktivität ein. Der gültige Bereich liegt zwischen 1 und 4000 Sekunden.
6. Wählen Sie Änderungen speichern aus.

Um den Wert für das Leerlauf-Timeout mit dem zu aktualisieren AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl mit dem `idle_timeout.timeout_seconds` Attribut.

Keepalive-Dauer des HTTP-Clients

Die Keepalive-Dauer des HTTP-Clients ist die maximale Zeitdauer, für die ein Application Load Balancer eine persistente HTTP-Verbindung zu einem Client unterhält. Nach Ablauf der konfigurierten Keepalive-Dauer des HTTP-Clients akzeptiert der Application Load Balancer eine weitere Anfrage und gibt dann eine Antwort zurück, mit der die Verbindung ordnungsgemäß geschlossen wird.

Die Art der vom Load Balancer gesendeten Antwort hängt von der HTTP-Version ab, die von der Client-Verbindung verwendet wird.

- Für Clients, die über HTTP 1.x verbunden sind, sendet der Load Balancer einen HTTP-Header, der das Feld enthält. `Connection: close`
- Für Clients, die über HTTP/2 verbunden sind, sendet der Load Balancer einen Frame. `GOAWAY`

Standardmäßig legt Application Load Balancer den Wert für die Keepalive-Dauer des HTTP-Clients für Load Balancer auf 3600 Sekunden oder 1 Stunde fest. Die Keepalive-Dauer des HTTP-Clients kann nicht ausgeschaltet oder unter die Mindestdauer von 60 Sekunden gesetzt werden. Sie können die Keepalive-Dauer des HTTP-Clients jedoch auf maximal 604.800 Sekunden oder 7 Tage erhöhen. Ein Application Load Balancer beginnt mit der Dauer der HTTP-Client-Keepalive-Dauer, wenn eine HTTP-Verbindung zu einem Client zum ersten Mal hergestellt wird. Die Dauer wird fortgesetzt, wenn kein Datenverkehr vorhanden ist, und wird erst zurückgesetzt, wenn eine neue Verbindung hergestellt ist.

Wenn der Load Balancer-Verkehr mithilfe von Zonal Shift oder Zonal Autoshift von einer beeinträchtigten Availability Zone weg verlagert wird, stellen Clients mit bestehenden offenen Verbindungen möglicherweise weiterhin Anfragen an den beeinträchtigten Standort, bis die Clients wieder eine Verbindung herstellen. Um eine schnellere Wiederherstellung zu unterstützen, sollten Sie einen niedrigeren Wert für die Keepalive-Dauer festlegen, um die Dauer zu begrenzen, für die Clients mit einem Load Balancer verbunden bleiben. Weitere Informationen finden Sie unter Beschränken der Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben, im Amazon Application Recovery Controller (ARC) Developer Guide.

> **Note**
>
> Wenn der Load Balancer den IP-Adresstyp Ihres Application Load Balancer auf umstelltdualstack-without-public-ipv4, wartet der Load Balancer, bis alle aktiven Verbindungen abgeschlossen sind. Um den Zeitaufwand für den Wechsel des IP-Adresstyps für Ihren Application Load Balancer zu verringern, sollten Sie die Dauer der HTTP-Client-Keepalive-Dauer verringern.

Der Application Load Balancer weist dem HTTP-Client bei der ersten Verbindung einen Wert für die Keepalive-Dauer zu. Wenn Sie die Keepalive-Dauer des HTTP-Clients aktualisieren, kann dies zu gleichzeitigen Verbindungen mit unterschiedlichen Werten für die Keepalive-Dauer des HTTP-Clients

führen. Bei bestehenden Verbindungen wird der Wert für die Keepalive-Dauer des HTTP-Clients beibehalten, der bei der ersten Verbindung angewendet wurde. Neue Verbindungen erhalten den aktualisierten Wert für die Keepalive-Dauer des HTTP-Clients.

Um den Wert für die Keepalive-Dauer des Clients mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Geben Sie unter Verkehrskonfiguration einen Wert für die Keepalive-Dauer des HTTP-Clients ein. Der gültige Bereich liegt zwischen 60 und 604800 Sekunden.
6. Wählen Sie Änderungen speichern aus.

Um den Wert für die Keepalive-Dauer des Clients zu aktualisieren, verwenden Sie den AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl mit dem `client_keep_alive.seconds` Attribut.

Löschschutz

Um zu verhindern, dass der Load Balancer versehentlich gelöscht wird, können Sie den Löschschutz aktivieren. Standardmäßig ist der Löschschutz für Ihren Load Balancer deaktiviert.

Wenn Sie den Löschschutz für Ihren Load Balancer aktivieren, müssen Sie ihn deaktivieren, bevor Sie den Load Balancer löschen.

So aktivieren Sie mithilfe der Konsole den Löschschutz:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren Sie unter Konfiguration die Option Löschschutz.
6. Wählen Sie Änderungen speichern aus.

So deaktivieren Sie mithilfe der Konsole den Löschschutz:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Schalten Sie auf der Seite Konfiguration den Löschschutz aus.
6. Wählen Sie Änderungen speichern aus.

Um den Löschschutz zu aktivieren oder zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl mit dem `deletion_protection.enabled` Attribut.

Desynchroner Mitigationsmodus

Der desynchrone Mitigationsmodus schützt Ihre Anwendung vor Problemen aufgrund von HTTP-Desync-Angriffen. Der Load Balancer klassifiziert jede Anforderung anhand ihrer Bedrohungsstufe, lässt sichere Anforderungen zu und mindert dann das Risiko gemäß dem von Ihnen angegebenen Mitigationsmodus. Die desynchronen Mitigationsmodi lauten „Überwachen“, „Defensiv“ und „Am strengsten“. Der Standardmodus ist „Defensiv“, der eine dauerhafte Abwehr gegen HTTP-Desync-Angriffe bietet und gleichzeitig die Verfügbarkeit Ihrer Anwendung gewährleistet. Sie können in den Modus „Am strengsten“ wechseln, um sicherzustellen, dass Ihre Anwendung nur Anforderungen empfängt, die RFC 7230 entsprechen.

Die Bibliothek „http_desync_guardian“ analysiert HTTP-Anforderungen, um HTTP-Desync-Angriffe zu verhindern. Weitere Informationen finden Sie unter HTTP Desync Guardian on. GitHub

Klassifizierungen

Diese Klassifizierungen lauten wie folgt:

- Konform – Die Anforderung entspricht RFC 7230 und stellt keine bekannten Sicherheitsbedrohungen dar.
- Akzeptabel – Die Anforderung entspricht nicht RFC 7230, stellt jedoch keine bekannten Sicherheitsbedrohungen dar.
- Mehrdeutig – Die Anforderung entspricht nicht RFC 7230, stellt jedoch ein Risiko dar, da verschiedene Webserver und Proxys sie unterschiedlich behandeln könnten.

- Schwerwiegend – Die Anforderung stellt ein hohes Sicherheitsrisiko dar. Der Load Balancer blockiert die Anforderung, sendet dem Client eine 400-Antwort und schließt die Client-Verbindung.

Wenn eine Anforderung nicht RFC 7230 entspricht, erhöht der Load Balancer die `DesyncMitigationMode_NonCompliant_Request_Count`-Metrik. Weitere Informationen finden Sie unter Application-Load-Balancer-Metriken.

Die Klassifizierung für jede Anforderung ist in den Load-Balancer-Zugriffsprotokollen enthalten. Wenn die Anforderung nicht entspricht, enthalten die Zugriffsprotokolle einen Ursachencode für die Klassifizierung. Weitere Informationen finden Sie unter Gründe für die Klassifizierung.

Modi

In der folgenden Tabelle wird beschrieben, wie Application Load Balancer Anforderungen basierend auf Modus und Klassifizierung behandeln.

Klassifizierung	Modus „Überwachen“	Modus „Defensiv“	Modus „Am strengsten“
Konform	Zulässig	Zulässig	Zulässig
Akzeptabel	Zulässig	Zulässig	Blocked
Mehrdeutig	Zulässig	Zulässig[1]	Blocked
Schwerwiegend	Zulässig	Blocked	Blocked

[1] Leitet die Anforderungen weiter, schließt aber die Client- und Zielverbindungen. Es können zusätzliche Gebühren anfallen, wenn Ihr Load Balancer im Modus „Defensiv“ eine große Anzahl von mehrdeutigen Anforderungen empfängt. Dies liegt daran, dass die erhöhte Anzahl neuer Verbindungen pro Sekunde dazu beiträgt, dass die Load-Balancer-Kapazitätseinheiten (LCU) pro Stunde verwendet werden. Sie können die `NewConnectionCount`-Metrik verwenden, um zu vergleichen, wie Ihr Load Balancer im Modus „Überwachen“ und im Modus „Defensiv“ neue Verbindungen herstellt.

So aktualisieren Sie den desynchronen Mitigationsmodus über die Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie unter Paketverarbeitung für Desynchroner Mitigationsmodus die Option Defensiv, Am strengsten oder Überwachen aus.
6. Wählen Sie Änderungen speichern aus.

Um den Desync-Minimationsmodus mit dem zu aktualisieren AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl, wobei das `routing.http.desync_mitigation_mode` Attribut auf`monitor`, `defensive` oder gesetzt ist. `strictest`

Beibehalten der Host-Header

Wenn Sie das Attribut Beibehalten des Host-Headers aktivieren, behält Application Load Balancer den `Host`-Header der HTTP-Anforderung bei und sendet den Header ohne Änderung an Ziele. Wenn der Application Load Balancer mehrere `Host`-Header empfängt, behält er sie alle bei. Listener-Regeln werden nur auf den ersten empfangenen `Host`-Header angewendet.

Wenn das Attribut Beibehalten des Host-Headers nicht aktiviert ist, ändert der Application Load Balancer den `Host`-Header standardmäßig wie folgt:

Wenn „Beibehalten des Host-Headers“ nicht aktiviert ist und der Listener-Port kein Standardport ist: Wenn die Standardports (Port 80 oder 443) nicht verwendet werden, hängen wir die Portnummer an den Host-Header an, sofern sie nicht bereits vom Client hinzugefügt wurde. Zum Beispiel würde der `Host`-Header in der HTTP-Anforderung mit `Host: www.example.com` in `Host: www.example.com:8080` geändert werden, wenn der Listener-Port ein nicht standardmäßiger Port ist, wie z. B. `8080`.

Wenn „Beibehalten des Host-Headers“ nicht aktiviert ist und der Listener-Port ein Standardport ist (Port 80 oder 443): Bei Standard-Listener-Ports (entweder Port 80 oder 443) fügen wir die Portnummer nicht an den ausgehenden Host-Header an. Jede Portnummer, die sich bereits im eingehenden Host-Header befand, wird entfernt.

Die folgende Tabelle zeigt weitere Beispiele dafür, wie Application Load Balancer die Host-Header in der HTTP-Anforderung auf der Grundlage des Listener-Ports behandeln.

Listener-Port	Beispielanforderung	Host-Header der Anforderung	„Beibehaltung des Host-Headers“ ist deaktiviert (Standardverhalten)	„Beibehaltung des Host-Headers“ ist aktiviert
Die Anfrage wird über den HTTP/HTTPS Standard-Listener gesendet.	`GET /index.html HTTP/1.1 Host: example.com`	example.com	example.com	example.com
Die Anfrage wird über den Standard-HTTP-Listener gesendet und der Host-Header hat einen Port (z. B. 80 oder 443).	`GET /index.html HTTP/1.1 Host: example.com:80`	example.com:80	example.com	example.com:80
Die Anforderung hat einen absoluten Pfad.	`GET https://dns_name/index.html HTTP/1.1 Host: example.com`	example.com	dns_name	example.com
Die Anfrage wird über einen nicht standardmäßigen Listener-Port gesendet (z. B. 8080)	`GET /index.html HTTP/1.1 Host: example.com`	example.com	example.com:8080	example.com

Listener-Port	Beispielanforderung	Host-Header der Anforderung	„Beibehaltung des Host-Headers“ ist deaktiviert (Standardverhalten)	„Beibehaltung des Host-Headers“ ist aktiviert
Die Anforderung wird über einen nicht standardmäßigen Listener-Port gesendet und der Host-Header enthält einen Port (z. B. 8080).	`GET /index.html HTTP/1.1 Host: example.com:8080`	example.com:8080	example.com:8080	example.com:8080

Um die Aufbewahrung von Host-Headern mithilfe der Konsole zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren Sie unter Paketverarbeitung die Option Beibehaltung des Host-Headers.
6. Wählen Sie Änderungen speichern aus.

Um die Aufbewahrung von Host-Headern zu aktivieren, verwenden Sie den AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl, bei dem das `routing.http.preserve_host_header.enabled` Attribut auf gesetzt ist`true`.

Einen Application Load Balancer taggen

Tags helfen Ihnen, Ihre Load Balancer auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung.

Sie können mehrere Tags für jeden Load Balancer hinzufügen. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der dem Load Balancer bereits zugeordnet ist, ändert sich der Wert dieses Tags.

Wenn Sie ein Tag nicht mehr benötigen, können Sie es von Ihrem Load Balancer entfernen.

Einschränkungen

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen
- Maximale Wertlänge: 255 Unicode-Zeichen
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen.
- Verwenden Sie das `aws:` Präfix nicht in Ihren Tag-Namen oder -Werten, da es für die AWS Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

So aktualisieren Sie die Tags für einen Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Tags die Option Tags verwalten aus und führen Sie einen oder mehrere der folgenden Schritte aus:
   a. Um ein Tag zu aktualisieren, bearbeiten Sie die Werte von Schlüssel und Wert.
   b. Um ein neues Tag hinzuzufügen, wählen Sie Tag hinzufügen aus und geben Sie Werte für Schlüssel und Wert ein.
   c. Um ein Tag zu löschen, wählen Sie Entfernen neben dem zu löschenden Tag aus.
5. Wenn Sie die Aktualisierung der Tags abgeschlossen haben, wählen Sie Änderungen speichern.

Um die Tags für einen Load Balancer mit dem zu aktualisieren AWS CLI

Verwenden Sie die Befehle add-tags und remove-tags.

Löschen eines Application Load Balancers

Sobald der Load Balancer verfügbar ist, wird Ihnen jede ganze oder angebrochene Stunde in Rechnung gestellt, in der er ausgeführt wird. Wenn Sie den Load Balancer nicht mehr benötigen, können Sie ihn löschen. Sobald der Load Balancer gelöscht wurde, fallen keine weiteren Kosten dafür mehr an.

Sie können einen Load Balancer nicht löschen, solange der Löschschutz aktiviert ist. Weitere Informationen finden Sie unter Löschschutz.

Beachten Sie, dass das Löschen eines Load Balancers sich nicht auf seine registrierten Ziele auswirkt. Beispielsweise laufen Ihre EC2 Instances weiterhin und sind weiterhin für ihre Zielgruppen registriert. Informationen zum Löschen Ihrer Zielgruppen finden Sie unter Löschen Sie eine Application Load Balancer Balancer-Zielgruppe.

So löschen Sie einen Load Balancer mithilfe der Konsole

1. Wenn Sie einen DNS-Eintrag für Ihre Domain haben, der auf Ihren Load Balancer verweist, verweisen Sie ihn an den neuen Standort und warten Sie, bis die DNS-Änderungen wirksam werden, bevor Sie den Load Balancer löschen.

   Beispiel:

   - Wenn es sich bei dem Datensatz um einen CNAME-Eintrag mit einer Time To Live (TTL) von 300 Sekunden handelt, warten Sie mindestens 300 Sekunden, bevor Sie mit dem nächsten Schritt fortfahren.
   - Wenn es sich bei dem Datensatz um einen Route 53-Alias(A)-Eintrag handelt, warten Sie mindestens 60 Sekunden.
   - Wenn Sie Route 53 verwenden, dauert es 60 Sekunden, bis die Datensatzänderung an alle globalen Route 53-Nameserver weitergegeben wird. Fügen Sie diese Zeit zum TTL-Wert des Datensatzes hinzu, der aktualisiert wird.
2. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Load Balancers aus.
4. Wählen Sie den Load Balancer aus und klicken Sie dann auf Aktionen und auf Load Balancer löschen.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um einen Load Balancer mit dem zu löschen AWS CLI

Verwenden Sie den delete-load-balancer-Befehl.

Sehen Sie sich die Application Load Balancer Balancer-Ressourcenübersicht an

Die Application Load Balancer Balancer-Ressourcenübersicht bietet eine interaktive Darstellung der Architektur Ihres Load Balancers, einschließlich der zugehörigen Listener, Regeln, Zielgruppen und Ziele. In der Ressourcenübersicht werden auch die Beziehungen und Routingpfade zwischen allen Ressourcen hervorgehoben, sodass die Konfiguration Ihres Load Balancers visuell dargestellt wird.

So zeigen Sie die Ressourcenübersicht Ihres Application Load Balancers mithilfe der Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie die Registerkarte Ressourcenübersicht, um die Ressourcenübersicht des Load Balancers anzuzeigen.

Komponenten der Ressourcenübersicht

Kartenansichten

In der Application Load Balancer Balancer-Ressourcenübersicht sind zwei Ansichten verfügbar: Overview und Unhealthy Target Map. Die Option „Übersicht“ ist standardmäßig ausgewählt und zeigt alle Ressourcen Ihres Load Balancers an. Wenn Sie die Kartenansicht für fehlerhafte Ziele auswählen, werden nur die fehlerhaften Ziele und die ihnen zugewiesenen Ressourcen angezeigt.

Die Ansicht Unhealthy Target Map kann verwendet werden, um Fehler bei Zielen zu beheben, bei denen die Zustandsprüfungen nicht bestanden wurden. Weitere Informationen finden Sie unter Beheben Sie fehlerhafte Ziele mithilfe der Ressourcenübersicht.

Ressourcengruppen

Die Application Load Balancer Balancer-Ressourcenübersicht enthält vier Ressourcengruppen, eine für jeden Ressourcentyp. Bei den Ressourcengruppen handelt es sich um Listener, Regeln, Zielgruppen und Ziele.

Ressourcenkacheln

Jede Ressource innerhalb einer Gruppe hat ihre eigene Kachel, auf der Details zu dieser bestimmten Ressource angezeigt werden.

- Wenn Sie den Mauszeiger über eine Ressourcenkachel bewegen, werden die Beziehungen zwischen dieser und anderen Ressourcen hervorgehoben.
- Wenn Sie eine Ressourcenkachel auswählen, werden die Beziehungen zwischen ihr und anderen Ressourcen hervorgehoben und zusätzliche Details zu dieser Ressource angezeigt.
  - Regelbedingungen: Die Bedingungen für jede Regel.
  - Zusammenfassung des Gesundheitszustands der Zielgruppe: Die Anzahl der registrierten Ziele für jeden Gesundheitsstatus.
  - Zielgesundheitsstatus Der aktuelle Gesundheitszustand und die Beschreibung des Ziels.

> **Note**
>
> Sie können die Option „Ressourcendetails anzeigen“ deaktivieren, um zusätzliche Details in der Ressourcenübersicht auszublenden.

- Jede Ressourcenkachel enthält einen Link, der, wenn er ausgewählt ist, zur Detailseite der Ressource navigiert.
  - Listeners - Wählen Sie den Listeners protocol:port aus. Beispiel: `HTTP:80`
  - Regeln - Wählen Sie die Regelaktion aus. Beispiel: `Forward to target group`
  - Zielgruppen - Wählen Sie den Namen der Zielgruppe aus. Beispiel: `my-target-group`
  - Ziele - Wählen Sie die Ziel-ID aus. Beispiel: `i-1234567890abcdef0`

Exportieren Sie die Ressourcenübersicht

Wenn Sie Exportieren auswählen, haben Sie die Möglichkeit, die aktuelle Ansicht der Ressourcenübersicht Ihres Application Load Balancers als PDF zu exportieren.

Kapazitätsreservierungen für Ihren Application Load Balancer

Mit Reservierungen für Load Balancer Capacity Unit (LCU) können Sie eine statische Mindestkapazität für Ihren Load Balancer reservieren. Application Load Balancer skalieren automatisch, um erkannte Workloads zu unterstützen und den Kapazitätsbedarf zu decken. Wenn

die Mindestkapazität konfiguriert ist, skaliert Ihr Load Balancer auf der Grundlage des empfangenen Datenverkehrs weiter nach oben oder unten, verhindert aber auch, dass die Kapazität unter die konfigurierte Mindestkapazität fällt.

Erwägen Sie die Verwendung der LCU-Reservierung in den folgenden Situationen:

- Sie haben ein bevorstehendes Ereignis, das plötzlich ungewöhnlich viel Traffic haben wird, und Sie möchten sicherstellen, dass Ihr Load Balancer den plötzlichen Anstieg des Datenverkehrs während des Ereignisses bewältigen kann.
- Sie haben aufgrund der Art Ihrer Arbeitslast für einen kurzen Zeitraum einen unvorhersehbaren Anstieg des Datenverkehrs.
- Sie richten Ihren Load Balancer so ein, dass er Ihre Dienste zu einer bestimmten Startzeit integriert oder migriert, und müssen mit einer hohen Kapazität beginnen, anstatt darauf zu warten, dass die auto-scaling wirksam wird.
- Sie müssen eine Mindestkapazität aufrechterhalten, um Service Level Agreements oder Compliance-Anforderungen zu erfüllen.
- Sie migrieren Workloads zwischen Load Balancern und möchten das Ziel so konfigurieren, dass es dem Umfang der Quelle entspricht.

Schätzen Sie die Kapazität, die Sie benötigen

Bei der Festlegung der Kapazität, die Sie für Ihren Load Balancer reservieren sollten, empfehlen wir, Lasttests durchzuführen oder historische Workload-Daten zu überprüfen, die den erwarteten kommenden Traffic darstellen. Mithilfe der Elastic Load Balancing Balancing-Konsole können Sie anhand des überprüften Datenverkehrs abschätzen, wie viel Kapazität Sie reservieren müssen.

Alternativ können Sie die CloudWatch Metrik verwenden`PeakLCUs`, um die benötigte Kapazität zu ermitteln. Die `PeakLCUs` Metrik berücksichtigt Spitzen in Ihrem Datenverkehrsmuster, die der Load Balancer über alle Skalierungsdimensionen hinweg skalieren muss, um Ihre Arbeitslast zu unterstützen. Die `PeakLCUs` Metrik unterscheidet sich von der `ConsumedLCUs` Metrik, die nur die Abrechnungsdimensionen Ihres Traffics aggregiert. Es wird empfohlen, die `PeakLCUs` Metrik zu verwenden, um sicherzustellen, dass Ihre LCU-Reservierung während der Load Balancer-Skalierung ausreichend ist. Verwenden Sie bei der Schätzung der Kapazität einen Wert von pro Minute. `Sum` `PeakLCUs`

Wenn Sie keine historischen Workload-Daten als Referenz haben und keine Lasttests durchführen können, können Sie den Kapazitätsbedarf mithilfe des LCU-Reservierungsrechners abschätzen.

Der LCU-Reservierungsrechner verwendet Daten, die auf historischen Workloads basieren, AWS beobachten und stellen möglicherweise nicht Ihre spezifische Arbeitslast dar. Weitere Informationen finden Sie unter Load Balancer Capacity Unit Reservation Calculator.

Kontingente für LCU-Reservierungen

Ihr Konto hat Kontingente für LCUs. Weitere Informationen finden Sie unter the section called “Load Balancer Balancer-Kapazitätseinheiten”.

Fordern Sie die Reservierung einer Load Balancer-Kapazitätseinheit für Ihren Application Load Balancer an

Bevor Sie die LCU-Reservierung nutzen, sollten Sie Folgendes überprüfen:

- Die Kapazität wird auf regionaler Ebene reserviert und gleichmäßig auf die Availability Zones verteilt. Stellen Sie sicher, dass Sie über genügend gleichmäßig verteilte Ziele in jeder Availability Zone verfügen, bevor Sie die LCU-Reservierung aktivieren.
- LCU-Reservierungsanfragen werden nach dem Prinzip „Wer zuerst kommt, mahlt zuerst“ bearbeitet und hängen von der zu diesem Zeitpunkt verfügbaren Kapazität für eine Zone ab. Die meisten Anfragen werden in der Regel innerhalb weniger Minuten bearbeitet, können aber bis zu einigen Stunden dauern.
- Um eine bestehende Reservierung zu aktualisieren, muss die vorherige Anfrage bereitgestellt werden oder sie ist fehlgeschlagen. Sie können die reservierte Kapazität beliebig oft erhöhen, Sie können die reservierte Kapazität jedoch nur zweimal täglich verringern.
- Für reservierte oder bereitgestellte Kapazitäten fallen weiterhin Gebühren an, bis diese gekündigt oder storniert werden.

Fordern Sie eine LCU-Reservierung an

In den Schritten in diesem Verfahren wird erklärt, wie Sie eine LCU-Reservierung auf Ihrem Load Balancer beantragen.

So fordern Sie eine LCU-Reservierung über die Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Namen eines Load Balancers aus.

4. Wählen Sie auf der Registerkarte Kapazität die Option LCU-Reservierung bearbeiten aus.
5. Wählen Sie Historische referenzbasierte Schätzung und dann den Load Balancer aus der Drop-down-Liste aus.
6. Wählen Sie den Referenzzeitraum aus, um die empfohlene reservierte LCU-Stufe anzuzeigen.
7. Wenn Sie in der Vergangenheit nicht über einen Referenz-Workload verfügen, können Sie „Manuelle Schätzung“ wählen und die Anzahl der LCUs zu reservierenden Workloads eingeben.
8. Wählen Sie Speichern.

Um eine LCU-Reservierung anzufordern, verwenden Sie AWS CLI

Verwenden Sie den modify-capacity-reservation-Befehl.

Load Balancer Capacity Unit-Reservierungen für Ihren Application Load Balancer aktualisieren oder beenden

Eine LCU-Reservierung aktualisieren oder beenden

In den Schritten in diesem Verfahren wird erklärt, wie Sie eine LCU-Reservierung auf Ihrem Load Balancer aktualisieren oder beenden.

So aktualisieren oder beenden Sie eine LCU-Reservierung mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Namen eines Load Balancers aus.
4. Vergewissern Sie sich auf der Registerkarte Kapazität, dass der Status der Reservierung bereitgestellt lautet.
    a. Um die LCU-Reservierung zu aktualisieren, wählen Sie LCU-Reservierung bearbeiten.
    b. Um die LCU-Reservierung zu beenden, wählen Sie Kapazität stornieren.

Um eine LCU-Reservierung zu aktualisieren oder zu beenden, verwenden Sie AWS CLI

Verwenden Sie den modify-capacity-reservation-Befehl.

Überwachen Sie die Reservierung von Load Balancer-Kapazitätseinheiten für Ihren Application Load Balancer

Status der Reservierung

Die LCU-Reservierung hat vier verfügbare Status:

- Ausstehend - Zeigt an, dass die Reservierung gerade bereitgestellt wird.
- bereitgestellt — Zeigt an, dass die reservierte Kapazität bereit und nutzbar ist.
- fehlgeschlagen - Zeigt an, dass die Anfrage derzeit nicht abgeschlossen werden kann.
- Neuverteilung — Zeigt an, dass eine Availability Zone hinzugefügt oder entfernt wurde und der Load Balancer die Kapazität neu verteilt.

Reservierte LCU

Die `ReservedLCUs` Metrik wird auf Minutenbasis gemeldet. Die Kapazität wird auf Stundenbasis reserviert. Wenn Sie beispielsweise eine LCU-Reservierung von 6.000 haben, `ReservedLCUs` beträgt die Summe für eine Stunde 6.000 und die Summe für eine Minute 100. Anhand der Metrik können Sie Ihre reservierte LCU-Auslastung ermitteln. `PeakLCUs` Sie können CloudWatch Alarme einrichten, um den Wert pro Minute `Sum` mit Ihrem Wert für reservierte Kapazität oder den Wert pro Stunde `Sum` zu vergleichen`ReservedLCUs`, um festzustellen, ob Sie genügend Kapazität reserviert haben, um Ihren Anforderungen gerecht zu werden. `PeakLCUs`

Überwachen Sie reservierte Kapazität

In den Schritten in diesem Prozess wird erklärt, wie Sie den Status einer LCU-Reservierung auf Ihrem Load Balancer überprüfen können.

So zeigen Sie den Status einer LCU-Reservierung mithilfe der Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Namen eines Load Balancers aus.
4. Auf der Registerkarte Kapazität können Sie den Reservierungsstatus und den Wert für reservierte LCU einsehen.

Um den Status der LCU-Reservierung zu überwachen, verwenden Sie AWS CLI

Verwenden Sie den describe-capacity-reservation-Befehl.

Listener für Ihre Application Load Balancer

Ein Listener ist ein Prozess, der mit dem Protokoll und dem Port, das bzw. den Sie konfigurieren, Verbindungsanforderungen prüft. Bevor Sie Ihren Application Load Balancer verwenden können, müssen Sie mindestens einen Listener hinzufügen. Wenn Ihr Load Balancer keine Listener hat, kann er keinen Datenverkehr von Clients empfangen. Die Regeln, die Sie für Ihre Listener definieren, bestimmen, wie der Load Balancer Anfragen an die von Ihnen registrierten Ziele weiterleitet, z. B. EC2 Instances.

Inhalt

- Listener-Konfiguration
- Listener-Attribute
- Listener-Regeln
- Regelaktionstypen
- Regelbedingungstypen
- HTTP-Header und Application Load Balancer
- Erstellen eines HTTP-Listeners für Ihren Application Load Balancer
- SSL-Zertifikate für Ihren Application Load Balancer
- Sicherheitsrichtlinien für Ihren Application Load Balancer
- Erstellen eines HTTPS-Listeners für Ihren Application Load Balancer
- Listener-Regeln für Ihren Application Load Balancer
- Aktualisieren eines HTTPS-Listeners für Ihren Application Load Balancer
- Gegenseitige Authentifizierung mit TLS im Application Load Balancer
- Authentifizieren von Benutzern mithilfe eines Application Load Balancers
- Tags für Ihre Application Load Balancer Balancer-Listener und Regeln
- Löschen eines Listeners für Ihren Application Load Balancer
- Änderung des HTTP-Headers für Ihren Application Load Balancer

Listener-Konfiguration

Listener unterstützen die folgenden Protokolle und Ports:

- Protocols (Protokolle): HTTP, HTTPS
- Ports: 1-65535

Sie können einen HTTPS-Listener verwenden, um die Ver- und Entschlüsselung auf Ihren Load Balancer auszulagern, damit sich Ihre Anwendungen auf die Geschäftslogik konzentrieren können. Wenn das Listener-Protokoll HTTPS ist, müssen Sie auf dem Listener mindestens ein SSL-Serverzertifikat bereitstellen. Weitere Informationen finden Sie unter Erstellen eines HTTPS-Listeners für Ihren Application Load Balancer.

Wenn Sie sicherstellen müssen, dass die Ziele den HTTPS-Verkehr anstelle des Load Balancers entschlüsseln, können Sie einen Network Load Balancer mit einem TCP-Listener an Port 443 erstellen. Bei einem TCP-Listener leitet der Load Balancer verschlüsselten Datenverkehr an die Ziele weiter, ohne ihn zu entschlüsseln. Weitere Informationen finden Sie im Benutzerhandbuch für Network Load Balancers.

WebSockets

Application Load Balancers bieten native Unterstützung für. WebSockets Sie können eine bestehende HTTP/1.1-Verbindung in eine WebSocket (`wsoderwss`) -Verbindung umwandeln, indem Sie ein HTTP-Verbindungs-Upgrade verwenden. Wenn Sie ein Upgrade durchführen, wird die für Anfragen (sowohl zum Load Balancer als auch zum Ziel) verwendete TCP-Verbindung über den Load Balancer zu einer dauerhaften WebSocket Verbindung zwischen dem Client und dem Ziel. Sie können sie sowohl WebSockets mit HTTP- als auch mit HTTPS-Listenern verwenden. Die Optionen, die Sie für Ihren Listener auswählen, gelten sowohl für WebSocket Verbindungen als auch für HTTP-Verkehr. Weitere Informationen finden Sie unter So funktioniert das WebSocket Protokoll im Amazon CloudFront Developer Guide.

HTTP/2

Application Load Balancer verfügen über native Unterstützung für HTTP/2 mit HTTPS-Listener. Sie können mit einer einzigen HTTP/2-Verbindung bis zu 128 Anforderungen parallel senden. Sie können die Protokollversion verwenden, um die Anforderung mit HTTP/2 an die Ziele zu senden. Weitere Informationen finden Sie unter Protokollversion. Da HTTP/2 Frontend-Verbindungen effizienter verwendet, gibt es möglicherweise weniger Verbindungen zwischen Clients und dem Load Balancer. Sie können das Server-Push-Feature von HTTP/2 nicht verwenden.

Die gegenseitige TLS-Authentifizierung für Application Load Balancers unterstützt HTTP/2 sowohl im Passthrough- als auch im Verifizierungsmodus. Weitere Informationen finden Sie unter Gegenseitige Authentifizierung mit TLS im Application Load Balancer.

Weitere Informationen finden Sie unter Weiterleitung von Anforderungen im Benutzerhandbuch zu Elastic Load Balancing.

Listener-Attribute

Im Folgenden sind die Listener-Attribute für Application Load Balancers aufgeführt:

`routing.http.request.x_amzn_mtls_clientcert_serial_number.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Mtls-Clientcert-Serial-Number-HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_mtls_clientcert_issuer.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Mtls-Clientcert-Issuer-HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_mtls_clientcert_subject.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Mtls-Clientcert-Suject-HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_mtls_clientcert_validity.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Mtls-Clientcert-Validity-HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_mtls_clientcert_leaf.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Mtls-Clientcert-Leaf HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_mtls_clientcert.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Mtls-Clientcert-HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_tls_version.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Tls-Version HTTP-Anforderungsheaders zu ändern.

`routing.http.request.x_amzn_tls_cipher_suite.header_name`

Ermöglicht es Ihnen, den Header-Namen des X-Amzn-Tls-Cipher-Suite-HTTP-Anforderungsheaders zu ändern.

`routing.http.response.server.enabled`

Ermöglicht es Ihnen, den HTTP-Antwortserver-Header zuzulassen oder zu entfernen.

`routing.http.response.strict_transport_security.header_value`

Informiert Browser darüber, dass auf die Website nur über HTTPS zugegriffen werden sollte und dass alle future Versuche, über HTTP darauf zuzugreifen, automatisch in HTTPS umgewandelt werden sollten.

`routing.http.response.access_control_allow_origin.header_value`

Gibt an, welche Ursprünge auf den Server zugreifen dürfen.

`routing.http.response.access_control_allow_methods.header_value`

Gibt zurück, welche HTTP-Methoden zulässig sind, wenn von einem anderen Ursprung aus auf den Server zugegriffen wird.

`routing.http.response.access_control_allow_headers.header_value`

Gibt an, welche Header während der Anfrage verwendet werden können.

`routing.http.response.access_control_allow_credentials.header_value`

Gibt an, ob der Browser bei Anfragen Anmeldeinformationen wie Cookies oder Authentifizierung angeben soll.

`routing.http.response.access_control_expose_headers.header_value`

Gibt zurück, welche Header der Browser dem anfragenden Client zur Verfügung stellen kann.

`routing.http.response.access_control_max_age.header_value`

Gibt in Sekunden an, wie lange die Ergebnisse einer Preflight-Anfrage zwischengespeichert werden können.

`routing.http.response.content_security_policy.header_value`

Gibt Einschränkungen an, die vom Browser durchgesetzt werden, um das Risiko bestimmter Arten von Sicherheitsbedrohungen zu minimieren.

`routing.http.response.x_content_type_options.header_value`

Gibt an, ob die in den Content-Type-Headern angegebenen MIME-Typen befolgt und nicht geändert werden sollen.

`routing.http.response.x_frame_options.header_value`

Gibt an, ob der Browser eine Seite in einem Frame, Iframe, Embed oder Objekt rendern darf.

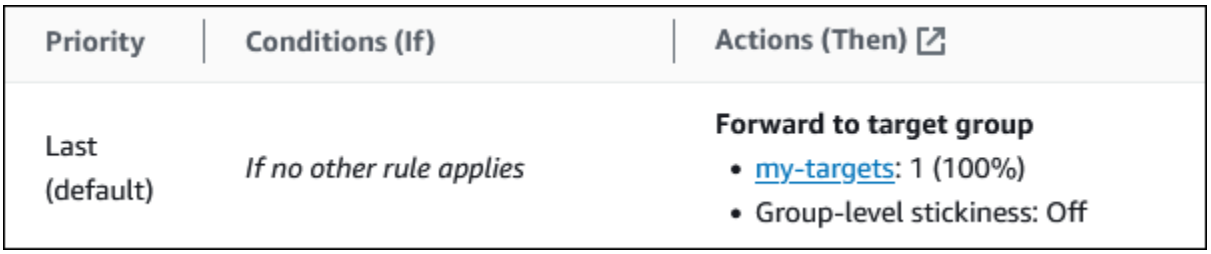
Listener-Regeln

Jeder Listener hat eine Standardaktion, auch als Standardregel bezeichnet. Die Standardregel kann nicht gelöscht werden und wird immer zuletzt ausgeführt. Es können zusätzliche Regeln erstellt werden, die aus einer Priorität, mindestens einer Aktion und mindestens einer Bedingung bestehen. Sie können jederzeit Regel hinzufügen oder bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer Regel.

Standardregeln

Beim Erstellen eines Listeners definieren Sie Aktionen für die Standardregel. Standardregeln können keine Bedingungen aufweisen. Wenn für die Regeln eines Listeners keine Bedingungen erfüllt werden, wird die Aktion für die Standardregel durchgeführt.

Es folgt ein Beispiel für eine Standardregel, wie in der Konsole dargestellt:



Priorität der Regel

Jede Regel hat eine Priorität. Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet. Sie können die Priorität einer nicht standardmäßigen Regel jederzeit ändern. Sie können die Priorität der Standardregel nicht ändern. Weitere Informationen finden Sie unter Aktualisieren der Regelpriorität.

Regelaktionen

Jede Regelaktion verfügt über einen Typ, eine Priorität und die für die Durchführung der Aktion erforderlichen Informationen. Weitere Informationen finden Sie unter Regelaktionstypen.

Regelbedingungen

Jede Regelbedingung weist einen Typ und Bedingungsinformationen auf. Wenn die Bedingungen für eine Regel erfüllt sind, wird die dazugehörige Aktion durchgeführt. Weitere Informationen finden Sie unter Regelbedingungstypen.

Regelaktionstypen

Im Folgenden finden Sie die unterstützten Aktionstypen einer Listener-Regel:

`authenticate-cognito`

[HTTPS-Listener] Verwenden von Amazon Cognito zum Authentifizieren von Benutzern. Weitere Informationen finden Sie unter Authentifizieren von Benutzern mithilfe eines Application Load Balancers.

`authenticate-oidc`

[HTTPS-Listener] Verwenden eines Identitätsanbieters, der mit OpenID Connect (OIDC) konform ist, um Benutzer zu authentifizieren

`fixed-response`

Zurückgeben einer benutzerdefinierten HTTP-Antwort Weitere Informationen finden Sie unter Aktionen mit feststehender Antwort.

`forward`

Weiterleiten von Anforderungen an die angegebenen Zielgruppen. Weitere Informationen finden Sie unter Weiterleitungsaktionen.

`redirect`

Weiterleiten von Anforderungen von einer URL an eine andere Weitere Informationen finden Sie unter Weiterleitungsaktionen.

Die Aktion mit der niedrigsten Priorität wird zuerst durchgeführt. Jede Regel muss genau eine der folgenden Aktionen enthalten: `forward`, `redirect` oder `fixed-response`. Außerdem muss es die letzte auszuführende Regel sein.

Wenn die Protokollversion gRPC oder HTTP/2 ist, sind `forward`-Aktionen die einzigen unterstützten Aktionen.

Aktionen mit feststehender Antwort

Verwenden Sie `fixed-response`-Aktionen, um Client-Anforderungen zu verwerfen und eine benutzerdefinierte HTTP-Antwort zurückzugeben. Sie können mit dieser Aktion einen 2XX-, 4XX- 5XX-Antwortcode und optional eine Nachricht zurückgeben.

Wenn eine `fixed-response`-Aktion ausgeführt wird, werden die Aktion und die URL des Weiterleitungsziels in den Zugriffsprotokollen aufgezeichnet. Weitere Informationen finden Sie unter Zugriffsprotokolleinträge. Die Anzahl der erfolgreichen `fixed-response`-Aktionen wird in der Metrik `HTTP_Fixed_Response_Count` erfasst. Weitere Informationen finden Sie unter Application-Load-Balancer-Metriken.

Example Beispiel für eine Aktion mit fester Antwort für AWS CLI

Sie können eine Aktion angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Mit der folgenden Aktion wird mit dem angegebenen Statuscode und dem Textkörper eine festgelegte Antwort gesendet.

```
[
  {
      "Type": "fixed-response",
      "FixedResponseConfig": {
          "StatusCode": "200",
          "ContentType": "text/plain",
          "MessageBody": "Hello world"
      }
  }
]
```

Weiterleitungsaktionen

Sie können mithilfe von `forward`-Aktionen Anforderungen an eine oder mehrere Zielgruppen weiterleiten. Wenn Sie mehrere Zielgruppen für eine `forward`-Aktion angeben, müssen Sie für jede Zielgruppe eine Gewichtung angeben. Jede Zielgruppengewichtung ist ein Wert zwischen 0 und 999. Anforderungen, die einer Listener-Regel mit gewichteten Zielgruppen entsprechen, werden basierend auf ihren Gewichtungen an diese Zielgruppen verteilt. Wenn Sie beispielsweise zwei Zielgruppen mit einer Gewichtung von 10 angeben, erhält jede Zielgruppe die Hälfte der Anforderungen. Wenn Sie zwei Zielgruppen angeben, eine mit einer Gewichtung von 10 und die andere mit einer Gewichtung von 20, erhält die Zielgruppe mit der Gewichtung von 20 doppelt so viele Anforderungen wie die andere Zielgruppe.

Wenn Sie eine Regel zur Verteilung des Datenverkehrs auf gewichtete Zielgruppen konfigurieren und eine der Zielgruppen leer ist oder nur fehlerhafte Ziele hat, führt der Load Balancer nicht automatisch ein Failover zu einer Zielgruppe mit fehlerfreien Zielen durch.

Standardmäßig garantiert das Konfigurieren einer Regel für die Verteilung des Datenverkehrs zwischen gewichteten Zielgruppen nicht, dass Sticky Sessions eingehalten werden. Um sicherzustellen, dass Sticky Sessions eingehalten werden, aktivieren Sie die Klebrigkeit der Zielgruppe für die Regel. Wenn der Load Balancer eine Anfrage zum ersten Mal an eine gewichtete Zielgruppe weiterleitet, generiert er ein Cookie mit dem Namen AWSALBTG , das Informationen über die ausgewählte Zielgruppe kodiert, das Cookie verschlüsselt und das Cookie in die Antwort an den Client einbezieht. Der Client sollte das erhaltene Cookie in nachfolgende Anfragen an den Load Balancer aufnehmen. Wenn der Load Balancer eine Anforderung empfängt, die mit einer Regel mit aktivierter Zielgruppenklebrigkeit übereinstimmt und das Cookie enthält, wird die Anforderung an die im Cookie angegebene Zielgruppe weitergeleitet.

Application Load Balancer unterstützen keine Cookie-Werte, die URL-codiert sind.

Bei CORS (Cross-Origin Resource Sharing)-Anforderungen benötigen einige Browser `SameSite=None; Secure` zum Aktivieren von Stickiness. In diesem Fall generiert Elastic Load Balancing ein zweites Cookie AWSALBTGCORS, das dieselben Informationen wie das ursprüngliche Stickiness-Cookie plus dieses `SameSite` Attribut enthält. Kunden erhalten beide Cookies.

Example Beispiel einer Weiterleitungsaktion mit einer Zielgruppe

Sie können eine Aktion angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die folgende Aktion leitet die Anforderungen an die angegebene Zielgruppe weiter.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067"
              }
          ]
      }
  }
]
```

Example Beispiel einer Weiterleitungsaktion mit zwei gewichteten Zielgruppen

Die folgende Aktion leitet Anforderungen an die beiden angegebenen Zielgruppen basierend auf der Gewichtung jeder Zielgruppe weiter.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
                  "Weight": 10
              },
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                  "Weight": 20
              }
          ]
      }
  }
]
```

Example Beispiel einer Weiterleitungsaktion mit aktivierter Stickiness

Wenn Sie über eine Weiterleitungsaktion mit mehreren Zielgruppen verfügen und für eine oder mehrere Zielgruppen Sticky Sessions aktiviert sind, müssen Sie die Stickiness der Zielgruppe aktivieren.

Die folgende Aktion leitet Anforderungen an die beiden angegebenen Zielgruppen weiter, wobei die Klebrigkeit der Zielgruppe aktiviert ist. Anforderungen, die die Stickiness-Cookies nicht enthalten, werden basierend auf der Gewichtung jeder Zielgruppe weitergeleitet.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
```

```
                "Weight": 10
            },
            {
                "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                "Weight": 20
            }
        ],
        "TargetGroupStickinessConfig": {
            "Enabled": true,
            "DurationSeconds": 1000
        }
    }
  }
]
```

Weiterleitungsaktionen

Mithilfe von `redirect`-Aktionen können Sie Client-Anforderungen von einer URL an eine andere weiterleiten. Konfigurieren Sie Weiterleitungen je nach Bedarf entweder als temporär (HTTP 302) oder permanent (HTTP 301).

eine URI umfasst folgende Komponenten:

```
protocol://hostname:port/path?query
```

Sie müssen mindestens eine der folgenden Komponenten modifizieren, um eine Weiterleitungsschleife zu verhindern: Protokoll, Hostname, Port oder Pfad. Für alle Komponenten, an denen Sie keine Änderungen vornehmen, wird der ursprüngliche Wert beibehalten.

Protokoll

> Das Protokoll (HTTP oder HTTPS). Sie können von HTTP nach HTTP, von HTTP nach HTTPS und von HTTPS nach HTTPS weiterleiten. Eine Weiterleitung von HTTPS nach HTTP ist nicht möglich.

hostname

> Der Hostname Bei einem Hostnamen wird die Groß- und Kleinschreibung nicht beachtet. Er kann bis zu 128 Zeichen lang sein und aus alphanumerischen Zeichen, Platzhaltern (* und ?) und Bindestrichen (-) bestehen.

port

Der Port (1 bis 65535)

Pfad

Der absolute Pfad, beginnend mit dem vorangestellten "/" Bei einem Pfad muss die Groß- und Kleinschreibung nicht beachtet werden. Er kann 128 Zeichen lang sein und aus alphanumerischen Zeichen, Platzhaltern (* und ?), & (mittels &) sowie die Sonderzeichen _-. $/~'"@:+ bestehen.

query

Die Abfrageparameter Die maximale Länge beträgt 128 Zeichen.

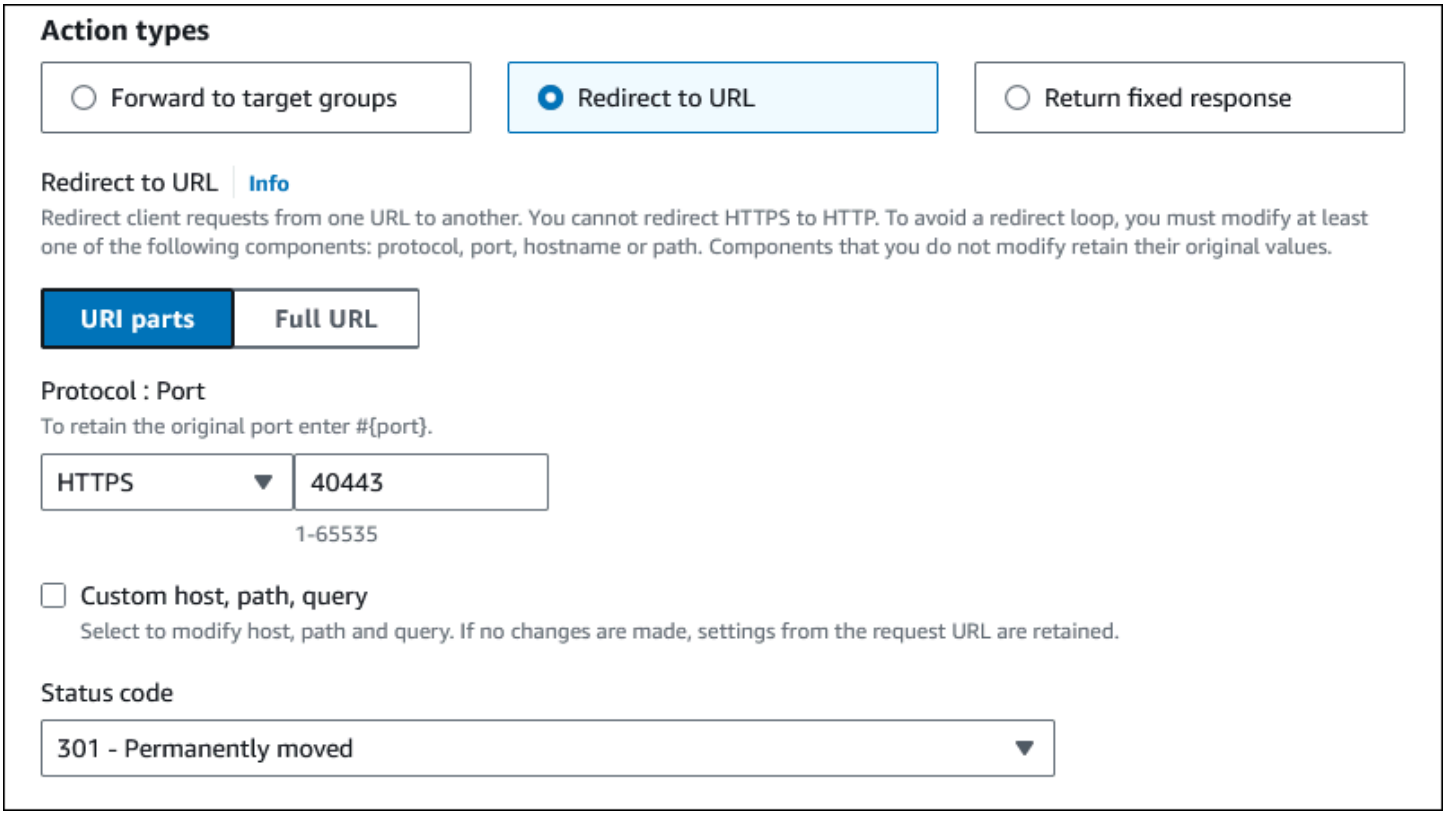
Sie können URI-Komponenten der ursprünglichen URL in der Ziel-URL weiter nutzen. Verwenden Sie dazu die folgenden reservierten Schlüsselwörter:

- `#{protocol}` – zur Beibehaltung des Protokolls. In den Protokoll- und Abfragekomponenten zu verwenden.
- `#{host}` – Zur Beibehaltung der Domain. In den Hostnamen-, Pfad- und Abfragekomponenten zu verwenden.
- `#{port}` – Zur Beibehaltung des Ports. In den Port-, Pfad- und Abfragekomponenten zu verwenden.
- `#{path}` – Zur Beibehaltung des Pfads. In den Pfad- und Abfragekomponenten zu verwenden.
- `#{query}` – Zur Beibehaltung der Abfrageparameter. In der Abfragekomponente zu verwenden.

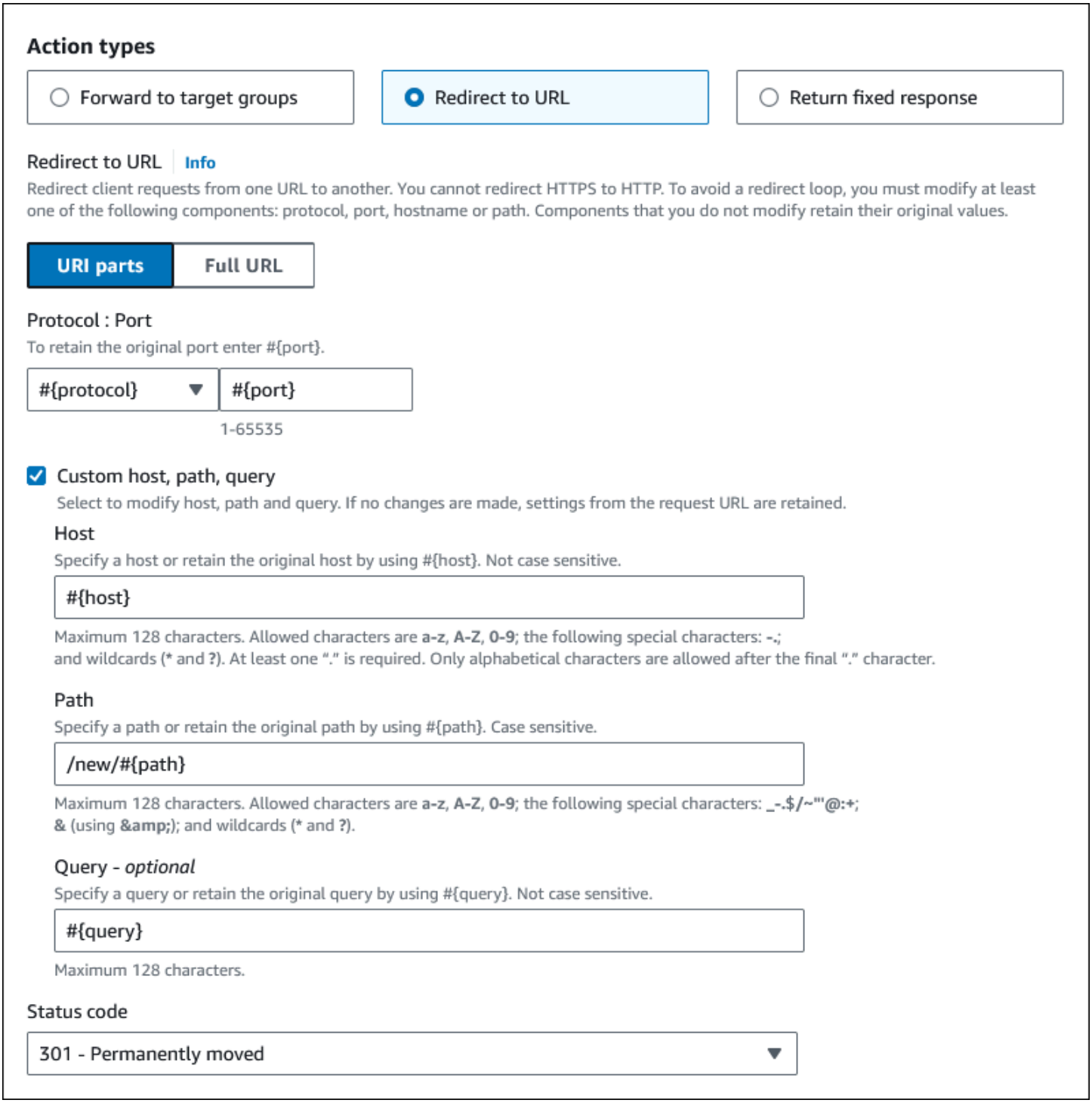
Wenn eine `redirect`-Aktion ausgeführt wird, wird diese in den Zugriffsprotokollen aufgezeichnet. Weitere Informationen finden Sie unter Zugriffsprotokolleinträge. Die Anzahl der erfolgreichen `redirect`-Aktionen wird in der Metrik `HTTP_Redirect_Count` erfasst. Weitere Informationen finden Sie unter Application-Load-Balancer-Metriken.

Example Beispiel für Weiterleitungsaktionen mithilfe der Konsole

Mit der folgenden Regel wird beispielsweise eine permanente Weiterleitung auf eine URL mit dem HTTPS-Protokoll und dem festgelegten Port 40443 eingerichtet. Beibehalten werden der ursprüngliche Hostname, der Pfad und die Abfrageparameter. Dieser Bildschirm entspricht "https://#{host}:40443/#{path}?#{query}".



Mit der folgenden Regel wird eine permanente Weiterleitung auf eine URL mit dem ursprünglichen Protokoll, Port, Hostnamen und Abfrageparametern eingerichtet. Der Pfad wird mit dem Schlüsselwort `#{path}` modifiziert. Dieser Bildschirm entspricht "#{protocol}://#{host}:#{port}/new/#{path}?#{query}".



Example Beispiel für eine Umleitungsaktion für AWS CLI

Sie können eine Aktion angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Mit der folgenden Aktion wird eine HTTP-Anforderung an eine HTTPS-Anforderung an Port 443 weitergeleitet, die denselben Hostnamen, Pfad und die gleiche Abfragezeichenfolge wie die HTTP-Anforderung aufweist.

```
[
  {
      "Type": "redirect",
      "RedirectConfig": {
          "Protocol": "HTTPS",
          "Port": "443",
          "Host": "#{host}",
          "Path": "/#{path}",
          "Query": "#{query}",
          "StatusCode": "HTTP_301"
      }
  }
]
```

Regelbedingungstypen

Im Folgenden finden Sie die unterstützten Bedingungstypen für eine Regel:

`host-header`

Die Route basiert auf dem Hostnamen jeder Anforderung. Weitere Informationen finden Sie unter Hostbedingungen.

`http-header`

Die Route basiert auf den HTTP-Headern für jede Anforderung. Weitere Informationen finden Sie unter HTTP-Header-Bedingungen.

`http-request-method`

Die Route basiert auf der HTTP-Anforderungsmethode jeder Anforderung. Weitere Informationen finden Sie unter Bedingungen für HTTP-Anforderungsmethoden.

`path-pattern`

Route basierend auf Pfadmustern in der Anfrage URLs. Weitere Informationen finden Sie unter Pfadbedingungen.

`query-string`

Route basierend auf key/value Paaren oder Werten in den Abfragezeichenfolgen. Weitere Informationen finden Sie unter Abfragezeichenfolgebedingungen.

`source-ip`

Die Route basiert auf der Quell-IP-Adresse jeder Anforderung. Weitere Informationen finden Sie unter Bedingungen für die Quell-IP-Adresse.

Jede Regel kann optional jeweils eine der folgenden Bedingungen umfassen: `host-header`, `http-request-method`, `path-pattern`, und `source-ip`. Jede Regel kann optional auch eine oder mehrere der folgenden Bedingungen enthalten: `http-header` und `query-string`.

Sie können bis zu drei Übereinstimmungsbewertungen pro Bedingung angeben. Beispiel: Für jede `http-header`-Bedingung können Sie bis zu drei Zeichenfolgen angeben, die mit dem Wert des HTTP-Headers in der Anforderung vergleichen werden. Die Bedingung wird erfüllt, wenn eine der Zeichenfolgen dem Wert des HTTP-Headers entspricht. Wenn alle drei Zeichenfolgen eine Übereinstimmung aufweisen sollen, erstellen Sie eine Bedingung pro Übereinstimmungsbewertung.

Sie können bis zu fünf Übereinstimmungsbewertungen pro Regel angeben. Beispiel: Sie können eine Regel mit fünf Bedingungen erstellen, wobei jede Bedingung eine Übereinstimmungsbewertung aufweist.

Sie können Platzhalterzeichen in die Übereinstimmungsbewertung für die Bedingungen `http-header`, `host-header`, `path-pattern` und `query-string` einschließen. Die Anzahl der Platzhalterzeichen pro Bedingung ist auf 5 beschränkt.

Regeln werden nur auf sichtbare ASCII-Zeichen angewendet; Steuerzeichen (0x00 bis 0x1f und 0x7f) sind ausgeschlossen.

Demos finden Sie unter Erweiterte Anfrageweiterleitung.

HTTP-Header-Bedingungen

Mit HTTP-Header-Bedingungen können Sie Regeln konfigurieren, mit denen Anforderungen auf Grundlage der HTTP-Header für die Anforderung weitergeleitet werden. Sie können die Namen der standardmäßigen oder benutzerdefinierten HTTP-Header-Felder angeben. Beim Headernamen und bei der Übereinstimmungsbewertung wird nicht zwischen die Groß- und Kleinschreibung unterschieden. Die folgenden Platzhalterzeichen werden in den Vergleichszeichenfolgen unterstützt: * (findet eine Übereinstimmung mit 0 oder mehr Zeichen) und ? (findet Übereinstimmungen für genau 1 Zeichen). Platzhalterzeichen werden im Header-Namen nicht unterstützt.

Wenn das Application Load Balancer Balancer-Attribut aktiviert `routing.http.drop_invalid_header_fields` ist, werden Header-Namen gelöscht, die nicht

den regulären Ausdrücken () `A-Z,a-z,0-9` entsprechen. Header-Namen, die nicht den regulären Ausdrücken entsprechen, können ebenfalls hinzugefügt werden.

Example Beispiel für eine HTTP-Header-Bedingung für AWS CLI

Sie können Bedingungen angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die folgende Bedingung wird von Anforderungen mit einem User-Agent-Header erfüllt, der mindestens einer der angegeben Zeichenfolgen entspricht.

```
[
  {
      "Field": "http-header",
      "HttpHeaderConfig": {
          "HttpHeaderName": "User-Agent",
          "Values": ["*Chrome*", "*Safari*"]
      }
  }
]
```

Bedingungen für HTTP-Anforderungsmethoden

Mit Bedingungen für HTTP-Anforderungsmethoden können Sie Regeln konfigurieren, mit denen Anforderungen auf Grundlage der HTTP-Anforderungsmethode der Anforderung weitergeleitet werden. Sie können standardmäßige oder benutzerdefinierte HTTP-Methoden angeben. Bei der Übereinstimmungsbewertung wird die Groß- und Kleinschreibung nicht beachtet, Platzhalterzeichen werden nicht unterstützt. Der Methodenname muss also eine genaue Übereinstimmung sein.

Wir empfehlen, dass Sie GET- und HEAD-Anforderungen auf die gleiche Weise weiterleiten, da die Antwort auf eine HEAD-Anforderung möglicherweise zwischengespeichert wird.

Example Beispiel für eine HTTP-Methodenbedingung für AWS CLI

Sie können Bedingungen angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die folgende Bedingung wird von Anforderungen erfüllt, bei der die angegebene Methode verwendet wird.

```
[
  {
      "Field": "http-request-method",
```

```
      "HttpRequestMethodConfig": {
          "Values": ["CUSTOM-METHOD"]
      }
  }
]
```

Hostbedingungen

Mit Hostbedingungen können Sie Regeln definieren, die Anforderungen basierend auf dem Hostnamen im Host-Header weiterleiten (auch als hostbasierte Weiterleitung bezeichnet). Auf diese Weise können Sie mit einem einzigen Load Balancer mehrere Unterdomains und verschiedene Top-Level-Domains unterstützen.

Beim Hostnamen wird die Groß-/Kleinschreibung nicht berücksichtigt, er kann maximal 128 Zeichen lang sein und kann folgende Zeichen enthalten:

- A-Z, a-z, 0-9
- - .
- * (entspricht 0 oder mehr Zeichen)
- ? (entspricht genau 1 Zeichen)

Sie müssen mindestens ein "."-Zeichen einschließen. Es können nur alphabethische Zeichen nach dem letzten "."-Zeichen angegeben werden.

Beispiele für Hostnamen

- **`example.com`**
- **`test.example.com`**
- **`*.example.com`**

Die Regel **`*.example.com`** entspricht **`test.example.com`**, nicht jedoch **`example.com`**.

Example Beispiel für eine Host-Header-Bedingung für AWS CLI

Sie können Bedingungen angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die folgende Bedingung wird von Anforderungen mit einem Host-Header erfüllt, der mindestens einer der angegeben Zeichenfolgen entspricht.

```
[
  {
      "Field": "host-header",
      "HostHeaderConfig": {
          "Values": ["*.example.com"]
      }
  }
]
```

Pfadbedingungen

Mit Pfadbedingungen können Sie Regeln definieren, mit denen Anforderungen auf Grundlage der URL in der Anforderung weitergeleitet werden (auch bekannt als pfadbasierte Weiterleitung

Das Pfadmuster wird nur auf den Pfad der URL, nicht auf dessen Abfrageparameter, angewendet. Es wird nur auf sichtbare ASCII-Zeichen angewendet; Steuerzeichen (0x00 bis 0x1f und 0x7f) sind ausgeschlossen.

Die Regelauswertung wird erst durchgeführt, nachdem die URI-Normalisierung erfolgt ist.

Beim Pfadmuster wird die Groß-/Kleinschreibung berücksichtigt, es kann maximal 128 Zeichen lang sein und kann folgende Zeichen enthalten.

- A-Z, a-z, 0-9
- _ - . $ / ~ " ' @ : +
- & (Verwendung von &)
- * (entspricht 0 oder mehr Zeichen)
- ? (entspricht genau 1 Zeichen)

Wenn die Protokollversion gRPC ist, können Bedingungen für ein Paket, einen Dienst oder eine Methode spezifisch sein.

Beispiel für HTTP-Pfadmuster

- `/img/*`
- `/img/*/pics`

Beispiel für gRPC-Pfadmuster

- /paket
- /paket.dienst
- /paket.dienst/methode

Das Pfadmuster wird verwendet, um Anforderungen weiterzuleiten. Die Anforderungen werden bei diesem Vorgang aber nicht geändert. Wenn eine Regel beispielsweise das Pfadmuster `/img/*` aufweist, leitet die Regel eine Anforderung von `/img/picture.jpg` an die angegebene Zielgruppe als Anforderung von `/img/picture.jpg` weiter.

Example Beispiel für eine Pfadmusterbedingung für AWS CLI

Sie können Bedingungen angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die folgende Bedingung wird von Anforderungen mit einer URL erfüllt, die die angegebene Zeichenfolge enthält.

```
[
  {
      "Field": "path-pattern",
      "PathPatternConfig": {
          "Values": ["/img/*"]
      }
  }
]
```

Abfragezeichenfolgebedingungen

Sie können Bedingungen für Abfragezeichenfolgen verwenden, um Regeln zu konfigurieren, die Anfragen auf der Grundlage von key/value Paaren oder Werten in der Abfragezeichenfolge weiterleiten. Bei der Übereinstimmungsbewertung wird die Groß- und Kleinschreibung nicht beachtet, Die folgenden Platzhalterzeichen werden unterstützt: * (findet Übereinstimmungen mit 0 oder mehr Zeichen) und ? (findet Übereinstimmungen für genau 1 Zeichen).

Example Beispiel für eine Bedingung für eine Abfragezeichenfolge für AWS CLI

Sie können Bedingungen angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die folgende Bedingung wird

durch Anfragen mit einer Abfragezeichenfolge erfüllt, die entweder ein key/value Paar „version=v1" oder einen beliebigen Schlüssel enthält, der auf „Beispiel“ gesetzt ist.

```
[
  {
      "Field": "query-string",
      "QueryStringConfig": {
          "Values": [
            {
                "Key": "version",
                "Value": "v1"
            },
            {
                "Value": "*example*"
            }
          ]
      }
  }
]
```

Bedingungen für die Quell-IP-Adresse

Mit Bedingungen für die Quell-IP-Adresse können Sie Regeln konfigurieren, mit denen Anforderungen auf Grundlage der Quell-IP-Adresse der Anforderung weitergeleitet werden. Die IP-Adresse muss im CIDR-Format angegeben werden. Sie können sowohl als auch IPv4 Adressen verwenden. IPv6 Platzhalterzeichen werden nicht unterstützt. Sie können den `255.255.255.255/32`-CIDR für die Quell-IP-Regelbedingung nicht angeben.

Befindet sich ein Client hinter einem Proxy, ist dies die IP-Adresse des Proxys, nicht die des Clients.

Diese Bedingung wird von den Adressen in der X-Forwarded-For Kopfzeile nicht erfüllt. Verwenden Sie eine `http-header` Bedingung, um in der X-Forwarded-For Kopfzeile nach Adressen zu suchen.

Example Beispiel für eine Quell-IP-Bedingung für AWS CLI

Sie können Bedingungen angeben, wenn Sie eine Regel erstellen oder ändern. Weitere Informationen finden Sie bei den Befehlen create-rule und modify-rule. Die Folgende Bedingung wird von Anforderungen mit einer Quell-IP-Adresse in einem der angegebenen CIDR-Blöcken erfüllt.

```
[
  {
```

```
      "Field": "source-ip",
      "SourceIpConfig": {
          "Values": ["192.0.2.0/24", "198.51.100.10/32"]
      }
  }
]
```

HTTP-Header und Application Load Balancer

Die HTTP-Anforderungen und -Antworten verwenden Header-Felder, um Informationen über HTTP-Nachrichten zu senden. HTTP-Header werden automatisch hinzugefügt. Header-Felder sind durch einen Doppelpunkt getrennte Name/Wert-Paare, die durch eine Zeilenumschaltung und einen Zeilenvorschub getrennt sind. Ein Standardsatz von HTTP-Header-Feldern ist in RFC 2616, Nachrichten-Header definiert. Es sind auch Nicht-Standard-HTTP-Header verfügbar, die automatisch hinzugefügt und weithin von den Anwendungen verwendet werden. Einige der Nicht-Standard-HTTP-Header besitzen ein `X-Forwarded`-Präfix. Application Load Balancer unterstützen die folgenden `X-Forwarded`-Header.

Weitere Informationen zu HTTP-Verbindungen finden Sie unter Weiterleitung von Anforderungen im Benutzerhandbuch zu Elastic Load Balancing.

X-Forwarded-Header

- X-Forwarded-For
- X-Forwarded-Proto
- X-Forwarded-Port

X-Forwarded-For

Der `X-Forwarded-For`-Anforderungs-Header hilft Ihnen, die IP-Adresse eines Clients zu identifizieren, wenn Sie einen HTTP- oder HTTPS-Load Balancer verwenden. Da Load Balancer Datenverkehr zwischen Clients und Servern abfangen, enthalten Ihre Server-Zugriffsprotokolle nur die IP-Adresse des Load Balancers. Verwenden Sie das `routing.http.xff_header_processing.mode`-Attribut, um die IP-Adresse des Clients anzuzeigen. Dieses Attribut ermöglicht das Ändern, Beibehalten oder Entfernen der `X-Forwarded-For`-Header in der HTTP-Anforderung, bevor der Application Load Balancer die Anforderung an das Ziel sendet. Die möglichen Werte für dieses Attribut sind `append`, `preserve` und `remove`. Der Standardwert für dieses Attribut ist `append`.

> **Important**
>
> Der `X-Forwarded-For` Header sollte aufgrund potenzieller Sicherheitsrisiken mit Vorsicht verwendet werden. Die Einträge können nur dann als vertrauenswürdig angesehen werden, wenn sie von Systemen hinzugefügt werden, die innerhalb des Netzwerks ordnungsgemäß gesichert sind.

Anfügen

Der Application Load Balancer speichert die IP-Adresse des Clients standardmäßig im `X-Forwarded-For`-Anforderungs-Header und übergibt den Header an Ihren Server. Wenn der `X-Forwarded-For`-Anforderungsheader nicht in der ursprünglichen Anforderung enthalten ist, erstellt der Load Balancer einen Header mit der Client-IP-Adresse als Anforderungswert. Andernfalls hängt der Load Balancer die Client-IP-Adresse an den vorhandenen Header an und leitet den Header dann an Ihren Server weiter. Der `X-Forwarded-For`-Anforderungsheader kann mehrere IP-Adressen enthalten, die durch Kommas getrennt sind.

Der `X-Forwarded-For`-Anforderungs-Header besitzt das folgende Format:

```
X-Forwarded-For: client-ip-address
```

Nachfolgend finden Sie ein Beispiel für einen `X-Forwarded-For`-Anforderungs-Header für einen Client mit der IP-Adresse `203.0.113.7`.

```
X-Forwarded-For: 203.0.113.7
```

Im Folgenden finden Sie ein Beispiel für einen `X-Forwarded-For` Anforderungsheader für einen Client mit der IPv6 Adresse. `2001:DB8::21f:5bff:febf:ce22:8a2e`

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

Wenn das Attribut zur Beibehaltung des Client-Ports (`routing.http.xff_client_port.enabled`) im Load Balancer aktiviert ist, enthält der `X-Forwarded-For`-Anforderungsheader die an die `client-port-number` angehängte `client-ip-address`, durch einen Doppelpunkt getrennt. Der Header nimmt dann das folgende Format an:

```
IPv4 -- X-Forwarded-For: client-ip-address:client-port-number
```

```
IPv6 -- X-Forwarded-For: [client-ip-address]:client-port-number
```

Beachten Sie IPv6 nämlich, dass der Load Balancer, wenn er den `client-ip-address` an den vorhandenen Header anhängt, die Adresse in eckige Klammern setzt.

Im Folgenden finden Sie ein Beispiel für einen `X-Forwarded-For` Anforderungsheader für einen Client mit der IPv4 Adresse `12.34.56.78` und der Portnummer von. `8080`

```
X-Forwarded-For: 12.34.56.78:8080
```

Im Folgenden finden Sie ein Beispiel für einen `X-Forwarded-For` Anforderungsheader für einen Client mit der IPv6 Adresse `2001:db8:85a3:8d3:1319:8a2e:370:7348` und der Portnummer von`8080`.

```
X-Forwarded-For: [2001:db8:85a3:8d3:1319:8a2e:370:7348]:8080
```

Beibehalten

Der `preserve`-Modus im Attribut stellt sicher, dass der `X-Forwarded-For`-Header in der HTTP-Anforderung in keiner Weise geändert wird, bevor er an Ziele gesendet wird.

Remove

Der `remove`-Modus im Attribut entfernt den `X-Forwarded-For`-Header in der HTTP-Anforderung, bevor er an Ziele gesendet wird.

> **Note**
>
> Wenn Sie das Attribut zur Beibehaltung des Client-Ports (`routing.http.xff_client_port.enabled`) aktivieren und auch `preserve` oder `remove` für das `routing.http.xff_header_processing.mode` Attribut auswählen, überschreibt der Application Load Balancer das Attribut zur Erhaltung des Client-Ports. Je nach ausgewähltem Modus bleibt der `X-Forwarded-For`-Header unverändert oder wird entfernt, bevor er an die Ziele gesendet wird.

Die folgende Tabelle zeigt Beispiele für den `X-Forwarded-For`-Header, den das Ziel erhält, wenn Sie entweder den Modus `append`, `preserve` oder den Modus `remove` auswählen. In diesem Beispiel lautet die IP-Adresse des letzten Hops `127.0.0.1`.

Beschreibung der Anforderung	Beispielanforderung	XFF im **append**-Modus	XFF im **preserve**-Modus	XFF im **remove**-Modus
Anforderung wird ohne XFF-Header gesendet	`GET / index.html HTTP/1.1 Host: example.com`	`X-Forwarded-For: 127.0.0.1`	Nicht vorhanden	Nicht vorhanden
Anforderung wird mit einem XFF-Header und einer Client-IP-Adresse gesendet.	`GET / index.html HTTP/1.1 Host: example.com X-Forwarded-For: 127.0.0.4`	`X-Forwarded-For: 127.0.0.4, 127.0.0.1`	`X-Forwarded-For: 127.0.0.4`	Nicht vorhanden
Anforderung wird mit einem XFF-Header mit mehreren Client-IP-Adressen gesendet.	`GET / index.html HTTP/1.1 Host: example.com X-Forwarded-For: 127.0.0.4, 127.0.0.8`	`X-Forwarded-For: 127.0.0.4, 127.0.0.8, 127.0.0.1`	`X-Forwarded-For: 127.0.0.4, 127.0.0.8`	Nicht vorhanden

So können Sie den X-Forwarded-For-Header mithilfe der Konsole ändern, beibehalten oder entfernen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.

5. Wählen Sie im Bereich Datenverkehrskonfiguration unter Paketverarbeitung für X-Forwarded-For Header die Option Anhängen (Standard), Beibehalten oder Entfernen aus.
6. Wählen Sie Änderungen speichern aus.

Um den X-Forwarded-For Header zu ändern, beizubehalten oder zu entfernen, verwenden Sie AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl mit dem `routing.http.xff_header_processing.mode` Attribut.

X-Forwarded-Proto

Der `X-Forwarded-Proto`-Anforderungs-Header hilft Ihnen, das Protokoll (HTTP oder HTTPS) zu identifizieren, das ein Client für die Verbindung zu Ihrem Load Balancer verwendet hat. Ihre Server-Zugriffsprotokolle enthalten nur das Protokoll zwischen dem Server und dem Load Balancer. Sie enthalten keine Informationen über das Protokoll zwischen dem Client und dem Load Balancer. Verwenden Sie den `X-Forwarded-Proto`-Anforderungs-Header, um das Protokoll zwischen dem Client und dem Load Balancer zu überprüfen. Elastic Load Balancing speichert das Protokoll zwischen dem Client und dem Load Balancer im `X-Forwarded-Proto`-Anforderungs-Header und übergibt den Header an den Server.

Ihre Anwendung oder Website kann das im `X-Forwarded-Proto`-Anforderungs-Header gespeicherte Protokoll verwenden, um eine Rückmeldung auszugeben, die auf die entsprechende URL umleitet.

Der `X-Forwarded-Proto`-Anforderungs-Header besitzt das folgende Format:

```
X-Forwarded-Proto: originatingProtocol
```

Das folgende Beispiel enthält einen `X-Forwarded-Proto`-Anforderungs-Header für eine Anforderung, die vom Client als HTTPS-Anforderung ausgegeben wurde:

```
X-Forwarded-Proto: https
```

X-Forwarded-Port

Mit dem `X-Forwarded-Port`-Anforderungs-Header können Sie den Zielport identifizieren, den der Client für die Verbindung mit dem Load Balancer verwendet hat.

Erstellen eines HTTP-Listeners für Ihren Application Load Balancer

Ein Listener überprüft Verbindungsanforderungen. Sie definieren einen Listener, wenn Sie Ihren Load Balancer erstellen, und Sie können Listener jederzeit zu Ihrem Load Balancer hinzufügen.

Die Informationen auf dieser Seite helfen Ihnen bei der Erstellung eines HTTP-Listeners für Ihren Load Balancer. Informationen zum Hinzufügen eines HTTPS-Listeners zu Ihrem Load Balancer finden Sie unter Erstellen eines HTTPS-Listeners für Ihren Application Load Balancer.

Voraussetzungen

- Um eine Weiterleitungsaktion zur Standard-Listener-Regel hinzuzufügen, müssen Sie eine verfügbare Zielgruppe angeben. Weitere Informationen finden Sie unter Erstellen Sie eine Zielgruppe für Ihren Application Load Balancer.
- Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Load Balancer angehören. Um eine Zielgruppe mit einem Load Balancer zu verwenden, müssen Sie sicherstellen, dass sie nicht von einem Listener verwendet wird, der einem anderen Load Balancer angehört.

Hinzufügen eines HTTP-Listeners

Sie konfigurieren einen Listener mit einem Protokoll und einem Port für Verbindungen von Clients zum Load Balancer und einer Zielgruppe für die standardmäßige Listener-Regel. Weitere Informationen finden Sie unter Listener-Konfiguration.

So fügen Sie einen HTTP-Listener mithilfe der Konsole hinzu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln die Option Listener hinzufügen aus.
5. Wählen Sie unter Protokoll : Port die Option HTTP aus und belassen Sie den Standardport bei oder wählen Sie einen anderen Port aus.
6. Wählen Sie unter Standardaktionen eine der folgenden Optionen:

    - Zu Zielgruppen weiterleiten – Wählen Sie eine oder mehrere Zielgruppen aus, an die der Datenverkehr weitergeleitet werden soll. Um Zielgruppen hinzuzufügen, wählen Sie

Zielgruppe hinzufügen aus. Wenn Sie mehr als eine Zielgruppe verwenden, wählen Sie für jede Zielgruppe eine Gewichtung aus und überprüfen Sie den zugehörigen Prozentsatz. Sie müssen die Stickiness auf Gruppenebene für eine Regel aktivieren, wenn Sie die Stickiness für eine oder mehrere Zielgruppen aktiviert haben.

- Umleitung zu URL – Geben Sie die URL an, an die Client-Anforderungen umgeleitet werden. Das ist möglich, indem Sie jeden Teil einzeln auf der Registerkarte URI-Teile eingeben oder indem Sie die vollständige Adresse auf der Registerkarte Vollständige URL eingeben. Für Statuscode können Sie Weiterleitungen je nach Bedarf entweder als temporär (HTTP 302) oder permanent (HTTP 301) konfigurieren.
- Feststehende Antwort zurückgeben – Geben Sie den Antwortcode an, der bei verworfenen Client-Anforderungen zurückgegeben wird. Darüber hinaus können Sie den Inhaltstyp und den Antworttext angeben. Diese sind jedoch nicht erforderlich.

7. Wählen Sie Hinzufügen aus.

Um einen HTTP-Listener hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-listener, um den Listener und die Standardregel zu erstellen, und den Befehl create-rule, um zusätzliche Listener-Regeln zu definieren.

SSL-Zertifikate für Ihren Application Load Balancer

Wenn Sie einen sicheren Listener für Ihren Application Load Balancer erstellen, müssen Sie mindestens ein Zertifikat auf dem Load Balancer bereitstellen. Der Load Balancer erfordert X.509-Zertifikate (SSL/TLS-Serverzertifikate). Zertifikate sind eine digitale Methode zur Identifizierung. Sie werden von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt. Ein Zertifikat enthält Identifizierungsdaten, einen Gültigkeitszeitraum, den öffentlichen Schlüssel, eine Seriennummer und die digitale Signatur des Ausstellers.

Wenn Sie ein Zertifikat zur Verwendung mit Ihrem Load Balancer erstellen, müssen Sie einen Domainnamen angeben. Der Domainname auf dem Zertifikat muss mit dem Datensatz für den benutzerdefinierten Domainnamen übereinstimmen, damit wir die TLS-Verbindung überprüfen können. Stimmen sie nicht überein, wird der Datenverkehr nicht verschlüsselt.

Sie müssen einen vollqualifizierten Domainnamen (Fully Qualified Domain Name, FQDN) für Ihr Zertifikat wie `www.example.com` oder einen Apex-Domainnamen wie `example.com` angeben. Sie können auch ein Sternchen (*) als Platzhalter verwenden, um mehrere Websitenamen in derselben Domain zu schützen. Wenn Sie ein Platzhalter-Zertifikat anfordern, muss sich das Sternchen (*)

ganz links im Domainnamen befinden und es kann nur eine Subdomain-Ebene geschützt werden. `*.example.com` schützt beispielsweise `corp.example.com` und `images.example.com`, aber es kann `test.login.example.com` nicht schützen. Beachten Sie außerdem, dass `*.example.com` nur die Subdomains von `example.com` schützt, jedoch nicht die bare- oder apex-Domain (`example.com`). Der Platzhaltername wird im Feld Subjekt und in der Erweiterung Alternativer Subjekt-Name des ACM-Zertifikats angezeigt. Weitere Informationen zu öffentlichen Zertifikaten finden Sie unter Anfordern eines öffentlichen Zertifikats im AWS Certificate Manager Benutzerhandbuch.

Wir empfehlen, Zertifikate für Ihren Load Balancer mit AWS Certificate Manager (ACM) zu erstellen. ACM unterstützt RSA-Zertifikate mit Schlüssellängen von 2 048, 3 072 und 4 096 Bit sowie alle ECDSA-Zertifikate. ACM lässt sich in Elastic Load Balancing integrieren, sodass Sie das Zertifikat in Ihrem Load Balancer bereitstellen können. Weitere Informationen finden Sie im AWS Certificate Manager -Benutzerhandbuch.

Alternativ können Sie SSL/TLS Tools verwenden, um eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) zu erstellen. Anschließend können Sie die CSR von einer Zertifizierungsstelle signieren lassen, um ein Zertifikat zu erstellen. Anschließend können Sie das Zertifikat in ACM importieren oder das Zertifikat in AWS Identity and Access Management (IAM) hochladen. Weitere Informationen zum Importieren von Zertifikaten in ACM finden Sie unter Importieren von Zertifikaten im AWS Certificate Manager -Leitfaden. Weitere Informationen zum Hochladen von Zertifikaten in IAM finden Sie unter Arbeiten mit Serverzertifikaten im IAM-Benutzerhandbuch.

Standardzertifikat

Wenn Sie einen HTTPS-Listener erstellen, müssen Sie genau ein Zertifikat angeben. Dieses Zertifikat wird als Standardzertifikat bezeichnet. Sie können das Standardzertifikat ersetzen, nachdem Sie den HTTPS-Listener erstellt haben. Weitere Informationen finden Sie unter Ersetzen des Standardzertifikats.

Wenn Sie weitere Zertifikate in einer Zertifikatliste angeben, wird das Standardzertifikat nur verwendet, wenn ein Client eine Verbindung ohne SNI- (Server Name Indication)-Protokoll herstellt, um einen Hostnamen anzugeben, oder falls keine passenden Zertifikate in der Zertifikatliste gefunden werden.

Wenn Sie keine weiteren Zertifikate angeben, aber mehrere sichere Anwendungen über einen einzelnen Load Balancer hosten müssen, können Sie ein Platzhalterzertifikat verwenden oder Ihrem Zertifikat einen SAN (Subject Alternative Name) für jede weitere Domain hinzufügen.

Zertifikatliste

Nachdem Sie einen HTTPS-Listener erstellt haben, können Sie der Zertifikatsliste Zertifikate hinzufügen. Wenn Sie den Listener mit dem erstellt haben AWS Management Console, haben wir das Standardzertifikat für Sie zur Zertifikatsliste hinzugefügt. Andernfalls ist die Zertifikatsliste leer. Ein Load Balancer kann dann mehrere Domains über denselben Port unterstützen und ein anderes Zertifikat für jede Domain bereitstellen. Weitere Informationen finden Sie unter Hinzufügen von Zertifikaten zu einer Zertifikatliste.

Der Load Balancer verwendet einen intelligenten Algorithmus für die Zertifikatsauswahl, bei dem SNI unterstützt wird. Wenn der von einem Client bereitgestellte Hostname nur mit einem Zertifikat in der Zertifikatliste übereinstimmt, wählt der Load Balancer das entsprechende Zertifikat aus. Wenn ein von einem Client bereitgestellter Hostname mehreren Zertifikaten in der Zertifikatliste entspricht, wählt der Load Balancer das beste vom Client unterstützte Zertifikat. Die Auswahl des Zertifikats basiert auf den folgenden Kriterien in der angegebenen Reihenfolge:

- Algorithmus für öffentlichen Schlüssel (ECDSA gegenüber RSA bevorzugt)
- Ablauf (lieber nicht abgelaufen)
- Hash-Algorithmus (lieber SHA als MD5). Wenn es mehrere SHA-Zertifikate gibt, bevorzugen Sie die höchste SHA-Nummer.
- Schlüssellänge (der längste Schlüssel wird bevorzugt)
- Gültigkeitszeitraum

Die Load Balancer-Zugriffsprotokolleinträge enthalten den vom Client angegebenen Hostnamen und das dem Client präsentierte Zertifikat. Weitere Informationen finden Sie unter Zugriffsprotokolleinträge.

Zertifikatserneuerung

Jedes Zertifikat verfügt über einen Gültigkeitszeitraum. Sie müssen sicherstellen, dass Sie jedes Zertifikat für Ihren Load Balancer vor dem Ablauf des Gültigkeitszeitraum erneuern oder ersetzen. Dies schließt das Standardzertifikat und Zertifikate in der Zertifikatliste ein. Das Verlängern oder Ersetzen eines Zertifikats wirkt sich nicht auf Anforderungen aus, die bereits verarbeitet werden, von einem Load Balancer-Knoten empfangen wurden und deren Weiterleitung an ein fehlerfreies Ziel aussteht. Nachdem ein Zertifikat verlängert wurde, verwenden neue Anforderungen das verlängerte Zertifikat. Nachdem ein Zertifikat ersetzt wurde, verwenden neue Anforderungen das neue Zertifikat.

Sie können das Verlängern und Ersetzen von Zertifikaten folgendermaßen verwalten:

- Zertifikate, die von Ihrem Load Balancer bereitgestellt AWS Certificate Manager und dort bereitgestellt werden, können automatisch erneuert werden. ACM versucht, die Zertifikate zu verlängern, bevor sie ablaufen. Weitere Informationen finden Sie unter Verwaltete Erneuerung im AWS Certificate Manager -Benutzerhandbuch.
- Wenn Sie ein Zertifikat in ACM importiert haben, müssen Sie das Ablaufdatum des Zertifikats überwachen und es vor dem Ablauf verlängern. Weitere Informationen finden Sie unter Importieren von Zertifikaten im AWS Certificate Manager -Benutzerhandbuch.
- Wenn Sie ein Zertifikat in IAM importiert haben, müssen Sie ein neues Zertifikat erstellen, das neue Zertifikat in ACM oder IAM importieren, es dem Load Balancer hinzufügen und das abgelaufene Zertifikat aus dem Load Balancer entfernen.

Sicherheitsrichtlinien für Ihren Application Load Balancer

Elastic Load Balancing verwendet eine Secure Socket Layer (SSL)-Aushandlungskonfiguration, die als Sicherheitsrichtlinie bezeichnet wird, um SSL-Verbindungen zwischen einem Client und dem Load Balancer auszuhandeln. Eine Sicherheitsrichtlinie ist eine Kombination aus Protokollen und Verschlüsselungen. Das Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her und stellt sicher, dass alle Daten, die zwischen dem Client und Ihres Load Balancers übertragen werden, privat sind. Ein Verschlüsselungsverfahren ist ein Algorithmus, der eine kodierte Nachricht mithilfe von Verschlüsselungsschlüsseln erstellt. Protokolle verwenden mehrere Verschlüsselungsverfahren zum Verschlüsseln von Daten über das Internet. Während der Verbindungsaushandlung präsentieren der Client und der Load Balancer eine Liste von Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Standardmäßig wird für die sichere Verbindung die erste Verschlüsselung auf der Liste des Servers ausgewählt, die mit einem der Verschlüsselungsverfahren des Clients übereinstimmt.

Überlegungen

- Application Load Balancer unterstützen die erneute SSL-Aushandlung nur für Zielverbindungen.
- Wenn Sie einen HTTPS-Listener erstellen, müssen Sie eine Sicherheitsrichtlinie auswählen.
- Die `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` Richtlinie ist die Standard-Sicherheitsrichtlinie für HTTPS-Listener, die mit dem erstellt wurden. AWS Management Console Diese Richtlinie unterstützt TLS 1.3 und ist abwärtskompatibel mit TLS 1.2.

- Die `ELBSecurityPolicy-2016-08` Richtlinie ist die Standardsicherheitsrichtlinie für HTTPS-Listener, die mit dem erstellt wurden. AWS CLI
- Application Load Balancer unterstützen keine benutzerdefinierten Sicherheitsrichtlinien.
- Sie können die Sicherheitsrichtlinie wählen, die für Front-End-Verbindungen verwendet wird, aber nicht für Back-End-Verbindungen.
  - Wenn einer Ihrer HTTPS-Listener für Back-End-Verbindungen eine TLS 1.3-Sicherheitsrichtlinie verwendet, wird die `ELBSecurityPolicy-TLS13-1-0-2021-06` Sicherheitsrichtlinie verwendet. Andernfalls wird die `ELBSecurityPolicy-2016-08`-Sicherheitsrichtlinie für Backend-Verbindungen verwendet.
  - Hinweis: Wenn Sie eine FIPS-TLS-Richtlinie für Ihren HTTPS-Listener verwenden, `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` wird diese für Backend-Verbindungen verwendet.
- Um die Compliance- und Sicherheitsstandards zu erfüllen, die die Deaktivierung bestimmter TLS-Protokollversionen erfordern, oder um ältere Clients zu unterstützen, die veraltete Verschlüsselungen benötigen, können Sie eine der Sicherheitsrichtlinien verwenden. `ELBSecurityPolicy-TLS-` Um die TLS-Protokollversion für Anfragen an Ihren Application Load Balancer anzuzeigen, aktivieren Sie die Zugriffsprotokollierung für Ihren Load Balancer und überprüfen Sie die entsprechenden Zugriffsprotokolleinträge. Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihren Application Load Balancer.
- Sie können einschränken, welche Sicherheitsrichtlinien Benutzern in Ihrem AWS-Konten Land zur Verfügung stehen, AWS Organizations indem Sie die Elastic Load Balancing Balancing-Bedingungsschlüssel in Ihren IAM- bzw. Service Control-Richtlinien (SCPs) verwenden. Weitere Informationen finden Sie unter Richtlinien zur Servicesteuerung (SCPs) im AWS Organizations Benutzerhandbuch
- Richtlinien, die nur TLS 1.3 unterstützen, unterstützen Forward Secrecy (FS). Richtlinien, die TLS 1.3 und TLS 1.2 unterstützen und nur Chiffren der Form TLS_* und ECDHE_* enthalten, bieten auch FS.
- Application Load Balancers unterstützen die TLS-Wiederaufnahme mithilfe von PSK (TLS 1.3) und Sitzungstickets (TLS 1.2 und älter). IDs/session Wiederaufnahmen werden nur bei Verbindungen mit derselben Application Load Balancer Balancer-IP-Adresse unterstützt. Die 0-RTT-Datenfunktion und die Erweiterung early_data sind nicht implementiert.
- Application Load Balancers unterstützen die Erweiterung Extended Master Secret (EMS) für TLS 1.2.

Sie können die Protokolle und Chiffren mit dem describe-ssl-policies AWS CLI Befehl beschreiben oder in den folgenden Tabellen nachschlagen.

Sicherheitsrichtlinien

- TLS-Sicherheitsrichtlinien
  - Protokolle nach Richtlinie
  - Chiffren nach Richtlinien
  - Richtlinien nach Chiffre
- FIPS-Sicherheitsrichtlinien
  - Protokolle nach Richtlinien
  - Chiffren nach Richtlinie
  - Richtlinien nach Chiffre
- Von FS unterstützte Richtlinien
  - Protokolle nach Richtlinie
  - Chiffren nach Richtlinien
  - Richtlinien nach Chiffre

TLS-Sicherheitsrichtlinien

Sie können die TLS-Sicherheitsrichtlinien verwenden, um Konformitäts- und Sicherheitsstandards zu erfüllen, die die Deaktivierung bestimmter TLS-Protokollversionen erfordern, oder um ältere Clients zu unterstützen, die veraltete Verschlüsselungen benötigen.

Richtlinien, die nur TLS 1.3 unterstützen, unterstützen Forward Secrecy (FS). Richtlinien, die TLS 1.3 und TLS 1.2 unterstützen und nur Chiffren der Form TLS_* und ECDHE_* enthalten, bieten auch FS.

Inhalt

- Protokolle nach Richtlinie
- Chiffren nach Richtlinien
- Richtlinien nach Chiffre

Protokolle nach Richtlinie

In der folgenden Tabelle werden die Protokolle beschrieben, die von den einzelnen TLS-Sicherheitsrichtlinien unterstützt werden.

Sicherheitsrichtlinien	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityRichtlinie- TLS13 -1-3-2021-06	Ja	Nein	Nein	Nein
ELBSecurityPolitik- -1-2-2021-06 TLS13	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-1-2021-06	Ja	Ja	Ja	Nein
ELBSecurityPolitik- -1-0-2021-06 TLS13	Ja	Ja	Ja	Ja
ELBSecurityRichtlinie TLS-1-2-EXT-2018-06	Nein	Ja	Nein	Nein
ELBSecurityRichtlinie-TLS-1-2-2017-01	Nein	Ja	Nein	Nein
ELBSecurityRichtlinie-TLS-1-1-2017-01	Nein	Ja	Ja	Nein
ELBSecurityPolitik-2016-08	Nein	Ja	Ja	Ja

Sicherheitsrichtlinien	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitik-2015-05	Nein	Ja	Ja	Ja

Chiffren nach Richtlinien

In der folgenden Tabelle werden die Verschlüsselungen beschrieben, die von den einzelnen TLS-Sicherheitsrichtlinien unterstützt werden.

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie- -1-3-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256
ELBSecurityPolitik- TLS13 -1-2-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256

Sicherheitsrichtlinie	Verschlüsselungen
	• ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384
ELBSecurityRichtlinie- TLS13 -1-2-Ext2 -2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie- -1-2-Ext1-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik- -1-1-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik- -1-0-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie-TLS-1-2-EXT-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie-TLS-1-2-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie-TLS-1-1-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik - 2016-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik 2015-05	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Richtlinien nach Chiffre

In der folgenden Tabelle werden die TLS-Sicherheitsrichtlinien beschrieben, die die einzelnen Verschlüsselungen unterstützen.

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — TLS_AES_128_GCM_SHA256	• ELBSecurityRichtlinie- TLS13 -1-3-2021-06	1301

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitik- -1-2-2021-06 TLS13 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13	
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-3-2021-06 • ELBSecurityPolitik- -1-2-2021-06 TLS13 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13	1302

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 IANA — TLS_ 0_ 05_ CHACHA2 POLY13 SHA256	• ELBSecurityPolitik- TLS13 -1-3-2021 -06 • ELBSecurityPolitik- -1-2-2021-06 TLS13 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13	1303

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c02b

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13-1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13-1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c02f

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Ext2 -2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c023

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Ext2 -2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c027
OpenSSL — 128-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie- TLS13 1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c009

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — 128-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie- TLS13 1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c013

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c02c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 256-GCM- SHA384 IANA — TLS_ECCHE_RSA_WITH _AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Res-2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c030

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Ext2 -2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c024

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-2021-06 • ELBSecurityRichtlinie- -1-2-Ext2 -2021-06 TLS13 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c028
OpenSSL — 256-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie- TLS13 1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c00a

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — 256-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie- TLS13 1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-E XT-2018-06 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	c014
OpenSSL — AES128 -GCM- SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-E XT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	9c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — - AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	3c
OpenSSL — -SHA AES128 IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	2f

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES256 -GCM- SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	9d

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — - AES256 SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-2-Ext1-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	3d
OpenSSL — -SHA AES256 IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-Ext2-2021-06 • ELBSecurityRichtlinie- TLS13 -1-1-2021-06 • ELBSecurityPolitik- -1-0-2021-06 TLS13 • ELBSecurityRichtlinie TLS-1-2-EXT-2018-06 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08	35

FIPS-Sicherheitsrichtlinien

> **Important**
>
> Alle sicheren Listener, die an einen Application Load Balancer angeschlossen sind, müssen entweder FIPS-Sicherheitsrichtlinien oder Nicht-FIPS-Sicherheitsrichtlinien verwenden; sie können nicht gemischt werden. Wenn ein vorhandener Application Load Balancer über zwei oder mehr Listener verfügt, die Nicht-FIPS-Richtlinien verwenden, und Sie möchten, dass die Listener stattdessen FIPS-Sicherheitsrichtlinien verwenden, entfernen Sie alle Listener, bis nur noch einer vorhanden ist. Ändern Sie die Sicherheitsrichtlinie des Listeners in FIPS und erstellen Sie dann weitere Listener mithilfe von FIPS-Sicherheitsrichtlinien. Alternativ können Sie einen neuen Application Load Balancer mit neuen Listenern erstellen, die nur FIPS-Sicherheitsrichtlinien verwenden.

Der Federal Information Processing Standard (FIPS) ist ein US-amerikanischer und kanadischer Regierungsstandard, der die Sicherheitsanforderungen für kryptografische Module zum Schutz vertraulicher Informationen festlegt. Weitere Informationen finden Sie unter Federal Information Processing Standard (FIPS) 140 auf der Seite AWS Cloud Security Compliance.

Alle FIPS-Richtlinien nutzen das FIPS-validierte kryptografische Modul von AWS-LC. Weitere Informationen finden Sie auf der Seite AWS-LC Cryptographic Module auf der Website des NIST Cryptographic Module Validation Program.

> **Important**
>
> Richtlinien `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` und `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` werden nur aus Gründen der Kompatibilität mit älteren Versionen bereitgestellt. Sie verwenden zwar FIPS-Kryptografie mit dem Modul FIPS14 0, entsprechen aber möglicherweise nicht den neuesten NIST-Richtlinien für die TLS-Konfiguration.

Inhalt

- Protokolle nach Richtlinien
- Chiffren nach Richtlinie
- Richtlinien nach Chiffre

Protokolle nach Richtlinien

In der folgenden Tabelle werden die Protokolle beschrieben, die von den einzelnen FIPS-Sicherheitsrichtlinien unterstützt werden.

Sicherheitsrichtlinien	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityRichtlinie- -1-3-FIPS-2023-04 TLS13	Ja	Nein	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04	Ja	Ja	Ja	Nein
ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	Ja	Ja	Ja	Ja

Chiffren nach Richtlinie

In der folgenden Tabelle werden die Verschlüsselungen beschrieben, die von den einzelnen FIPS-Sicherheitsrichtlinien unterstützt werden.

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie- -1-3-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384
ELBSecurityRichtlinie- -1-2-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityRichtlinie- -1-2-RES-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384
ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384

Sicherheitsrichtlinie	Verschlüsselungen
	• ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA
ELBSecurityRichtlinie- -1-2-ext1-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie- -1-2-ext0-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie- -1-1-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie- -1-0-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA

Richtlinien nach Chiffre

In der folgenden Tabelle werden die FIPS-Sicherheitsrichtlinien beschrieben, die die einzelnen Verschlüsselungen unterstützen.

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — TLS_AES_128_GCM_SHA256 IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-3-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	1301
OpenSSL — TLS_AES_256_GCM_SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-3-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04	1302

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
	• ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	
OpenSSL — ECDHE-ECDSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c02b

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c02f
OpenSSL — ECDHE-ECDSA-AES 128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c023

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c027
OpenSSL — 128-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c009
OpenSSL — 128-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c013

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c02c
OpenSSL — ECDHE-RSA-AES 256-GCM- SHA384 IANA — TLS_ECCHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c030

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c024
OpenSSL — ECDHE-RSA-AES 256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c028

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — 256-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c00a
OpenSSL — 256-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	c014
OpenSSL — AES128 -GCM- SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	9c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — - AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	3c
OpenSSL — -SHA AES128 IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	2f
OpenSSL — AES256 -GCM- SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	9d

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — - AES256 SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	3d
OpenSSL — -SHA AES256 IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-1-FIPS-2023-04 • ELBSecurityRichtlinie- TLS13 -1-0-FIPS-2023-04	35

Von FS unterstützte Richtlinien

Von FS (Forward Secrecy) unterstützte Sicherheitsrichtlinien bieten zusätzliche Schutzmaßnahmen gegen das Abhören verschlüsselter Daten durch die Verwendung eines eindeutigen zufälligen Sitzungsschlüssels. Dadurch wird die Entschlüsselung erfasster Daten verhindert, selbst wenn der geheime Langzeitschlüssel kompromittiert wird.

Die Richtlinien in diesem Abschnitt unterstützen FS, und „FS“ ist in ihren Namen enthalten. Dies sind jedoch nicht die einzigen Richtlinien, die FS unterstützen. Richtlinien, die nur TLS 1.3 unterstützen, unterstützen FS. Richtlinien, die TLS 1.3 und TLS 1.2 unterstützen und nur Chiffren der Form TLS_* und ECDHE_* enthalten, bieten auch FS.

Inhalt

- Protokolle nach Richtlinie
- Chiffren nach Richtlinien

- Richtlinien nach Chiffre

Protokolle nach Richtlinie

In der folgenden Tabelle werden die Protokolle beschrieben, die von jeder FS-unterstützten Sicherheitsrichtlinie unterstützt werden.

Sicherheitsrichtlinien	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityRichtlinie-FS-1-2-RES-2020-10	Nein	Ja	Nein	Nein
ELBSecurityRichtlinie-FS-1-2-RES-2019-08	Nein	Ja	Nein	Nein
ELBSecurityPolitik-FS-1-2-2019-08	Nein	Ja	Nein	Nein
ELBSecurityPolitik-FS-1-1-2019-08	Nein	Ja	Ja	Nein
ELBSecurityPolitik-FS-2018-06	Nein	Ja	Ja	Ja

Chiffren nach Richtlinien

In der folgenden Tabelle werden die Chiffren beschrieben, die von jeder FS-unterstützten Sicherheitsrichtlinie unterstützt werden.

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie-FS-1-2-RES-2020-10	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik-FS-1-2-RES-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityRichtlinie-FS-1-2-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik-FS-1-1-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256
ELBSecurityRichtlinie-FS-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA-SHA AES256

Richtlinien nach Chiffre

In der folgenden Tabelle werden die von FS unterstützten Sicherheitsrichtlinien beschrieben, die die einzelnen Verschlüsselungen unterstützen.

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie-FS-1-2-RES-2020-10 • ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c02b
OpenSSL — ECDHE-RSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie-FS-1-2-RES-2020-10 • ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c02f
OpenSSL — ECDHE-ECDSA-AES 128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c023
OpenSSL — ECDHE-RSA-AES 128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c027
OpenSSL — 128-SHA ECDHE-ECDSA-AES	• ELBSecurityRichtlinie-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08	c009

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitik-FS-2018-06	
OpenSSL — 128-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c013
OpenSSL — ECDHE-ECDSA-AES 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie-FS-1-2-RES-2020-10 • ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c02c
OpenSSL — ECDHE-RSA-AES 256-GCM- SHA384 IANA — TLS_ECCHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie-FS-1-2-RES-2020-10 • ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c030
OpenSSL — ECDHE-ECDSA-AES 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c024

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie-FS-1-2-RES-2019-08 • ELBSecurityPolitik-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c028
OpenSSL — 256-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c00a
OpenSSL — 256-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie-FS-1-2-2019-08 • ELBSecurityPolitik-FS-1-1-2019-08 • ELBSecurityPolitik-FS-2018-06	c014

Erstellen eines HTTPS-Listeners für Ihren Application Load Balancer

Ein Listener überprüft Verbindungsanforderungen. Sie definieren einen Listener, wenn Sie Ihren Load Balancer erstellen, und Sie können Listener jederzeit zu Ihrem Load Balancer hinzufügen.

Um einen HTTPS-Listener zu erstellen, müssen Sie mindestens ein SSL-Serverzertifikat auf Ihrem Load Balancer bereitstellen. Der Load Balancer verwendet ein Serverzertifikat, um die Frontend-Verbindung zu beenden und dann Anfragen von Clients zu entschlüsseln, bevor er sie an die Ziele sendet. Sie müssen auch eine Sicherheitsrichtlinie angeben, die verwendet wird, um sichere Verbindungen zwischen Clients und dem Load Balancer auszuhandeln.

Wenn Sie verschlüsselten Datenverkehr an Ziele weiterleiten müssen, ohne dass der Load Balancer diesen Datenverkehr entschlüsselt, können Sie einen Network Load Balancer oder Classic Load

Balancer mit einem TCP-Listener an Port 443 erstellen. Bei einem TCP-Listener leitet der Load Balancer verschlüsselten Datenverkehr an die Ziele weiter, ohne ihn zu entschlüsseln.

Die Informationen auf dieser Seite helfen Ihnen bei der Erstellung eines HTTPS-Listeners für Ihren Load Balancer. Informationen zum Hinzufügen eines HTTP-Listeners zu Ihrem Load Balancer finden Sie unter Erstellen eines HTTP-Listeners für Ihren Application Load Balancer.

Voraussetzungen

- Um einen HTTPS-Listener zu erstellen, müssen Sie ein Zertifikat und eine Sicherheitsrichtlinie angeben. Der Load Balancer verwendet ein Zertifikat, um die Verbindung zu beenden und Anforderungen von Clients zu entschlüsseln, bevor er sie an Ziele weiterleitet. Der Load Balancer verwendet die Sicherheitsrichtlinie beim Aushandeln von SSL-Verbindungen mit den Clients.

  Application Load Balancer unterstützen ED25519 keine Schlüssel.
- Um eine Weiterleitungsaktion zur Standard-Listener-Regel hinzuzufügen, müssen Sie eine verfügbare Zielgruppe angeben. Weitere Informationen finden Sie unter Erstellen Sie eine Zielgruppe für Ihren Application Load Balancer.
- Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Load Balancer angehören. Um eine Zielgruppe mit einem Load Balancer zu verwenden, müssen Sie sicherstellen, dass sie nicht von einem Listener verwendet wird, der einem anderen Load Balancer angehört.

Hinzufügen eines HTTPS-Listeners

Sie konfigurieren einen Listener mit einem Protokoll und einem Port für Verbindungen von Clients zum Load Balancer und einer Zielgruppe für die standardmäßige Listener-Regel. Weitere Informationen finden Sie unter Listener-Konfiguration.

So fügen Sie einen HTTPS-Listeners mithilfe der Konsole hinzu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln die Option Listener hinzufügen aus.
5. Wählen Sie unter Protokoll : Port die Option HTTPS aus und belassen Sie den Standardport bei oder wählen Sie einen anderen Port aus.

6. (Optional) Um die Authentifizierung zu aktivieren, wählen Sie unter Authentifizierung die Option OpenID oder Amazon Cognito verwenden aus und geben Sie die angeforderten Informationen ein. Weitere Informationen finden Sie unter Authentifizieren von Benutzern mithilfe eines Application Load Balancers.
7. Führen Sie für Routing-Aktionen einen der folgenden Schritte aus:

   - An Zielgruppen weiterleiten — Wählen Sie die Zielgruppen aus, an die der Traffic weitergeleitet werden soll. Um Zielgruppen hinzuzufügen, wählen Sie Zielgruppe hinzufügen aus. Wenn Sie mehr als eine Zielgruppe verwenden, wählen Sie für jede Zielgruppe eine Gewichtung aus und überprüfen Sie den zugehörigen Prozentsatz. Sie müssen die Stickiness auf Gruppenebene für eine Regel aktivieren, wenn Sie die Stickiness für eine oder mehrere Zielgruppen aktiviert haben.
   - Zur URL weiterleiten — Geben Sie die URL ein, an die Kundenanfragen umgeleitet werden. Das ist möglich, indem Sie jeden Teil einzeln auf der Registerkarte URI-Teile eingeben oder indem Sie die vollständige Adresse auf der Registerkarte Vollständige URL eingeben. Für Statuscode können Sie Weiterleitungen je nach Bedarf entweder als temporär (HTTP 302) oder permanent (HTTP 301) konfigurieren.
   - Feste Antwort zurückgeben — Geben Sie den Antwortcode ein, um zu verworfenen Kundenanfragen zurückzukehren. Optional können Sie den Inhaltstyp und den Antworttext angeben.
8. Wir empfehlen, dass Sie für Sicherheitsrichtlinie immer die neueste vordefinierte Sicherheitsrichtlinie verwenden.
9. Wählen Sie für SSL/TLS Standardzertifikat das Standardzertifikat aus. Wir fügen auch das Standardzertifikat zur SNI-Liste hinzu. Sie können das Zertifikat aus einer der folgenden Quellen auswählen:

   - Wenn Sie ein Zertifikat mit erstellt oder importiert haben AWS Certificate Manager, wählen Sie „Aus ACM“ und dann das Zertifikat aus „Zertifikat (von ACM)“.
   - Wenn Sie ein Zertifikat mithilfe von IAM importiert haben, wählen Sie „Aus IAM“ und dann das Zertifikat aus „Zertifikat (aus IAM)“ aus.
   - Wenn Sie über ein Zertifikat verfügen, wählen Sie Zertifikat importieren. Wählen Sie entweder In ACM importieren oder In IAM importieren. Kopieren Sie für den privaten Schlüssel des Zertifikats den Inhalt der privaten Schlüsseldatei (PEM-kodiert) und fügen Sie ihn ein. Kopieren Sie für Certificate Body den Inhalt der Zertifikatsdatei mit öffentlichem Schlüssel (PEM-kodiert) und fügen Sie ihn ein. Kopieren Sie für Certificate Chain den Inhalt der Zertifikatskettendatei

(PEM-kodiert) und fügen Sie ihn ein, es sei denn, Sie verwenden ein selbstsigniertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.

10. (Optional) Um die gegenseitige Authentifizierung zu aktivieren, aktivieren Sie unter Verwaltung von Client-Zertifikaten die Option Gegenseitige Authentifizierung (mTLS).

    Wenn diese Option aktiviert ist, ist der standardmäßige Modus für gegenseitiges TLS Passthrough.

    Wenn Sie „Mit Trust Store verifizieren“ auswählen:

    - Standardmäßig werden Verbindungen mit abgelaufenen Client-Zertifikaten abgelehnt. Um dieses Verhalten zu ändern, erweitern Sie die erweiterten mTLS-Einstellungen und wählen Sie dann unter Ablauf des Client-Zertifikats die Option Abgelaufene Client-Zertifikate zulassen aus.
    - Wählen Sie unter Trust Store einen vorhandenen Trust Store aus, oder wählen Sie Neuer Trust Store aus.
      - Wenn Sie Neuer Vertrauensspeicher ausgewählt haben, geben Sie einen Namen für den Vertrauensspeicher, den Speicherort der S3-URI-Zertifizierungsstelle und optional einen Speicherort für die Sperrliste für S3-URI-Zertifikate an.
    - (Optional) Wählen Sie aus, ob Sie Advertise TrustStore CA Subject Names aktivieren möchten.
11. Wählen Sie Hinzufügen aus.
12. Informationen zum Hinzufügen von Zertifikaten zur Liste der optionalen Zertifikate finden Sie unterHinzufügen von Zertifikaten zu einer Zertifikatliste.

Um einen HTTPS-Listener hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-listener, um den Listener und die Standardregel zu erstellen, und den Befehl create-rule, um zusätzliche Listener-Regeln zu definieren.

Listener-Regeln für Ihren Application Load Balancer

Die Regeln, die Sie für Ihren Listener definieren, bestimmen, wie der Load Balancer Anforderungen an die Ziele in einer oder mehreren Zielgruppen weiterleitet.

Jede Rolle besteht aus einer Priorität, mindestens einer Aktion und mindestens einer Bedingung. Weitere Informationen finden Sie unter Listener-Regeln.

Voraussetzungen

- Jede Regel muss genau eine der folgenden Aktionen enthalten: `forward`, `redirect` oder `fixed-response`. Außerdem muss es die letzte auszuführende Regel sein.
- Jede Rolle kann keine oder eine der folgenden Bedingungen enthalten: `host-header`, `http-request-method`, `path-pattern` und `source-ip` sowie keine oder mehrere der folgenden Bedingungen; `http-header` und `query-string`.
- Sie können bis zu drei Vergleichszeichenfolgen pro Bedingung und bis zu fünf pro Regel angeben.
- Eine `forward`-Aktion leitet Anforderungen an ihre Zielgruppe weiter. Bevor Sie eine `forward`-Aktion hinzufügen, erstellen Sie ihre Zielgruppe und fügen Sie Ziele hinzu. Weitere Informationen finden Sie unter Erstellen Sie eine Zielgruppe für Ihren Application Load Balancer.

Hinzufügen einer Regel

Sie definieren eine Standardregel, wenn Sie einen Listener erstellen, und Sie können jederzeit zusätzliche nicht standardmäßige Regeln definieren.

Hinzufügen einer Regel mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus, um die dazugehörigen Details anzuzeigen.
4. Führen Sie auf der Registerkarte Listener und Regeln einen der folgenden Schritte durch:

   a. Wählen Sie den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.

      Wählen Sie auf der Registerkarte Regeln die Option Regel hinzufügen aus.

   b. Wählen Sie den Listener aus, dem Sie eine Regel hinzufügen möchten.

      Wählen Sie Regeln verwalten und dann Regel hinzufügen aus.
5. Sie können unter Name und Tags einen Namen für Ihre Regel angeben, obwohl dies nicht erforderlich ist.

   Um zusätzliche Tags hinzuzufügen, wählen Sie Hinzufügen zusätzlicher Tags aus.
6. Wählen Sie Weiter aus.

7. Klicken Sie auf Bedingung hinzufügen.
8. Fügen Sie mindestens eine der folgenden Bedingungen hinzu:

   - Host-Header – Definieren Sie den Host-Header. Beispiel: `*.example.com`. Wählen Sie Bestätigen aus, um die Bedingung zu speichern.

     Maximal 128 Zeichen. Die Groß- und Kleinschreibung muss nicht berücksichtigt werden. Zulässige Zeichen sind a-z, A-Z, 0-9; die folgenden Sonderzeichen: -_.; und Platzhalter (* und ?). Sie müssen mindestens ein "."-Zeichen einschließen. Es können nur alphabethische Zeichen nach dem letzten "."-Zeichen angegeben werden.
   - Pfad – Definieren Sie den Pfad. Beispiel: `/item/*` . Wählen Sie Bestätigen aus, um die Bedingung zu speichern.

     Maximal 128 Zeichen. Groß-/Kleinschreibung ist zu beachten. Zulässige Zeichen sind a-z, A-Z, 0-9; die folgenden Sonderzeichen: _-.$/~"'@:+; &; und Platzhalter (* und ?).
   - HTTP-Anforderungsmethode – Definieren Sie die HTTP-Anforderungsmethode. Wählen Sie Bestätigen aus, um die Bedingung zu speichern.

     Maximal 40 Zeichen. Groß-/Kleinschreibung ist zu beachten. Zulässige Zeichen sind A-Z und die folgenden Sonderzeichen: -_. Platzhalter werden nicht unterstützt.
   - Quell-IP – Definieren Sie die Quell-IP-Adresse im CIDR-Format. Wählen Sie Bestätigen aus, um die Bedingung zu speichern.

     Beides IPv4 und IPv6 CIDRs sind erlaubt. Platzhalter werden nicht unterstützt.
   - HTTP-Header – Geben Sie den Namen des Headers ein und fügen Sie mindestens eine Vergleichszeichenfolge ein. Wählen Sie Bestätigen aus, um die Bedingung zu speichern.
     - HTTP-Header-Name – Die Regel bewertet Anforderungen, die diesen Header enthalten, um zu bestätigen, dass die Werte übereinstimmen.

       Maximal 40 Zeichen. Die Groß- und Kleinschreibung muss nicht berücksichtigt werden. Zulässige Zeichen sind a-z, A-Z, 0-9 und die folgenden Sonderzeichen: *?-!#$%&'+.^_`|~. Platzhalter werden nicht unterstützt.
     - HTTP-Header-Wert – Geben Sie Zeichenfolgen ein, die mit dem HTTP-Header-Wert verglichen werden sollen.

Maximal 128 Zeichen. Die Groß- und Kleinschreibung muss nicht berücksichtigt werden. Zulässige Zeichen sind a-z, A-Z, 0-9; Leerzeichen; die folgenden Sonderzeichen:!“ #$%&' () +,. /:; <=>@ [] ^_` {|} ~-; und Platzhalter (* und?).

- Abfragezeichenfolge – Sie können Anforderungen basierend auf Schlüssel/Wert-Paaren oder Werten in den Abfragezeichenfolgen weiterleiten. Wählen Sie Bestätigen aus, um die Bedingung zu speichern.

  Maximal 128 Zeichen. Die Groß- und Kleinschreibung muss nicht berücksichtigt werden. Zulässige Zeichen sind a-z, A-Z, 0-9; die folgenden Sonderzeichen: _-.$/~'"@:+&()!,;=; und Platzhalter (* und ?).

9. Wählen Sie Weiter aus.
10. Definieren Sie eine der folgenden Aktionen für Ihre Regel:

    - Zu Zielgruppen weiterleiten – Wählen Sie eine oder mehrere Zielgruppen aus, an die der Datenverkehr weitergeleitet werden soll. Um Zielgruppen hinzuzufügen, wählen Sie Zielgruppe hinzufügen aus. Wenn Sie mehr als eine Zielgruppe verwenden, wählen Sie für jede Zielgruppe eine Gewichtung aus und überprüfen Sie den zugehörigen Prozentsatz. Sie müssen die Stickiness auf Gruppenebene für eine Regel aktivieren, wenn Sie die Stickiness für eine oder mehrere Zielgruppen aktiviert haben.
    - Umleitung zu URL – Geben Sie die URL an, an die Client-Anforderungen umgeleitet werden. Das ist möglich, indem Sie jeden Teil einzeln auf der Registerkarte URI-Teile eingeben oder indem Sie die vollständige Adresse auf der Registerkarte Vollständige URL eingeben. Für Statuscode können Sie Weiterleitungen je nach Bedarf entweder als temporär (HTTP 302) oder permanent (HTTP 301) konfigurieren.
    - Feststehende Antwort zurückgeben – Geben Sie den Antwortcode an, der bei verworfenen Client-Anforderungen zurückgegeben wird. Darüber hinaus können Sie den Inhaltstyp und den Antworttext angeben. Diese sind jedoch nicht erforderlich.

11. Wählen Sie Weiter aus.
12. Geben Sie die Priorität Ihrer Regel an, indem Sie einen Wert zwischen 1 und 50000 eingeben.
13. Wählen Sie Weiter aus.
14. Überprüfen Sie alle Details und Einstellungen, die derzeit für Ihre neue Regel konfiguriert sind. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Erstellen aus.

Um eine Regel hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-rule zum Erstellen der Regel. Verwenden Sie den Befehl describe-rules, um Informationen zur Regel anzuzeigen.

Bearbeiten einer Regel

Sie können die Aktion und Bedingungen für eine Regel jederzeit bearbeiten. Regelaktualisierungen werden nicht sofort wirksam, so dass Anforderungen nach dem Aktualisieren einer Regel für kurze Zeit mit der vorherigen Regelkonfiguration weitergeleitet werden können. Alle in der Übertragung befindlichen Anforderungen sind abgeschlossen.

Bearbeiten einer Regel mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Führen Sie auf der Registerkarte Listener und Regeln einen der folgenden Schritte durch:
   - Wählen Sie den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.
     i. Wählen Sie auf der Registerkarte Regeln im Abschnitt Listener-Regeln den Text in der Spalte Namens-Tag für die Regel aus, die Sie bearbeiten möchten.

        Wählen Sie Aktionen und dann Regel bearbeiten aus.
     ii. Wählen Sie auf der Registerkarte Regeln im Abschnitt Listener-Regeln die Regel aus, die Sie bearbeiten möchten.

        Wählen Sie Aktionen und dann Regel bearbeiten aus.
5. Ändern Sie den Namen und die Tags nach Bedarf. Um zusätzliche Tags hinzuzufügen, wählen Sie Hinzufügen zusätzlicher Tags aus.
6. Wählen Sie Weiter
7. Ändern Sie die Bedingungen nach Bedarf. Sie können Bedingungen hinzufügen, bestehende bearbeiten oder löschen.
8. Wählen Sie Weiter
9. Ändern Sie die Aktionen nach Bedarf.
10. Wählen Sie Weiter

11. Ändern Sie die Regelpriorität nach Bedarf. Sie können einen Wert zwischen 1 und 50000 eingeben.
12. Wählen Sie Weiter
13. Überprüfen Sie alle Details und aktualisierten Einstellungen, die für Ihre Regel konfiguriert wurden. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Änderungen speichern.

Um eine Regel mit dem zu bearbeiten AWS CLI

Verwenden Sie den Befehl modify-rule.

Aktualisieren der Regelpriorität

Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet. Sie können die Priorität einer nicht standardmäßigen Regel jederzeit ändern. Sie können die Priorität der Standardregel nicht ändern.

Um die Regelpriorität mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Führen Sie auf der Registerkarte Listener und Regeln einen der folgenden Schritte durch:

   a. Wählen Sie den Text in den Spalten Protokoll: Port oder Regeln aus, um die Detailseite für den Listener zu öffnen.

      i. Wählen Sie Aktionen und anschließend Regeln neu priorisieren aus.

      ii. Wählen Sie auf der Registerkarte Regeln im Abschnitt Listener-Regeln die Option Aktionen und dann Regeln neu priorisieren aus.

   b. Wählen Sie den Listener aus.

      - Wählen Sie Regeln verwalten und dann Regeln neu priorisieren aus.

5. Im Bereich Listener-Regeln wird in der Spalte Priorität die aktuelle Regelpriorität angezeigt. Sie können die Priorität einer Regel aktualisieren, indem Sie einen Wert zwischen 1 und 50000 eingeben.
6. Wenn Sie mit Ihren Änderungen zufrieden sind, klicken Sie auf Änderungen speichern.

Um die Regelprioritäten zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den set-rule-priorities-Befehl.

Löschen einer Regel

Sie können die nicht standardmäßigen Regeln für einen Listener jederzeit ändern. Sie können die Standardregel für einen Listener nicht löschen. Wen Sie einen Listener löschen, werden all seine Regeln gelöscht.

Löschen einer Regel mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Führen Sie auf der Registerkarte Listener und Regeln einen der folgenden Schritte durch:

    a. Wählen Sie den Text in den Spalten Protokoll: Port oder Regeln aus, um die Detailseite für den Listener zu öffnen.

        i. Wählen Sie die Regel aus, die Sie löschen möchten.
        ii. Wählen Sie Aktionen und dann Regel löschen aus.
        iii. Geben Sie `confirm` in das Texteingabefeld ein und wählen Sie dann Löschen aus.

    b. Wählen Sie den Text in der Spalte Namens-Tag aus, um die Detailseite für die Regel zu öffnen.

        i. Wählen Sie Aktionen und dann Regel löschen aus.
        ii. Geben Sie `confirm` in das Texteingabefeld ein und wählen Sie dann Löschen aus.

Um eine Regel mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-rule.

Aktualisieren eines HTTPS-Listeners für Ihren Application Load Balancer

Nach der Erstellung eines HTTPS-Listeners können Sie das Standardzertifikat ersetzen, die Zertifikatliste aktualisieren oder die Sicherheitsrichtlinie ersetzen.

Aufgaben

- Ersetzen des Standardzertifikats
- Hinzufügen von Zertifikaten zu einer Zertifikatliste
- Entfernen eines Zertifikats aus der Zertifikatliste
- Aktualisieren der Sicherheitsrichtlinie
- Änderung des HTTP-Headers

Ersetzen des Standardzertifikats

Sie können das Standardzertifikat für den Listener mit den folgenden Schritten ersetzen. Weitere Informationen finden Sie unter SSL-Zertifikate für Ihren Application Load Balancer.

So ersetzen Sie das Standardzertifikat mit der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.
5. Wählen Sie auf der Registerkarte Zertifikate die Option Standard ändern aus.
6. Wählen Sie in der Tabelle ACM- und IAM-Zertifikate ein neues Standardzertifikat aus.
7. Wählen Sie Als Standard speichern aus.

Um das Standardzertifikat mit dem zu ersetzen AWS CLI

Verwenden Sie den Befehl modify-listener.

Hinzufügen von Zertifikaten zu einer Zertifikatliste

Sie können der Zertifikatliste für den Listener mit den folgenden Schritten Zertifikate hinzufügen. Wenn Sie den Listener mit dem erstellt haben AWS Management Console, haben wir das Standardzertifikat für Sie zur Zertifikatsliste hinzugefügt. Andernfalls ist die Zertifikatsliste leer. Durch das Hinzufügen des Standardzertifikats zur Zertifikatsliste wird sichergestellt, dass dieses Zertifikat mit dem SNI-Protokoll verwendet wird, auch wenn es als Standardzertifikat ersetzt wird. Weitere Informationen finden Sie unter SSL-Zertifikate für Ihren Application Load Balancer.

So entfernen Sie die Zertifikatliste über die Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.
5. Wählen Sie auf der Registerkarte Zertifikate die Option Zertifikat hinzufügen aus.
6. Um Zertifikate hinzuzufügen, die bereits von ACM oder IAM verwaltet werden, aktivieren Sie die Kontrollkästchen für die Zertifikate und wählen Sie dann unten Als ausstehend einschließen aus.
7. Wenn Sie über ein Zertifikat verfügen, das nicht von ACM oder IAM verwaltet wird, wählen Sie Zertifikat importieren, füllen Sie das Formular aus und wählen Sie Importieren aus.
8. Wählen Sie Ausstehende Zertifikate hinzufügen aus.

Um der Zertifikatsliste ein Zertifikat hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den add-listener-certificates-Befehl.

Entfernen eines Zertifikats aus der Zertifikatliste

Sie können mit den folgenden Schritten Zertifikate aus der Zertifikatsliste für einen HTTPS-Listener entfernen. Nachdem Sie ein Zertifikat entfernt haben, kann der Listener mit diesem Zertifikat keine Verbindungen mehr herstellen. Um sicherzustellen, dass Clients nicht beeinträchtigt werden, fügen Sie der Liste ein neues Zertifikat hinzu und vergewissern Sie sich, dass die Verbindungen funktionieren, bevor Sie ein Zertifikat aus der Liste entfernen.

Informationen zum Entfernen des Standardzertifikats für einen TLS-Listener finden Sie unter Ersetzen des Standardzertifikats.

So entfernen Sie Zertifikate über die Konsole aus der Zertifikatliste

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.

5. Aktivieren Sie auf der Registerkarte Zertifikate die Kontrollkästchen für die Zertifikate und wählen Sie Entfernen aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Entfernen.

Um ein Zertifikat aus der Zertifikatsliste zu entfernen, verwenden Sie AWS CLI

Verwenden Sie den remove-listener-certificates-Befehl.

Aktualisieren der Sicherheitsrichtlinie

Wenn Sie einen HTTPS-Listener erstellen, können Sie die Sicherheitsrichtlinie auswählen, die Ihre Anforderungen erfüllt. Wenn eine neue Sicherheitsrichtlinie hinzugefügt wird, können Sie Ihren HTTPS-Listener aktualisieren, sodass die neue Sicherheitsrichtlinie verwendet wird. Application Load Balancer unterstützen keine benutzerdefinierten Sicherheitsrichtlinien. Weitere Informationen finden Sie unter Sicherheitsrichtlinien für Ihren Application Load Balancer.

Die Aktualisierung der Sicherheitsrichtlinie kann zu Störungen führen, wenn der Load Balancer ein hohes Datenvolumen verarbeitet. Um die Wahrscheinlichkeit von Störungen zu verringern, wenn Ihr Load Balancer ein hohes Datenverkehrsvolumen verarbeitet, richten Sie einen zusätzlichen Load Balancer ein, der Sie bei der Bewältigung des Datenverkehrs unterstützt, oder fordern Sie eine LCU-Reservierung an.

Verwenden von FIPS-Richtlinien auf Ihrem Application Load Balancer

Alle sicheren Listener, die an einen Application Load Balancer angeschlossen sind, müssen entweder FIPS-Sicherheitsrichtlinien oder Nicht-FIPS-Sicherheitsrichtlinien verwenden; sie können nicht gemischt werden. Wenn ein vorhandener Application Load Balancer über zwei oder mehr Listener verfügt, die Nicht-FIPS-Richtlinien verwenden, und Sie möchten, dass die Listener stattdessen FIPS-Sicherheitsrichtlinien verwenden, entfernen Sie alle Listener, bis nur noch einer vorhanden ist. Ändern Sie die Sicherheitsrichtlinie des Listeners in FIPS und erstellen Sie dann weitere Listener mithilfe von FIPS-Sicherheitsrichtlinien. Alternativ können Sie einen neuen Application Load Balancer mit neuen Listenern erstellen, die nur FIPS-Sicherheitsrichtlinien verwenden.

Aktualisieren der Sicherheitsrichtlinie mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.

3. Wählen Sie den Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.
5. Wählen Sie dann auf der Seite Details zuerst Aktionen und dann Listener bearbeiten aus.
6. Wählen Sie im Abschnitt Secure Listener Settings unter Sicherheitsrichtlinie eine neue Sicherheitsrichtlinie aus.
7. Wählen Sie Änderungen speichern aus.

Um die Sicherheitsrichtlinie zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl modify-listener.

Änderung des HTTP-Headers

Durch die Änderung des HTTP-Headers können Sie bestimmte vom Load Balancer generierte Header umbenennen, bestimmte Antwortheader einfügen und den Serverantwortheader deaktivieren. Application Load Balancers unterstützen die Header-Änderung sowohl für Anforderungs- als auch für Antwortheader.

Weitere Informationen finden Sie unter Aktivieren Sie die HTTP-Header-Änderung für Ihren Application Load Balancer.

Gegenseitige Authentifizierung mit TLS im Application Load Balancer

Die gegenseitige TLS-Authentifizierung ist eine Variante von Transport Layer Security (TLS). Herkömmliches TLS ermöglicht eine sichere Kommunikation zwischen einem Server und einem Client, wobei der Server seinen Clients seine Identität mitteilen muss. Bei Mutual TLS handelt ein Load Balancer bei der Aushandlung von TLS die gegenseitige Authentifizierung zwischen dem Client und dem Server aus. Wenn Sie Mutual TLS mit Application Load Balancer verwenden, vereinfachen Sie das Authentifizierungsmanagement und reduzieren die Belastung Ihrer Anwendungen.

Durch die Verwendung von Mutual TLS mit Application Load Balancer kann Ihr Load Balancer die Client-Authentifizierung verwalten, um sicherzustellen, dass nur vertrauenswürdige Clients mit Ihren Backend-Anwendungen kommunizieren. Wenn Sie diese Funktion verwenden, authentifiziert Application Load Balancer Clients mit Zertifikaten von einer Zertifizierungsstelle (CA) eines

Drittanbieters oder mithilfe der AWS Private Certificate Authority (PCA), optional, mit Sperrprüfungen. Application Load Balancer leitet Client-Zertifikatsinformationen an das Backend weiter, die Ihre Anwendungen für die Autorisierung verwenden können. Durch die Verwendung von Mutual TLS in Application Load Balancer erhalten Sie eine integrierte, skalierbare, verwaltete Authentifizierung für zertifikatsbasierte Entitäten, die etablierte Bibliotheken verwendet.

Mutual TLS for Application Load Balancers bietet die folgenden zwei Optionen für die Validierung Ihrer X.509v3-Client-Zertifikate:

Hinweis: X.509v1-Clientzertifikate werden nicht unterstützt.

- Gegenseitiger TLS-Passthrough: Wenn Sie den Mutual TLS-Passthrough-Modus verwenden, sendet Application Load Balancer die gesamte Client-Zertifikatskette mithilfe von HTTP-Headern an das Ziel. Mithilfe der Client-Zertifikatskette können Sie dann die entsprechende Load Balancer-Authentifizierung und Zielautorisierungslogik in Ihrer Anwendung implementieren.
- Gegenseitige TLS-Überprüfung: Wenn Sie den Modus für die gegenseitige TLS-Überprüfung verwenden, führt Application Load Balancer die X.509-Client-Zertifikatsauthentifizierung für Clients durch, wenn ein Load Balancer TLS-Verbindungen aushandelt.

Um mit Mutual TLS in Application Load Balancer mithilfe von Passthrough zu beginnen, müssen Sie den Listener nur so konfigurieren, dass er Zertifikate von Clients akzeptiert. Um Mutual TLS mit Verifizierung zu verwenden, müssen Sie wie folgt vorgehen:

- Erstellen Sie eine neue Trust Store-Ressource.
- Laden Sie Ihr Zertifizierungsstellenpaket (CA) und optional Sperrlisten hoch.
- Hängen Sie den Trust Store an den Listener an, der für die Überprüfung von Client-Zertifikaten konfiguriert ist.

step-by-stepVerfahren zur Konfiguration des Modus für die gegenseitige TLS-Überprüfung mit Ihrem Application Load Balancer finden Sie unterKonfiguration von Mutual TLS auf einem Application Load Balancer.

Bevor Sie mit der Konfiguration von Mutual TLS auf Ihrem Application Load Balancer beginnen

Bevor Sie mit der Konfiguration von Mutual TLS auf Ihrem Application Load Balancer beginnen, sollten Sie Folgendes beachten:

Kontingente

Application Load Balancers enthalten bestimmte Beschränkungen, die sich auf die Anzahl der in Ihrem AWS Konto verwendeten Trust Stores, CA-Zertifikate und Zertifikatssperrlisten beziehen.

Weitere Informationen finden Sie unter Kontingente für Ihre Application Load Balancers.

Anforderungen für Zertifikate

Application Load Balancers unterstützen Folgendes für Zertifikate, die mit gegenseitiger TLS-Authentifizierung verwendet werden:

- Unterstütztes Zertifikat: X.509v3
- Unterstützte öffentliche Schlüssel: RSA 2K — 8K oder ECDSA secp256r1, secp384r1, secp521r1
- Unterstützte SHA256 Signaturalgorithmen:, 384, RSA/SHA256, 384, 512 with EC/SHA 512 mit 256.384.512 Hash mit RSASSA-PSS mit MGF1

CA-Zertifikatspakete

Folgendes gilt für Zertifizierungsstellen-Pakete (CA):

- Application Load Balancers laden jedes Zertifikatspaket der Zertifizierungsstelle (CA) als Batch hoch. Application Load Balancers unterstützen das Hochladen einzelner Zertifikate nicht. Wenn Sie neue Zertifikate hinzufügen müssen, müssen Sie die Zertifikatspaketdatei hochladen.
- Verwenden Sie die ModifyTrustStoreAPI, um ein CA-Zertifikatspaket zu ersetzen.

Reihenfolge der Zertifikate für Passthrough

Wenn Sie den gegenseitigen TLS-Passthrough verwenden, fügt der Application Load Balancer Header ein, um den Backend-Zielen die Zertifikatskette des Clients zu präsentieren. Die Reihenfolge der Präsentation beginnt mit den Leaf-Zertifikaten und endet mit dem Stammzertifikat.

Wiederaufnahme der Sitzung

Die Sitzungswiederaufnahme wird nicht unterstützt, wenn der Modus Mutual TLS Passthrough oder Verify mit einem Application Load Balancer verwendet wird.

HTTP-Header

Application Load Balancer verwenden `X-Amzn-Mtls` Header, um Zertifikatsinformationen zu senden, wenn es Clientverbindungen mit gegenseitigem TLS aushandelt. Weitere Informationen und Beispiel-Header finden Sie unter. HTTP-Header und gegenseitiges TLS

CA-Zertifikatsdateien

CA-Zertifikatsdateien müssen die folgenden Anforderungen erfüllen:

- Die Zertifikatsdatei muss das PEM-Format (Privacy Enhanced Mail) verwenden.
- Der Inhalt des Zertifikats muss innerhalb der `-----END CERTIFICATE-----` Grenzen `-----BEGIN CERTIFICATE-----` und liegen.
- Den Kommentaren muss ein # Zeichen vorangestellt werden und sie dürfen keine - Zeichen enthalten.
- Es dürfen keine Leerzeilen vorhanden sein.

Beispielzertifikat, das nicht akzeptiert wird (ungültig):

```
# comments

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 01
    Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=US, O=EXAMPLE, OU=EXAMPLE, CN=EXAMPLE
        Validity
            Not Before: Jan 11 23:57:57 2024 GMT
            Not After : Jan 10 00:57:57 2029 GMT
        Subject: C=US, O=EXAMPLE, OU=EXAMPLE, CN=EXAMPLE
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    00:01:02:03:04:05:06:07:08
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                00:01:02:03:04:05:06:07:08
            X509v3 Subject Alternative Name:
                URI:EXAMPLE.COM
    Signature Algorithm: ecdsa-with-SHA384
         00:01:02:03:04:05:06:07:08
```

```
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Beispielzertifikate, die akzeptiert werden (gültig):

1. Einzelzertifikat (PEM-kodiert):

```
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

2. Mehrere Zertifikate (PEM-kodiert):

```
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

HTTP-Header und gegenseitiges TLS

In diesem Abschnitt werden die HTTP-Header beschrieben, die Application Load Balancers verwenden, um Zertifikatsinformationen zu senden, wenn Verbindungen mit Clients, die gegenseitiges TLS verwenden, aushandeln. Die spezifischen `X-Amzn-Mtls` Header, die der Application Load Balancer verwendet, hängen vom von Ihnen angegebenen gegenseitigen TLS-Modus ab: Passthrough-Modus oder Verifizierungsmodus.

Hinweise zu anderen HTTP-Headern, die von Application Load Balancers unterstützt werden, finden Sie unter. HTTP-Header und Application Load Balancer

HTTP-Header für den Passthrough-Modus

Für Mutual TLS im Passthrough-Modus verwenden Application Load Balancer den folgenden Header.

X-Amzn-Mtls-Clientcert

Dieser Header enthält das URL-kodierte PEM-Format der gesamten Client-Zertifikatskette, die in der Verbindung dargestellt wird, mit sicheren Zeichen. `+=/`

Inhalt eines Beispiel-Headers:

```
X-Amzn-Mtls-Clientcert: -----BEGIN%20CERTIFICATE-----%0AMIID<...reduced...>do0g
%3D%3D%0A-----END%20CERTIFICATE-----%0A-----BEGIN%20CERTIFICATE-----
%0AMIID1<...reduced...>3eZlyKA%3D%3D%0A-----END%20CERTIFICATE-----%0A
```

HTTP-Header für den Überprüfungsmodus

Für gegenseitiges TLS im Überprüfungsmodus verwenden Application Load Balancer die folgenden Header.

X-Amzn-Mtls-Clientcert-Seriennummer

Dieser Header enthält eine hexadezimale Darstellung der Seriennummer des Leaf-Zertifikats.

Beispiel für den Inhalt der Kopfzeile:

```
X-Amzn-Mtls-Clientcert-Serial-Number: 03A5B1
```

X-Amzn-Mtls-Clientcert-Issuer

Dieser Header enthält eine RFC2253 Zeichenkettendarstellung des definierten Namens (DN) des Emittenten.

Beispiel für den Inhalt der Kopfzeile:

```
X-Amzn-Mtls-Clientcert-Issuer:
 CN=rootcamtls.com,OU=rootCA,O=mTLS,L=Seattle,ST=Washington,C=US
```

X-Amzn-Mtls-Clientcert-Betreff

Dieser Header enthält eine RFC2253 Zeichenkettendarstellung des definierten Namens (DN) des Betreffs.

Beispiel für den Inhalt einer Kopfzeile:

```
X-Amzn-Mtls-Clientcert-Subject: CN=client_.com,OU=client-3,O=mTLS,ST=Washington,C=US
```

X-Amzn-Mtls-Clientcert-Validität

Dieser Header enthält das Und-Datum im Format 01. ISO86 `notBefore` `notAfter`

Beispiel für den Inhalt einer Kopfzeile:

```
X-Amzn-Mtls-Clientcert-Validity:
 NotBefore=2023-09-21T01:50:17Z;NotAfter=2024-09-20T01:50:17Z
```

X-Amzn-Mtls-Clientcert-Leaf

Dieser Header enthält ein URL-codiertes PEM-Format des Leaf-Zertifikats mit sicheren Zeichen. `+=/`

Beispiel für den Inhalt einer Kopfzeile:

```
X-Amzn-Mtls-Clientcert-Leaf: -----BEGIN%20CERTIFICATE-----%0AMIIG<...reduced...>NmrUlw
%0A-----END%20CERTIFICATE-----%0A
```

Geben Sie den Betreffnamen der Zertifizierungsstelle (CA) bekannt

Die Betreffnamen der Advertising Certificate Authority (CA) verbessern den Authentifizierungsprozess, indem sie Kunden dabei helfen, zu bestimmen, welche Zertifikate bei der gegenseitigen TLS-Authentifizierung akzeptiert werden.

Wenn Sie die Option Betreffnamen von Zertifizierungsstellen ankündigen aktivieren, kündigt der Application Load Balancer die Liste der Zertifizierungsstellen (CAs), denen er vertraut, basierend auf dem Vertrauensspeicher, dem er zugeordnet ist, an. Wenn ein Client über den Application Load Balancer eine Verbindung zu einem Ziel herstellt, erhält der Client die Liste der vertrauenswürdigen CA-Betreffnamen.

Wenn der Application Load Balancer während des TLS-Handshakes ein Client-Zertifikat anfordert, nimmt er eine Liste vertrauenswürdiger CA Distinguished Names (DNs) in seine Zertifikatsanforderungsnachricht auf. Dies hilft den Clients bei der Auswahl gültiger Zertifikate, die mit den angekündigten CA-Betreffnamen übereinstimmen, wodurch der Authentifizierungsprozess optimiert und Verbindungsfehler reduziert werden.

Sie können den Betreffnamen der Zertifizierungsstelle für neue und bestehende Listener ankündigen aktivieren. Weitere Informationen finden Sie unter Hinzufügen eines HTTPS-Listeners.

Verbindungsprotokolle für Application Load Balancer

Elastic Load Balancing stellt Verbindungsprotokolle bereit, die Attribute der Anfragen erfassen, die an Ihre Application Load Balancer gesendet wurden. Verbindungsprotokolle enthalten Informationen wie die Client-IP-Adresse und den Port, Informationen zum Client-Zertifikat, die Verbindungsergebnisse und die verwendeten TLS-Chiffren. Diese Verbindungsprotokolle können dann verwendet werden, um Anforderungsmuster und andere Trends zu überprüfen.

Weitere Informationen zu Verbindungsprotokollen finden Sie unter Verbindungsprotokolle für Ihren Application Load Balancer

Konfiguration von Mutual TLS auf einem Application Load Balancer

Dieser Abschnitt enthält die Verfahren zur Konfiguration des gegenseitigen TLS-Überprüfungsmodus für die Authentifizierung auf Application Load Balancers.

Um den Mutual TLS-Passthrough-Modus zu verwenden, müssen Sie den Listener nur so konfigurieren, dass er Zertifikate von Clients akzeptiert. Wenn Sie gegenseitiges TLS-Passthrough verwenden, sendet der Application Load Balancer die gesamte Client-Zertifikatskette mithilfe von HTTP-Headern an das Ziel, sodass Sie die entsprechende Authentifizierungs- und Autorisierungslogik in Ihrer Anwendung implementieren können. Weitere Informationen finden Sie unter Einen HTTPS-Listener für Ihren Application Load Balancer erstellen.

Wenn Sie Mutual TLS im Überprüfungsmodus verwenden, führt der Application Load Balancer eine X.509-Client-Zertifikatsauthentifizierung für Clients durch, wenn ein Load Balancer TLS-Verbindungen aushandelt.

Gehen Sie wie folgt vor, um den Modus für die gegenseitige TLS-Überprüfung zu verwenden:

- Erstellen Sie eine neue Trust Store-Ressource.
- Laden Sie Ihr Zertifizierungsstellenpaket (CA) und optional Sperrlisten hoch.
- Hängen Sie den Trust Store an den Listener an, der für die Überprüfung von Client-Zertifikaten konfiguriert ist.

Folgen Sie den Verfahren in diesem Abschnitt, um den Modus für die gegenseitige TLS-Überprüfung auf Ihrem Application Load Balancer in der AWS Management Console zu konfigurieren. Informationen zur Konfiguration von Mutual TLS mithilfe von API-Vorgängen anstelle der Konsole finden Sie im Application Load Balancer API-Referenzhandbuch.

Aufgaben

- Erstellen Sie einen Trust Store
- Ordnen Sie einen Trust Store zu
- Details zum Trust Store anzeigen
- Ändern Sie einen Trust Store
- Löschen Sie einen Trust Store

Erstellen Sie einen Trust Store

Es gibt drei Möglichkeiten, einen Trust Store zu erstellen: wenn Sie einen Application Load Balancer erstellen, wenn Sie einen sicheren Listener erstellen und indem Sie die Trust Store-Konsole verwenden. Wenn Sie beim Erstellen eines Load Balancers oder Listeners einen Trust Store hinzufügen, wird der Trust Store automatisch dem neuen Listener zugeordnet. Wenn Sie mithilfe der Trust Store-Konsole einen Trust Store erstellen, müssen Sie ihn selbst einem Listener zuordnen.

In diesem Abschnitt wird das Erstellen eines Trust Stores mithilfe der Trust Store-Konsole behandelt. Die Schritte beim Erstellen eines Application Load Balancer oder Listeners sind jedoch dieselben. Weitere Informationen finden Sie unter Konfiguration eines Load Balancers und eines Listeners und Erstellen eines HTTPS-Listeners.

Voraussetzungen:

- Um einen Trust Store zu erstellen, benötigen Sie ein Zertifikatspaket von Ihrer Zertifizierungsstelle (CA).

Um einen Trust Store mit der Konsole zu erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie Trust Store erstellen aus.
4. Konfiguration des Vertrauensspeichers
   a. Geben Sie unter Name des Vertrauensspeichers einen Namen für Ihren Vertrauensspeicher ein.
   b. Geben Sie für Certificate Authority Bundle den Amazon S3 S3-Pfad zu dem CA-Zertifikatspaket ein, das Ihr Trust Store verwenden soll.

Optional: Verwenden Sie die Objektversion, um eine frühere Version des CA-Zertifikatspakets auszuwählen. Andernfalls wird die aktuelle Version verwendet.

5. Für Widerrufe können Sie optional eine Zertifikatssperrliste zu Ihrem Trust Store hinzufügen.

   - Geben Sie unter Certificate Revocation List den Amazon S3 S3-Pfad zu der Zertifikatssperrliste ein, die Ihr Trust Store verwenden soll.

     Optional: Verwenden Sie Objektversion, um eine frühere Version der Zertifikatssperrliste auszuwählen. Andernfalls wird die aktuelle Version verwendet.

6. Für Trust Store-Tags können Sie optional bis zu 50 Tags eingeben, die auf Ihren Trust Store angewendet werden sollen.
7. Wählen Sie Trust Store erstellen aus.

Ordnen Sie einen Trust Store zu

Nachdem Sie einen Trust Store erstellt haben, müssen Sie ihn einem Listener zuordnen, bevor Ihr Application Load Balancer den Trust Store verwenden kann. Sie können jedem Ihrer sicheren Listener nur einen Trust Store zuordnen, aber ein Trust Store kann mehreren Listenern zugeordnet werden.

In diesem Abschnitt wird das Zuordnen eines Vertrauensspeichers zu einem vorhandenen Listener beschrieben. Alternativ können Sie beim Erstellen eines Application Load Balancer oder Listeners einen Trust Store zuordnen. Weitere Informationen finden Sie unter Konfiguration eines Load Balancers und eines Listeners und Erstellen eines HTTPS-Listeners.

So ordnen Sie mithilfe der Konsole einen Trust Store zu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus, um seine Detailseite aufzurufen.
4. Wählen Sie auf der Registerkarte Listener und Regeln den Link in der Spalte Protokoll:Port, um die Detailseite für den sicheren Listener zu öffnen.
5. Wählen Sie auf der Registerkarte Sicherheit die Option Einstellungen für sicheren Listener bearbeiten aus.
6. (Optional) Wenn Mutual TLS nicht aktiviert ist, wählen Sie Mutual Authentication (mTLS) unter Client Certificate Handling und dann Verify with Trust Store aus.

7. Wählen Sie unter Trust Store den Trust Store aus, den Sie erstellt haben.
8. Wählen Sie Änderungen speichern aus.

Details zum Trust Store anzeigen

CA-Zertifikatspakete

Das CA-Zertifikatspaket ist eine erforderliche Komponente des Trust Store. Es handelt sich um eine Sammlung vertrauenswürdiger Stamm- und Zwischenzertifikate, die von einer Zertifizierungsstelle validiert wurden. Diese validierten Zertifikate stellen sicher, dass der Client darauf vertrauen kann, dass das vorgelegte Zertifikat dem Load Balancer gehört.

Sie können den Inhalt des aktuellen CA-Zertifikatspakets jederzeit in Ihrem Trust Store einsehen.

Ein CA-Zertifikatspaket anzeigen

So zeigen Sie ein CA-Zertifikatspaket mit der Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie den Trust Store aus, um die Detailseite anzuzeigen.
4. Wählen Sie Actions und dann Get CA Bundle aus.
5. Wählen Sie Link teilen oder Herunterladen aus.

Listen zum Widerruf von Zertifikaten

Optional können Sie eine Zertifikatssperrliste für einen Vertrauensspeicher erstellen. Sperrlisten werden von Zertifizierungsstellen veröffentlicht und enthalten Daten für Zertifikate, die gesperrt wurden. Application Load Balancers unterstützen nur Zertifikatssperrlisten im PEM-Format.

Wenn eine Zertifikatssperrliste zu einem Vertrauensspeicher hinzugefügt wird, erhält sie eine Sperr-ID. Die Sperrung IDs erhöht sich für jede Sperrliste, die dem Trust Store hinzugefügt wird, und sie können nicht geändert werden. Wenn eine Zertifikatssperrliste aus einem Vertrauensspeicher gelöscht wird, wird auch ihre Sperr-ID gelöscht und für die gesamte Lebensdauer des Vertrauensspeichers nicht wiederverwendet.

> **Note**
>
> Application Load Balancers können in einer Zertifikatssperrliste keine Zertifikate mit einer negativen Seriennummer widerrufen.

Eine Zertifikatssperrliste anzeigen

So zeigen Sie eine Sperrliste mit der Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie den Trust Store aus, um die Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte Zertifikatsperrlisten die Optionen Aktionen und dann Sperrliste abrufen aus.
5. Wählen Sie Link teilen oder Herunterladen aus.

Ändern Sie einen Trust Store

Ein Trust Store kann jeweils nur ein CA-Zertifikatpaket enthalten, aber Sie können das CA-Zertifikatpaket jederzeit ersetzen, nachdem der Trust Store erstellt wurde.

Ersetzen Sie ein CA-Zertifikatspaket

Um ein CA-Zertifikatspaket mithilfe der Konsole zu ersetzen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie den Trust Store aus, um die Detailseite anzuzeigen.
4. Wählen Sie „Aktionen“ und dann „CA-Bundle ersetzen“.
5. Geben Sie auf der Seite CA-Bundle ersetzen unter Certificate Authority Bundle den Amazon S3 S3-Standort des gewünschten CA-Bundles ein.
6. (Optional) Verwenden Sie Objektversion, um eine frühere Version der Zertifikatssperrliste auszuwählen. Andernfalls wird die aktuelle Version verwendet.
7. Wählen Sie CA-Bundle ersetzen aus.

Fügen Sie eine Sperrliste für Zertifikate hinzu

Um mit der Konsole eine Sperrliste hinzuzufügen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie den Trust Store aus, um seine Detailseite aufzurufen.
4. Wählen Sie auf der Registerkarte Zertifikatsperrlisten die Option Aktionen und dann Sperrliste hinzufügen aus.
5. Geben Sie auf der Seite Sperrliste hinzufügen unter Zertifikatssperrliste den Amazon S3 S3-Speicherort der gewünschten Zertifikatssperrliste ein.
6. (Optional) Verwenden Sie Objektversion, um eine frühere Version der Zertifikatssperrliste auszuwählen. Andernfalls wird die aktuelle Version verwendet.
7. Wählen Sie Sperrliste hinzufügen

Löschen Sie eine Zertifikatssperrliste

Um eine Sperrliste mit der Konsole zu löschen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie den Trust Store aus, um die Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte Zertifikatsperrlisten die Optionen Aktionen und dann Sperrliste löschen aus.
5. Bestätigen Sie den Löschvorgang, indem Sie Folgendes eingeben`confirm`.
6. Wählen Sie Löschen aus.

Löschen Sie einen Trust Store

Wenn Sie einen Trust Store nicht mehr benötigen, können Sie ihn löschen.

Hinweis: Sie können keinen Trust Store löschen, der derzeit einem Listener zugeordnet ist.

Um einen Trust Store mit der Konsole zu löschen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Trust Stores aus.
3. Wählen Sie den Trust Store aus, um seine Detailseite aufzurufen.
4. Wählen Sie Aktionen und dann Trust Store löschen aus.
5. Bestätigen Sie den Löschvorgang, indem Sie Folgendes eingeben`confirm`.
6. Wählen Sie Löschen

Teilen Sie Ihren Elastic Load Balancing Trust Store für Application Load Balancers

Elastic Load Balancing ist in AWS Resource Access Manager (AWS RAM) integriert, um die gemeinsame Nutzung von Trust Stores zu ermöglichen. AWS RAM ist ein Service, mit dem Sie Ihre Elastic Load Balancing Trust Store-Ressourcen sicher innerhalb AWS-Konten und innerhalb Ihrer Organisation oder Organisationseinheiten teilen können (OUs). Wenn Sie mehrere Konten haben, können Sie einen Trust Store einmal erstellen und ihn dann für andere Konten nutzbar machen. AWS RAM Wenn Ihr Konto von verwaltet wird AWS Organizations, können Sie Trust Stores für alle Konten in der Organisation oder nur für Konten innerhalb bestimmter Organisationseinheiten (OUs) freigeben.

Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. In diesem Modell teilt sich derjenige AWS-Konto , dem der Trust Store gehört (Eigentümer), ihn mit anderen AWS-Konten (Verbrauchern). Verbraucher können Shared Trust Stores ihren Application Load Balancer Balancer-Listenern genauso zuordnen, wie sie Trust Stores in ihrem eigenen Konto zuordnen.

Ein Trust Store-Besitzer kann einen Trust Store teilen mit:

- AWS-Konten Spezifisch innerhalb oder außerhalb seiner Organisation in AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations
- Ihre gesamte Organisation ist in AWS Organizations

Inhalt

- Voraussetzungen für die gemeinsame Nutzung von Trust Stores
- Berechtigungen für gemeinsam genutzte Vertrauensspeicher
- Teilen Sie einen Trust Store

- Beenden Sie die gemeinsame Nutzung eines Trust Stores
- Fakturierung und Messung

Voraussetzungen für die gemeinsame Nutzung von Trust Stores

- Sie müssen eine Ressourcenfreigabe mit erstellen AWS Resource Access Manager. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Erstellen einer Ressourcenfreigabe.
- Um einen Trust Store gemeinsam zu nutzen, müssen Sie ihn in Ihrem besitzen AWS-Konto. Sie können einen Trust Store, der mit Ihnen geteilt wurde, nicht gemeinsam nutzen.
- Um einen Vertrauensspeicher mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzen AWS Organizations, müssen Sie das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

Berechtigungen für gemeinsam genutzte Vertrauensspeicher

Vertraue Ladenbesitzern

- Besitzer von Trust Stores können einen Trust Store einrichten.
- Trust Store-Besitzer können einen Trust Store mit Load Balancern im selben Konto verwenden.
- Inhaber eines Trust Stores können einen Trust Store mit anderen AWS Konten teilen oder AWS Organizations.
- Inhaber eines Trust Stores können die gemeinsame Nutzung eines Trust Stores für jedes AWS Konto aufheben oder AWS Organizations.
- Besitzer eines Trust Stores können nicht verhindern, dass Load Balancer einen Trust Store im selben Konto verwenden.
- Besitzer eines Trust Stores können alle Application Load Balancer auflisten, die einen gemeinsamen Vertrauensspeicher verwenden.
- Besitzer eines Trust Stores können einen Trust Store löschen, wenn keine aktuellen Verknüpfungen bestehen.
- Inhaber eines Trust Stores können Verknüpfungen mit einem gemeinsamen Trust Store löschen.
- Besitzer eines Vertrauensspeichers erhalten CloudTrail Protokolle, wenn ein gemeinsam genutzter Vertrauensspeicher verwendet wird.

Kunden von Trust-Stores

- Trust Store-Verbraucher können sich Shared Trust Stores ansehen.
- Trust Store-Verbraucher können Listener mithilfe eines Trust Stores in demselben Konto erstellen oder ändern.
- Trust-Store-Nutzer können Listener mithilfe eines gemeinsamen Vertrauensspeichers erstellen oder ändern.
- Trust-Store-Nutzer können keinen Listener mit einem Trust Store erstellen, der nicht mehr gemeinsam genutzt wird.
- Vertrauensspeicher-Nutzer können einen gemeinsamen Vertrauensspeicher nicht ändern.
- Trust Store-Verbraucher können einen gemeinsamen Trust Store-ARN anzeigen, wenn er einem Listener zugeordnet ist.
- Trust Store-Verbraucher erhalten CloudTrail Protokolle, wenn sie einen Listener mithilfe eines gemeinsamen Vertrauensspeichers erstellen oder ändern.

Verwaltete Berechtigungen

Bei der gemeinsamen Nutzung eines Trust Stores verwendet die Ressourcenfreigabe verwaltete Berechtigungen, um zu steuern, welche Aktionen vom Trust Store-Nutzer zugelassen werden. Sie können die standardmäßigen verwalteten Berechtigungen verwenden`AWSRAMPermissionElasticLoadBalancingTrustStore`, die alle verfügbaren Berechtigungen enthalten, oder Ihre eigenen vom Kunden verwalteten Berechtigungen erstellen. Die `DescribeTrustStoreAssociations` Berechtigungen `DescribeTrustStoresDescribeTrustStoreRevocations`, und sind immer aktiviert und können nicht entfernt werden.

Die folgenden Berechtigungen werden für Trust Store-Ressourcenfreigaben unterstützt:

elastischer Lastenausgleich: CreateListener

Kann einen gemeinsamen Vertrauensspeicher an einen neuen Listener anhängen.

elastischer Lastenausgleich: ModifyListener

Kann einen gemeinsamen Vertrauensspeicher an einen vorhandenen Listener anhängen.

elastischer Lastenausgleich: GetTrustStoreCaCertificatesBundle

Kann das CA-Zertifikatspaket herunterladen, das dem Shared Trust Store zugeordnet ist.

elastischer Lastenausgleich: GetTrustStoreRevocationContent

Kann die mit dem Shared Trust Store verknüpfte Sperrdatei herunterladen.

elasticloadbalancing: DescribeTrustStores (Standard)

Kann alle Trust Stores auflisten, die dem Konto gehören und mit diesem geteilt werden.

elasticloadbalancing: DescribeTrustStoreRevocations (Standard)

Kann den gesamten Sperrinhalt für den angegebenen Trust Store-ARN auflisten.

elasticloadbalancing: DescribeTrustStoreAssociations (Standard)

Kann alle Ressourcen im Trust Store-Verbraucherkonto auflisten, die dem gemeinsamen Vertrauensspeicher zugeordnet sind.

Teilen Sie einen Trust Store

Um einen Trust Store gemeinsam zu nutzen, müssen Sie ihn zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM -Ressource, mit der Sie Ihre Ressourcen in mehreren AWS-Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt an, welche Ressourcen gemeinsam genutzt werden sollen, mit welchen Verbrauchern sie gemeinsam genutzt werden und welche Aktionen Principals ausführen können. Wenn Sie einen Trust Store über die EC2 Amazon-Konsole teilen, fügen Sie ihn zu einer vorhandenen Ressourcenfreigabe hinzu. Um den Trust Store zu einer neuen Resource Share hinzuzufügen, müssen Sie zuerst die Resource Share mithilfe der AWS RAM Konsole erstellen.

Wenn Sie einen Trust Store, den Sie besitzen, mit anderen teilen AWS-Konten, ermöglichen Sie diesen Konten, ihre Application Load Balancer Balancer-Listener mit Trust Stores in Ihrem Konto zu verknüpfen.

Wenn Sie Teil einer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation automatisch Zugriff auf den gemeinsamen Vertrauensspeicher. Andernfalls erhalten Verbraucher eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf den Shared Trust Store.

Sie können einen Trust Store, den Sie besitzen, mit der EC2 Amazon-Konsole, der AWS RAM Konsole oder dem teilen AWS CLI.

Um einen Trust Store, den Sie besitzen, über die EC2 Amazon-Konsole zu teilen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Trust Stores aus.
3. Wählen Sie den Namen des Trust Stores aus, um die zugehörige Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte Teilen die Option Vertrauensspeicher teilen aus.
5. Wählen Sie auf der Seite Vertrauensspeicher teilen unter Ressourcenfreigaben aus, mit welchen Ressourcenfreigaben Ihr Vertrauensspeicher geteilt werden soll.
6. (Optional) Wenn Sie eine neue Ressourcenfreigabe erstellen müssen, wählen Sie den Link Ressourcenfreigabe in der RAM-Konsole erstellen aus.
7. Wählen Sie Vertrauensspeicher teilen aus.

Um einen Vertrauensspeicher, den Sie besitzen, mithilfe der AWS RAM Konsole zu teilen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um einen Vertrauensspeicher, den Sie besitzen, mit dem AWS CLI

Verwenden Sie den create-resource-share-Befehl.

Beenden Sie die gemeinsame Nutzung eines Trust Stores

Wenn Sie einen Vertrauensspeicher, den Sie besitzen, nicht mehr teilen möchten, müssen Sie ihn aus der Ressourcenfreigabe entfernen. Bestehende Verknüpfungen bleiben bestehen, nachdem Sie die gemeinsame Nutzung Ihres Vertrauensspeichers beendet haben. Neue Verknüpfungen zu einem zuvor gemeinsam genutzten Vertrauensspeicher sind jedoch nicht zulässig. Wenn entweder der Trust-Store-Besitzer oder der Trust-Store-Nutzer eine Zuordnung löscht, wird sie aus beiden Konten gelöscht. Wenn ein Trust-Store-Nutzer eine Ressourcenfreigabe verlassen möchte, muss er den Besitzer der Ressourcenfreigabe bitten, das Konto zu entfernen.

> ⚠ Löschen von Zuordnungen
>
> Besitzer eines Trust Stores können bestehende Trust Store-Verknüpfungen mithilfe des DeleteTrustStoreAssociationBefehls zwangsweise löschen. Wenn eine Zuordnung gelöscht wird, können alle Load Balancer-Listener, die den Trust Store verwenden, die Client-Zertifikate nicht mehr verifizieren und TLS-Handshakes schlagen fehl.

Sie können die gemeinsame Nutzung eines Trust Stores über die EC2 Amazon-Konsole, AWS RAM -Konsole oder über beenden AWS CLI.

So beenden Sie das Teilen eines Trust Stores, den Sie besitzen, über die EC2 Amazon-Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Trust Stores aus.
3. Wählen Sie den Namen des Trust Stores aus, um die zugehörige Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte Freigabe unter Gemeinsam genutzte Ressourcen die Ressourcenfreigaben aus, für die das Teilen beendet werden soll.
5. Wählen Sie Remove (Entfernen) aus.

Um die gemeinsame Nutzung eines Trust Stores, dessen Eigentümer Sie sind, mithilfe der AWS RAM Konsole zu beenden

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um die gemeinsame Nutzung eines Vertrauensspeichers, den Sie besitzen, zu beenden, verwenden Sie AWS CLI

Verwenden Sie den disassociate-resource-share-Befehl.

Fakturierung und Messung

Für Shared Trust Stores gilt derselbe Standard-Trust-Store-Tarif, der pro Stunde und pro Trust Store-Zuordnung zu einem Application Load Balancer abgerechnet wird.

Weitere Informationen, einschließlich des spezifischen Tarifs pro Region, finden Sie unter Elastic Load Balancing — Preise

Authentifizieren von Benutzern mithilfe eines Application Load Balancers

Sie können einen Application Load Balancer so konfigurieren, dass Benutzer auf sichere Weise authentifiziert werden, wenn sie auf ihre Anwendungen zugreifen. So können Sie den Aufwand für das Authentifizieren der Benutzer auf Ihren Load Balancer verlagern, damit sich Ihre Anwendungen auf die Geschäftslogik konzentrieren können.

Die folgenden Anwendungsfälle werden unterstützt:

- Authentifizieren von Benutzern über einen Identitätsanbieter (IdP), der mit OpenID Connect (OIDC) konform ist
- Authentifizieren Sie Benutzer über soziale Netzwerke IdPs wie Amazon, Facebook oder Google über die von Amazon Cognito unterstützten Benutzerpools.
- Authentifizieren Sie Benutzer über Unternehmensidentitäten, mithilfe von SAML, OpenID Connect (OIDC) oder OAuth über die von Amazon Cognito unterstützten Benutzerpools.

Vorbereiten der Nutzung eines OIDC-konformen Identitätsanbieters

Gehen Sie wie folgt vor, wenn Sie für Ihren Application Load Balancer einen OIDC-konformen Identitätsanbieter verwenden:

- Erstellen Sie unter Ihrem Identitätsanbieter eine neue OIDC-App. Das DNS des Identitätsanbieters muss öffentlich auflösbar sein.
- Sie müssen eine Client-ID und einen Clientschlüssel konfigurieren.
- Rufen Sie die folgenden Arten von Endpunkten ab, die vom Identitätsanbieter veröffentlicht werden: Autorisierung, Token und Benutzerinformationen. Sie finden diese Informationen in der Konfiguration.
- Die Identitätsanbieter-Endpunktzertifikate sollten von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle ausgestellt werden.
- Die DNS-Datensätze für die Endpunkte müssen öffentlich auflösbar sein, auch wenn sie in private IP-Adressen aufgelöst werden.
- Erlauben Sie eine der folgenden Weiterleitungen URLs in Ihrer IdP-App, je nachdem, welche Ihre Benutzer verwenden, wobei DNS der Domainname Ihres Load Balancers und CNAME der DNS-Alias für Ihre Anwendung ist:
  - https:///oauth2/idpresponse *DNS*
  - *CNAME*https://oauth2/idpresponse

Vorbereitung für die Verwendung von Amazon Cognito

Verfügbare Regionen

Die Amazon Cognito Cognito-Integration für Application Load Balancers ist in den folgenden Regionen verfügbar:

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Kanada (Zentral)
- Kanada West (Calgary)
- Europa (Stockholm)
- Europa (Milan)
- Europa (Frankfurt)
- Europa (Zürich)
- Europa (Irland)
- Europa (London)
- Europa (Paris)
- Europa (Spain)
- Südamerika (São Paulo)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Tokio)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Naher Osten (VAE)
- Naher Osten (Bahrain)
- Afrika (Kapstadt)

- Israel (Tel Aviv)

Gehen Sie wie folgt vor, wenn Sie Amazon-Cognito-Benutzerpools für Ihren Application Load Balancer verwenden:

- Erstellen Sie einen Benutzerpool. Weitere Informationen finden Sie unter Amazon-Cognito-Benutzerpools im Amazon-Cognito-Entwicklerhandbuch.
- Erstellen Sie einen Benutzerpool-Client. Sie müssen den Client so konfigurieren, dass er einen geheimen Client-Schlüssel generiert, den Code Grant-Flow verwendet und dieselben OAuth Bereiche unterstützt, die der Load Balancer verwendet. Weitere Informationen finden Sie unter Konfigurieren eines Benutzerpool-App-Clients im Amazon-Cognito-Entwicklerhandbuch.
- Erstellen Sie eine Benutzerpool-Domain. Weitere Informationen finden Sie unter Konfiguration einer Benutzerpool-Domain im Amazon Cognito Developer Guide.
- Überprüfen Sie, ob der angeforderte Bereich ein ID-Token zurückgibt. Beispiel: Der Standardbereich `openid` gibt ein ID-Token zurück, der Bereich `aws.cognito.signin.user.admin` hingegen nicht.
- Aktivieren Sie den Identitätsanbieter im Verbundabschnitt, um einen Verbund mit einem Anbieter von Social Identities bzw. Unternehmensidentitäten einzurichten. Weitere Informationen finden Sie unter Benutzerpool-Anmeldung mit einem externen Identitätsanbieter im Amazon Cognito Developer Guide.
- Erlauben Sie die folgende Weiterleitung URLs im Callback-URL-Feld für Amazon Cognito, wobei DNS der Domainname Ihres Load Balancers und CNAME der DNS-Alias für Ihre Anwendung ist (falls Sie einen verwenden):
  - https:///oauth2/idpresponse *DNS*
  - *CNAME*https://oauth2/idpresponse
- Erlauben Sie Ihre Benutzerpool-Domain für die Rückruf-URL Ihrer Identitätsanbieter-App. Verwenden Sie das für Ihren Identitätsanbieter erforderliche Format. Zum Beispiel:
  - https:*domain-prefix*//.auth. *region*.amazoncognito. com/saml2/idpresponse
  - *user-pool-domain*https://saml2/idpresponse

Die Callback-URL in den App-Client-Einstellungen darf ausschließlich Kleinbuchstaben enthalten.

Damit ein Benutzer einen Load Balancer für die Verwendung von Amazon Cognito zum Authentifizieren von Benutzern konfigurieren kann, müssen Sie dem Benutzer die Berechtigung zum Aufrufen der Aktion `cognito-idp:DescribeUserPoolClient` gewähren.

Bereiten Sie sich auf die Nutzung von Amazon vor CloudFront

Aktivieren Sie die folgenden Einstellungen, wenn Sie eine CloudFront Distribution vor Ihrem Application Load Balancer verwenden:

- Anforderungsheader weiterleiten (alle) — Stellt sicher, dass Antworten für authentifizierte Anfragen CloudFront nicht zwischengespeichert werden. Damit wird vermieden, dass sie nach Ablauf der Authentifizierungssitzung aus dem Zwischenspeicher geladen werden. Um dieses Risiko zu verringern, wenn das Caching aktiviert ist, können Besitzer einer CloudFront Distribution alternativ festlegen, dass der time-to-live (TTL-) Wert abläuft, bevor das Authentifizierungscookie abläuft.
- Abfragezeichenfolge weiterleiten und zwischenspeichern (alle) – Stellt sicher, dass der Load Balancer Zugriff auf die Abfragezeichenfolgenparameter hat, die für die Authentifizierung des Benutzers beim IdP erforderlich sind.
- Cookie-Weiterleitung (alle) — Stellt sicher, dass alle Authentifizierungs-Cookies an den Load Balancer CloudFront weitergeleitet werden.
- Stellen Sie bei der Konfiguration der OpenID Connect (OIDC) -Authentifizierung in Verbindung mit Amazon sicher CloudFront, dass der HTTPS-Port 443 über den gesamten Verbindungspfad konsistent verwendet wird. Andernfalls können Authentifizierungsfehler auftreten, da die Client-OIDC-Umleitung URLs nicht mit der Portnummer der ursprünglich generierten URI übereinstimmt.

Konfigurieren der Benutzerauthentifizierung

Sie konfigurieren die Benutzerauthentifizierung, indem Sie eine Authentifizierungsaktion für eine oder mehrere Listener-Regeln erstellen. Die Aktionstypen `authenticate-cognito` und `authenticate-oidc` werden nur mit HTTPS-Listenern unterstützt. Eine Beschreibung der entsprechenden Felder finden Sie unter AuthenticateCognitoActionConfigund AuthenticateOidcActionConfigin der Elastic Load Balancing API-Referenzversion 2015-12-01.

Der Load Balancer sendet ein Session-Cookie an den Client, um den Authentifizierungsstatus beizubehalten. Dieses Cookie enthält immer das Attribut `secure`, da die Benutzerauthentifizierung einen HTTPS-Listener erfordert. Dieses Cookie enthält das Attribut `SameSite=None` mit CORS-Anforderungen (Cross-Origin Resource Sharing).

Für einen Load Balancer, der mehrere Anwendungen unterstützt, die eine unabhängige Client-Authentifizierung verlangen, sollte jede Listener-Regel mit einer Authentifizierungsaktion einen eindeutigen Cookie-Namen haben. Dadurch wird sichergestellt, dass Clients immer beim IdP authentifiziert werden, bevor sie an die in der Regel angegebene Zielgruppe weitergeleitet werden.

Application Load Balancer unterstützen keine Cookie-Werte, die URL-codiert sind.

Das Feld `SessionTimeout` ist standardmäßig auf 7 Tage festgelegt. Wenn Sie kürzere Sitzungen benötigen, können Sie auch eine Sitzungs-Zeitbeschränkung von bis zu lediglich einer Sekunde konfigurieren. Weitere Informationen finden Sie unter Sitzungs-Timeout.

Legen Sie das Feld `OnUnauthenticatedRequest` je nach Bedarf für Ihre Anwendung fest. Zum Beispiel:

- Anwendungen, bei denen sich der Benutzer mit einer Social Identity oder Unternehmensidentität anmelden muss: Dies wird von der Standardoption `authenticate` unterstützt. Wenn der Benutzer nicht angemeldet ist, leitet der Load Balancer die Anforderung an den Identitätsanbieter-Autorisierungsendpunkt weiter. Der Benutzer wird dann vom Identitätsanbieter aufgefordert, sich über die entsprechende Benutzeroberfläche anzumelden.
- Anwendungen mit einer personalisierten Ansicht für angemeldete Benutzer und einer allgemeinen Ansicht für nicht angemeldete Benutzer: Verwenden Sie die Option `allow`, um diese Art von Anwendung zu unterstützen. Wenn der Benutzer angemeldet ist, stellt der Load Balancer die Benutzeransprüche bereit und die Anwendung kann eine personalisierte Ansicht anzeigen. Wenn der Benutzer nicht angemeldet ist, leitet der Load Balancer die Anforderung ohne die Benutzeransprüche weiter und die Anwendung kann die allgemeine Ansicht anzeigen.
- Einseitige Anwendungen JavaScript , die alle paar Sekunden geladen werden — Wenn Sie die `deny` Option verwenden, gibt der Load Balancer bei AJAX-Aufrufen, die keine Authentifizierungsinformationen enthalten, den Fehler HTTP 401 Unauthorized zurück. Wenn die Authentifizierungsinformationen des Benutzers jedoch abgelaufen sind, wird der Client zum IdP-Autorisierungsendpunkt weitergeleitet.

Der Load Balancer muss mit dem Identitätsanbieter-Tokenendpunkt (`TokenEndpoint`) und dem Endpunkt mit den Benutzerinformationen (`UserInfoEndpoint`) des Identitätsanbieters kommunizieren können. Application Load Balancer unterstützen nur die Kommunikation mit diesen IPv4 Endpunkten. Wenn Ihr IdP öffentliche Adressen verwendet, stellen Sie sicher, dass die Sicherheitsgruppen für Ihren Load Balancer und das Netzwerk ACLs für Ihre VPC den Zugriff auf die Endpunkte zulassen. Wenn Sie einen internen Load Balancer oder den IP-Adresstyp verwenden`dualstack-without-public-ipv4`, kann ein NAT-Gateway dem Load Balancer die Kommunikation mit den Endpunkten ermöglichen. Weitere Informationen finden Sie unter Grundlagen zu NAT-Gateways im Amazon-VPC-Benutzerhandbuch.

Verwenden Sie den folgenden create-rule-Befehl, um die Benutzerauthentifizierung zu konfigurieren.

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--conditions Field=path-pattern,Values="/login" --actions file://actions.json
```

Im Folgenden finden Sie ein Beispiel für die `actions.json`-Datei, die eine `authenticate-oidc`-Aktion und eine `forward`-Aktion angibt. `AuthenticationRequestExtraParams` ermöglicht es Ihnen, während der Authentifizierung zusätzliche Parameter an einen IdP zu übergeben. In der Dokumentation Ihres Identitätsanbieters ist angegeben, welche Felder unterstützt werden.

```
[{
    "Type": "authenticate-oidc",
    "AuthenticateOidcConfig": {
        "Issuer": "https://idp-issuer.com",
        "AuthorizationEndpoint": "https://authorization-endpoint.com",
        "TokenEndpoint": "https://token-endpoint.com",
        "UserInfoEndpoint": "https://user-info-endpoint.com",
        "ClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "ClientSecret": "12345678901234567890123456789O",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Unten ist ein Beispiel für die Datei `actions.json` angegeben, in der die Aktion `authenticate-cognito` und die Aktion `forward` enthalten sind.

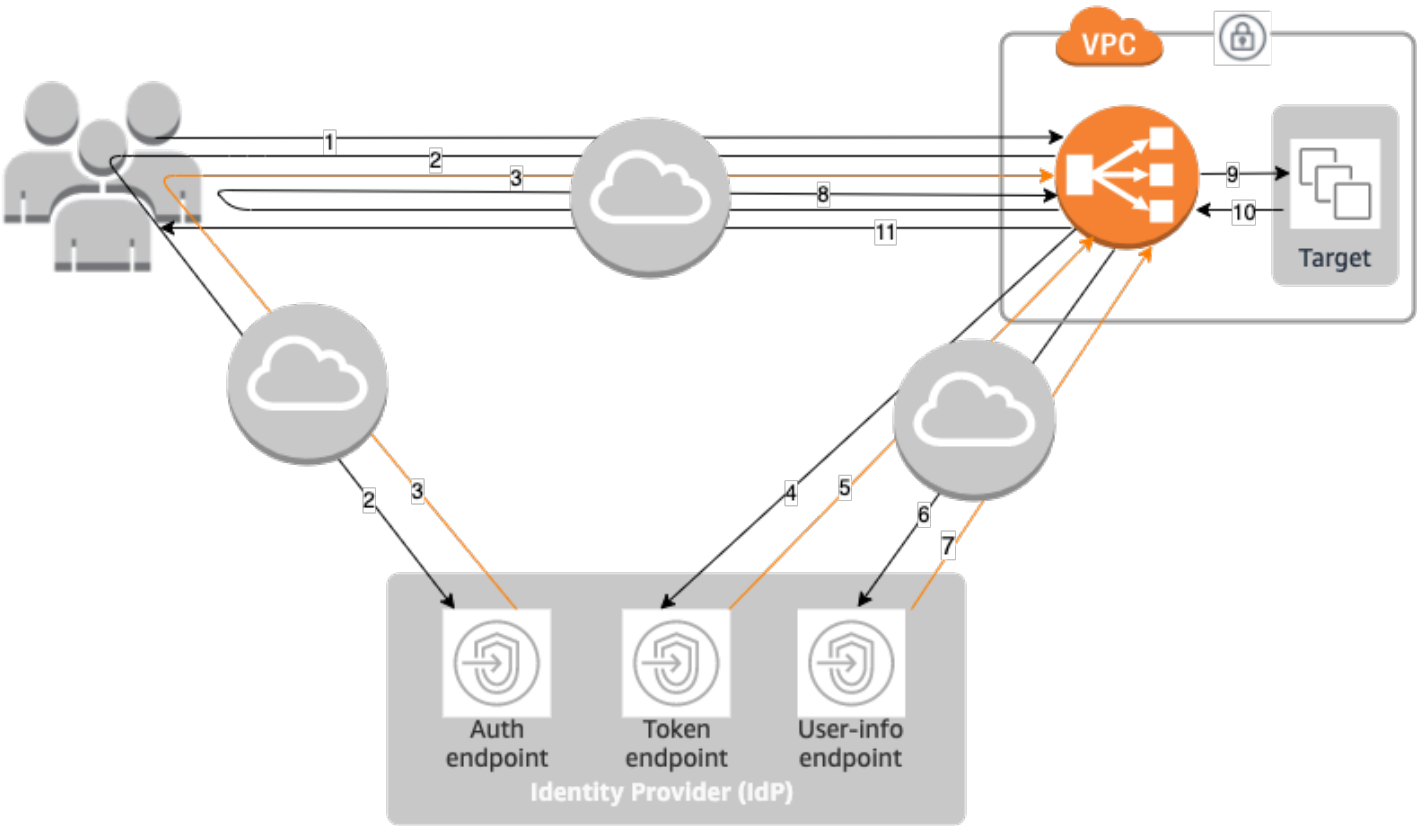
```
[{
    "Type": "authenticate-cognito",
    "AuthenticateCognitoConfig": {
```

```
        "UserPoolArn": "arn:aws:cognito-idp:region-code:account-id:userpool/user-pool-
id",
        "UserPoolClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "UserPoolDomain": "userPoolDomain1",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Weitere Informationen finden Sie unter Listener-Regeln.

Authentifizierungsfluss

Das folgende Netzwerkdiagramm ist eine visuelle Darstellung dazu, wie ein Application Load Balancer OIDC zur Benutzerauthentifizierung verwendet.



Die folgenden nummerierten Punkte heben die im vorangehenden Netzwerkdiagramm gezeigten Elemente hervor und erläutern sie.

1. Der Benutzer sendet eine HTTPS-Anforderung an eine Website, die hinter einem Application Load Balancer gehostet wird. Wenn die Bedingungen für eine Regel mit einer Authentifizierungsaktion erfüllt sind, führt der Load Balancer in den Headern der Anforderungen eine Prüfung auf ein Cookie für eine Authentifizierungssitzung durch.
2. Falls das Cookie nicht vorhanden ist, leitet der Load Balancer den Benutzer an den Identitätsanbieter-Autorisierungsendpunkt um, damit der Benutzer vom Identitätsanbieter authentifiziert werden kann.
3. Nachdem der Benutzer authentifiziert wurde, wird er vom Identitätsanbieter mit einem Code für die Gewährung der Autorisierung zurück an den Load Balancer gesendet.
4. Der Load Balancer präsentiert dem IdP-Token-Endpunkt den Code für die Gewährung der Autorisierung.
5. Nach Erhalt eines gültigen Codes für die Gewährung der Autorisierung stellt der IdP dem Application Load Balancer das ID-Token und das Zugriffstoken zur Verfügung.
6. Der Application Load Balancer sendet dann das Zugriffstoken an den Endpunkt für Benutzerinformationen.

7. Der Endpunkt der Benutzerinformationen tauscht das Zugriffstoken gegen Benutzeransprüche aus.
8. Der Application Load Balancer leitet den Benutzer mit dem `AWSELB`-Cookie für die Authentifizierungssitzung zur ursprünglichen URI weiter. Da für die meisten Browser in Bezug auf Cookies eine Größenbeschränkung von 4 KB gilt, unterteilt der Load Balancer Anwendungs-Cookie, die größer als 4 KB sind, in mehrere Cookies. Wenn die Gesamtgröße der Benutzeransprüche und des Zugriffstokens, die vom Identitätsanbieter eingehen, über 11 KB liegt, gibt der Load Balancer die HTTP 500-Fehlermeldung an den Client zurück und erhöht die Metrik `ELBAuthUserClaimsSizeExceeded`.
9. Der Application Load Balancer validiert das Cookie und leitet die Benutzerinformationen an Ziele in den festgelegten `X-AMZN-OIDC-*`-HTTP-Headern weiter. Weitere Informationen finden Sie unter Codierung von Benutzeransprüchen und Signaturverifizierung.
10. Das Ziel sendet eine Antwort zurück an den Application Load Balancer.
11. Der Application Load Balancer sendet die endgültige Antwort an den Benutzer.

Jede neue Anforderung durchläuft die Schritte 1 bis 11, während nachfolgende Anforderungen die Schritte 9 bis 11 durchlaufen. Das heißt, jede nachfolgende Anforderung beginnt bei Schritt 9, solange das Cookie nicht abgelaufen ist.

Das `AWSALBAuthNonce`-Cookie wird dem Anforderungsheader hinzugefügt, nachdem sich der Benutzer beim IdP authentifiziert hat. Dies ändert nichts daran, wie der Application Load Balancer Anfragen zur Umleitung vom IdP verarbeitet.

Wenn der Identitätsanbieter ein gültiges Aktualisierungstoken im ID-Token bereitstellt, speichert der Load Balancer das Aktualisierungstoken und nutzt es jeweils zum Aktualisieren der Benutzeransprüche, sobald das Zugriffstoken abgelaufen ist. Dieser Vorgang wird fortgesetzt, bis für die Sitzung der Wert für die Zeitüberschreitung erreicht ist oder die Identitätsanbieter-Aktualisierung fehlschlägt. Wenn sich der Benutzer abmeldet, tritt für die Aktualisierung ein Fehler auf und der Load Balancer leitet den Benutzer an den Identitätsanbieter-Autorisierungsendpunkt weiter. Auf diese Weise kann der Load Balancer Sitzungen verwerfen, nachdem sich der Benutzer abgemeldet hat. Weitere Informationen finden Sie unter Sitzungs-Timeout.

> **Note**
>
> Der Ablauf des Cookies unterscheidet sich vom Ablauf der Authentifizierungssitzung. Der Ablauf des Cookies ist ein Attribut des Cookies, das auf 7 Tage festgelegt ist. Die tatsächliche Länge der Authentifizierungssitzung wird durch die Sitzungs-Zeitüberschreitung bestimmt,

das im Application Load Balancer für das Authentifizierungsfeature konfiguriert wurde. Dieses Sitzungs-Timeout ist im Wert des Authentifizierungs-Cookies enthalten, der ebenfalls verschlüsselt ist.

Codierung von Benutzeransprüchen und Signaturverifizierung

Nachdem der Load Balancer einen Benutzer erfolgreich authentifiziert hat, sendet er die vom Identitätsanbieter erhaltenen Benutzeransprüche an das Ziel. Der Load Balancer signiert den Benutzeranspruch, damit diese Anwendungen die Signatur prüfen und sicherstellen können, dass die Ansprüche vom Load Balancer gesendet wurden.

Der Load Balancer fügt die folgenden HTTP-Header hinzu:

`x-amzn-oidc-accesstoken`

Das Zugriffstoken des Tokenendpunkts als Klartext

`x-amzn-oidc-identity`

Das Betrefffeld (`sub`) vom Endpunkt mit den Benutzerinformationen als Klartext

Hinweis: Der sub-Anspruch ist der beste Weg, um einen bestimmten Benutzer zu identifizieren..

`x-amzn-oidc-data`

Die Benutzeransprüche im JWT-Format (JSON-Web-Tokens)

Zugriffstoken und Benutzeransprüche unterscheiden sich von den ID-Token. Zugriffstoken und Benutzeransprüche ermöglichen nur den Zugriff auf Serverressourcen, während ID-Token zusätzliche Informationen zur Authentifizierung eines Benutzers enthalten. Der Application Load Balancer erstellt bei der Authentifizierung eines Benutzers ein neues Zugriffstoken und leitet nur die Zugriffstoken und Ansprüche an das Backend weiter, nicht jedoch die ID-Token-Informationen.

Diese Token weisen zwar das JWT-Format auf, sind aber keine ID-Token. Das JWT-Format umfasst einen Header, eine Nutzlast und eine Signatur (jeweils mit base64-URL-Verschlüsselung) und beinhalten Padding-Zeichen am Ende. Ein Application Load Balancer verwendet ES256 (ECDSA verwendet P-256 und SHA256), um die JWT-Signatur zu generieren.

Der JWT-Header ist ein JSON-Objekt mit den folgenden Feldern:

```
{
   "alg": "algorithm",
   "kid": "12345678-1234-1234-1234-123456789012",
   "signer": "arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/
app/load-balancer-name/load-balancer-id",
   "iss": "url",
   "client": "client-id",
   "exp": "expiration"
}
```

Die JWT-Nutzlast ist ein JSON-Objekt mit den Benutzeransprüchen, die vom Identitätsanbieterendpunkt mit den Benutzerinformationen empfangen wurden.

```
{
   "sub": "1234567890",
   "name": "name",
   "email": "alias@example.com",
   ...
}
```

Wenn Sie möchten, dass der Load Balancer Ihre Benutzeransprüche verschlüsselt, müssen Sie Ihre Zielgruppe für die Verwendung von HTTPS konfigurieren. Aus Sicherheitsgründen empfehlen wir Ihnen außerdem, Ihre Ziele so zu beschränken, dass sie nur Traffic von Ihrem Application Load Balancer empfangen. Sie können dies erreichen, indem Sie die Sicherheitsgruppe Ihrer Ziele so konfigurieren, dass sie auf die Sicherheitsgruppen-ID des Load Balancers verweist.

Um die Sicherheit zu gewährleisten, müssen Sie die Signatur überprüfen, bevor Sie eine Autorisierung auf der Grundlage der Ansprüche vornehmen, und überprüfen, ob das `signer` Feld im JWT-Header den erwarteten Application Load Balancer Balancer-ARN enthält.

Sie erhalten den öffentlichen Schlüssel, indem Sie die Schlüssel-ID aus dem JWT-Header verwenden, um den öffentlichen Schlüssel aus dem Endpunkt zu suchen. Der Endpunkt für jede AWS -Region lautet wie folgt:

```
https://public-keys.auth.elb.region.amazonaws.com/key-id
```

Denn AWS GovCloud (US) die Endpunkte lauten wie folgt:

```
https://s3-us-gov-west-1.amazonaws.com/aws-elb-public-keys-prod-us-gov-west-1/key-id
```

```
https://s3-us-gov-east-1.amazonaws.com/aws-elb-public-keys-prod-us-gov-east-1/key-id
```

AWS bietet eine Bibliothek, mit der Sie überprüfen können, ob sie von Amazon Cognito, Application Load Balancers und anderen OIDC-kompatiblen Geräten JWTs signiert wurde. IDPs Weitere Informationen finden Sie unter JWT Verify.AWS

Zeitüberschreitung

Sitzungs-Timeout

Das Aktualisierungstoken und die Sitzungs-Zeitüberschreitung arbeiten wie folgt zusammen:

- Wenn das Sitzungstimeout kürzer als die Ablaufzeit des Zugriffstokens ist, berücksichtigt der Load Balancer das Sitzungstimeout. Wenn der Benutzer eine aktive Sitzung mit dem IdP hat, wird der Benutzer möglicherweise nicht aufgefordert, sich erneut anzumelden. Andernfalls wird der Benutzer zur Anmeldung umgeleitet.
  - Wenn das IdP-Sitzungs-Timeout länger als das Application-Load-Balancer-Sitzungs-Timeout ist, muss der Benutzer keine Anmeldeinformationen angeben, um sich erneut anzumelden. Stattdessen leitet der IdP die Anforderung mit einem neuen Code für die Gewährung der Autorisierung zurück zum Application Load Balancer. Autorisierungscodes können nur einmal verwendet werden, auch wenn keine erneute Anmeldung erfolgt.
  - Wenn das IdP-Sitzungs-Timeout gleich lang oder kürzer als das Application-Load-Balancer-Sitzungs-Timeout ist, wird der Benutzer aufgefordert, Anmeldeinformationen einzugeben, um sich erneut anzumelden. Nachdem sich der Benutzer angemeldet hat, leitet der IdP mit einem neuen Code für die Gewährung der Autorisierung die Anforderung zurück zum Application Load Balancer und der Rest des Authentifizierungsvorgangs wird fortgesetzt, bis die Anfrage das Backend erreicht.
- Wenn das Sitzungs-Timeout länger als die Ablaufzeit des Zugriffstokens ist und der Identitätsanbieter keine Aktualisierungstoken unterstützt, behält der Load Balancer die Authentifizierungssitzung bei, bis sie abgelaufen ist. Anschließend muss der Benutzer sich erneut anmelden.
- Wenn die Sitzungs-Zeitüberschreitung länger als die Ablaufzeit des Zugriffstokens ist und der Identitätsanbieter Aktualisierungstoken unterstützt, aktualisiert der Load Balancer die Benutzersitzung jedes Mal, wenn das Zugriffstoken abläuft. Der Load Balancer fordert den Benutzer erst zum erneuten Anmelden auf, nachdem für die Authentifizierungssitzung die Zeitüberschreitung erreicht wurde oder der Aktualisierungsablauf fehlgeschlagen ist.

Client-Anmelde-Timeout

Ein Client muss den Authentifizierungsprozess innerhalb von 15 Minuten einleiten und abschließen. Wenn ein Client die Authentifizierung nicht innerhalb der 15-minütigen Frist abschließt, erhält er vom Load Balancer einen HTTP-401-Fehler. Dieses Timeout kann nicht geändert oder entfernt werden.

Wenn ein Benutzer beispielsweise die Anmeldeseite über den Application Load Balancer lädt, muss er den Anmeldevorgang innerhalb von 15 Minuten abschließen. Wenn der Benutzer wartet und dann versucht, sich nach Ablauf des 15-Minuten-Timeouts anzumelden, gibt der Load Balancer einen HTTP-401-Fehler zurück. Der Benutzer muss die Seite aktualisieren und erneut versuchen, sich anzumelden.

Authentifizierung und Abmeldung

Wenn eine Anwendung einen authentifizierten Benutzer abmelden muss, sollte die Ablaufzeit des Cookies für die Authentifizierungssitzung auf „-1“ festgelegt und der Client an den Identitätsanbieteredpunkt für die Abmeldung (falls vom Identitätsanbieter unterstützt) weitergeleitet werden. Um zu verhindern, dass Benutzer ein gelöschtes Cookie wiederverwenden, empfehlen wir Ihnen, die Ablaufzeit für das Zugriffstoken so kurz wie möglich zu konfigurieren. Wenn ein Client dem Load Balancer ein Sitzungscookie mit einem abgelaufenen Zugriffstoken mit einem Aktualisierungstoken ungleich NULL zur Verfügung stellt, kontaktiert der Load Balancer den IdP, um festzustellen, ob der Benutzer noch angemeldet ist.

Landingpages zur Client-Abmeldung sind nicht authentifiziert. Das bedeutet, dass sie nicht hinter einer Application Load Balancer Balancer-Regel stehen können, die eine Authentifizierung erfordert.

- Wenn eine Anforderung an das Ziel gesendet wird, muss die Anwendung den Ablauf für alle Authentifizierungs-Cookies auf -1 setzen. Application Load Balancer unterstützen Cookies mit einer Größe von bis zu 16 KB und können daher bis zu 4 Shards erstellen, die an den Client gesendet werden.
  - Wenn der IdP einen Abmeldeendpunkt hat, sollte er eine Umleitung zum IdP-Abmeldeendpunkt ausgeben, z. B. zu dem im Amazon-Cognito-Entwicklerhandbuch dokumentierten LOGOUT-Endpunkt.
  - Wenn der IdP keinen Abmeldeendpunkt hat, geht die Anfrage zurück zur Client-Abmelde-Zielseite und der Anmeldevorgang wird neu gestartet.
- Unter der Annahme, dass der IdP über einen Abmeldeendpunkt verfügt, muss der IdP Zugriffs- und Aktualisierungstoken ablaufen lassen und den Benutzer zurück zur Zielseite für die Client-Abmeldung weiterleiten.

- Nachfolgende Anforderungen folgen dem ursprünglichen Authentifizierungsablauf.

Tags für Ihre Application Load Balancer Balancer-Listener und Regeln

Mit Tags können Sie Ihre Listener und Regeln auf unterschiedliche Weise kategorisieren. Sie können Ressourcen beispielsweise nach Zweck, Inhaber oder Umgebung taggen.

Sie können jedem Listener und jeder Regel mehrere Tags hinzufügen. Tag-Schlüssel müssen für jeden Listener und jede Regel eindeutig sein. Wenn Sie eine Markierung mit einem Schlüssel hinzufügen, der dem Listener und der Regel bereits zugeordnet ist, ändert sich der Wert dieses Tags.

Wenn Sie ein Tag nicht mehr benötigen, können Sie es entfernen.

Einschränkungen

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen
- Maximale Wertlänge: 255 Unicode-Zeichen
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen.
- Verwenden Sie das `aws:` Präfix nicht in Ihren Tagnamen oder -Werten, da es für die AWS Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

Aktualisieren der Listener-Tags

So aktualisieren Sie die Tags für einen Listener mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, der den Listener enthält, den Sie aktualisieren möchten, um dessen Detailseite zu öffnen.

4. Führen Sie auf der Registerkarte Listener und Regeln einen der folgenden Schritte durch:

   a. Wählen Sie den Text in der Spalte Protokoll: Port aus, um die Detailseite für den Listener zu öffnen.

      Wählen Sie auf der Registerkarte Tags die Option Manage tags (Tags verwalten).

   b. Wählen Sie den Listener aus, für den Sie Tags aktualisieren möchten.

      Wählen Sie Listener verwalten und dann Tags verwalten aus.

   c. Wählen Sie den Text in der Spalte Tags aus, um die Seite mit den Listener-Details auf der Registerkarte „Tags“ zu öffnen.

      Wählen Sie Tags verwalten aus.

5. Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

   a. Um ein Tag zu aktualisieren, geben Sie neue Werte für Schlüssel und Wert ein.

   b. Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen aus und geben Sie Werte für Schlüssel und Wert ein.

   c. Um ein Tag zu löschen, wählen Sie Entfernen neben dem Tag.

6. Wenn Sie die Aktualisierung der Tags abgeschlossen haben, wählen Sie Änderungen speichern.

Um die Tags für einen Listener mit dem zu aktualisieren AWS CLI

Verwenden Sie die Befehle add-tags und remove-tags.

Aktualisieren von Regel-Tags

So aktualisieren Sie die Tags für eine Regel mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, der die Regel enthält, die Sie aktualisieren möchten, um dessen Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listener und Regeln den Text in der Spalte Protokoll: Port des Listeners aus, der die zu aktualisierende Regel enthält, um die Detailseite für den Listener zu öffnen.
5. Führen Sie auf der Detailseite des Listeners einen der folgenden Schritte aus:

a. Wählen Sie den Text in der Spalte Namens-Tag aus, um die Detailseite für die Regel zu öffnen.

   Wählen Sie auf der Seite mit den Details der Regel die Option Tags verwalten aus.

b. Wählen Sie den Text in der Spalte Tags für die Regel aus, die Sie aktualisieren möchten.

   Wählen Sie im Pop-up-Fenster mit der Zusammenfassung der Tags die Option Tags verwalten aus.

6. Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

   a. Um ein Tag zu aktualisieren, geben Sie neue Werte für Schlüssel und Wert ein.
   b. Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen aus und geben Sie Werte für Schlüssel und Wert ein.
   c. Um ein Tag zu löschen, wählen Sie Entfernen neben dem Tag.

7. Wenn Sie die Aktualisierung der Tags abgeschlossen haben, wählen Sie Änderungen speichern.

Um die Tags für eine Regel mit dem zu aktualisieren AWS CLI

Verwenden Sie die Befehle add-tags und remove-tags.

Löschen eines Listeners für Ihren Application Load Balancer

Sie können einen Listener jederzeit löschen. Wenn Sie einen Load Balancer löschen, werden all seine Listener gelöscht.

Löschen eines Listener mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Aktivieren Sie auf der Registerkarte Listener und Regeln das Kontrollkästchen für den Listener und wählen Sie Listener verwalten, Listener löschen aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie Löschen aus.

Um einen Listener mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-listener.

Änderung des HTTP-Headers für Ihren Application Load Balancer

Die Änderung von HTTP-Headern wird von Application Load Balancers sowohl für Anforderungs- als auch für Antwortheader unterstützt. Durch die Header-Änderung haben Sie mehr Kontrolle über den Datenverkehr und die Sicherheit Ihrer Anwendung, ohne dass Sie Ihren Anwendungscode aktualisieren müssen.

Informationen zum Aktivieren der Header-Änderung finden Sie unterAktivieren Sie die Header-Änderung.

mTLS/TLS Header umbenennen

Mit der Funktion zum Umbenennen von Headern können Sie die Namen der mTLS- und TLS-Header konfigurieren, die der Application Load Balancer generiert und zu Anfragen hinzufügt.

Durch diese Fähigkeit, HTTP-Header zu ändern, kann Ihr Application Load Balancer problemlos Anwendungen unterstützen, die speziell formatierte Anfrage- und Antwortheader verwenden.

Header	Beschreibung
X-Amzn-Mtls-Clientcert-Serial-Number	Stellt sicher, dass das Ziel das vom Client beim TLS-Handshake vorgelegte spezifische Zertifikat identifizieren und verifizieren kann.
X-Amzn-Mtls-Clientcert-Issuer	Hilft dem Ziel, das Client-Zertifikat zu validiere n und zu authentifizieren, indem die Zertifizi erungsstelle identifiziert wird, die das Zertifikat ausgestellt hat.
X-Amzn-Mtls-Clientcert-Subject	Stellt der Zielperson detaillierte Informationen über die Entität zur Verfügung, für die das Client-Zertifikat ausgestellt wurde, was bei der Identifizierung, Authentifizierung, Autorisierung und Protokollierung während der mTLS-Auth entifizierung hilfreich ist.

Header	Beschreibung
X-Amzn-Mtls-Clientcert-Validity	Ermöglicht es dem Ziel, zu überprüfen, ob das verwendete Client-Zertifikat innerhalb des definierten Gültigkeitszeitraums liegt, und stellt so sicher, dass das Zertifikat nicht abgelaufen ist oder vorzeitig verwendet wird.
X-Amzn-Mtls-Clientcert-Leaf	Stellt das im mTLS-Handshake verwendete Client-Zertifikat bereit, sodass der Server den Client authentifizieren und die Zertifikatskette validieren kann. Dadurch wird sichergestellt, dass die Verbindung sicher und autorisiert ist.
X-Amzn-Mtls-Clientcert	Trägt das vollständige Client-Zertifikat. Ermöglicht es dem Ziel, die Echtheit des Zertifikats zu überprüfen, die Zertifikatskette zu validieren und den Client während des mTLS-Handshake-Prozesses zu authentifizieren.
X-Amzn-TLS-Version	Gibt die Version des TLS-Protokolls an, das für eine Verbindung verwendet wird. Es erleichte rt die Bestimmung des Sicherheitsniveaus der Kommunikation, die Behebung von Verbindun gsproblemen und die Sicherstellung der Einhaltung von Vorschriften.
X-Amzn-TLS-Cipher-Suite	Gibt die Kombination von kryptografischen Algorithmen an, die zur Sicherung einer Verbindung in TLS verwendet werden. Auf diese Weise kann der Server die Sicherheit der Verbindung beurteilen, was bei der Behebung von Kompatibilitätsproblemen hilft und die Einhaltung der Sicherheitsrichtlinien gewährlei stet.

Fügen Sie Antwort-Header hinzu

Mithilfe von Insert-Headern können Sie Ihren Application Load Balancer so konfigurieren, dass sicherheitsrelevante Header zu Antworten hinzugefügt werden. Mit diesen Attributen können Sie Header wie HSTS, CORS und CSP einfügen.

Standardmäßig sind diese Header leer. In diesem Fall ändert der Application Load Balancer diesen Antwortheader nicht.

Wenn Sie einen Antwort-Header aktivieren, fügt der Application Load Balancer allen Antworten den Header mit dem konfigurierten Wert hinzu. Wenn die Antwort vom Ziel den HTTP-Antwort-Header enthält, aktualisiert der Load Balancer den Header-Wert auf den konfigurierten Wert. Andernfalls fügt der Load Balancer der Antwort den HTTP-Antwort-Header mit dem konfigurierten Wert hinzu.

Header	Beschreibung
Strict-Transport-Security	Erzwingt reine HTTPS-Verbindungen durch den Browser für eine bestimmte Dauer und trägt so zum Schutz vor man-in-the-middle Angriffen, Protokollherabstufungen und Benutzerfehlern bei. Dabei wird sichergestellt, dass die gesamte Kommunikation zwischen dem Client und dem Ziel verschlüsselt ist.
Access-Control-Allow-Origin	Steuert, ob auf Ressourcen auf einem Ziel von unterschiedlichen Quellen aus zugegriff en werden kann. Dies ermöglicht sichere ursprungsübergreifende Interaktionen und verhindert gleichzeitig unbefugten Zugriff.
Access-Control-Allow-Methods	Gibt die HTTP-Methoden an, die zulässig sind, wenn ursprungsübergreifende Anfragen an das Ziel gestellt werden. Es ermöglicht die Kontrolle darüber, welche Aktionen von unterschiedlichen Ursprüngen aus ausgeführt werden können.
Access-Control-Allow-Headers	Gibt an, welche benutzerdefinierten oder nicht einfachen Header in eine ursprungsübergreif

Header	Beschreibung
	ende Anfrage aufgenommen werden können. Dieser Header gibt Zielen die Kontrolle darüber, welche Header von Clients unterschiedlicher Herkunft gesendet werden können.
Access-Control-Allow-Credentials	Gibt an, ob der Client Anmeldeinformation en wie Cookies, HTTP-Authentifizierung oder Client-Zertifikate in ursprungsübergreifende Anfragen aufnehmen soll.
Access-Control-Expose-Headers	Ermöglicht dem Ziel, anzugeben, auf welche zusätzlichen Antwortheader der Client bei ursprungsübergreifenden Anfragen zugreifen kann.
Access-Control-Max-Age	Definiert, wie lange der Browser das Ergebnis einer Preflight-Anfrage zwischenspeichern kann, wodurch die Notwendigkeit wiederholter Preflight-Checks reduziert wird. Dies trägt zur Leistungsoptimierung bei, indem die Anzahl der OPTIONS-Anfragen reduziert wird, die für bestimmte ursprungsübergreifende Anfragen erforderlich sind.
Content-Security-Policy	Sicherheitsfunktion, die Code-Injection-Ang riffe wie XSS verhindert, indem gesteuert wird, welche Ressourcen wie Skripte, Stile, Bilder usw. von einer Website geladen und ausgeführ t werden können.
X-Content-Type-Options	Verbessert mit der No-Sniff-Direktive die Websicherheit, indem verhindert wird, dass Browser den MIME-Typ einer Ressource erraten. Sie stellt sicher, dass Browser Inhalte nur gemäß dem deklarierten Content-Type interpretieren

Header	Beschreibung
X-Frame-Options	Header-Sicherheitsmechanismus, der Click-Jacking-Angriffe verhindert, indem gesteuert wird, ob eine Webseite in Frames eingebett et werden kann. Werte wie DENY und SAMEORIGIN können sicherstellen, dass Inhalte nicht auf bösartigen oder nicht vertrauen swürdigen Websites eingebettet werden.

Header deaktivieren

Mithilfe von Headern können Sie Ihren Application Load Balancer so konfigurieren, dass der `server:awselb/2.0` Header aus den Antworten deaktiviert wird. Dadurch wird die Offenlegung serverspezifischer Informationen reduziert und gleichzeitig eine zusätzliche Schutzebene für Ihre Anwendung hinzugefügt.

Der Name des Attributs lautet`routing.http.response.server.enabled`. Die verfügbaren Werte sind `true` oder`false`. Der Standardwert ist `true`.

Einschränkungen

- Header-Werte können die folgenden Zeichen enthalten
  - Alphanumerische Zeichen: `a-zA-Z`, und `0-9`
  - Sonderzeichen: `_ :;.,\/'?!(){}[]@<>=-+*#&`|~^%`
- Der Wert für das Attribut darf eine Größe von 1 KB nicht überschreiten.
- Elastic Load Balancing führt grundlegende Eingabevalidierungen durch, um zu überprüfen, ob der Header-Wert gültig ist. Die Validierung kann jedoch nicht bestätigen, ob der Wert für einen bestimmten Header unterstützt wird.
- Wenn Sie für ein Attribut einen leeren Wert angeben, kehrt der Application Load Balancer zum Standardverhalten zurück.

Aktivieren Sie die HTTP-Header-Änderung für Ihren Application Load Balancer

Die Header-Änderung ist standardmäßig ausgeschaltet und muss auf jedem Listener aktiviert werden.

Um die Header-Änderung mit der Konsole zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Load Balancers aus.
3. Wählen Sie den Application Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listener und Regeln das Protokoll und den Port aus, um die Detailseite für Ihren Listener zu öffnen.
5. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.

   Listener-Attribute sind in Gruppen organisiert. Sie wählen aus, welche Funktionen aktiviert werden sollen.
6. [HTTPS-Listener] Modifizierbare mTLS/TLS Header-Namen

   a. Erweitern Sie Modifizierbare Header-Namen mTLS/TLS .

   b. Ermöglicht es den Anforderungsheadern, sie zu ändern, und geben Sie ihnen Namen. Weitere Informationen finden Sie unter the section called “ mTLS/TLS Header umbenennen”.
7. Fügen Sie Antwort-Header hinzu

   a. Erweitern Sie Antwort-Header hinzufügen.

   b. Aktivieren Sie die Antwort-Header, um Werte für sie hinzuzufügen und bereitzustellen. Weitere Informationen finden Sie unter the section called “Fügen Sie Antwort-Header hinzu”.
8. Antwort-Header des ALB-Servers

   - Aktiviert oder deaktiviert den Server-Header.
9. Wählen Sie Änderungen speichern aus.

Um die Header-Änderung mit dem zu aktivieren AWS CLI

Verwenden Sie den modify-listener-attributesBefehl mit den folgenden Attributen:

`routing.http.request.x_amzn_mtls_clientcert_serial_number.header_name`

Ändern Sie den Header-Namen von X-Amzn-Mtls-Clientcert-Serial-Number.

`routing.http.request.x_amzn_mtls_clientcert_issuer.header_name`

Ändern Sie den Header-Namen von X-Amzn-Mtls-Clientcert-Issuer.

`routing.http.request.x_amzn_mtls_clientcert_subject.header_name`

Ändern Sie den Header-Namen von X-Amzn-Mtls-Clientcert-Suject.

`routing.http.request.x_amzn_mtls_clientcert_validity.header_name`

Ändern Sie den Header-Namen von X-Amzn-Mtls-Clientcert-Validity.

`routing.http.request.x_amzn_mtls_clientcert_leaf.header_name`

Ändern Sie den Header-Namen von X-Amzn-Mtls-Clientcert-Leaf.

`routing.http.request.x_amzn_mtls_clientcert.header_name`

Ändern Sie den Header-Namen von X-Amzn-Mtls-Clientcert.

`routing.http.request.x_amzn_tls_version.header_name`

Ändern Sie den Header-Namen von X-Amzn-Tls-Version.

`routing.http.request.x_amzn_tls_cipher_suite.header_name`

Ändern Sie den Header-Namen von X-Amzn-Tls-Cipher-Suite.

`routing.http.response.server.enabled`

Gibt an, ob der HTTP-Antwortserver-Header zugelassen oder entfernt werden soll.

`routing.http.response.strict_transport_security.header_value`

Fügen Sie den Strict-Transport-Security-Header hinzu, um Browser darüber zu informieren, dass auf die Site nur über HTTPS zugegriffen werden sollte und dass alle future Zugriffsversuche über HTTP automatisch in HTTPS umgewandelt werden sollten.

`routing.http.response.access_control_allow_origin.header_value`

Fügen Sie den Header Access-Control-Allow-Origin hinzu, um anzugeben, welche Ursprünge auf den Server zugreifen dürfen.

`routing.http.response.access_control_allow_methods.header_value`

Fügen Sie den Header Access-Control-Allow-Methods hinzu, um anzugeben, welche HTTP-Methoden zulässig sind, wenn von einem anderen Ursprung aus auf den Server zugegriffen wird.

`routing.http.response.access_control_allow_headers.header_value`

Fügen Sie den Header Access-Control-Allow-Headers hinzu, um anzugeben, welche Header bei einer ursprungsübergreifenden Anfrage zulässig sind.

`routing.http.response.access_control_allow_credentials.header_value`

Fügen Sie den Header Access-Control-Allow-Credentials hinzu, um anzugeben, ob der Browser Anmeldeinformationen wie Cookies oder Authentifizierung in ursprungsübergreifende Anfragen aufnehmen soll.

`routing.http.response.access_control_expose_headers.header_value`

Fügen Sie den Header Access-Control-Expose-Headers hinzu, um anzugeben, welche Header der Browser dem anfragenden Client zur Verfügung stellen kann.

`routing.http.response.access_control_max_age.header_value`

Fügen Sie den Access-Control-Max-Age-Header hinzu, um anzugeben, wie lange die Ergebnisse einer Preflight-Anfrage zwischengespeichert werden können (in Sekunden).

`routing.http.response.content_security_policy.header_value`

Fügen Sie den Content-Security-Policy-Header hinzu, um Einschränkungen anzugeben, die vom Browser durchgesetzt werden, um das Risiko bestimmter Arten von Sicherheitsbedrohungen zu minimieren.

`routing.http.response.x_content_type_options.header_value`

Fügen Sie den Header X-Content-Type-Options hinzu, um anzugeben, ob die in den Content-Type-Headern angekündigten MIME-Typen befolgt und nicht geändert werden sollen.

`routing.http.response.x_frame_options.header_value`

Fügen Sie den X-Frame-Options-Header hinzu, um anzugeben, ob der Browser eine Seite in einem Frame, Iframe, Embed oder Objekt rendern darf.

Zielgruppen für Ihre Application Load Balancer

Zielgruppen leiten Anfragen mithilfe des von Ihnen angegebenen Protokolls und der Portnummer an einzelne registrierte Ziele, z. B. EC2 Instances, weiter. Sie können ein Ziel bei mehreren Zielgruppen registrieren. Sie können Zustandsprüfungen pro Zielgruppe konfigurieren. Zustandsprüfungen werden auf allen Zielen ausgeführt, die bei einer Zielgruppe registriert sind, welche in einer Listener-Regel für Ihren Load Balancer abgegeben ist.

Jede Zielgruppe wird verwendet, um Anfragen an ein oder mehrere registrierte Ziele weiterzuleiten. Beim Erstellen der jeweiligen Listener-Regeln geben Sie eine Zielgruppe und Bedingungen an. Wenn die Bedingung einer Regel erfüllt ist, wird der Datenverkehr an die entsprechende Zielgruppe weitergeleitet. Sie können unterschiedliche Zielgruppen für verschiedene Arten von Anfragen erstellen. Erstellen Sie beispielsweise eine Zielgruppe für allgemeine Anfragen und andere Zielgruppen für Anfragen an die Microservices für Ihre Anwendung. Sie können für jede Zielgruppe nur einen Load Balancer verwenden. Weitere Informationen finden Sie unter Application-Load-Balancer-Komponenten.

Sie definieren Zustandsprüfungseinstellungen für Ihren Load Balancer pro Zielgruppe. Jede Zielgruppe verwendet die standardmäßigen Zustandsprüfungseinstellungen, es sei denn, Sie überschreiben diese, wenn Sie die Zielgruppe erstellen, oder ändern sie später. Nachdem Sie eine Zielgruppe in einer Regel für einen Listener angegeben haben, überwacht der Load Balancer kontinuierlich den Zustand aller mit der Zielgruppe registrierten Ziele, die in einer Availability Zone vorhanden sind, die für den Load Balancer aktiviert ist. Der Load Balancer leitet Anfragen an die registrierten Ziele weiter, die fehlerfrei sind.

Inhalt

- Weiterleitungskonfiguration
- Zieltyp
- IP-Adresstyp
- Protokollversion
- Registrierte Ziele
- Zielgruppenattribute
- Routing-Algorithmen
- Zustand der Zielgruppe

- Erstellen Sie eine Zielgruppe für Ihren Application Load Balancer
- Aktualisieren Sie die Gesundheitseinstellungen für Ihre Application Load Balancer Balancer-Zielgruppe
- Gesundheitschecks für Application Load Balancer Balancer-Zielgruppen
- Zielgruppenattribute für Ihren Application Load Balancer bearbeiten
- Registrieren Sie Ziele bei Ihrer Application Load Balancer Balancer-Zielgruppe
- Verwenden Sie Lambda-Funktionen als Ziele eines Application Load Balancer
- Tags für Ihre Application Load Balancer Balancer-Zielgruppe
- Löschen Sie eine Application Load Balancer Balancer-Zielgruppe

Weiterleitungskonfiguration

Ein Load Balancer leitet standardmäßig mithilfe des Protokolls und der Portnummer, die Sie beim Erstellen der Zielgruppe angegeben haben, Anfragen an die Ziele weiter. Alternativ können Sie den für Weiterleitung von Datenverkehr zu einem Ziel verwendeten Port überschreiben, wenn Sie es bei der Zielgruppe registrieren.

Zielgruppen unterstützen die folgenden Protokolle und Ports:

- Protocols (Protokolle): HTTP, HTTPS
- Ports: 1-65535

Wenn eine Zielgruppe mit dem HTTPS-Protokoll konfiguriert ist oder HTTPS-Integritätsprüfungen verwendet und ein HTTPS-Listener eine TLS 1.3-Sicherheitsrichtlinie verwendet, wird die `ELBSecurityPolicy-TLS13-1-0-2021-06` Sicherheitsrichtlinie für Zielverbindungen verwendet. Andernfalls wird die `ELBSecurityPolicy-2016-08` Sicherheitsrichtlinie verwendet. Der Load Balancer stellt TLS-Verbindungen mit den Zielen her, wobei er die auf den Zielen installierten Zertifikate verwendet. Der Load Balancer überprüft diese Zertifikate nicht. Daher können Sie selbstsignierte Zertifikate oder Zertifikate verwenden, die abgelaufen sind. Da sich der Load Balancer und seine Ziele in einer Virtual Private Cloud (VPC) befinden, wird der Verkehr zwischen dem Load Balancer und den Zielen auf Paketebene authentifiziert, sodass kein Risiko von man-in-the-middle Angriffen oder Spoofing besteht, selbst wenn die Zertifikate auf den Zielen nicht gültig sind. Für den ausgehenden Datenverkehr AWS gilt nicht der gleiche Schutz, und es sind möglicherweise zusätzliche Schritte erforderlich, um den Datenverkehr weiter zu sichern.

Zieltyp

Wenn Sie eine Zielgruppe erstellen, legen Sie ihren Zieltyp fest, wodurch festgelegt wird, welchen Zieltyp Sie beim Registrieren von Zielen bei dieser Zielgruppe angeben. Nachdem Sie eine Zielgruppe erstellt haben, können Sie ihren Zieltyp nicht mehr ändern.

Die folgenden Zieltypen sind möglich:

`instance`

Die Ziele werden nach Instance-ID angegeben.

`ip`

Die Ziele sind IP-Adressen.

`lambda`

Das Ziel ist eine Lambda-Funktion.

Wenn der Zieltyp `ip` ist, können Sie IP-Adressen von einem der folgenden CIDR-Blöcke angeben:

- Die Subnetze der VPC für die Zielgruppe
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

> **Important**
>
> Sie können keine öffentlich weiterleitungsfähigen IP-Adressen angeben.

Mit allen unterstützten CIDR-Blöcken können Sie die folgenden Ziele bei einer Zielgruppe registrieren:

- Instances in einer VPC, die durch Peering mit der Load-Balancer-VPC verbunden sind (dieselbe Region oder eine andere Region).
- AWS Ressourcen, die über IP-Adresse und Port adressierbar sind (z. B. Datenbanken).

- Lokale Ressourcen, mit denen AWS über eine VPN-Verbindung AWS Direct Connect oder eine Site-to-Site VPN-Verbindung verbunden ist.

> **Note**
>
> Bei Application Load Balancern, die in einer lokalen Zone bereitgestellt werden, müssen sich die `ip`-Ziele in derselben lokalen Zone befinden, um Datenverkehr empfangen zu können. Weitere Informationen finden Sie unter Was sind AWS Local Zones?

Wenn Sie Ziele unter Verwendung einer Instance-ID angeben, wird Datenverkehr an Instances unter Verwendung der primären privaten IP-Adresse weitergeleitet, die in der primären Netzwerkschnittstelle für die Instance angegeben ist. Wenn Sie Ziele unter Verwendung von IP-Adressen angeben, können Sie den Datenverkehr über eine beliebige private IP-Adresse aus einer oder mehreren Netzwerkschnittstellen an eine Instance weiterleiten. Auf diese Weise können mehrere Anwendungen auf eine Instance denselben Port verwenden. Jede Netzwerkschnittstelle kann über eine eigene Sicherheitsgruppe verfügen.

Wenn der Zieltyp der Zielgruppe `lambda` lautet, können Sie eine einzelne Lambda-Funktion registrieren. Wenn der Load Balancer eine Anfrage für eine Lambda-Funktion empfängt, ruft er die Lambda-Funktion auf. Weitere Informationen finden Sie unter Verwenden Sie Lambda-Funktionen als Ziele eines Application Load Balancer.

Sie können Amazon Elastic Container Service (Amazon ECS) als Ziel für Ihren Application Load Balancer konfigurieren. Weitere Informationen finden Sie unter Verwenden eines Application Load Balancer für Amazon ECS im Amazon Elastic Container Service Developer Guide.

IP-Adresstyp

Wenn Sie eine neue Zielgruppe erstellen, können Sie den IP-Adresstyp Ihrer Zielgruppe auswählen. Dadurch wird die IP-Version gesteuert, die für die Kommunikation mit Zielen und die Überprüfung ihres Status verwendet wird.

Zielgruppen für Ihre Application Load Balancer unterstützen die folgenden IP-Adresstypen:

`ipv4`

Der Load Balancer kommuniziert mit Zielen über. IPv4

`ipv6`

Der Load Balancer kommuniziert mit Zielen über. IPv6

Überlegungen

- Der Load Balancer kommuniziert mit Zielen auf der Grundlage des IP-Adresstyps der Zielgruppe. Die Ziele einer IPv4 Zielgruppe müssen IPv4 Traffic vom Load Balancer akzeptieren und die Ziele einer IPv6 Zielgruppe müssen IPv6 Traffic vom Load Balancer akzeptieren.
- Sie können keine IPv6 Zielgruppe mit einem `ipv4` Load Balancer verwenden.
- Sie können eine Lambda-Funktion nicht bei einer IPv6 Zielgruppe registrieren.

Protokollversion

Standardmäßig senden Application Load Balancer Anforderungen über HTTP/1.1 an Ziele. Sie können die Protokollversion verwenden, um Anforderungen mit HTTP/2 oder gRPC an Ziele zu senden.

In der folgenden Tabelle sind die Ergebnisse für die Kombinationen aus Anforderungsprotokoll und Zielgruppen-Protokollversion zusammengefasst.

Anforderungsprotokoll	Protokollversion	Ergebnis
HTTP/1.1	HTTP/1.1	Herzlichen Glückwunsch
HTTP/2	HTTP/1.1	Herzlichen Glückwunsch
gRPC	HTTP/1.1	Fehler
HTTP/1.1	HTTP/2	Fehler
HTTP/2	HTTP/2	Herzlichen Glückwunsch
gRPC	HTTP/2	Erfolg, wenn Ziele gRPC unterstützen
HTTP/1.1	gRPC	Fehler

Anforderungsprotokoll	Protokollversion	Ergebnis
HTTP/2	gRPC	Erfolg bei einer POST-Anfo rderung
gRPC	gRPC	Herzlichen Glückwunsch

Überlegungen zur gRPC-Protokollversion

- Das einzige unterstützte Listener-Protokoll ist HTTPS.
- Der einzige unterstützte Aktionstyp für Listener-Regeln ist `forward`.
- Die einzigen unterstützten Zieltypen sind `instance` und `ip`.
- Der Load Balancer analysiert gRPC-Anfragen und leitet gRPC-Aufrufe basierend auf dem Paket, dem Dienst und der Methode an die entsprechenden Zielgruppen weiter.
- Der Load Balancer unterstützt unäres, clientseitiges Streaming, serverseitiges Streaming und bidirektionales Streaming.
- Sie müssen eine benutzerdefinierte Zustandsprüfungsmethode mit dem Format `/package.service/method` bereitstellen.
- Sie müssen die gRPC-Statuscodes angeben, die verwendet werden, um ein Ziel auf eine erfolgreiche Antwort zu überprüfen.
- Sie können Lambda-Funktionen nicht als Ziele verwenden.

Überlegungen zur HTTP/2-Protokollversion

- Das einzige unterstützte Listener-Protokoll ist HTTPS.
- Der einzige unterstützte Aktionstyp für Listener-Regeln ist `forward`.
- Die einzigen unterstützten Zieltypen sind `instance` und `ip`.
- Der Load Balancer unterstützt unäres, clientseitiges Streaming, serverseitiges Streaming und bidirektionales Streaming. Die maximale Anzahl von Streams pro Client-HTTP/2-Verbindung beträgt 128.

Registrierte Ziele

Ihr Load Balancer dient als zentraler Kontaktpunkt für Clients und verteilt eingehenden Datenverkehr an die fehlerfreien registrierten Ziele. Sie können jedes Ziel bei einer oder mehreren Zielgruppen registrieren.

Wenn die Nachfrage nach Ihrer Anwendung steigt, können Sie zusätzliche Ziele bei einer oder mehreren Zielgruppen registrieren, um die Nachfrage zu bewältigen. Der Load Balancer leitet den Datenverkehr an ein neu registriertes Ziel weiter, sobald der Registrierungsprozess abgeschlossen ist und das Ziel die erste Zustandsprüfung bestanden hat, unabhängig vom konfigurierten Schwellenwert.

Wenn die Nachfrage nach Ihrer Anwendung sinkt oder Sie Ihre Ziele warten müssen, können Sie die Registrierung von Zielen bei Ihren Zielgruppen aufheben. Bei der Aufhebung der Registrierung eines Ziels wird es aus Ihrer Zielgruppe entfernt. Ansonsten hat dies keine Auswirkungen auf das Ziel. Der Load Balancer stoppt das Weiterleiten von Anfragen an ein Ziel, sobald die Registrierung des Ziels aufgehoben wird. Das Ziel wechselt in den Zustand `draining`, bis laufende Anfragen abgeschlossen wurden. Sie können das Ziel erneut bei der Zielgruppe registrieren, wenn es bereit ist, wieder Anfragen zu erhalten.

Wenn Sie Ziele nach Instance-ID registrieren, können Sie Ihren Load Balancer mit einer Auto-Scaling-Gruppe verwenden. Nachdem Sie eine Zielgruppe einer Auto-Scaling-Gruppe angefügt haben, registriert Auto Scaling Ihre Ziele bei der Zielgruppe für Sie, wenn es sie startet. Weitere Informationen finden Sie unter Einen Load Balancer zu Ihrer Auto Scaling Scaling-Gruppe hinzufügen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Einschränkungen

- Sie können die IP-Adressen eines anderen Application Load Balancer nicht in derselben VPC registrieren. Wenn der andere Application Load Balancer sich in einer VPC befindet, die durch Peering mit dem Load Balancer verbunden ist, können Sie die IP-Adressen registrieren.
- Sie können Instances nicht anhand der Instance-ID registrieren, wenn sie sich in einer VPC befinden, die über ein Peering mit der Load Balancer-VPC verbunden ist (dieselbe Region oder eine andere Region). Sie können diese Instances nach IP-Adresse registrieren.

Zielgruppenattribute

Sie können eine Zielgruppe konfigurieren, indem Sie ihre Attribute bearbeiten. Weitere Informationen finden Sie unter Zielgruppenattribute bearbeiten.

Die folgenden Zielgruppenattribute werden unterstützt, wenn die Zielgruppe vom Typ `instance` oder `ip` ist:

`deregistration_delay.timeout_seconds`

Die Zeit, die Elastic Load Balancing wartet, bevor die Registrierung eines Ziels aufgehoben wird. Der Bereich liegt zwischen 0 und 3 600 Sekunden. Der Standardwert beträgt 300 Sekunden.

`load_balancing.algorithm.type`

Der Lastausgleichsalgorithmus bestimmt, wie der Load Balancer Ziele beim Routing von Anforderungen auswählt. Der Wert ist `round_robinleast_outstanding_requests`, oder`weighted_random`. Der Standardwert ist `round_robin`.

`load_balancing.algorithm.anomaly_mitigation`

Nur verfügbar, wenn `load_balancing.algorithm.type` ist`weighted_random`. Zeigt an, ob die Minimierung von Anomalien aktiviert ist. Der Wert ist entweder `on` oder `off`. Der Standardwert ist `off`.

`load_balancing.cross_zone.enabled`

Gibt an, ob zonenübergreifendes Load Balancing aktiviert ist. Der Wert ist entweder `true`, `false` oder `use_load_balancer_configuration`. Der Standardwert ist `use_load_balancer_configuration`.

`slow_start.duration_seconds`

Der Zeitraum in Sekunden, in dem der Load Balancer für ein neu registriertes Ziel einen linear zunehmenden Anteil des Datenverkehrs an die Zielgruppe sendet. Der Bereich liegt zwischen 30 und 900 Sekunden (15 Minuten). Die Standardwert ist 0 Sekunden (deaktiviert).

`stickiness.enabled`

Gibt an, ob Sticky Sessions aktiviert sind. Der Wert ist entweder `true` oder `false`. Der Standardwert ist `false`.

`stickiness.app_cookie.cookie_name`

Der Name der Anwendungs-Cookies. Der Name des Anwendungscookies darf nicht die folgenden Präfixe haben:`AWSALB`,`AWSALBAPP`, oder`AWSALBTG`; sie sind für die Verwendung durch den Load Balancer reserviert.

`stickiness.app_cookie.duration_seconds`

Die Ablaufzeit anwendungsbasierter Cookies in Sekunden. Nach Ablauf dieses Zeitraums wird das Cookie als veraltet eingestuft. Der Mindestwert ist 1 Sekunde und der Maximalwert ist 7 Tage (604800 Sekunden). Die Standardwert ist 1 Tag (86 400 Sekunden).

`stickiness.lb_cookie.duration_seconds`

Die Ablaufzeit der auf Dauer basierenden Cookies in Sekunden. Nach Ablauf dieses Zeitraums wird das Cookie als veraltet eingestuft. Der Mindestwert ist 1 Sekunde und der Maximalwert ist 7 Tage (604800 Sekunden). Die Standardwert ist 1 Tag (86 400 Sekunden).

`stickiness.type`

Die Art der „Sticky Sessions“. Die möglichen Werte sind `lb_cookie` und `app_cookie`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

Die Mindestanzahl von Zielen, die fehlerfrei sein müssen. Wenn die Anzahl der fehlerfreien Ziele unter diesem Wert liegt, markieren Sie den Knoten im DNS als fehlerhaft, sodass der Datenverkehr nur an fehlerfreie Knoten weitergeleitet wird. Die möglichen Werte sind `off` oder eine ganze Zahl von 1 bis zur maximalen Anzahl von Zielen. Wenn `off` DNS-Failaway deaktiviert ist, was bedeutet, dass der Knoten nicht aus dem DNS entfernt wird, auch wenn alle Ziele in der Zielgruppe fehlerhaft sind. Der Standardwert ist 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

Der Mindestprozentzatz der Ziele, die fehlerfrei sein müssen. Wenn der Prozentsatz fehlerfreier Ziele unter diesem Wert liegt, markieren Sie den Knoten im DNS als fehlerhaft, sodass der Datenverkehr nur an fehlerfreie Knoten weitergeleitet wird. Die möglichen Werte sind `off` oder eine Ganzzahl von 1 bis 100. Wenn `off` DNS-Failaway deaktiviert ist, was bedeutet, dass der Knoten nicht aus dem DNS entfernt wird, auch wenn alle Ziele in der Zielgruppe fehlerhaft sind. Der Standardwert ist `off`.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

Die Mindestanzahl von Zielen, die fehlerfrei sein müssen. Wenn die Anzahl fehlerfreier Ziele unter diesem Wert liegt, senden Sie Datenverkehr an alle Ziele, einschließlich nicht fehlerfreier Ziele. Der Bereich reicht von 1 bis zur maximalen Anzahl von Zielen. Der Standardwert ist 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

Der Mindestprozentzatz der Ziele, die fehlerfrei sein müssen. Wenn der Prozentsatz fehlerfreier Ziele unter diesem Wert liegt, senden Sie Datenverkehr an alle Ziele, einschließlich nicht fehlerfreier Ziele. Die möglichen Werte sind `off` oder eine Ganzzahl von 1 bis 100. Der Standardwert ist `off`.

Das folgende Zielgruppenattribut wird unterstützt, wenn der Zielgruppentyp `lambda` ist:

`lambda.multi_value_headers.enabled`

Gibt an, ob die Anfrage- und Antwort-Header, die zwischen dem Load Balancer und der Lambda-Funktion ausgetauscht werden, Arrays von Werten oder Zeichenfolgen enthalten. Die möglichen Werte sind `true` oder `false`. Der Standardwert ist `false`. Weitere Informationen finden Sie unter Header mit mehreren Werten.

Routing-Algorithmen

Ein Routing-Algorithmus ist die Methode, mit der der Load Balancer bestimmt, welche Ziele Anfragen erhalten. Der Round-Robin-Routing-Algorithmus wird standardmäßig verwendet, um Anfragen auf Zielgruppenebene weiterzuleiten. Je nach den Anforderungen Ihrer Anwendung sind auch die am wenigsten ausstehenden Anfragen und gewichtete zufällige Routing-Algorithmen verfügbar. Eine Zielgruppe kann jeweils nur über einen aktiven Routing-Algorithmus verfügen, der Routing-Algorithmus kann jedoch bei Bedarf aktualisiert werden.

Wenn Sie Sticky Sessions aktivieren, wird der ausgewählte Routing-Algorithmus für die anfängliche Zielauswahl verwendet. Künftige Anfragen von demselben Client werden an dasselbe Ziel weitergeleitet, wobei der ausgewählte Routing-Algorithmus umgangen wird.

Rundenturnier

- Der Round-Robin-Routing-Algorithmus leitet Anfragen gleichmäßig in einer sequentiellen Reihenfolge an gesunde Ziele in der Zielgruppe weiter.

- Dieser Algorithmus wird häufig verwendet, wenn die eingehenden Anfragen eine ähnliche Komplexität aufweisen, die registrierten Ziele eine ähnliche Verarbeitungsfähigkeit aufweisen oder wenn Sie Anfragen gleichmäßig auf die Ziele verteilen müssen.

Am wenigsten ausstehende Anfragen

- Der Routing-Algorithmus für die wenigsten ausstehenden Anfragen leitet Anfragen an die Ziele mit der geringsten Anzahl an laufenden Anfragen weiter.
- Dieser Algorithmus wird häufig verwendet, wenn die eingehenden Anfragen unterschiedlich komplex sind und die Verarbeitungskapazität der registrierten Ziele unterschiedlich ist.
- Wenn ein Load Balancer, der HTTP/2 unterstützt, Ziele verwendet, die nur HTTP/1.1 unterstützen, konvertiert er die Anfrage in mehrere HTTP/1.1-Anfragen. In dieser Konfiguration behandelt der Algorithmus für die wenigsten ausstehenden Anfragen jede HTTP/2-Anfrage als mehrere Anfragen.
- Bei Verwendung wird WebSockets das Ziel anhand des Algorithmus für die wenigsten ausstehenden Anfragen ausgewählt. Nach der Auswahl stellt der Load Balancer eine Verbindung zum Ziel her und sendet alle Nachrichten über diese Verbindung.
- Der Routing-Algorithmus für die wenigsten ausstehenden Anfragen kann nicht im langsamen Startmodus verwendet werden.

Zufällig gewichtet

- Der gewichtete Zufalls-Routing-Algorithmus leitet Anfragen gleichmäßig und in zufälliger Reihenfolge an gesunde Ziele in der Zielgruppe weiter.
- Dieser Algorithmus unterstützt die Minimierung von ATW-Anomalien (Automatic Target Weights).
- Der Algorithmus für gewichtetes zufälliges Routing kann nicht im langsamen Startmodus verwendet werden.
- Der Algorithmus für gewichtetes zufälliges Routing kann nicht für Sticky-Sessions verwendet werden.

Ändern Sie den Routing-Algorithmus einer Zielgruppe

Sie können den Routing-Algorithmus für Ihre Zielgruppe jederzeit ändern.

Um den Routing-Algorithmus mit der neuen Konsole zu ändern

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Detailseite der Zielgruppen auf der Registerkarte Attribute die Option Bearbeiten aus.
5. Wählen Sie auf der Seite Zielgruppenattribute bearbeiten im Abschnitt Verkehrskonfiguration unter Load Balancing Algorithm die Optionen Round Robin, Least Outstanding Requests oder Weighted Random aus.
6. Wählen Sie Änderungen speichern aus.

Um den Routing-Algorithmus mit dem zu ändern AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit dem `load_balancing.algorithm.type` Attribut.

Zustand der Zielgruppe

Standardmäßig gilt eine Zielgruppe als fehlerfrei, solange sie mindestens ein fehlerfreies Ziel hat. Wenn Sie eine große Flotte haben, reicht es nicht aus, nur ein fehlerfreies Ziel zu haben, das den Datenverkehr bereitstellt. Stattdessen können Sie eine Mindestanzahl oder einen Prozentsatz von Zielen angeben, die fehlerfrei sein müssen, und angeben, welche Aktionen der Load Balancer ergreift, wenn die fehlerfreien Ziele unter den angegebenen Schwellenwert fallen. Dies verbessert die Verfügbarkeit Ihrer Anwendung.

Inhalt

- Maßnahmen bei fehlerhaftem Zustand
- Anforderungen und Überlegungen
- Überwachen
- Beispiel
- Verwenden des Route-53-DNS-Failover für Ihren Load Balancer

Maßnahmen bei fehlerhaftem Zustand

Sie können fehlerhafte Schwellenwerte für die folgenden Aktionen konfigurieren:

- DNS-Failover — Wenn die fehlerfreien Ziele in einer Zone unter den Schwellenwert fallen, markieren wir die IP-Adressen des Load Balancer-Knotens für die Zone im DNS als fehlerhaft. Wenn Clients den DNS-Namen des Load Balancers auflösen, wird der Datenverkehr daher nur an fehlerfreie Zonen weitergeleitet.
- Routing-Failover — Wenn die fehlerfreien Ziele in einer Zone unter den Schwellenwert fallen, sendet der Load Balancer Traffic an alle Ziele, die für den Load Balancer-Knoten verfügbar sind, einschließlich fehlerhafter Ziele. Dies erhöht die Wahrscheinlichkeit, dass eine Client-Verbindung erfolgreich ist, insbesondere wenn Ziele vorübergehend die Integritätsprüfungen nicht bestehen, und verringert das Risiko, dass die fehlerfreien Ziele überlastet werden.

Anforderungen und Überlegungen

- Dieses Feature kann nicht für Zielgruppen verwendet werden, bei denen das Ziel eine Lambda-Funktion ist. Wenn der Application Load Balancer das Ziel für einen Network Load Balancer oder Global Accelerator ist, konfigurieren Sie keinen Schwellenwert für ein DNS-Failover.
- Wenn Sie beide Arten von Schwellenwerten für eine Aktion angeben (Anzahl und Prozentsatz), ergreift der Load Balancer die Aktion, wenn einer der Schwellenwerte überschritten wird.
- Wenn Sie Schwellenwerte für beide Aktionen angeben, muss der Schwellenwert für DNS-Failover größer oder gleich dem Schwellenwert für Routing-Failover sein, sodass der DNS-Failover entweder mit oder vor dem Routing-Failover erfolgt.
- Wenn Sie den Schwellenwert als Prozentsatz angeben, berechnen wir den Wert dynamisch auf der Grundlage der Gesamtzahl der Ziele, die bei den Zielgruppen registriert sind.
- Die Gesamtzahl der Ziele hängt davon ab, ob zonenübergreifendes Load Balancing deaktiviert oder aktiviert ist. Wenn zonenübergreifendes Load Balancing deaktiviert ist, sendet jeder Knoten Datenverkehr nur an die Ziele in seiner eigenen Zone, was bedeutet, dass die Schwellenwerte für die Anzahl der Ziele in jeder aktivierten Zone separat gelten. Wenn zonenübergreifende Load Balancing aktiviert ist, sendet jeder Knoten Datenverkehr an alle aktivierten Ziele, was bedeutet, dass die angegebenen Schwellenwerte für die Gesamtanzahl der Ziele in allen aktivierten Zonen gelten. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing für Application Load Balancer Balancer-Zielgruppen.
- Wenn ein DNS-Failover auftritt, wirkt sich dies auf alle Zielgruppen aus, die dem Load Balancer zugeordnet sind. Stellen Sie sicher, dass Sie in Ihren verbleibenden Zonen über genügend Kapazität verfügen, um diesen zusätzlichen Datenverkehr zu bewältigen, insbesondere wenn das zonenübergreifende Load Balancing deaktiviert ist.

- Beim DNS-Failover entfernen wir die IP-Adressen der fehlerhaften Zonen aus dem DNS-Hostnamen für den Load Balancer. Der DNS-Cache des lokalen Clients kann diese IP-Adressen jedoch enthalten, bis die time-to-live (TTL) im DNS-Eintrag abläuft (60 Sekunden).
- Wenn beim DNS-Failover mehrere Zielgruppen an einen Application Load Balancer angeschlossen sind und eine Zielgruppe in einer Zone fehlerhaft ist, sind DNS-Zustandsprüfungen erfolgreich, wenn mindestens eine andere Zielgruppe in dieser Zone fehlerfrei ist.
- Wenn beim DNS-Failover alle Load-Balancer-Zonen als fehlerhaft eingestuft werden, sendet der Load Balancer Datenverkehr an alle Zonen, einschließlich der fehlerhaften Zonen.
- Neben der Frage, ob genügend fehlerfreie Ziele vorhanden sind, die zu einem DNS-Failover führen könnten, gibt es noch andere Faktoren, z. B. den Zustand der Zone.

Überwachen

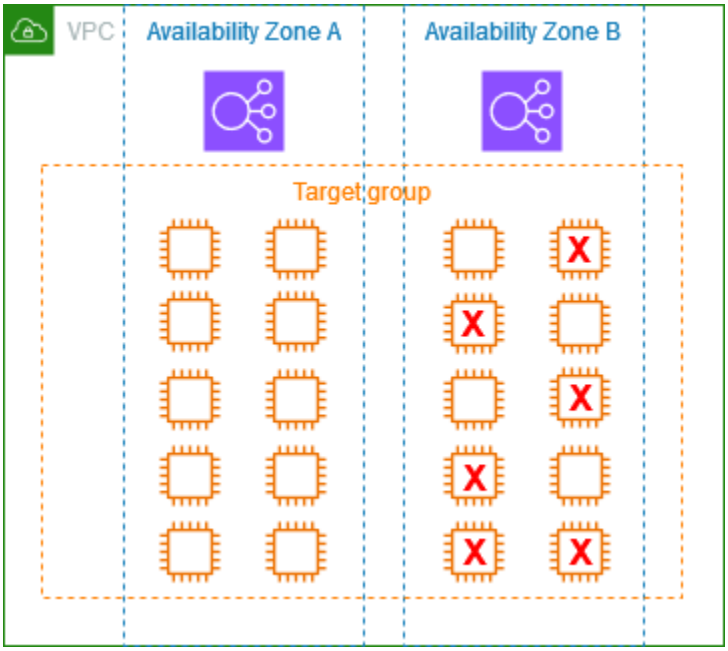
Informationen zur Überwachung des Zustands Ihrer Zielgruppen finden Sie unter CloudWatch Kennzahlen zur Zielgruppengesundheit.

Beispiel

Im folgenden Beispiel wird veranschaulicht, wie Zustandseinstellungen für Zielgruppen angewendet werden.

Szenario

- Ein Load Balancer, der zwei Availability Zones, A und B, unterstützt
- Jede Availability Zone enthält 10 registrierte Ziele
- Die Zielgruppe hat die folgenden Zustandseinstellungen für Zielgruppen:
  - DNS-Failover – 50 %
  - Routing-Failover – 50 %
- Sechs Ziele fallen in der Availability Zone B aus



Wenn zonenübergreifendes Load Balancing deaktiviert ist

- Der Load-Balancer-Knoten in jeder Availability Zone kann Datenverkehr nur an die 10 Ziele in seiner Availability Zone senden.
- In der Availability Zone A gibt es 10 fehlerfreie Ziele, sodass der erforderliche Prozentsatz fehlerfreier Ziele erreicht wird. Der Load Balancer verteilt weiterhin den Datenverkehr zwischen den 10 fehlerfreien Zielen.
- In der Availability Zone B gibt es nur 4 fehlerfreie Ziele, was 40 % der Ziele für den Load-Balancer-Knoten in Availability Zone B entspricht. Da dies weniger ist als der erforderliche Prozentsatz fehlerfreier Ziele, ergreift der Load Balancer die folgenden Aktionen:
  - DNS-Failover – Die Availability Zone B ist im DNS als fehlerhaft markiert. Da Clients den Load-Balancer-Namen nicht in den Load-Balancer-Knoten in Availability Zone B auflösen können und Availability Zone A fehlerfrei ist, senden Clients neue Verbindungen zur Availability Zone A.
  - Routing-Failover – Wenn neue Verbindungen explizit an Availability Zone B gesendet werden, verteilt der Load Balancer den Datenverkehr an alle Ziele in Availability Zone B, einschließlich der fehlerhaften Ziele. Dadurch werden Ausfälle bei den verbleibenden fehlerlosen Zielen verhindert.

Wenn zonenübergreifendes Load Balancing aktiviert ist

- Jeder Load-Balancer-Knoten kann Datenverkehr an alle 20 registrierten Ziele in beiden Availability Zones senden.

- Es gibt 10 fehlerfreie Ziele in Availability Zone A und 4 fehlerfreie Ziele in Availability Zone B, also insgesamt 14 fehlerfreie Ziele. Das sind 70 % der Ziele für die Load-Balancer-Knoten in beiden Availability Zones, wodurch der erforderliche Prozentsatz fehlerfreier Ziele erreicht wird.
- Der Load Balancer verteilt den Datenverkehr zwischen den 14 fehlerfreien Zielen in beiden Availability Zones.

Verwenden des Route-53-DNS-Failover für Ihren Load Balancer

Wenn Sie mithilfe von Route 53 DNS-Abfragen an Ihren Load Balancer leiten, können Sie mithilfe von Route 53 auch DNS-Failover für Ihren Load Balancer konfigurieren. In einer Failover-Konfiguration prüft Route 53 die Integrität der Zielgruppen für den Load Balancer, um zu ermitteln, ob diese verfügbar sind. Wenn keine funktionsfähigen Ziele für den Load Balancer registriert sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 den Datenverkehr an eine andere verfügbare Ressource, z. B. einen fehlerfreien Load Balancer oder eine statische Website in Amazon S3, weiter.

Beispiel: Sie haben eine Webanwendung `www.example.com` und möchten, dass redundante Instances hinter zwei Load Balancers in verschiedenen Regionen laufen. Sie möchten, dass der Datenverkehr in erster Linie auf den Load Balancer in einer Region weitergeleitet wird, und der Load Balancer in der anderen Region soll bei Ausfällen als Sicherung dienen. Wenn Sie DNS Failover konfigurieren, können Sie einen primären und einen sekundären (Sicherung) Load Balancer festlegen. Route 53 leitet den Datenverkehr direkt zum primären Load Balancer, und wenn dieser nicht verfügbar ist, wird der Datenverkehr zum sekundären Load Balancer geleitet.

Wie funktioniert Evaluation Target Health

- Wenn die Option Zielintegrität auswerten für einen Aliaseintrag für einen Application Load Balancer aktiviert ist, bewertet Route 53 den Zustand der durch den `alias target` Wert angegebenen Ressource. `Yes` Route 53 verwendet die Zustandsprüfungen der Zielgruppe.
- Wenn alle an einen Application Load Balancer angeschlossenen Zielgruppen fehlerfrei sind, markiert Route 53 den Aliaseintrag als fehlerfrei. Wenn Sie einen Schwellenwert für eine Zielgruppe konfiguriert haben und diese diesen Schwellenwert erreicht, besteht sie die Integritätsprüfungen. Andernfalls besteht eine Zielgruppe, wenn sie mindestens ein gesundes Ziel enthält, die Integritätsprüfungen. Wenn die Zustandsprüfungen erfolgreich sind, gibt Route 53 Datensätze gemäß Ihrer Routing-Richtlinie zurück. Wenn eine Failover-Routing-Richtlinie verwendet wird, gibt Route 53 den primären Datensatz zurück.
- Wenn eine der an einen Application Load Balancer angehängten Zielgruppen fehlerhaft ist, besteht der Aliaseintrag die Route 53-Zustandsprüfung (Fail-Open) nicht. Wenn Sie „Zielstatus auswerten“

verwenden, leitet die Failover-Routing-Richtlinie den Datenverkehr an die sekundäre Ressource weiter.

- Wenn alle an einen Application Load Balancer angehängten Zielgruppen leer sind (keine Ziele), betrachtet Route 53 den Datensatz als fehlerhaft (Fail-Open). Wenn die Option Zielstatus auswerten verwendet wird, leitet die Failover-Routing-Richtlinie den Datenverkehr an die sekundäre Ressource weiter.

Weitere Informationen finden Sie unter Verwenden von Load Balancer-Gesundheitsgrenzwerten für Zielgruppen zur Verbesserung der Verfügbarkeit im AWS Blog und Konfiguration von DNS-Failover im Amazon Route 53-Entwicklerhandbuch.

Erstellen Sie eine Zielgruppe für Ihren Application Load Balancer

Sie registrieren Ihre Ziele bei einer Zielgruppe. Der Load Balancer sendet standardmäßig Anfragen an registrierte Ziele mithilfe des Ports und des Protokolls, den bzw. das Sie für die Zielgruppe angegeben haben. Sie können diesen Port überschreiben, wenn Sie jedes Ziel bei der Zielgruppe registrieren.

Nachdem Sie eine Zielgruppe erstellt haben, können Sie Tags hinzufügen.

Um Datenverkehr an die Ziele in einer Zielgruppe weiterzuleiten, geben Sie die Zielgruppe in einer Aktion an, wenn Sie einen Listener erstellen oder eine Regel für den Listener erstellen. Weitere Informationen finden Sie unter Listener-Regeln. Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Application Load Balancer angehören. Um eine Zielgruppe mit einem Load Balancer zu verwenden, müssen Sie sicherstellen, dass die Zielgruppe nicht von einem Listener verwendet wird, der einem anderen Load Balancer angehört.

Sie können jederzeit Ziele zu Ihrer Zielgruppe hinzufügen oder aus dieser entfernen. Weitere Informationen finden Sie unter Registrieren Sie Ziele bei Ihrer Application Load Balancer Balancer-Zielgruppe. Sie können auch die Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern. Weitere Informationen finden Sie unter Aktualisieren Sie die Einstellungen für die Integritätsprüfung einer Application Load Balancer Balancer-Zielgruppe.

Erstellen einer Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.

3. Wählen Sie Zielgruppe erstellen aus.
4. Wählen Sie für Zieltyp auswählen die Option Instances aus, um Ziele nach Instance-ID zu registrieren, IP-Adressen, um Ziele nach IP-Adresse zu registrieren, oder Lambda-Funktion, um eine Lambda-Funktion als Ziel zu registrieren.
5. Geben Sie im Feld Target group name (Zielgruppenname) einen Namen für die neue Zielgruppe ein. Dieser Name muss für jede Region und jedes Konto eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen oder Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.
6. (Optional) Ändern Sie ggf. die Standardwerte im Feld Protocol (Protokoll) und Port nach Bedarf.
7. Wenn der Zieltyp Instances oder IP-Adressen ist, wählen Sie IPv4oder IPv6als IP-Adresstyp, andernfalls fahren Sie mit dem nächsten Schritt fort.

   Beachten Sie, dass nur Ziele, die den ausgewählten IP-Adresstyp haben, in diese Zielgruppe eingefügt werden können. Der IP-Adresstyp kann nicht geändert werden, nachdem die Zielgruppe erstellt wurde.
8. Wählen Sie im Feld VPC eine Virtual Private Cloud (VPC) aus. Beachten Sie, dass für IP-Adressen die Zieltypen zur Auswahl VPCs stehen, die den IP-Adresstyp unterstützen, den Sie im vorherigen Schritt ausgewählt haben.
9. (Optional) Ändern Sie den Standardwert im Feld Protokollversion nach Bedarf.
10. (Optional) Behalten Sie im Abschnitt Zustandsprüfungen die Standardeinstellungen nach Bedarf bei.
11. Wenn der Zieltyp Lambda-Funktion ist, können Sie Zustandsprüfungen aktivieren, indem Sie im Abschnitt Zustandsprüfungen die Option Aktivieren auswählen.
12. (Optional) Fügen Sie einen oder mehrere Tags wie folgt hinzu:

    a. Erweitern Sie den Abschnitt Tags.

    b. Wählen Sie Add tag.

    c. Geben Sie den Tag-Schlüssel und den Tag-Wert ein.
13. Wählen Sie Weiter aus.
14. (Optional) Fügen Sie ein oder mehrere Ziele wie folgt hinzu:

    - Wenn der Zieltyp Instances ist, wählen Sie eine oder mehrere Instances aus, geben Sie einen oder mehrere Ports ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus.

Hinweis: Den Instances muss eine zugewiesene IPv6 Primäradresse zugewiesen sein, um bei einer IPv6 Zielgruppe registriert zu werden.

- Wenn der Zieltyp IP-Adressen lautet, gehen Sie wie folgt vor:

  a. Wählen Sie eine Netzwerk-VPC in der Liste aus oder wählen Sie Andere private IP-Adresse aus.

  b. Geben Sie die IP-Adresse manuell ein oder suchen Sie die IP-Adresse anhand der Instance-Details. Sie können bis zu fünf IP-Adressen gleichzeitig eingeben.

  c. Geben Sie die Ports für die Weiterleitung des Datenverkehrs an die angegebenen IP-Adressen ein.

  d. Wählen Sie Schließen Sie die unten angeführten als ausstehend ein aus.

- Wenn der Zieltyp eine Lambda-Funktion ist, geben Sie eine einzelne Lambda-Funktion an oder lassen Sie diesen Schritt aus und geben Sie später eine Lambda-Funktion an.

15. Wählen Sie Zielgruppe erstellen aus.
16. (Optional) Sie können die Zielgruppe in einer Listener-Regel angeben. Weitere Informationen finden Sie unter Listener-Regeln.

Um eine Zielgruppe mit dem zu erstellen AWS CLI

Verwenden Sie den create-target-groupBefehl, um die Zielgruppe zu erstellen, den Befehl add-tags, um Ihre Zielgruppe zu taggen, und den Befehl register-targets, um Ziele hinzuzufügen.

Aktualisieren Sie die Gesundheitseinstellungen für Ihre Application Load Balancer Balancer-Zielgruppe

Sie können die Zustandseinstellungen für Ihre Zielgruppe wie folgt ändern.

So ändern Sie die Zustandseinstellungen für eine Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancer aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.

5. Überprüfen Sie, ob zonenübergreifendes Load Balancing aktiviert oder deaktiviert ist. Aktualisieren Sie diese Einstellung nach Bedarf, um sicherzustellen, dass Sie über genügend Kapazität verfügen, um den zusätzlichen Datenverkehr zu bewältigen, falls eine Zone ausfällt.
6. Erweitern Sie die Anforderungen an den Zustand der Zielgruppe.
7. Wir empfehlen, dass Sie als Konfigurationstyp die Option Einheitliche Konfiguration wählen, wodurch für beide Aktionen derselbe Schwellenwert festgelegt wird.
8. Führen Sie für Anforderungen für fehlerfreie Zustände einen der folgenden Schritte aus:
   - Wählen Sie Mindestanzahl fehlerfreier Ziele aus und geben Sie dann eine Zahl zwischen 1 und der maximalen Anzahl von Zielen für Ihre Zielgruppe ein.
   - Wählen Sie Mindestprozentsatz fehlerfreier Ziele und geben Sie dann eine Zahl zwischen 1 und 100 ein.
9. Wählen Sie Änderungen speichern aus.

Um die Gesundheitseinstellungen für Zielgruppen zu ändern, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributes-Befehl. Im folgenden Beispiel wird der Schwellenwert für den fehlerfreien Zustand für beide Aktionen mit einem fehlerhaften Zustand auf 50 % festgelegt.

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

Gesundheitschecks für Application Load Balancer Balancer-Zielgruppen

Ihr Application Load Balancer sendet regelmäßig Anforderungen an die registrierten Ziele, um deren Status zu überprüfen. Diese Tests werden als Zustandsprüfungen bezeichnet.

Jeder Load Balancer-Knoten leitet Anfragen nur an die betriebsbereiten Ziele in den aktivierten Availability Zones des Balancer. Jeder Load Balancer-Knoten überprüft den Zustand jedes Ziels mit den Zustandsprüfungseinstellungen für die Zielgruppen, in denen das Ziel registriert ist. Nachdem

Ihr Ziel registriert wurde, muss es die Zustandsprüfung fehlerfrei bestehen, um als stabil eingestuft zu werden. Nachdem die einzelnen Zustandsprüfungen abgeschlossen wurden, schließt der Load Balancer-Knoten die Verbindung, die für die Zustandsprüfung eingerichtet wurde.

Wenn eine Zielgruppe nur fehlerhafte registrierte Ziele enthält, leitet der Load Balancer Anforderungen an all diese Ziele weiter, unabhängig von ihrem Zustandstatus. Das bedeutet, dass sich der Load Balancer nicht öffnen lässt, wenn alle Ziele gleichzeitig die Zustandsprüfungen in allen aktivierten Availability Zones nicht bestehen. Das Fail-Open hat zur Folge, dass der Datenverkehr an alle Ziele in allen aktivierten Availability Zones unabhängig von deren Zustandsstatus auf der Grundlage des Load-Balancing-Algorithmus aktiviert wird.

Gesundheitschecks werden nicht unterstützt WebSockets.

Weitere Informationen finden Sie unter the section called “Zustand der Zielgruppe”.

Zustandsprüfungseinstellungen

Sie können Zustandsprüfungen für die Ziele in einer Zielgruppe konfigurieren, wie in der folgenden Tabelle beschrieben. Die in der Tabelle verwendeten Einstellungsnamen sind die in der API verwendeten Namen. Der Load Balancer sendet alle HealthCheckIntervalSecondsSekunden eine Integritätsprüfanforderung an jedes registrierte Ziel. Dabei werden der angegebene Port, das Protokoll und der Pfad zur Integritätsprüfung verwendet. Jede Anfrage nach einer Zustandsprüfung ist unabhängig und das Ergebnis hält über das gesamte Intervall an. Die Zeit, die das Ziel für die Antwort benötigt, hat keinen Einfluss auf das Intervall für die nächste Anfrage zur Zustandsprüfung. Wenn die Zustandsprüfungen mehrere UnhealthyThresholdCountaufeinanderfolgende Fehler überschreiten, nimmt der Load Balancer das Ziel außer Betrieb. Wenn die Zustandsprüfungen mehrere HealthyThresholdCountaufeinanderfolgende Erfolge überschreiten, nimmt der Load Balancer das Ziel wieder in Betrieb.

Beachten Sie, dass, wenn Sie die Registrierung eines Ziels aufheben, dieser Wert HealthyHostCountzwar abnimmt, aber nicht zunimmt. UnhealthyHostCount

Einstellung	Beschreibung
HealthCheckProtocol	Das Protokoll, das der Load Balancer für die Zustandsprüfungen der Ziele verwendet. Für Application Load Balancer sind die möglichen Protokolle HTTP und HTTPS. Das Standardp rotokoll ist HTTP.

Einstellung	Beschreibung
	Diese Protokolle verwenden die HTTP-GET-Methode, um Gibt den Pfad an, um Zustandsprüfungsanforderungen zu senden.
HealthCheckPort	Der Port, den der Load Balancer für die Zustandsprüfungen der Ziele verwendet . Standardmäßig wird der Port verwendet, auf dem jedes Ziel Datenverkehr vom Load Balancer empfängt.
HealthCheckPath	Das Ziel für Zustandsprüfungen der Ziele. Wenn die Protokollversion HTTP/1.1 oder HTTP/2 ist, geben Sie einen gültigen URI an (/Pfad?Abfrage). Der Standardwert ist /. Wenn die Protokollversion gRPC ist, geben Sie den Pfad einer benutzerdefinierten Zustandsprüfungsmethode mit dem Format `/package.service/method` an. Der Standardwert ist `/AWS.ALB/healthcheck` .
HealthCheckTimeoutSeconds	Die Anzahl der Sekunden, in denen keine Antwort von einem Ziel bedeutet, dass die Zustandsprüfung fehlgeschlagen ist. Der Bereich liegt zwischen 2 und 120 Sekunden. Standardmäßig ist bei dem Zieltyp `instance` oder `ip`ein Zeitraum von 5 Sekunden und bei dem Zieltyp `lambda` ein Zeitraum von 30 Sekunden festgelegt.

Einstellung	Beschreibung
HealthCheckIntervalSeconds	Der etwaige Zeitraum in Sekunden zwischen den Zustandsprüfungen der einzelnen Ziele. Der Bereich liegt zwischen 5 und 300 Sekunden. Standardmäßig ist bei dem Zieltyp `instance` oder `ip`ein Zeitraum von 30 Sekunden und bei dem Zieltyp `lambda` ein Zeitraum von 35 Sekunden festgelegt.
HealthyThresholdCount	Die Anzahl der aufeinanderfolgenden erfolgreichen Zustandsprüfungen, die erforderlich ist, damit ein fehlerhaftes Ziel als stabil eingestuft wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 5.
UnhealthyThresholdCount	Die Anzahl fortlaufender fehlgeschlagener Zustandsprüfungen, die erforderlich ist, damit ein Ziel als nicht betriebsbereit eingestuft wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 2.

Einstellung	Beschreibung
Matcher	Die Codes, die verwendet werden, um ein Ziel auf eine erfolgreiche Antwort zu überprüfen. Diese werden in der Konsole als Erfolgscodes bezeichnet. Wenn die Protokollversion HTTP/1.1 oder HTTP/2 ist, liegen die möglichen Werte zwischen 200 und 499. Sie können mehrere Werte angeben (z. B. "200,202") oder einen Wertebereich (z. B. "200-299"). Der Standardwert ist 200. Wenn die Protokollversion gRPC ist, liegen die möglichen Werte zwischen 0 und 99. Sie können mehrere Werte angeben (z. B. "0,1") oder einen Wertebereich (z. B. "0-5"). Der Standardwert lautet 12.

Zustandsstatus des Ziels

Bevor der Load Balancer eine Zustandsprüfungsanforderung an ein Ziel sendet, müssen Sie dieses Ziel in einer Zielgruppe registrieren, die Zielgruppe in einer Listener-Regel spezifizieren und sicherstellen, dass die Availability Zone des Ziels für den Load Balancer aktiviert ist. Damit ein Ziel Anforderungen vom Load Balancer erhalten kann, muss es die anfänglichen Zustandsprüfungen bestehen. Nachdem ein Ziel die anfänglichen Zustandsprüfungen bestanden hat, ist sein Status `Healthy`.

Die folgende Tabelle beschreibt die möglichen Werte für den Zustandsstatus eines registrierten Ziels.

Wert	Beschreibung
`initial`	Der Load Balancer befindet sich im Prozess der Registrierung eines Ziels oder der Durchführung der anfänglichen Zustandsprüfungen für das Ziel.

Wert	Beschreibung
	Zugehörige Ursachencodes: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	Das Ziel ist fehlerfrei. Zugehörige Ursachencodes: Keine
`unhealthy`	Das Ziel hat nicht auf eine Zustandsprüfung geantwortet oder die Zustandsprüfung ist fehlgeschlagen. Zugehörige Ursachencodes: `Target.ResponseCodeMismatch` | `Target.Timeout` | `Target.FailedHealthChecks` | `Elb.InternalError`
`unused`	Das Ziel wurde nicht für eine Zielgruppe registriert, die Zielgruppe wird nicht in einer Listener-Regel verwendet oder das Ziel befindet sich in einer Availability Zone, die nicht aktiviert ist, oder das Ziel sich im Status „Angehalten“ oder „Beendet“. Zugehörige Ursachencodes: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`
`draining`	Die Registrierung für das Ziel wird aufgehoben, und Connection Draining wird durchgeführt. Zugehöriger Ursachencode: `Target.DeregistrationInProgress`
`unavailable`	Die Zustandsprüfungen sind für die Zielgruppe deaktiviert. Zugehöriger Ursachencode: `Target.HealthCheckDisabled`

Ursachencodes für Zustandsprüfungen

Ist der Status eines Ziels ein anderer Wert als `Healthy`, gibt die API einen Ursachencode und eine Beschreibung des Problems zurück und die Konsole zeigt die gleiche Beschreibung an. Ursachencodes, die mit `Elb` beginnen, haben ihren Ursprung auf dem Load Balancer, und Ursachencodes, die mit `Target` beginnen, haben ihren Ursprung auf der Seite des Ziels. Weitere Informationen zu möglichen Ursachen für Fehler bei der Zustandsprüfung finden Sie unter Fehlerbehebung.

Ursachencode	Beschreibung
`Elb.InitialHealthChecking`	Anfängliche Zustandsprüfungen in Bearbeitung
`Elb.InternalError`	Zustandsprüfungen aufgrund eines internen Fehles fehlgeschlagen
`Elb.RegistrationInProgress`	Zielregistrierung wird durchgeführt
`Target.DeregistrationInProgress`	Zielregistrierung wird aufgehoben
`Target.FailedHealthChecks`	Zustandsprüfungen fehlgeschlagen
`Target.HealthCheckDisabled`	Zustandsprüfungen sind deaktiviert
`Target.InvalidState`	Ziel hat den Status „Angehalten“ Ziel hat den Status „Beendet“ Ziel hat den Status „Beendet oder Angehalten“ Ziel hat den Status „Ungültig“
`Target.IpUnusable`	Die IP-Adresse kann nicht als Ziel verwendet werden, da sie von einem Load Balancer verwendet wird.
`Target.NotInUse`	Zielgruppe ist nicht konfiguriert, um Verkehr vom Load Balancer zu erhalten

Ursachencode	Beschreibung
	Ziel ist in einer Availability Zone, die nicht für den Load Balancer aktiviert ist
`Target.NotRegistered`	Ziel ist nicht in der Zielgruppe registriert
`Target.ResponseCodeMismatch`	Zustandsprüfungen sind mit diesen Codes fehlgesch lagen: [Code]
`Target.Timeout`	Zeitlimit für Anforderung überschritten

Überprüfen Sie den Zustand Ihrer Application Load Balancer Balancer-Ziele

Sie können den Zustand der Ziele, die in Ihren Zielgruppen registriert sind, überprüfen.

Überprüfen des Zustands Ihrer Ziele mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. In der Registerkarte Targets (Ziele) gibt die Spalte Status den Status der einzelnen Ziele wider.
5. Wenn der Status einen anderen Wert als `Healthy` hat, enthält die Spalte Statusdetails weitere Informationen. Hilfe bei fehlgeschlagenen Zustandsprüfungen finden Sie unter Fehlerbehebung.

Um den Zustand Ihrer Ziele zu überprüfen, verwenden Sie AWS CLI

Verwenden Sie den describe-target-health-Befehl. Die Ausgabe dieses Befehls enthält den Zustand des Ziels. Wenn der Status einen anderen Wert als `Healthy` aufweist, enthält die Ausgabe auch einen Ursachencode.

So erhalten Sie E-Mail-Benachrichtigungen über fehlerhafte Ziele

Verwenden Sie CloudWatch Alarme, um eine Lambda-Funktion auszulösen, um Details über fehlerhafte Ziele zu senden. step-by-stepAnweisungen finden Sie im folgenden Blogbeitrag: Identifizieren fehlerhafter Ziele Ihres Load Balancers.

Aktualisieren Sie die Einstellungen für die Integritätsprüfung einer Application Load Balancer Balancer-Zielgruppe

Sie können die Einstellungen für den Gesundheitscheck für Ihre Zielgruppe jederzeit aktualisieren.

Um die Einstellungen für die Gesundheitsprüfung einer Zielgruppe mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Einstellungen für die Zustandsprüfung die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Einstellungen für die Zustandsprüfung bearbeiten die Einstellungen nach Bedarf und wählen Sie dann Änderungen speichern.

Um die Einstellungen für den Gesundheitscheck einer Zielgruppe zu ändern, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-Befehl.

Zielgruppenattribute für Ihren Application Load Balancer bearbeiten

Nachdem Sie eine Zielgruppe für Ihren Application Load Balancer erstellt haben, können Sie deren Zielgruppenattribute bearbeiten.

Zielgruppenattribute

- Verzögerung der Registrierungsaufhebung
- Modus des langsamen Hochfahrens
- Zonenübergreifendes Load Balancing für Application Load Balancer Balancer-Zielgruppen
- Automatische Zielgewichte (ATW)
- Sticky Sessions für Ihren Application Load Balancer

Verzögerung der Registrierungsaufhebung

Elastic Load Balancing stoppt das Senden von Anforderungen an Ziele, deren Registrierung aufgehoben wird. Standardmäßig wartet Elastic Load Balancing 300 Sekunden, bevor die Registrierungsaufhebung abgeschlossen wird. So können laufende Anforderungen an das Ziel abgeschlossen werden. Um die Zeitdauer zu ändern, die Elastic Load Balancing wartet, müssen Sie den Wert für die Verzögerung der Registrierungsaufhebung anpassen.

Der ursprüngliche Zustand eines Ziels, dessen Registrierung aufgehoben wird, lautet `draining`. Nach Ablauf der Verzögerung der Registrierungsaufhebung wird die Registrierungsaufhebung abgeschlossen und der Zustand es Ziels lautet `unused`. Wenn das Ziel Teil einer Auto-Scaling-Gruppe ist, kann es beendet und ersetzt werden.

Falls ein Ziel, dessen Registrierung aufgehoben wird, keine aktiven Anforderungen und keine aktiven Verbindungen aufweist, wird der Aufhebungsprozess von Elastic Load Balancing sofort abgeschlossen, ohne auf das Verstreichen der Verzögerung für die Registrierungsaufhebung zu warten. Auch wenn die Zielregistrierung aufgehoben wurde, wird bis zum Ablauf des Timeouts der Verzögerung der Registrierungsaufhebung `draining` als Status des Ziels angezeigt. Nach Ablauf des Timeouts wechselt das Ziel in einen `unused`-Zustand.

Wenn ein Ziel, dessen Registrierung aufgehoben wird, die Verbindung beendet, bevor die Verzögerung der Registrierungsaufhebung abgelaufen ist, erhält der Client eine 500-Level-Fehlerantwort.

So aktualisieren Sie den Wert für die Verzögerung der Registrierungsaufhebung mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Attribute bearbeiten den Wert für Abmeldeverzögerung nach Bedarf.
6. Wählen Sie Änderungen speichern aus.

Um den Wert für die Verzögerung bei der Abmeldung zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit dem `deregistration_delay.timeout_seconds` Attribut.

Modus des langsamen Hochfahrens

Standardmäßig beginnt ein Ziel mit dem Empfang seines vollständigen Anteils an Anfragen, sobald es bei einer Zielgruppe registriert ist und die anfängliche Zustandsprüfung bestanden hat. Der Modus des langsamen Hochfahrens bietet Zielen mehr Zeit zum Warmlaufen, bevor der Load Balancer ihnen den vollständigen Anteil an Anfragen sendet.

Nachdem Sie das langsame Hochfahren für eine Zielgruppe aktiviert haben, wechseln die Ziele in den Modus des langsamen Hochfahrens, wenn sie von der Zielgruppe als fehlerfrei eingestuft werden. Ein Ziel im Modus des langsamen Hochfahrens beendet diesen, wenn die konfigurierte Dauer des langsamen Hochfahrens abgelaufen ist oder das Ziel fehlerhaft ist. Der Load Balancer erhöht linear die Anzahl von Anfragen, die er im Modus des langsamen Hochfahrens an ein Ziel senden kann. Nachdem ein fehlerfreies Ziel den Modus des langsamen Hochfahrens beendet hat, kann der Load Balancer diesem den vollständigen Anteil von Anfragen senden.

Überlegungen

- Wenn Sie das langsame Hochfahren für eine Zielgruppe aktivieren, gehen die bei der Zielgruppe registrierten fehlerfreien Ziele nicht in den Modus des langsamen Hochfahrens über.
- Wenn Sie das langsame Hochfahren für eine leere Zielgruppe aktivieren und dann mit einer einzigen Registrierungsoperation auf ein Ziel anwenden, dann gehen diese Ziele nicht in den Modus des langsamen Hochfahrens über. Neu registrierte Ziele gehen nur dann in den Modus des langsamen Hochfahrens über, wenn mindestens ein fehlerfreies Ziel vorhanden ist, das sich nicht im Modus des langsamen Hochfahrens befindet.
- Wenn Sie die Registrierung eines Ziels im Modus des langsamen Hochfahrens aufheben, beendet das Ziel den Modus des langsamen Hochfahrens. Wenn Sie dasselbe Ziel erneut registrieren, wechselt es in den Modus des langsamen Hochfahrens, wenn es von der Zielgruppe als fehlerfrei eingestuft wird.
- Wenn ein Ziel im Modus des langsamen Hochfahrens fehlerhaft ist, beendet das Ziel den Modus des langsamen Hochfahrens. Wenn das Ziel dann fehlerfrei ist, wechselt es wieder in den Modus des langsamen Hochfahrens.
- Sie können den langsamen Startmodus nicht aktivieren, wenn Sie die wenigsten ausstehenden Anfragen oder gewichtete zufällige Routing-Algorithmen verwenden.

So aktualisieren Sie den Wert für die Dauer des langsamen Hochfahrens mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Attribute bearbeiten den Wert von Dauer des langsamen Hochfahrens nach Bedarf. Um den Modus des langsamen Hochfahrens zu deaktivieren, legen Sie als Dauer 0 fest.
6. Wählen Sie Änderungen speichern aus.

Um den Wert für die Dauer des langsamen Starts zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit dem `slow_start.duration_seconds` Attribut.

Zonenübergreifendes Load Balancing für Application Load Balancer Balancer-Zielgruppen

Die Knoten für Ihren Load Balancer verteilen Anforderungen von Clients auf registrierte Ziele. Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Load Balancer-Knoten den Datenverkehr gleichmäßig auf die registrierten Ziele in allen registrierten Availability Zones. Wenn zonenübergreifendes Load Balancing deaktiviert ist, verteilt jeder Load Balancer-Knoten den Datenverkehr gleichmäßig nur auf die registrierten Ziele in seiner Availability Zone. Dies könnte verwendet werden, wenn zonale Ausfalldomänen regionalen vorzuziehen sind, um sicherzustellen, dass eine fehlerfreie Zone nicht von einer fehlerhaften Zone beeinträchtigt wird, oder um die allgemeine Latenz zu verbessern.

Bei Application Load Balancern ist der zonenübergreifende Load Balancing immer auf Load Balancer-Ebene aktiviert und kann nicht ausgeschaltet werden. Für Zielgruppen wird standardmäßig die Load-Balancer-Einstellung verwendet. Sie können die Standardeinstellung jedoch überschreiben, indem Sie den zonenübergreifenden Load Balancing auf Zielgruppenebene explizit ausschalten.

Überlegungen

- Die Zielgruppenbindung wird nicht unterstützt, wenn zonenübergreifendes Load Balancing deaktiviert ist.
- Lambda-Funktionen als Ziele werden nicht unterstützt, wenn zonenübergreifendes Load Balancing deaktiviert ist.
- Beim Versuch, das zonenübergreifende Load Balancing über die `ModifyTargetGroupAttributes`-API zu deaktivieren, wenn bei Zielen der Parameter `AvailabilityZone` auf `all` gesetzt ist, tritt ein Fehler auf.
- Bei der Registrierung von Zielen ist der `AvailabilityZone`-Parameter erforderlich. Spezifische Availability Zone-Werte sind nur zulässig, wenn zonenübergreifendes Load Balancing deaktiviert ist. Andernfalls wird der Parameter ignoriert und als `all` behandelt.

Bewährte Methoden

- Planen Sie für jede Zielgruppe genügend Zielkapazität für alle Availability Zones ein, die Sie voraussichtlich nutzen werden. Wenn Sie nicht genügend Kapazität für alle teilnehmenden Availability Zones einplanen können, empfehlen wir Ihnen, das zonenübergreifende Load Balancing aktiviert zu lassen.
- Wenn Sie Ihren Application Load Balancer mit mehreren Zielgruppen konfigurieren, stellen Sie sicher, dass alle Zielgruppen innerhalb der konfigurierten Region an denselben Availability Zones teilnehmen. Dadurch soll verhindert werden, dass eine Availability Zone leer ist, während das zonenübergreifende Load Balancing deaktiviert ist, da dies für alle HTTP-Anfragen, die in die leere Availability Zone gelangen, einen 503-Fehler auslöst.
- Vermeiden Sie das Erstellen leerer Subnetze. Application Load Balancer stellen zonale IP-Adressen über DNS für die leeren Subnetze zur Verfügung, was 503-Fehler bei HTTP-Anfragen auslöst.
- Es kann vorkommen, dass eine Zielgruppe mit deaktiviertem zonenübergreifendem Load Balancing über genügend geplante Zielkapazität pro Availability Zone verfügt, aber alle Ziele in einer Availability Zone fehlerhaft werden. Wenn es mindestens eine Zielgruppe mit ausschließlich fehlerhaften Zielen gibt, werden die IP-Adressen der Load Balancer-Knoten aus dem DNS entfernt. Sobald die Zielgruppe mindestens ein fehlerfreies Ziel hat, werden die IP-Adressen im DNS wiederhergestellt.

Wenn zonenübergreifendes Load Balancing deaktivieren

Sie können das zonenübergreifende Load Balancing für Ihre Application Load Balancer-Zielgruppen jederzeit deaktivieren.

Deaktivieren des zonenübergreifenden Load Balancing mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie auf der Seite Zielgruppenattribute bearbeiten für zonenübergreifendes Load Balancing die Option Aus aus.
6. Wählen Sie Änderungen speichern aus.

Um den zonenübergreifenden Load Balancing zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl und setzen Sie das `load_balancing.cross_zone.enabled` Attribut auf`false`.

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=false
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "false"
        },
    ]
}
```

Zonenübergreifendes Load Balancing aktivieren

Sie können das zonenübergreifende Load Balancing für Ihre Application Load Balancer-Zielgruppen jederzeit aktivieren. Die Einstellung für das zonenübergreifende Load Balancing auf Zielgruppenebene hat Vorrang vor der Einstellung auf Load-Balancer-Ebene.

Aktivieren des zonenübergreifenden Load Balancing mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie auf der Seite Zielgruppenattribute bearbeiten für zonenübergreifendes Load Balancing die Option An aus.
6. Wählen Sie Änderungen speichern aus.

Um den zonenübergreifenden Load Balancing zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl und setzen Sie das `load_balancing.cross_zone.enabled` Attribut auf`true`.

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=true
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "true"
        },
    ]
}
```

Automatische Zielgewichte (ATW)

Automatic Target Weights (ATW) überwacht ständig die Ziele, auf denen Ihre Anwendungen ausgeführt werden, und erkennt signifikante Leistungsabweichungen, sogenannte Anomalien. ATW bietet die Möglichkeit, die Menge des an Ziele weitergeleiteten Datenverkehrs dynamisch anzupassen, indem Datenanomalien in Echtzeit erkannt werden.

Automatic Target Weights (ATW) führt automatisch eine Anomalieerkennung für jeden Application Load Balancer in Ihrem Konto durch. Wenn anomale Ziele identifiziert werden, kann ATW

automatisch versuchen, sie zu stabilisieren, indem es den Umfang des Datenverkehrs, den sie weiterleiten, reduziert. Dies wird als Abwehr von Anomalien bezeichnet. ATW optimiert kontinuierlich die Verteilung des Datenverkehrs, um die Erfolgsquoten pro Ziel zu maximieren und gleichzeitig die Ausfallraten der Zielgruppen zu minimieren.

Überlegungen:

- Die Anomalieerkennung überwacht derzeit HTTP 5xx-Antwortcodes, die von Ihren Zielen kommen, und Verbindungsfehler zu diesen. Die Anomalieerkennung ist immer aktiviert und kann nicht ausgeschaltet werden.
- ATW wird nicht unterstützt, wenn Lambda als Ziel verwendet wird.

Anomalie-Erkennung

Die ATW-Anomalieerkennung überwacht alle Ziele, die eine signifikante Abweichung im Verhalten von anderen Zielen in ihrer Zielgruppe aufweisen. Diese Abweichungen, die als Anomalien bezeichnet werden, werden ermittelt, indem die prozentualen Fehler eines Ziels mit den prozentualen Fehlern anderer Ziele in der Zielgruppe verglichen werden. Bei diesen Fehlern kann es sich sowohl um Verbindungsfehler als auch um HTTP-Fehlercodes handeln. Ziele, die deutlich höhere Werte als ihre Mitbewerber melden, werden dann als anomal eingestuft.

Für die Erkennung von Anomalien sind mindestens drei gesunde Zielpersonen in der Zielgruppe erforderlich. Wenn ein Ziel für eine Zielgruppe registriert ist, muss es zuerst die Gesundheitschecks bestehen, um Traffic empfangen zu können. Sobald das Ziel das Ziel empfängt, beginnt ATW mit der Überwachung des Ziels und veröffentlicht kontinuierlich das Ergebnis der Anomalie. Für Ziele ohne Anomalien lautet das Anomalieergebnis. `normal` Für Ziele mit Anomalien lautet das Anomalieergebnis. `anomalous`

Die ATW-Anomalieerkennung funktioniert unabhängig von den Gesundheitschecks der Zielgruppe. Ein Ziel kann alle Zustandsprüfungen für die Zielgruppe bestehen, aber aufgrund einer erhöhten Fehlerquote trotzdem als anomal eingestuft werden. Wenn Ziele anomal werden, hat das keinen Einfluss auf den Status ihrer Zielgruppen-Gesundheitschecks.

Status der Erkennung von Anomalien

ATW veröffentlicht kontinuierlich den Status der Anomalieerkennungen, die es an Zielen durchführt. Sie können den aktuellen Status jederzeit mit der Taste oder einsehen. AWS Management Console AWS CLI

Um den Status der Anomalieerkennung mithilfe der Konsole einzusehen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Detailseite der Zielgruppen den Tab Ziele aus.
5. In der Tabelle Registrierte Ziele können Sie den Anomaliestatus der einzelnen Ziele in der Spalte mit den Ergebnissen der Anomalieerkennung einsehen.

   Wenn keine Anomalien festgestellt wurden, lautet das Ergebnis. `normal`

   Wenn Anomalien festgestellt wurden, lautet das Ergebnis. `anomalous`

Um die Ergebnisse der Anomalieerkennung anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den describe-target-healthBefehl, bei dem der `Include.member.N` Attributwert auf `AnomalyDetection` gesetzt ist.

Minimierung von Anomalien

> **Important**
>
> Die Funktion zur Minimierung von Anomalien von ATW ist nur verfügbar, wenn der Algorithmus Weighted Random Routing verwendet wird.

Die ATW-Abwehr von Anomalien leitet den Verkehr automatisch von anomalen Zielen weg und gibt ihnen so die Möglichkeit, sich zu erholen.

Während der Schadensbegrenzung:

- ATW passt in regelmäßigen Abständen die Menge des Datenverkehrs an, der zu anomalen Zielen geleitet wird. Derzeit beträgt der Zeitraum alle fünf Sekunden.
- ATW reduziert die Menge des Datenverkehrs, der zu anomalen Zielen geleitet wird, auf das Minimum, das zur Behebung von Anomalien erforderlich ist.
- Bei Zielen, die nicht mehr als anomal erkannt werden, wird nach und nach mehr Traffic an sie weitergeleitet, bis sie die Parität mit anderen normalen Zielen in der Zielgruppe erreichen.

Schalten Sie die ATW-Abschwächung von Anomalien ein

Sie können die Minimierung von Anomalien jederzeit aktivieren.

Um die Minimierung von Anomalien mithilfe der Konsole zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Detailseite der Zielgruppen auf der Registerkarte Attribute die Option Bearbeiten aus.
5. Stellen Sie sicher, dass auf der Seite Zielgruppenattribute bearbeiten im Abschnitt Verkehrskonfiguration unter Load Balancing-Algorithmus die Option Weighted Random ausgewählt ist.

   Hinweis: Wenn der gewichtete Zufallsalgorhythmus anfänglich ausgewählt ist, ist die Anomalieerkennung standardmäßig aktiviert.
6. Stellen Sie sicher, dass unter Minimierung von Anomalien die Option Minimierung von Anomalien aktivieren ausgewählt ist.
7. Wählen Sie Änderungen speichern aus.

Um die Minimierung von Anomalien zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit dem `load_balancing.algorithm.anomaly_mitigation` Attribut.

Status der Minimierung von Anomalien

Immer wenn ATW eine Risikominderung an einem Ziel durchführt, können Sie den aktuellen Status jederzeit mit dem oder anzeigen. AWS Management Console AWS CLI

Um den Status zur Behebung von Anomalien mithilfe der Konsole einzusehen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.

4. Wählen Sie auf der Detailseite der Zielgruppen den Tab Ziele aus.
5. In der Tabelle „Registrierte Ziele“ können Sie den Status der einzelnen Ziele zur Minimierung von Anomalien in der Spalte Schadensbegrenzung in Kraft einsehen.

   Wenn die Schadensbegrenzung nicht im Gange ist, lautet der Status. `yes`

   Wenn die Schadensbegrenzung im Gange ist, lautet der Status. `no`

Um den Status der Minimierung von Anomalien anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den describe-target-healthBefehl, bei dem der `Include.member.N` Attributwert auf gesetzt ist. `AnomalyDetection`

Sticky Sessions für Ihren Application Load Balancer

Standardmäßig leitet ein Application Load Balancer jede Anforderung getrennt an ein registriertes Ziel weiter, basierend auf dem ausgewählten Load-Balancing-Algorithmus. Sie können jedoch das Feature „Sticky Session“ (auch als gebundene Sitzungen bezeichnet) verwenden, damit der Load Balancer die Sitzung eines Benutzers an ein bestimmtes Ziel binden kann. So wird sichergestellt, dass alle Anforderungen, die während der Sitzung vom Benutzer gesendet werden, an dasselbe Ziel weitergeleitet werden. Dieses Feature ist nützlich für Server, die Zustandsinformationen verwalten, um Clients eine kontinuierliche Erfahrung zu bieten. Um Sticky Sessions zu verwenden, muss der Client Cookies unterstützen.

Application Load Balancer unterstützen sowohl dauerbasierte Cookies als auch anwendungsbasierte Cookies. Sticky Sessions werden auf Ebene der Zielgruppe aktiviert. Sie können für Ihre Zielgruppen eine Kombination aus auf Dauer basierenden Sticky Sessions, anwendungsbasierten Sticky Sessions und keine Sticky Sessions verwenden.

Bei der Verwaltung von Sticky Sessions ist es besonders wichtig festzulegen, wie lange der Load Balancer die Anforderung des Benutzers an das gleiche Ziel leiten soll. Wenn Ihre Anwendung über ein eigenes Sitzungscookie verfügt, können Sie anwendungsbasierte Sticky Session verwenden. Das Sitzungscookie der Load-Balancer-Sitzung hält dann die durch das Sitzungscookie der Anwendung festgelegte Dauer ein. Wenn Ihre Anwendung kein eigenes Sitzungscookie hat, können Sie auf Dauer basierende Sticky Sessions verwenden, um ein Load-Balancer-Sitzungscookie mit einer von Ihnen angegebenen Dauer zu generieren.

Der Inhalt der von Load Balancern generierten Cookies wird mit einem rotierenden Schlüssel verschlüsselt. Sie können vom Load Balancer generierte Cookies nicht entschlüsseln oder ändern.

Bei beiden Stickiness-Typen setzt der Application Load Balancer den Ablauf der von ihm generierten Cookies nach jeder Anforderung zurück. Wenn ein Cookie abläuft, ist die Sitzung keine Sticky Session mehr und der Client sollte das Cookie aus seinem Cookiespeicher entfernen.

Voraussetzungen

- Ein HTTP/HTTPS Load Balancer.
- Mindestens eine funktionierende Instance in jeder Availability Zone.

Überlegungen

- Sticky Sessions werden nicht unterstützt, wenn zonenübergreifendes Load Balancing deaktiviert ist. Der Versuch, Sticky Sessions zu aktivieren, während zonenübergreifendes Load Balancing deaktiviert ist, scheitert.
- Bei anwendungsbasierten Cookies müssen die Namen der Cookies für jede Zielgruppe einzeln angegeben werden. Bei dauerbasierten Cookies ist `AWSALB` jedoch der einzige Name, der für alle Zielgruppen verwendet wird.
- Wenn Sie mehrere Ebenen von Application Load Balancern nutzen, können Sie mit anwendungsbasierten Cookies Sticky Sessions auf allen Ebenen aktivieren. Mit dauerbasierten Cookies können Sie Sticky Sessions jedoch nur auf einer Ebene aktivieren, weil `AWSALB` der einzige verfügbare Name ist.
- Wenn der Application Load Balancer `AWSALBCORS` sowohl ein als auch ein `AWSALB` dauerbasiertes Stickiness-Cookie empfängt, hat der Wert in `AWSALBCORS` Vorrang.
- Anwendungsbasierte Sticky Sessions funktionieren nicht bei gewichteten Zielgruppen.
- Wenn Sie über eine Weiterleitungsregel mit mehreren Zielgruppen verfügen und für mindestens eine Sticky Sessions aktiviert sind, müssen Sie die Stickiness der Zielgruppe aktivieren.
- WebSocket Verbindungen sind von Natur aus klebrig. Wenn der Client ein Verbindungs-Upgrade für anfordert WebSockets, ist das in der Verbindung verwendete Ziel das Ziel, das einen HTTP-101-Statuscode zurückgibt, um das WebSockets Verbindungs-Upgrade zu akzeptieren. Nach Abschluss des WebSockets Upgrades wird die auf Cookies basierende Stickiness nicht mehr verwendet.
- Application Load Balancer verwenden das `Expires`-Attribut im Cookie-Header anstelle des `Max-Age`-Attributs.
- Application Load Balancer unterstützen keine Cookie-Werte, die URL-codiert sind.

- Wenn der Application Load Balancer eine neue Anfrage empfängt, während das Ziel aufgrund einer Abmeldung leer ist, wird die Anfrage an ein fehlerfreies Ziel weitergeleitet.

Sticky Sessions auf Basis der Dauer

Bei auf Dauer basierenden Sticky Sessions werden Anforderungen mithilfe eines vom Load Balancer generierten Cookies (`AWSALB`) an dasselbe Ziel in einer Zielgruppe weitergeleitet. Das Cookie wird verwendet, um die Sitzung dem Ziel zuzuordnen. Wenn Ihre Anwendung kein eigenes Sitzungscookie hat, können Sie Ihre eigene Dauer der Sticky Sessions angeben und festlegen, wie lange Ihr Load Balancer die Anforderung des Benutzers konsistent an dasselbe Ziel weiterleiten soll.

Wenn ein Load Balancer eine Anforderung von einem Client erhält, leitet er die Anforderung (basierend auf der Grundlage des ausgewählten Algorithmus) an ein Ziel weiter und generiert ein Cookie namens `AWSALB`. Er codiert Informationen über das ausgewählte Ziel, verschlüsselt das Cookie und schließt das Cookie in die Antwort an den Client ein. Das vom Load Balancer generierte Cookie hat eine eigene Dauer der Gültigkeit von 7 Tagen. Dieses Ablaufdatum ist nicht konfigurierbar.

Bei nachfolgenden Anforderungen sollte der Client das `AWSALB`-Cookie enthalten. Wenn der Load Balancer eine Anforderung von einem Client erhält, die das Cookie enthält, erkennt er es und leitet die Anforderung an dasselbe Ziel weiter. Wenn das Cookie vorhanden ist, aber nicht dekodiert werden kann, oder wenn es sich auf ein Ziel bezieht, das abgemeldet wurde oder fehlerhaft ist, wählt der Load Balancer ein neues Ziel aus und aktualisiert das Cookie mit Informationen über das neue Ziel.

Für CORS-Anfragen (Cross-Origin Resource Sharing) müssen einige Browser Stickiness aktivieren. `SameSite=None; Secure` Um diese Browser zu unterstützen, generiert der Load Balancer immer ein zweites Stickiness-Cookie`AWSALBCORS`, das dieselben Informationen wie das ursprüngliche Stickiness-Cookie sowie das Attribut enthält. `SameSite` Kunden erhalten beide Cookies, auch Anfragen, die nicht von CORS stammen.

So aktivieren Sie auf Dauer basierende Sticky Sessions mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.

4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Führen Sie auf der Seite Edit attributes die folgenden Schritte aus:
   a. Wählen Sie Stickiness aus.
   b. Wählen Sie für den Stickiness-Typ die Option Vom Load Balancer generiertes Cookie aus.
   c. Geben Sie im Feld Stickiness duration(Erhaltungsdauer) einen Wert zwischen 1 Sekunde und 7 Tagen aus.
   d. Wählen Sie Änderungen speichern aus.

Um die dauerabhängige Klebrigkeit zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit den Attributen und`stickiness.enabled`. `stickiness.lb_cookie.duration_seconds`

Verwenden Sie den folgenden Befehl, um auf Dauer basierende Sticky Sessions zu aktivieren.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true
 Key=stickiness.lb_cookie.duration_seconds,Value=time-in-seconds
```

Die Ausgabe sollte in etwa wie folgt aussehen.

```
    {
       "Attributes": [
          ...
           {
                "Key": "stickiness.enabled",
                "Value": "true"
             },
             {
                 "Key": "stickiness.lb_cookie.duration_seconds",
                 "Value": "86500"

             },
          ...
         ]
     }
```

Anwendungsbasierte Sticky Sessions

Anwendungsbasierte Sticky Sessions geben Ihnen die Flexibilität, Ihre eigenen Kriterien für die Client-Ziel-Stickiness festzulegen. Wenn Sie die anwendungsbasierte Stickiness aktivieren, leitet der Load Balancer die erste Anforderung auf der Grundlage des ausgewählten Algorithmus an ein Ziel innerhalb der Zielgruppe weiter. Es wird erwartet, dass das Ziel ein benutzerdefiniertes Anwendungscookie setzt, das dem im Load Balancer konfigurierten Cookie entspricht, um Stickiness zu aktivieren. Dieses benutzerdefinierte Cookie kann jedes Cookie-Attribut enthalten, das von der Anwendung benötigt wird.

Wenn der Application Load Balancer das benutzerdefinierte Anwendungscookie vom Ziel empfängt, generiert er automatisch ein neues verschlüsseltes Anwendungscookie zum Erfassen von Stickiness-Informationen. Dieses vom Load Balancer generierte Anwendungscookie erfasst Stickiness-Informationen für jede Zielgruppe, für die anwendungsbasierte Sticky Sessions aktiviert sind.

Das vom Load Balancer generierte Anwendungscookie kopiert nicht die Attribute des vom Ziel gesetzten benutzerdefinierten Cookies. Es hat eine eigene Dauer der Gültigkeit von 7 Tagen. Dieses Ablaufdatum ist nicht konfigurierbar. In der Antwort an den Client validiert der Application Load Balancer nur den Namen, mit dem das benutzerdefinierte Cookie auf Zielgruppenebene konfiguriert wurde, und nicht den Wert oder das Ablaufattribut des benutzerdefinierten Cookies. Solange der Name übereinstimmt, sendet der Load Balancer in der Antwort beide Cookies an den Client: das vom Ziel gesetzte benutzerdefinierte Cookie und das vom Load Balancer generierte Anwendungscookie.

Bei nachfolgenden Anforderungen müssen die Clients beide Cookies zurücksenden, um die Stickiness aufrechtzuerhalten. Der Load Balancer entschlüsselt das Anwendungscookie und prüft, ob die konfigurierte Dauer der Stickiness noch gültig ist. Anschließend werden die im Cookie enthaltenen Informationen verwendet, um die Anforderung an dasselbe Ziel innerhalb der Zielgruppe zu senden, um die Stickiness aufrechtzuerhalten. Der Load Balancer leitet das benutzerdefinierte Anwendungscookie auch über einen Proxy an das Ziel weiter, ohne es zu überprüfen oder zu ändern. In nachfolgenden Antworten werden der Ablauf des vom Load Balancer generierten Anwendungs-Cookies und die im Load Balancer konfigurierte Dauer der Stickiness zurückgesetzt. Um die Stickiness zwischen Client und Target aufrechtzuerhalten, sollten das Cookie und die Dauer der Stickiness nicht ablaufen.

Wenn ein Ziel ausfällt oder fehlerhaft ist, leitet der Load Balancer keine Anforderungen mehr an dieses Ziel weiter und wählt basierend auf dem ausgewählten Load Balancing-Algorithmus ein neues fehlerfreies Ziel aus. Der Load Balancer behandelt die Sitzung jetzt als dem neuen fehlerfreien Ziel „angeheftet“ und leitet Anforderungen auch dann an dieses neue fehlerfreie Ziel, wenn das fehlerhafte Ziel wieder funktionsfähig ist.

Bei CORS-Anforderungen (Cross-Origin Resource Sharing) fügt der Load Balancer die `SameSite=None; Secure`-Attribute nur dann dem vom Load Balancer generierten Anwendungs-Cookie hinzu, um Stickiness zu aktivieren, wenn die Benutzeragent-Version Chromium80 oder höher ist.

Da für die meisten Browser in Bezug auf Cookies eine Größenbeschränkung von 4 KB gilt, unterteilt der Load Balancer Anwendungs-Cookie, die größer als 4 KB sind, in mehrere Cookies. Application Load Balancer unterstützen Cookies mit einer Größe von bis zu 16 KB und können daher bis zu 4 Shards erstellen, die an den Client gesendet werden. Der Name des Anwendungscookies, den der Client sieht, beginnt mit „AWSALBAPP-“ und enthält eine Fragmentnummer. Wenn die Größe des Cookies beispielsweise 0-4K ist, sieht der Client AWSALBAPP -0. Wenn die Größe des Cookies 4—8 KB beträgt, sieht der Client AWSALBAPP -0 und AWSALBAPP -1 und so weiter.

So aktivieren Sie anwendungsbasierte Sticky Sessions mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Führen Sie auf der Seite Edit attributes die folgenden Schritte aus:
   a. Wählen Sie Stickiness aus.
   b. Wählen Sie für den Stickiness-Typ die Option Anwendungsbasiertes Cookie aus.
   c. Geben Sie im Feld Stickiness duration(Erhaltungsdauer) einen Wert zwischen 1 Sekunde und 7 Tagen aus.
   d. Geben Sie unter App-Cookie-Name einen Namen für Ihr anwendungsbasiertes Cookie ein.

      Verwenden Sie nicht `AWSALB`, `AWSALBAPP` oder `AWSALBTG` für den Cookie-Namen. Sie sind für die Verwendung durch den Load Balancer reserviert.
   e. Wählen Sie Änderungen speichern aus.

Um die anwendungsbasierte Stickiness zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit den folgenden Attributen:

- stickiness.enabled
- stickiness.type
- stickiness.app_cookie.cookie_name
- stickiness.app_cookie.duration_seconds

Verwenden Sie den folgenden Befehl, um anwendungsbasierte Sticky Sessions zu aktivieren.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true Key=stickiness.type,Value=app_cookie
 Key=stickiness.app_cookie.cookie_name,Value=my-cookie-name
 Key=stickiness.app_cookie.duration_seconds,Value=time-in-seconds
```

Die Ausgabe sollte in etwa wie folgt aussehen.

```
      {
           "Attributes": [
               ...
               {
                   "Key": "stickiness.enabled",
                   "Value": "true"
               },
               {
                   "Key": "stickiness.app_cookie.cookie_name",
                   "Value": "MyCookie"
               },
               {
                   "Key": "stickiness.type",
                   "Value": "app_cookie"
               },
               {
                   "Key": "stickiness.app_cookie.duration_seconds",
                   "Value": "86500"
               },
               ...
           ]
       }
```

Manuelle Neuverteilung

Wenn beim Hochskalieren die Anzahl der Ziele erheblich zunimmt, besteht die Gefahr einer ungleichmäßigen Lastverteilung aufgrund von Stickiness. In diesem Szenario können Sie die Last mithilfe der folgenden zwei Optionen neu auf Ihre Ziele verteilen:

- Legen Sie für das von der Anwendung generierte Cookie ein Ablaufdatum fest, das vor dem aktuellen Datum und der aktuellen Uhrzeit liegt. Dadurch wird verhindert, dass Clients das Cookie an den Application Load Balancer senden, der den Prozess der Herstellung von Stickiness neu startet.
- Legen Sie für die Konfiguration der anwendungsbasierten Stickiness des Load Balancers eine sehr kurze Dauer fest, z. B. 1 Sekunde. Dadurch wird der Application Load Balancer gezwungen, die Stickiness wiederherzustellen, auch wenn das vom Ziel gesetzte Cookie nicht abgelaufen ist.

Registrieren Sie Ziele bei Ihrer Application Load Balancer Balancer-Zielgruppe

Sie registrieren Ihre Ziele bei einer Zielgruppe. Wenn Sie eine Zielgruppe erstellen, können Sie ihren Zieltyp angeben, durch den festgelegt wird, wie Sie ihre Ziele registrieren. Sie können beispielsweise Instance IDs, IP-Adressen oder Lambda-Funktionen registrieren. Weitere Informationen finden Sie unter Zielgruppen für Ihre Application Load Balancer.

Wenn die Nachfrage nach Ihren aktuell registrierten Zielen steigt, können Sie zusätzliche Ziele registrieren, um die Nachfrage zu bewältigen. Wenn Ihr Ziel für die Verarbeitung von Anfragen bereit ist, registrieren Sie es bei Ihrer Zielgruppe. Der Load Balancer beginnt, Anfragen an das Ziel weiterzuleiten, sobald der Registrierungsvorgang abgeschlossen ist und das Ziel die ersten Zustandsprüfungen bestanden hat.

Wenn die Nachfrage nach Ihren registrierten Zielen sinkt oder Sie ein Ziel warten müssen, können Sie dessen Registrierung bei Ihrer Zielgruppe aufheben. Der Load Balancer stoppt das Weiterleiten von Anfragen an ein Ziel, sobald Sie die Registrierung des Ziels aufheben. Wenn das Ziel für den Empfang von Anfragen bereit ist, können Sie es wieder bei der Zielgruppe registrieren.

Wenn Sie die Registrierung eines Ziels aufheben, wartet der Load Balancer, bis laufende Anfragen abgeschlossen wurden. Dies wird als Connection Draining bezeichnet. Der Status eines Ziels ist `draining`, während Connection Draining erfolgt.

Wenn Sie die Registrierung eines Ziels aufheben, das durch IP-Adresse registriert war, müssen Sie die Verzögerung der Registrierungsaufhebung abwarten, bevor Sie dieselbe IP-Adresse erneut registrieren können.

Wenn Sie Ziele nach Instance-ID registrieren, können Sie Ihren Load Balancer mit einer Auto-Scaling-Gruppe verwenden. Nachdem Sie eine Zielgruppe einer Auto-Scaling-Gruppe zugeordnet haben und die Gruppe hochskaliert wird, werden die von der Auto-Scaling-Gruppe gestarteten Instances automatisch bei der Zielgruppe registriert. Wenn Sie die Zielgruppe von der Auto-Scaling-Gruppe trennen, wird die Registrierung der Instances bei der Zielgruppe automatisch aufgehoben. Weitere Informationen finden Sie unter Einen Load Balancer zu Ihrer Auto Scaling Scaling-Gruppe hinzufügen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Wenn Sie eine Anwendung auf einem Ziel herunterfahren, müssen Sie das Ziel zunächst von seiner Zielgruppe abmelden und warten, bis die vorhandenen Verbindungen abgebaut sind. Sie können den Status der Abmeldung mit dem describe-target-health CLI-Befehl überwachen oder indem Sie die Zielgruppenansicht in der aktualisieren. AWS Management Console Nachdem Sie bestätigt haben, dass das Ziel deregistriert wurde, können Sie mit dem Stoppen oder Beenden der Anwendung fortfahren. Diese Reihenfolge verhindert, dass Benutzer 5XX-Fehler bekommen, wenn Anwendungen beendet werden, während der Verkehr noch verarbeitet wird.

Zielsicherheitsgruppen

Wenn Sie EC2 Instances als Ziele registrieren, müssen Sie sicherstellen, dass die Sicherheitsgruppen für Ihre Instances es dem Load Balancer ermöglichen, mit Ihren Instances sowohl am Listener-Port als auch am Health Check-Port zu kommunizieren.

Empfohlene Regeln

Inbound

Source	Port Range	Comment
load balancer security group	*instance listener*	Datenverkehr vom Load Balancer auf dem Listener-Port der Instance zulassen
load balancer security group	*health check*	Datenverkehr vom Load Balancer auf dem Zustandsprüfungs-Port zulassen

Außerdem sollten Sie eingehenden ICMP-Datenverkehr zur Unterstützung von Path MTU Discovery erlauben. Weitere Informationen finden Sie unter Path MTU Discovery im EC2 Amazon-Benutzerhandbuch.

Gemeinsam genutzte Subnetze

Teilnehmer können einen Application Load Balancer in einer gemeinsam genutzten VPC erstellen. Teilnehmer können kein Ziel registrieren, das in einem Subnetz ausgeführt wird, das nicht für sie freigegeben ist.

Registrieren oder Aufheben der Registrierung von Zielen

Der Zieltyp der Zielgruppe legt fest, wie Sie Ziele bei dieser Zielgruppe registrieren. Weitere Informationen finden Sie unter Zieltyp.

Inhalt

- Ziele nach Instance-ID registrieren oder die Registrierung aufheben
- Ziele nach IP-Adresse registrieren oder die Registrierung aufheben
- Registrieren und Aufheben der Registrierung einer Lambda-Funktion
- Registrieren oder Aufheben der Registrierung von Zielen mithilfe der AWS CLI

Ziele nach Instance-ID registrieren oder die Registrierung aufheben

> **Note**
>
> Bei der Registrierung von Zielen anhand der Instance-ID für eine IPv6 Zielgruppe müssen die Ziele über eine zugewiesene primäre IPv6 Adresse verfügen. Weitere Informationen finden Sie unter IPv6 Adressen im EC2 Amazon-Benutzerhandbuch

Die Instance muss sich in der Virtual Private Cloud (VPC) befinden, die Sie für die Zielgruppe angegeben haben. Die Instance muss sich auch im Status `running` befinden, wenn Sie sie registrieren.

So verfahren Sie zum Registrieren oder Aufheben der Registrierung von Zielen nach Instance-ID mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.

3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Ziele.
5. Um Instances zu registrieren, wählen Sie Ziele registrieren. Wählen Sie eine oder mehrere Instances aus, geben Sie bei Bedarf den Instance-Standardport ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus. Wenn Sie mit dem Hinzufügen der Instances fertig sind, wählen Sie Ausstehende Ziele registrieren aus.

   Hinweis:

   - Den Instances muss eine zugewiesene primäre IPv6 Adresse zugewiesen sein, um bei einer IPv6 Zielgruppe registriert zu werden.
   - AWS GovCloud (US) Region s unterstützen die Zuweisung einer primären IPv6 Adresse über die Konsole nicht. Sie müssen die API verwenden, um IPv6 Primäradressen in AWS GovCloud (US) Region s zuzuweisen.
6. Um die Registrierung von Instances aufzuheben, wählen Sie die Instances aus und klicken Sie dann auf Abmelden.

Ziele nach IP-Adresse registrieren oder die Registrierung aufheben

IPv4 Ziele

Die IP-Adressen, die Sie registrieren, müssen aus einem der folgenden CIDR-Blöcke stammen:

- Die Subnetze der VPC für die Zielgruppe
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Sie können die IP-Adressen eines anderen Application Load Balancer nicht in derselben VPC registrieren. Wenn der andere Application Load Balancer sich in einer VPC befindet, die durch Peering mit dem Load Balancer verbunden ist, können Sie die IP-Adressen registrieren.

IPv6 Ziele

- Die IP-Adressen, die Sie registrieren, müssen sich im VPC-CIDR-Block oder in einem Peer-VPC-CIDR-Block befinden.

So verfahren Sie zum Registrieren oder Aufheben der Registrierung von Zielen nach IP-Adresse mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Ziele.
5. Um IP-Adressen zu registrieren, wählen Sie Ziele registrieren. Wählen Sie für jede IP-Adresse das Netzwerk, die IP-Adresse und den Port aus und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus.
6. Optional: Wenn sich die IP-Adresse außerhalb der ausgewählten VPC befindet, müssen Sie eine Availability Zone angeben.
7. Wenn Sie die Eingabe der Adressen abgeschlossen haben, wählen Sie Ausstehende Ziele registrieren.
8. Um die Registrierung von IP-Adressen aufzuheben, wählen Sie die IP-Adressen aus und klicken Sie dann auf Abmelden. Wenn Sie viele registrierte IP-Adressen haben, können Sie einen Filter hinzufügen oder die Sortierreihenfolge ändern.

Registrieren und Aufheben der Registrierung einer Lambda-Funktion

Sie können für jede Zielgruppe eine einzelne Lambda-Funktion registrieren. Elastic Load Balancing benötigt Berechtigungen zum Aufrufen der Lambda-Funktion. Wenn Sie zu Ihrer Lambda-Funktion keinen Datenverkehr mehr senden müssen, können Sie ihre Registrierung aufheben. Nachdem Sie die Registrierung einer Lambda-Funktion aufgehoben haben, schlagen laufende Anfragen mit HTTP-5XX-Fehlermeldungen fehl. Zum Ersetzen einer Lambda-Funktion ist es daher besser, stattdessen eine neue Zielgruppe zu erstellen. Weitere Informationen finden Sie unter Verwenden Sie Lambda-Funktionen als Ziele eines Application Load Balancer.

So registrieren oder deregistrieren Sie eine Lambda-Funktion mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.

4. Wählen Sie die Registerkarte Ziele.
5. Wenn keine Lambda-Funktion registriert ist, wählen Sie Register (Registrieren). Wählen Sie die Lambda-Funktion und danach Register (Registrieren) aus.
6. Um die Registrierung einer Lambda-Funktion aufzuheben, wählen Sie Deregister (Registrierung aufheben). Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Deregister aus.

Registrieren oder Aufheben der Registrierung von Zielen mithilfe der AWS CLI

Verwenden Sie den Befehl register-targets zum Hinzufügen von Zielen und den Befehl deregister-targets zum Entfernen von Zielen.

Verwenden Sie Lambda-Funktionen als Ziele eines Application Load Balancer

Sie können Ihre Lambda-Funktionen als Ziele registrieren und eine Listener-Regel für das Weiterleiten von Anfragen an die Zielgruppe für Ihre Lambda-Funktion konfigurieren. Wenn der Load Balancer die Anfrage an eine Zielgruppe mit einer Lambda-Funktion als Ziel weiterleitet, ruft er Ihre Lambda-Funktion auf und übergibt den Inhalt der Anfrage im JSON-Format an die Lambda-Funktion.

Einschränkungen

- Die Lambda-Funktion und die Zielgruppe müssen sich im gleichen Konto und in der gleichen Region befinden.
- Der Anfragetext, den Sie an eine Lambda-Funktion senden können, darf maximal 1 MB betragen. Entsprechende Größenbeschränkungen finden Sie unter HTTP-Header-Limits.
- Die Lambda-Funktion darf als Antwort-JSON maximal 1 MB senden.
- WebSockets werden nicht unterstützt. Upgrade-Anfragen werden mit dem HTTP 400-Code abgelehnt.
- Local Zones werden nicht unterstützt.
- Automatic Target Weights (ATW) wird nicht unterstützt.

Inhalt

- Vorbereiten der Lambda-Funktion
- Erstellen Sie einer Zielgruppe für die Lambda-Funktion

- Empfangen von Ereignissen vom Load Balancer
- Antwort an den Load Balancer
- Header mit mehreren Werten
- Aktivieren von Zustandsprüfungen
- Aufheben der Registrierung der Lambda-Funktion

Eine Demo finden Sie unter Lambda-Ziel im Application Load Balancer.

Vorbereiten der Lambda-Funktion

Die folgenden Empfehlungen gelten, wenn Sie Ihre Lambda-Funktion mit einem Application Load Balancer verwenden.

Berechtigungen zum Aufrufen der Lambda-Funktion

Wenn Sie die Zielgruppe erstellen und die Lambda-Funktion mithilfe der AWS Management Console registrieren, fügt die Konsole in Ihrem Namen die erforderlichen Berechtigungen zu Ihrer Lambda-Funktionsrichtlinie hinzu. Andernfalls müssen Sie, nachdem Sie die Zielgruppe erstellt und die Funktion mit dem registriert haben AWS CLI, den Befehl add-permission verwenden, um Elastic Load Balancing die Berechtigung zum Aufrufen Ihrer Lambda-Funktion zu erteilen. Es wird empfohlen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zum Einschränken des Funktionsaufrufs an die angegebene Zielgruppe zu verwenden. Weitere Informationen finden Sie unter Das Problem des verwirrten Stellvertreters im IAM-Benutzerhandbuch.

```
aws lambda add-permission \
--function-name lambda-function-arn-with-alias-name \
--statement-id elb1 \
--principal elasticloadbalancing.amazonaws.com \
--action lambda:InvokeFunction \
--source-arn target-group-arn \
--source-account target-group-account-id
```

Versionsverwaltung der Lambda-Funktion

Sie können eine Lambda-Funktion pro Zielgruppe registrieren. Um sicherzustellen, dass Sie Ihre Lambda-Funktion ändern können und dass der Load Balancer immer die aktuelle Version der Lambda-Funktion aufruft, erstellen Sie einen Funktionsalias und schließen Sie den Alias in den Funktions-ARN ein, wenn Sie die Lambda-Funktion bei dem Load Balancer registrieren. Weitere

Informationen finden Sie unter AWS Lambda Funktionsaliasnamen im Developer Guide.AWS Lambda

Funktions-Timeout

Der Load Balancer wartet, bis die Lambda-Funktion reagiert oder eine Zeitüberschreitung auftritt. Es wird empfohlen, die Zeitüberschreitung der Lambda-Funktion auf der Grundlage Ihrer erwarteten Laufzeit zu konfigurieren. Informationen zum Standard-Timeout-Wert und wie Sie ihn ändern können, finden Sie unter Lambda-Funktions-Timeout konfigurieren. Informationen zum maximalen Timeout-Wert, den Sie konfigurieren können, finden Sie unter Kontingente.AWS Lambda

Erstellen Sie einer Zielgruppe für die Lambda-Funktion

Erstellen Sie eine Zielgruppe, die bei der Weiterleitung von Anforderungen verwendet wird. Wenn der Inhalt der Anfrage mit einer Listener-Regel mit einer Aktion für ihre Weiterleitung an diese Zielgruppe übereinstimmt, ruft der Load Balancer die registrierte Lambda-Funktion auf.

Um eine Zielgruppe zu erstellen und die Lambda-Funktion über die Konsole zu registrieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Wählen Sie unter Zieltyp auswählen die Option Lambda-Funktion aus.
5. Geben Sie im Feld Target group name (Zielgruppenname) einen Namen für die neue Zielgruppe ein.
6. (Optional) Um Zustandsprüfungen zu aktivieren, wählen Sie Aktivieren im Abschnitt Zustandsprüfungen aus.
7. (Optional) Fügen Sie einen oder mehrere Tags wie folgt hinzu:
   a. Erweitern Sie den Abschnitt Tags.
   b. Wählen Sie Add tag.
   c. Geben Sie den Tag-Schlüssel und den Tag-Wert ein.
8. Wählen Sie Weiter aus.
9. Geben Sie eine einzelne Lambda-Funktion an oder lassen Sie alternativ diesen Schritt aus und geben Sie später eine Lambda-Funktion an.
10. Wählen Sie Zielgruppe erstellen aus.

So erstellen und registrieren Sie eine Zielgruppe und registrieren die Lambda-Funktion mithilfe der AWS CLI

Verwenden Sie die create-target-groupBefehle und register-targets.

Empfangen von Ereignissen vom Load Balancer

Der Load Balancer unterstützt den Lambda-Aufruf für Anfragen über HTTP und HTTPS. Der Load Balancer sendet ein Ereignis im JSON-Format. Der Load Balancer fügt zu jeder Anfrage die folgenden Header hinzu: `X-Amzn-Trace-Id`, `X-Forwarded-For`, `X-Forwarded-Port` und `X-Forwarded-Proto`.

Wenn der `content-encoding`-Header vorhanden ist, codiert der Load Balancer mit Base64 den Text und setzt `isBase64Encoded` auf `true`.

Wenn der `content-encoding`-Header nicht vorhanden ist, hängt die Base64-Codierung vom Inhaltstyp ab. Bei den folgenden Typen sendet der Load Balancer den Text unverändert und setzt ihn `isBase64Encoded` auf`false`: text/*,. application/json, application/javascript, and application/xml Andernfalls codiert der Load Balancer den Text mit Base64 und stellt `isBase64Encoded` auf `true` ein.

Es folgt ein Beispielereignis.

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-target-
group/6d0ecf831eec9f09"
        }
    },
    "httpMethod": "GET",
    "path": "/",
    "queryStringParameters": {parameters},
    "headers": {
        "accept": "text/html,application/xhtml+xml",
        "accept-language": "en-US,en;q=0.8",
        "content-type": "text/plain",
        "cookie": "cookies",
        "host": "lambda-846800462-us-east-2.elb.amazonaws.com",
        "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)",
        "x-amzn-trace-id": "Root=1-5bdb40ca-556d8b0c50dc66f0511bf520",
```

```
        "x-forwarded-for": "72.21.198.66",
        "x-forwarded-port": "443",
        "x-forwarded-proto": "https"
    },
    "isBase64Encoded": false,
    "body": "request_body"
}
```

Antwort an den Load Balancer

Die Antwort von Ihrer Lambda-Funktion muss den Base64-codierten Status, Statuscode und die Header beinhalten. Sie können den Text weglassen.

Um den binären Inhalt in den Text der Antwort einzuschließen, müssen Sie den Inhalt mit Base64 codieren und `isBase64Encoded` auf `true` einstellen. Der Load Balancer decodiert die Inhalte, um den binären Inhalt abzurufen, und sendet ihn im Text der HTTP-Antwort zum Client.

Der Load Balancer berücksichtigt keine hop-by-hop Header wie oder. `Connection` `Transfer-Encoding` Sie können den `Content-Length`-Header weglassen, da der Load Balancer ihn berechnet, bevor er Antworten an Clients sendet.

Nachfolgend finden Sie eine Beispielantwort von einer auf nodejs basierenden Lambda-Funktion.

```
{
    "isBase64Encoded": false,
    "statusCode": 200,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
}
```

Lambda-Funktionsvorlagen, die mit Application Load Balancers funktionieren, finden Sie unter application-load-balancer-serverless-app auf github. Öffnen Sie alternativ die Lambda-Konsole, wählen Sie Anwendungen, Anwendung erstellen und dann eine der folgenden Optionen aus: AWS Serverless Application Repository

- ALB-Lambda-Ziel-S3 UploadFileto
- ALB-Lambda-Ziel- BinaryResponse

- ALB-Lambda-Ziel-IP WhatisMy

Header mit mehreren Werten

Wenn Anfragen von einem Client oder Antworten von einer Lambda-Funktion Header mit mehreren Werten, denselben Header mehrmals oder Abfrageparameter mit mehreren Werten für den gleichen Schlüssel enthalten, können Sie Unterstützung für die Syntax von Headern mit mehreren Werten aktivieren Nach dem Aktivieren von Headern mit mehreren Werten werden in den Headern und Abfrageparametern, die zwischen dem Load Balancer und der Lambda-Funktion ausgetauscht werden, Arrays anstelle von Zeichenfolgen verwendet. Wenn Sie die Syntax für Header mit mehreren Werten nicht aktivieren und ein Header oder Abfrageparameter mehrere Werte aufweist, verwendet der Load Balancer den zuletzt empfangenen Wert.

Inhalt

- Anfragen mit Headern mit mehreren Werten
- Antworten mit Headern mit mehreren Werten
- Aktivieren von Headern mit mehreren Werten

Anfragen mit Headern mit mehreren Werten

Die Namen der Felder, die für Header und Abfragezeichenfolgeparameter verwendet werden, unterscheiden sich abhängig davon, ob Sie Header mit mehreren Werten für die Zielgruppe aktivieren.

Die folgende Beispielanfrage enthält zwei Abfrageparameter mit demselben Schlüssel:

```
http://www.example.com?&myKey=val1&myKey=val2
```

Bei dem Standardformat verwendet der Load Balancer den letzten vom Client gesendeten Wert und sendet Ihnen mit `queryStringParameters` ein Ereignis, das Abfragezeichenfolgeparameter umfasst. Zum Beispiel:

```
"queryStringParameters": { "myKey": "val2"},
```

Wenn Sie Header mit mehreren Werten aktivieren, verwendet der Load Balancer beide vom Client gesendeten Schlüsselwerte und sendet Ihnen einen Zeichenfolgeparameter für eine Ereignisabfrage, der `multiValueQueryStringParameters` verwendet. Zum Beispiel:

```
"multiValueQueryStringParameters": { "myKey": ["val1", "val2"] },
```

Dementsprechend gilt Folgendes, wenn der Client eine Anfrage mit zwei Cookies im Header sendet:

```
"cookie": "name1=value1",
"cookie": "name2=value2",
```

Bei dem Standardformat verwendet der Load Balancer den letzten vom Client gesendeten Cookie und sendet Ihnen mit `headers` ein Ereignis, das Header umfasst. Zum Beispiel:

```
"headers": {
    "cookie": "name2=value2",
    ...
},
```

Bei Headern mit mehreren Werten verwendet der Load Balancer beide vom Client gesendeten Cookies und sendet Ihnen mit `multiValueHeaders` ein Ereignis, das Header umfasst: Zum Beispiel:

```
"multiValueHeaders": {
    "cookie": ["name1=value1", "name2=value2"],
    ...
},
```

Wenn die Abfrageparameter URL-kodiert sind, dekodiert der Load Balancer sie nicht. Sie müssen sie in Ihrer Lambda-Funktion dekodieren.

Antworten mit Headern mit mehreren Werten

Der Name der für Header verwendeten Felder unterscheidet sich abhängig davon, ob Sie Header mit mehreren Werten für die Zielgruppe verwenden. Sie müssen `multiValueHeaders` verwenden, wenn Sie Header mit mehreren Werten aktivieren. Andernfalls verwenden Sie `headers`.

Bei dem Standardformat können Sie ein einziges Cookie angeben:

```
{
  "headers": {
      "Set-cookie": "cookie-name=cookie-value;Domain=myweb.com;Secure;HttpOnly",
      "Content-Type": "application/json"
```

```
  },
}
```

Bei Headern mit mehreren Werten müssen Sie wie folgt mehrere Cookies angeben:

```
{
  "multiValueHeaders": {
      "Set-cookie": ["cookie-name=cookie-
value;Domain=myweb.com;Secure;HttpOnly","cookie-name=cookie-value;Expires=May 8,
 2019"],
      "Content-Type": ["application/json"]
  },
}
```

Der Load Balancer sendet die Header ggf. in einer anderen Reihenfolge als der in der Lambda-Antwortnutzlast angegebenen Reihenfolge an den Client. Verlassen Sie sich daher nicht darauf, dass Header in einer bestimmten Reihenfolge zurückgegeben werden.

Aktivieren von Headern mit mehreren Werten

Sie können Header mit mehreren Werten für eine Zielgruppe mit dem Zieltyp `lambda` aktivieren oder deaktivieren.

So aktivieren Sie die Header mit mehreren Werten mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Aktivieren oder deaktivieren Sie Header mit mehreren Werten.
6. Wählen Sie Änderungen speichern aus.

Um Header mit mehreren Werten zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit dem `lambda.multi_value_headers.enabled` Attribut.

Aktivieren von Zustandsprüfungen

Zustandsprüfungen sind für Zielgruppen des Typs `lambda` standardmäßig deaktiviert. Sie können Zustandsprüfungen aktivieren, um ein DNS Failover mit Amazon Route 53 zu implementieren. Die Lambda-Funktion kann den Zustand eines Downstream-Service prüfen, bevor sie auf die Anfrage einer Zustandsprüfung antwortet. Wenn die Antwort von der Lambda-Funktion auf eine nicht bestandene Zustandsprüfung hinweist, wird die nicht bestandene Zustandsprüfung an Amazon Route 53 übergeben. Sie können Amazon Route 53 für das Failover auf einen Sicherungsanwendungs-Stack konfigurieren.

Ihnen werden für Zustandsprüfungen genauso wie für jeden anderen Lambda-Funktionsaufruf Gebühren erhoben.

Im Folgenden finden Sie das Format des an Ihre Lambda-Funktion gesendeten Zustandsprüfungsereignisses. Um zu prüfen, ob ein Ereignis eine Zustandsprüfungsereignis ist, überprüfen Sie den Wert des Feldes "user-agent". Der Benutzeragent für Zustandsprüfungen ist `ELB-HealthChecker/2.0`.

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-target-
group/6d0ecf831eec9f09"
        }
    },
    "httpMethod": "GET",
    "path": "/",
    "queryStringParameters": {},
    "headers": {
        "user-agent": "ELB-HealthChecker/2.0"
    },
    "body": "",
    "isBase64Encoded": false
}
```

Um Integritätsprüfungen für eine Zielgruppe mithilfe der Konsole zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Einstellungen für die Zustandsprüfung die Option Bearbeiten aus.
5. Wählen Sie unter Zustandsprüfungen die Option Aktivieren aus.
6. Wählen Sie Änderungen speichern aus.

Um Gesundheitschecks für eine Zielgruppe zu aktivieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl modify-target-group mit der Option `--health-check-enabled`.

Aufheben der Registrierung der Lambda-Funktion

Wenn Sie zu Ihrer Lambda-Funktion keinen Datenverkehr mehr senden müssen, können Sie ihre Registrierung aufheben. Nachdem Sie die Registrierung einer Lambda-Funktion aufgehoben haben, schlagen laufende Anfragen mit HTTP-5XX-Fehlermeldungen fehl.

Zum Ersetzen einer Lambda-Funktion wird empfohlen, eine neue Zielgruppe zu erstellen, die neue Funktion bei der neuen Zielgruppe zu registrieren und die Listener-Regeln so zu aktualisieren, dass anstatt der vorhandenen die neue Zielgruppe verwendet wird.

So deregistrieren Sie die Lambda-Funktion mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Targets (Ziele) auf Deregister (Registrierung aufheben).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Deregister aus.

Um die Registrierung der Lambda-Funktion mit dem AWS CLI

Verwenden Sie den Befehl deregister-targets.

Tags für Ihre Application Load Balancer Balancer-Zielgruppe

Tags helfen Ihnen, Ihre Zielgruppen auf unterschiedliche Weise zu kategorisieren, z.B. nach Zweck, Eigentümer oder Umgebung.

Sie können mehrere Tags für jede Zielgruppe hinzufügen. Tag-Schlüssel müssen für jede Zielgruppe eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der der Zielgruppe bereits zugeordnet ist, ändert sich der Wert dieses Tags.

Wenn Sie ein Tag nicht mehr benötigen, können Sie es entfernen.

Einschränkungen

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen
- Maximale Wertlänge: 255 Unicode-Zeichen
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen.
- Verwenden Sie das `aws:` Präfix nicht in Ihren Tagnamen oder -Werten, da es für die AWS Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

So aktualisieren Sie die Tags für eine Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Tags die Option Tags verwalten und führen Sie einen oder mehrere der folgenden Schritte aus:
   a. Um ein Tag zu aktualisieren, geben Sie neue Werte für Schlüssel und Wert ein.
   b. Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen und geben Sie Werte für Schlüssel und Wert ein.

c. Um ein Tag zu löschen, wählen Sie Entfernen neben dem Tag.

5. Wenn Sie die Aktualisierung der Tags abgeschlossen haben, wählen Sie Änderungen speichern.

Um die Tags für eine Zielgruppe mit dem zu aktualisieren AWS CLI

Verwenden Sie die Befehle add-tags und remove-tags.

Löschen Sie eine Application Load Balancer Balancer-Zielgruppe

Sie können eine Zielgruppe löschen, wenn sie nicht von den Weiterleitungsaktionen der Listener-Regeln referenziert wird. Das Löschen einer Zielgruppe hat keine Auswirkungen auf die Ziele hat, die bei der Zielgruppe registriert sind. Wenn Sie eine registrierte EC2 Instance nicht mehr benötigen, können Sie sie beenden oder beenden.

Löschen einer Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Markieren Sie die Zielgruppe und wählen Sie Aktionen, Löschen.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja, löschen.

Um eine Zielgruppe mit dem zu löschen AWS CLI

Verwenden Sie den delete-target-group-Befehl.

Überwachen Ihrer Application Load Balancer

Sie können die folgenden Features verwenden, um Ihre Load Balancer zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihrem Load Balancer und Zielen zu beheben.

CloudWatch Metriken

Sie können Amazon verwenden CloudWatch , um Statistiken über Datenpunkte für Ihre Load Balancer und Ziele in Form eines geordneten Satzes von Zeitreihendaten, den so genannten Metriken, abzurufen. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Application Load Balancer.

Zugriffsprotokolle

Sie können Zugriffsprotokolle verwenden, um detaillierte Informationen zu den Anfragen, die an Ihren Load Balancer gestellt werden, zu erfassen und sie als Protokolldateien in Amazon S3 speichern. Sie können anhand dieser Zugriffsprotokolle Datenverkehrsmuster analysieren und Probleme mit Ihren Zielen beheben. Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihre Application Load Balancer.

Verbindungsprotokolle.

Sie können Verbindungsprotokolle verwenden, um Attribute der an Ihren Load Balancer gesendeten Anfragen zu erfassen und sie als Protokolldateien in Amazon S3 zu speichern. Sie können diese Verbindungsprotokolle verwenden, um die Client-IP-Adresse und den Port, die Client-Zertifikatsinformationen, die Verbindungsergebnisse und die verwendeten TLS-Chiffren zu ermitteln. Diese Verbindungsprotokolle können dann verwendet werden, um Anforderungsmuster und andere Trends zu überprüfen. Weitere Informationen finden Sie unter Verbindungsprotokolle für Ihren Application Load Balancer.

Anfragenachverfolgung

Sie können Anfragenachverfolgung verwenden, um HTTP-Anfragen nachzuverfolgen. Der Load Balancer fügt zu jede Anfrage, die er erhält, einen Header mit eine Ablaufverfolgungskennung hinzu. Weitere Informationen finden Sie unter Anfragenachverfolgung für Ihren Application Load Balancer.

CloudTrail Logs

Sie können AWS CloudTrail damit detaillierte Informationen zu den Aufrufen der Elastic Load Balancing API erfassen und sie als Protokolldateien in Amazon S3 speichern. Sie können diese

CloudTrail Protokolle verwenden, um festzustellen, welche Aufrufe getätigt wurden, von welcher Quell-IP-Adresse der Anruf kam, wer den Anruf getätigt hat, wann der Anruf getätigt wurde usw. Weitere Informationen finden Sie unter Protokollieren von API-Aufrufen für Elastic Load Balancing mit CloudTrail.

CloudWatch Metriken für Ihren Application Load Balancer

Elastic Load Balancing veröffentlicht Datenpunkte CloudWatch für Ihre Load Balancer und Ihre Ziele auf Amazon. CloudWatchermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Sie können z. B. die Gesamtanzahl der funktionierenden Ziele für einen Load Balancer für einen angegebenen Zeitraum überwachen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können beispielsweise einen CloudWatch Alarm erstellen, um eine bestimmte Metrik zu überwachen und eine Aktion einzuleiten (z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb des für Sie akzeptablen Bereichs liegt.

Elastic Load Balancing meldet Metriken CloudWatch nur dann, wenn Anfragen durch den Load Balancer fließen. Wenn Anforderungen über den Load Balancer erfolgen, misst Elastic Load Balancing diese und sendet seine Metriken in 60-Sekunden-Intervallen. Wenn es keine Anfragen über den Load Balancer gibt oder keine Daten für eine Metrik vorliegen, wird die Metrik nicht gemeldet.

Bei den Metriken für Application Load Balancer werden Anfragen zur Überprüfung des Systemzustands nicht berücksichtigt.

Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Inhalt

- Application-Load-Balancer-Metriken
- Metrik-Dimensionen für Application Load Balancer
- Statistiken für Application-Load-Balancer-Metriken
- CloudWatch Metriken für Ihren Load Balancer anzeigen

Application-Load-Balancer-Metriken

- Load Balancers
- Targets (Ziele)
- Zustand der Zielgruppe
- Lambda-Funktionen
- Benutzerauthentifizierung

Der `AWS/ApplicationELB`-Namespace enthält die folgenden Metriken für Load Balancer.

Metrik	Beschreibung
`ActiveConnectionCount`	Gesamtanzahl gleichzeitiger aktiver TCP-Verbindungen zwischen Clients und Load Balancer sowie zwischen Load Balancer und Zielen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`AnomalousHostCount`	Die Anzahl der Hosts, bei denen Anomalien festgestellt wurden. Berichtkriterien: Always reported Statistiken: Die nützlichsten Statistiken sind `Average`, `Minimum` und `Maximum`. Dimensionen • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
`BYoIPUtilPercentage`	Der Prozentsatz der Nutzung durch den IP-Pool. Berichtskriterien: BYo IP ist auf dem Load Balancer aktiviert. Statistiken: Die einzige aussagekräftige Statistik ist `Average`. Dimensionen • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `TargetGroup` , `AvailabilityZone`
`ClientTLSNegotiationErrorCount`	Die Anzahl der TLS-Verbindungen, die vom Client initiiert wurden und aufgrund eines TLS-Fehlers keine Sitzung mit dem Load Balancer hergestellt haben. Mögliche Ursachen sind eine Nichtübereinstimmung von Verschlüsselungen oder Protokollen oder der Client, der das Serverzertifikat nicht überprüft und die Verbindung schließt. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
ConsumedLCUs	Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden. Sie zahlen für die Anzahl der Geräte LCUs , die Sie pro Stunde nutzen. Wenn die LCU-Reser vierung aktiv ist, LCUs meldet „Verbraucht“, 0 ob die Nutzung unter der reservierten Kapazität liegt, und Werte darüber, 0 wenn die Nutzung die reservierte LCUs Kapazität überschreitet. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing. Berichtkriterien: Always reported Statistiken: Alle Dimensionen • LoadBalancer
PeakLCUs	Die maximale Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer zu einem bestimmten Zeitpunkt verwendet werden. Gilt nur, wenn Sie die LCU-Reservierung verwenden. Berichtskriterien: Immer Statistiken: Die nützlichsten Statistiken sind Sum und Max. Dimensionen • LoadBalancer

Metrik	Beschreibung
`ReservedLCUs`	Eine Abrechnungskennzahl, die die reservierte Kapazität pro Minute ausgibt. Der Gesamtbetrag, der LCUs über einen beliebige n Zeitraum reserviert wurde, entspricht dem Betrag, der LCUs Ihnen in Rechnung gestellt wird. Wenn beispielsweise 500 für eine Stunde reserviert LCUs sind, beträgt die Metrik pro Minute LCUs 8,33. Weitere Informationen finden Sie unter Überwachen Sie die Reservierung. Berichtkriterien: Ein Wert ungleich Null Statistiken: Alle Dimensionen • `LoadBalancer`
`DesyncMitigationMo de_NonCom pliant_Re quest_Count`	Die Anzahl der Anforderungen, die nicht RFC 7230 entsprechen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
`DroppedInvalidHeaderRequestCount`	Die Anzahl der Anforderungen, bei denen der Load Balancer HTTP-Header mit Header-Feldern entfernt hat, die nicht gültig sind, bevor die Anforderung nicht weitergeleitet wird. Der Load Balancer entfernt diese Header nur, wenn das `routing.http.drop_invalid_header_fields.enabled` -Attribut auf „`true`“ festgelegt ist. Berichtkriterien: Ein Wert ungleich Null Statistiken: Alle Dimensionen • `AvailabilityZone` , `LoadBalancer`
`MitigatedHostCount`	Die Anzahl der Ziele, die Gegenstand von Minderungsmaßnahmen sind. Berichtkriterien: Always reported Statistiken: Die nützlichsten Statistiken sind `Average`, `Minimum` und `Maximum`. Dimensionen • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
ForwardedInvalidHeaderRequestCount	Die Anzahl der vom Load Balancer weitergeleiteten Anforderungen mit HTTP-Headern mit ungültigen Header-Feldern. Der Load Balancer leitet Anfragen mit diesen Headern nur dann weiter, wenn das routing.http.drop_invalid_header_fields.enabled -Attribut auf „false“ festgelegt ist. Berichtkriterien: Always reported Statistiken: Alle Dimensionen • AvailabilityZone , LoadBalancer
GrpcRequestCount	Die Anzahl der über IPv4 und IPv6 verarbeiteten gRPC-Anfragen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Minimum, Maximum und Average geben alle 1 zurück. Dimensionen • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup • TargetGroup • AvailabilityZone , TargetGroup

Metrik	Beschreibung
HTTP_Fixed_Response_Count	Die Anzahl der Aktionen mit feststehender Antwort, die erfolgreich waren. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
HTTP_Redirect_Count	Die Anzahl der Redirect-Aktionen, die erfolgreich waren. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
HTTP_Redirect_Url_Limit_Exceeded_Count	Die Anzahl der Redirect-Aktionen, die nicht abgeschlossen werden konnten, weil die URL im Header der Antwortadresse größer als 8K ist. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Beschreibung
HTTPCode_ELB_3XX_Count	Die Anzahl der HTTP-3XX-Redirect-Codes, die vom Load Balancer stammen. Diese Anzahl enthält keine von Zielen erzeugte Antwortcodes. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
HTTPCode_ELB_4XX_Count	Anzahl von HTTP-4XX-Client-Fehlercodes, die vom Load Balancer verursacht werden. Diese Anzahl enthält keine von Zielen erzeugte Antwortcodes. Client-Fehler werden bei Anforderungen mit falschem Format oder unvollständigen Anforderungen generiert. Diese Anforderungen wurden vom Ziel nicht empfangen, anders als in dem Fall, in dem der Load Balancer einen HTTP 460-Fehlercode zurückgibt. Diese Anzahl enthält keine von Zielen erzeugte Antwortcodes. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Minimum, Maximum und Average geben alle 1 zurück. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Beschreibung
`HTTPCode_ELB_5XX_Count`	Anzahl von HTTP-5XX-Server-Fehlercodes, die vom Load Balancer verursacht werden. Diese Anzahl enthält keine von Zielen erzeugte Antwortcodes. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. `Minimum`, `Maximum` und `Average` geben alle 1 zurück. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`HTTPCode_ELB_500_Count`	Anzahl von HTTP-500-Fehlercodes, die vom Load Balancer verursacht werden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`HTTPCode_ELB_502_Count`	Anzahl von HTTP-502-Fehlercodes, die vom Load Balancer verursacht werden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
HTTPCode_ELB_503_Count	Anzahl von HTTP-503-Fehlercodes, die vom Load Balancer verursacht werden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
HTTPCode_ELB_504_Count	Anzahl von HTTP-504-Fehlercodes, die vom Load Balancer verursacht werden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
IPv6ProcessedBytes	Die Gesamtzahl der Byte, die vom Load Balancer über verarbeitet wurden. IPv6 Diese Anzahl ist in ProcessedBytes enthalten. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Beschreibung
IPv6RequestCount	Die Anzahl der vom Load Balancer empfangenen IPv6 Anfragen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Minimum, Maximum und Average geben alle 1 zurück. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
NewConnectionCount	Gesamtanzahl neuer TCP-Verbindungen, die zwischen Clients und Load Balancer und zwischen Load Balancer und Zielen hergestellt wurden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Beschreibung
NonStickyRequestCount	Die Anzahl von Anfragen, bei denen der Load Balancer ein neues Ziel wählte, da eine vorhandene Sticky Session nicht verwendet werden konnte. Beispiel: Die Anfrage war die erste Anfrage von einem neuen Client und es wurde kein Sticky-Cookie vorgelegt oder es wurde ein Sticky-Cookie vorgelegt, aber ohne Angabe eines Ziels, das bei dieser Zielgruppe registriert war, oder das Sticky-Cookie war falsch formatiert oder abgelaufen oder der Load Balancer konnte das Sticky-Cookie aufgrund eines internen Fehlers nicht lesen. Berichtkriterien: Sticky Sessions sind für die Zielgruppe aktiviert. Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes	Die Gesamtzahl der Byte, die vom Load Balancer über IPv4 und verarbeitet wurden IPv6 (HTTP-Header und HTTP-Payload). Diese Anzahl umfasst den Datenverkehr zu und von Clients und Lambda-Funktionen sowie den Datenverkehr von einem Identity Provider (IdP), wenn die Benutzerauthentifizierung aktiviert ist. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Beschreibung
RejectedConnectionCount	Anzahl der abgelehnten Verbindungen, weil der Load Balancer die maximale Anzahl an Verbindungen erreicht hat. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer
RequestCount	Die Anzahl der Anfragen, die über IPv4 und verarbeitet wurden. IPv6 Diese Metrik wird nur für Anforderungen erhöht, bei denen der Load-Balancer-Knoten ein Ziel auswählen konnte. Anforderungen, die abgelehnt werden, bevor ein Ziel ausgewählt wurde, werden in dieser Metrik nicht berücksichtigt. Berichtskriterien: Wird gemeldet, ob es registrierte Ziele gibt. Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer • LoadBalancer , AvailabilityZone • LoadBalancer , TargetGroup • LoadBalancer , AvailabilityZone , TargetGroup

Metrik	Beschreibung
RuleEvaluations	Die Anzahl der Regeln, die vom Load Balancer bei der Verarbeitung von Anfragen ausgewertet wurden. Die Standardregel wird nicht gezählt. Die 10 kostenlosen Regelauswertungen pro Anfrage sind in dieser Zählung enthalten. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer
ZonalShiftedHostCount	Die Anzahl der Ziele, die aufgrund von Zonenverschiebungen als deaktiviert gelten. Berichtskriterien: Wird gemeldet, wenn ein Wert vorhanden ist Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer , TargetGroup . • AvailabilityZone , LoadBalancer , TargetGroup .

Der AWS/ApplicationELB-Namespace enthält die folgenden Metriken für Ziele.

Metrik	Beschreibung
HealthyHostCount	Anzahl der als stabil betrachteten Ziele. Berichtskriterien: Wird gemeldet, wenn es registrierte Ziele gibt. Statistiken: Die nützlichsten Statistiken sind Average, Minimum und Maximum.

Metrik	Beschreibung
	Dimensionen • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`
`HTTPCode_Target_2XX_Count` , `HTTPCode_Target_3XX_Count` , `HTTPCode_Target_4XX_Count` , `HTTPCode_Target_5XX_Count`	Anzahl der HTTP-Antwortcodes, die von den Zielen generiert wurden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten. Berichtskriterien: Wird gemeldet, wenn es registrierte Ziele gibt. Statistiken: Die nützlichste Statistik ist `Sum`. `Minimum`, `Maximum` und `Average` geben alle 1 zurück. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
`RequestCountPerTarget`	Die durchschnittliche Anzahl der Anfragen pro Ziel in einer Zielgruppe. Sie müssen die Zielgruppe mithilfe der Dimension `TargetGroup` angeben. Diese Metrik gilt nicht, wenn das Ziel ist eine Lambda-Funktion ist. Diese Anzahl basiert auf der Gesamtzahl der Anfragen, die von der Zielgruppe eingegangen sind, geteilt durch die Anzahl der gesunden Ziele in der Zielgruppe. Wenn es in der Zielgruppe keine gesunden Ziele gibt, wird sie durch die Gesamtzahl der registrierten Ziele geteilt. Berichtkriterien: Always reported Statistiken: Die einzige zulässige Statistik ist `Sum`. Hier wird der Durchschnitt und nicht die Summe angegeben. Dimensionen • `TargetGroup` • `TargetGroup` , `AvailabilityZone` • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`

Metrik	Beschreibung
TargetConnectionErrorCount	Anzahl der Verbindungen, die zwischen dem Load Balancer und dem Ziel nicht erfolgreich hergestellt wurden. Diese Metrik gilt nicht, wenn das Ziel ist eine Lambda-Funktion ist. Diese Metrik wird für erfolglose Verbindungen mit Integritätsprüfungen nicht erhöht. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup , LoadBalancer • TargetGroup , AvailabilityZone , LoadBalancer
TargetResponseTime	Die verstrichene Zeit in Sekunden, nachdem die Anfrage den Load Balancer verlassen hat, bis das Ziel mit dem Senden der Antworthe ader beginnt. Dies entspricht dem Feld target_processing_time in den Zugriffsprotokollen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichsten Statistiken sind Average und pNN.NN (Perzentile). Dimensionen • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup , LoadBalancer • TargetGroup , AvailabilityZone , LoadBalancer

Metrik	Beschreibung
`TargetTLSNegotiationErrorCount`	Anzahl der TLS-Verbindungen, die vom Load Balancer initiiert wurden und keine Sitzung mit dem Ziel hergestellt haben. Als mögliche Ursachen kommen unter anderem fehlende Übereinstimmung bei Verschlüsselungsverfahren oder Protokollen infrage. Diese Metrik gilt nicht, wenn das Ziel ist eine Lambda-Funktion ist. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`
`UnHealthyHostCount`	Die Anzahl der als instabil betrachteten Ziele. Wenn Sie die Registrierung eines Ziels aufheben, verringert sich dieser Wert, nimmt aber nicht zu. `HealthyHostCount` `UnhealthyHostCount` Berichtskriterien: Wird gemeldet, wenn es registrierte Ziele gibt. Statistiken: Die nützlichsten Statistiken sind `Average`, `Minimum` und `Maximum`. Dimensionen • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`

Der `AWS/ApplicationELB`-Namespace enthält die folgenden Metriken für den Zustand der Zielgruppe. Weitere Informationen finden Sie unter the section called “Zustand der Zielgruppe”.

Metrik	Beschreibung
HealthyStateDNS	Die Anzahl der Zonen, die die Anforderungen an einen fehlerfreien DNS-Zustand erfüllen. Statistiken: Die nützlichste Statistik ist Max. Dimensionen • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
HealthyStateRouting	Die Anzahl der Zonen, die die Anforderungen an einen fehlerfreien Zustand für das Routing erfüllen. Statistiken: Die nützlichste Statistik ist Max. Dimensionen • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
UnhealthyRoutingRequestCount	Die Anzahl der Anforderungen, die mithilfe der Routing-Failover-Aktion (Fail-Open) weitergeleitet werden. Statistiken: Die nützlichste Statistik ist Sum. Dimensionen • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
UnhealthyStateDNS	Die Anzahl der Zonen, die die Anforderungen an einen fehlerfreien DNS-Zustand nicht erfüllen und daher in DNS als fehlerhaft markiert wurden. Statistiken: Die nützlichste Statistik ist Min.

Metrik	Beschreibung
	Dimensionen • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyStateRouting`	Die Anzahl der Zonen, die die Anforderungen an einen fehlerfreien Zustand für das Routing nicht erfüllen. Daher verteilt der Load Balancer den Datenverkehr an alle Ziele in der Zone, einschließlich der fehlerhaften Ziele. Statistiken: Die nützlichste Statistik ist `Min`. Dimensionen • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Der `AWS/ApplicationELB`-Namespace enthält die folgenden Metriken für Lambda-Funktionen, die als Ziele registriert sind.

Metrik	Beschreibung
`LambdaInternalError`	Die Anzahl von Anfragen an eine Lambda-Funktion, die aufgrund eines internen Problems des Load Balancer oder von AWS Lambda fehlgeschlagen sind. Um die Codes für die Fehlerursache zu erhalten, überprüfen Sie das Feld "error_reason" des Zugriffsprotokolls. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `TargetGroup` • `TargetGroup` , `LoadBalancer`

Metrik	Beschreibung
LambdaTargetProcessedBytes	Die Gesamtzahl von Bytes, die vom Load Balancer für Anfragen an und Antworten von einer Lambda-Funktion verarbeitet wurden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • LoadBalancer
LambdaUserError	Die Anzahl von Anfragen an eine Lambda-Funktion, die aufgrund eines Problems mit der Lambda-Funktion fehlgeschlagen sind. Beispiel: Der Load Balancer war nicht zum Aufrufen der Funktion berechtigt, der Load Balancer empfing eine JSON-Datei von der Funktion, die falsch formatiert war oder nicht alle erforderlichen Felder enthielt, oder die Größe des Anfragetextes oder der Antwort überschritt die maximale Größe von 1 MB. Um die Codes für die Fehlerursache zu erhalten, überprüfen Sie das Feld "error_reason" des Zugriffsprotokolls. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist Sum. Dimensionen • TargetGroup • TargetGroup , LoadBalancer

Der AWS/ApplicationELB-Namespace enthält die folgenden Metriken für die Benutzerauthentifizierung.

Metrik	Beschreibung
`ELBAuthError`	Die Anzahl der Benutzerauthentifizierungen, die nicht abgeschlossen werden konnten, weil eine Authentifizierungsaktion falsch konfiguriert war, der Load Balancer keine Verbindung mit dem Identitätsanbieter herstellen konnte oder der Load Balancer den Authentifizierungsfluss aufgrund eines internen Fehlers nicht abschließen konnte. Um die Codes für die Fehlerursache zu erhalten, überprüfen Sie das Feld "error_reason" des Zugriffsprotokolls. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthFailure`	Die Anzahl der Benutzerauthentifizierungen, die nicht abgeschlossen werden konnten, weil der Identitätsanbieter den Zugriff auf den Benutzer abgelehnt hat oder ein Autorisierungscode mehr als einmal verwendet wurde. Um die Codes für die Fehlerursache zu erhalten, überprüfen Sie das Feld "error_reason" des Zugriffsprotokolls. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthLatency`	Die verstrichene Zeit in Millisekunden zur Abfrage des Identitätsanbieter nach dem ID-Token und den Benutzerinformationen. Falls eine oder mehrere dieser Operationen ausfällt, wird ein Fehler ausgegeben.

Metrik	Beschreibung
	Berichtkriterien: Ein Wert ungleich Null Statistiken: Alle Statistiken sind aussagekräftig. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthRefreshTokenSuccess`	Gibt an, wie oft der Load Balancer Benutzeransprüche mit einem vom Identitätsanbieter bereitgestellten Aktualisierungs-Token erfolgreich aktualisiert hat. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthSuccess`	Die Anzahl der Authentifizierungsaktionen, die erfolgreich waren. Diese Metrik wird am Ende des Authentifizierungsworkflows erhöht, wenn der Load Balancer die Benutzeransprüche vom Identität sanbieter abgerufen hat. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
`ELBAuthUserClaimsSizeExceeded`	Gibt an, wie oft ein konfigurierter Identitätsanbieter Benutzeransprüche zurückgegeben hat, die eine Größe von 11 KB überschritten haben. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die einzige aussagekräftige Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik-Dimensionen für Application Load Balancer

Verwenden Sie die nachstehenden Dimensionen, um die Metriken für Ihren Application Load Balancer zu filtern.

Dimension	Beschreibung
`AvailabilityZone`	Filtert die Metrikdaten nach Availability Zone.
`LoadBalancer`	Filtert die Metrikdaten nach Load Balancer. Geben Sie den Load Balancer wie folgt an: app/ load-balancer-name/1234567890123456 (der letzte Teil des Load Balancer-ARN).
`TargetGroup`	Filtert die Metrikdaten nach der Zielgruppe. Geben Sie die Zielgruppe wie folgt an: targetgroup/ target-group-name/1234567890123456 (der letzte Teil des Zielgruppen-ARN).

Statistiken für Application-Load-Balancer-Metriken

CloudWatch stellt Statistiken bereit, die auf den von Elastic Load Balancing veröffentlichten metrischen Datenpunkten basieren. Statistiken sind Metrikdaten-Aggregationen über einen

bestimmten Zeitraum. Wenn Sie Statistiken anfordern, wird der zurückgegebene Datenstrom durch den Metriknamen und die Dimension identifiziert. Eine Dimension ist ein Name-Wert-Paar, durch das eine Metrik eindeutig identifiziert wird. Sie können beispielsweise Statistiken für alle intakten EC2 Instances anfordern, die hinter einem Load Balancer stehen, der in einer bestimmten Availability Zone gestartet wurde.

Die `Minimum`- und `Maximum`-Statistiken geben die Mindest- und Maximalwerte der Datenpunkte an, die von den einzelnen Load Balancer-Knoten in jedem Sampling-Fenster gemeldet werden. Nehmen wir beispielsweise an, es gibt 2 Load-Balancer-Knoten, die den Application Load Balancer bilden. Ein Knoten hat `HealthyHostCount` mit dem `Minimum`-Wert 2, dem `Maximum`-Wert 10 und dem `Average`-Wert 6, während der andere Knoten `HealthyHostCount` mit dem `Minimum`-Wert 1, dem `Maximum`-Wert 5 und dem `Average`-Wert 3 aufweist. Somit weist der Load Balancer den `Minimum`-Wert 1, den `Maximum`-Wert 10 und den `Average`-Wert von etwa 4 auf.

Wir empfehlen Ihnen, in der `Minimum`-Statistik auf `UnHealthyHostCount`-Werte ungleich Null zu achten und bei mehr als einem Datenpunkt einen Alarm zu senden, wenn ein Wert ungleich Null ist. Mithilfe von `Minimum` wird erkannt, wann Ziele von jedem Knoten und jeder Availability Zone Ihres Load Balancers als fehlerhaft eingestuft werden. Das Senden von Alarmen in Bezug auf `Average` oder `Maximum` ist nützlich, wenn Sie vor potenziellen Problemen gewarnt werden möchten. Wir empfehlen unseren Kunden, diese Metrik zu überprüfen und Vorkommnisse zu untersuchen, die ungleich Null sind. Die automatische Behebung von Ausfällen kann gemäß den bewährten Methoden zur Verwendung der Load Balancer-Zustandsprüfung in Amazon EC2 Auto Scaling oder Amazon Elastic Container Service (Amazon ECS) erfolgen.

Die `Sum`-Statistik stellt den Gesamtwert aller Load Balancer-Knoten dar. Da Metriken mehrere Berichte pro Zeitraum umfassen, gilt `Sum` nur für Metriken, die über alle Load Balancer-Knoten aggregiert werden.

Die `SampleCount`-Statistik ist die Zahl der gemessenen Stichproben. Da Metriken basierend auf Erfassungsintervallen und Ereignissen erfasst werden, ist diese Statistik in der Regel nicht nützlich. Bei `HealthyHostCount` basiert `SampleCount` z. B. auf der Anzahl der Stichproben, die jeder Load Balancer-Knoten meldet, nicht auf der Anzahl fehlerfreier Hosts.

Ein Perzentil gibt die relative Stelle eines Wertes in einem Datensatz an. Sie können ein beliebiges Perzentil mit bis zu zwei Dezimalstellen (z. B. p95,45) angeben. Ein 95. Perzentil bedeutet, dass 95 Prozent der Daten unter diesem Wert und 5 Prozent darüber liegen. Perzentile werden häufig genutzt, um Anomalien zu isolieren. Angenommen, eine Anwendung bedient die meisten Anforderungen aus einem Cache in 1-2 ms, aber benötigt 100 bis 200 ms, wenn der Cache leer ist.

Das Maximum spiegelt den langsamsten Fall wider, etwa 200 ms. Der Durchschnitt gibt nicht die Verteilung der Daten an. Perzentile bieten eine aussagekräftigere Darstellung der Anwendungs-Performance. Indem Sie das 99. Perzentil als Auto Scaling-Trigger oder CloudWatch Alarm verwenden, können Sie festlegen, dass die Verarbeitung von nicht mehr als 1 Prozent der Anfragen länger als 2 ms dauert.

CloudWatch Metriken für Ihren Load Balancer anzeigen

Sie können die CloudWatch Metriken für Ihre Load Balancer mithilfe der EC2 Amazon-Konsole anzeigen. Diese Metriken werden in Überwachungsdiagrammen dargestellt. Die Überwachungsdiagramme zeigen Datenpunkte, wenn der Load Balancer aktiv ist und Anforderungen erhält.

Alternativ können Sie Metriken für Ihren Load Balancer mit der CloudWatch-Konsole anzeigen.

So zeigen Sie Metriken mithilfe der -Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um nach Zielgruppe gefilterte Metriken anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Navigationsbereich Target Groups aus.
   b. Wählen Sie Ihre Zielgruppe und wählen Sie dann die Registerkarte Monitoring (Überwachung) aus.
   c. (Optional) Wählen Sie in Showing data for einen Zeitbereich aus., um die Ergebnisse nach Zeit zu filtern.
   d. Wenn Sie eine größere Ansicht einer Metrik aufrufen möchten, wählen Sie ihr Diagramm aus.
3. Um nach Load Balancer gefilterte Metriken anzuzeigen, gehen Sie wie folgt vor:
   a. Klicken Sie im Navigationsbereich auf Load Balancers.
   b. Wählen Sie Ihren Load Balancer aus und wählen Sie dann die Registerkarte Monitoring (Überwachung) aus.
   c. (Optional) Wählen Sie in Showing data for einen Zeitbereich aus., um die Ergebnisse nach Zeit zu filtern.
   d. Wenn Sie eine größere Ansicht einer Metrik aufrufen möchten, wählen Sie ihr Diagramm aus.

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Namespace ApplicationELB aus.
4. (Optional) Um eine Metrik in allen Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.
5. (Optional) Um nach Maß zu filtern, wählen Sie einen der folgenden Schritte aus:

   - Wenn Sie nur die für Ihre Load Balancer gemeldeten Metriken anzeigen möchten, wählen Sie Per AppELB Metrics (Pro AppELB-Metrik). aus . Um die Metriken für einen einzelnen Load Balancer anzuzeigen, geben Sie den Namen in das Suchfeld ein.
   - Wenn Sie ausschließlich die für Ihre Load Balancer gemeldeten Zielgruppen anzeigen möchten, wählen Sie Per AppELB, per TG Metrics (Metriken pro AppELB, pro Zielgruppe) aus. Um die Metriken für eine einzelne Zielgruppe anzuzeigen, geben Sie den Namen in das Suchfeld ein.
   - Wenn Sie ausschließlich die für Ihre Load Balancer gemeldeten Metriken nach Availability Zone anzeigen möchten, wählen Sie Per AppELB, per AZ Metrics (Metriken pro AZ, pro AppELB) aus. Um die Metriken für einen einzelnen Load Balancer anzuzeigen, geben Sie den Namen in das Suchfeld ein. Um die Metriken für eine einzelne Availability Zone anzuzeigen, geben Sie den Namen in das Suchfeld ein.
   - Wenn Sie ausschließlich die für Ihre Load Balancer gemeldeten Metriken nach Availability Zone und Zielgruppe anzeigen möchten, wählen Sie Per AppELB, per AZ, per TG Metrics (Metriken pro AZ, pro AppELB, pro Zielgruppe) aus. Um die Metriken für einen einzelnen Load Balancer anzuzeigen, geben Sie den Namen in das Suchfeld ein. Um die Metriken für eine einzelne Zielgruppe anzuzeigen, geben Sie den Namen in das Suchfeld ein. Um die Metriken für eine einzelne Availability Zone anzuzeigen, geben Sie den Namen in das Suchfeld ein.

Um Metriken mit dem anzuzeigen AWS CLI

Verwenden Sie den folgenden list-metrics-Befehl, um die verfügbaren Metriken aufzuführen:

```
aws cloudwatch list-metrics --namespace AWS/ApplicationELB
```

Um die Statistiken für eine Metrik abzurufen, verwenden Sie AWS CLI

Verwenden Sie den folgenden get-metric-statisticsBefehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. CloudWatch behandelt jede eindeutige Kombination von Dimensionen als separate Metrik. Sie können keine Statistiken abrufen, die Kombinationen von Dimensionen verwenden, die nicht speziell veröffentlicht wurden. Sie müssen die gleichen Dimensionen angeben, die bei der Erstellung der Metriken verwendet wurden.

```
aws cloudwatch get-metric-statistics --namespace AWS/ApplicationELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=app/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2016-04-18T00:00:00Z --end-time 2016-04-21T00:00:00Z
```

Das Folgende ist Ausgabebeispiel:

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2016-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Zugriffsprotokolle für Ihre Application Load Balancer

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen zu Anforderungen erfassen, die an Ihren Load Balancer gesendet werden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembehebung verwenden.

Zugriffsprotokolle sind ein optionales Feature von Elastic Load Balancing, das standardmäßig deaktiviert ist. Nachdem Sie die Zugriffsprotokolle für Ihren Load Balancer aktiviert haben, erfasst Elastic Load Balancing die Protokolle und speichert sie in dem von Ihnen angegebenen Amazon-S3-Bucket als komprimierte Dateien. Sie können die Zugriffsprotokolle jederzeit deaktivieren.

Sie zahlen Speicherkosten für Amazon S3, aber Sie zahlen nicht für die Bandbreite, die von Elastic Load Balancing zum Senden von Protokolldateien an Amazon S3 verwendet wird. Weitere Information zu Speicherkosten finden Sie unter Amazon S3 – Preise.

Inhalt

- Zugriffsprotokolldateien
- Zugriffsprotokolleinträge
- Beispiel-Protokolleinträge
- Verarbeiten von Zugriffsprotokolldateien
- Aktivieren der Zugriffsprotokolle für Ihren Application Load Balancer
- Deaktivieren der Zugriffsprotokolle für Ihren Application Load Balancer

Zugriffsprotokolldateien

Elastic Load Balancing veröffentlicht alle 5 Minuten eine Protokolldatei für jeden Load-Balancer-Knoten. Die Protokollbereitstellung ist letztendlich konsistent. Der Load Balancer kann mehrere Protokolle für denselben Zeitraum bereitstellen. Dies passiert in der Regel, wenn die Website hohen Datenverkehr aufweist.

Die Dateinamen der Zugriffsprotokolle verwenden das folgende Format:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_app.load-balancer-id_end-time_ip-address_random-string.log.gz
```

bucket

Der Name des S3-Buckets.

prefix

(Optional) Das Präfix (logische Hierarchie) für den Bucket. Das von Ihnen angegebene Präfix darf die Zeichenfolge `AWSLogs` nicht enthalten. Weitere Informationen finden Sie unter Organisieren von Objekten mit Präfixen.

`AWSLogs`

Wir fügen den Teil des Dateinamens hinzu, der mit `AWSLogs` nach dem von Ihnen angegebenen Bucket-Namen und dem optionalen Präfix beginnt.

aws-account-id

Die AWS Konto-ID des Besitzers.

Region

Die Region für Ihren Load Balancer und den S3-Bucket.

JJJJ/MM/TT

Das Datum, an dem das Protokoll übermittelt wurde.

load-balancer-id

Die Ressourcen-ID des Load Balancer. Wenn die Ressourcen-ID Schrägstriche (/) enthält, werden sie durch Punkte (.) ersetzt.

end-time

Das Datum und die Uhrzeit, an dem das Protokollierungsintervall endete. Beispiel: Die Endzeit 20140215T2340Z enthält Einträge für Anforderungen, die zwischen 23:35 und 23:40 in UTC- oder Zulu-Zeit durchgeführt wurden.

ip-address

Die IP-Adresse des Load Balancer-Knotens, der die Anforderung verarbeitet hat. Für einen internen Load Balancer handelt es sich hierbei um eine private IP-Adresse.

random-string

Eine vom System generierte zufällige Zeichenfolge.

Im Folgenden finden Sie ein Beispiel für einen Protokolldateinamen mit Präfix:

```
s3://amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/
elasticloadbalancing/us-east-2/2022/05/01/123456789012_elasticloadbalancing_us-
east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Im Folgenden finden Sie ein Beispiel für einen Protokolldateinamen ohne Präfix:

```
s3://amzn-s3-demo-logging-bucket/AWSLogs/123456789012/elasticloadbalancing/
us-east-2/2022/05/01/123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Sie können Ihre Protokolldateien beliebig lange im Bucket speichern. Sie können aber auch Amazon S3-Lebenszyklusregeln aufstellen, anhand derer die Protokolldateien automatisch archiviert oder gelöscht werden. Weitere Informationen finden Sie unter Object Lifecycle Management im Amazon S3 S3-Benutzerhandbuch.

Zugriffsprotokolleinträge

Elastic Load Balancing protokolliert Anforderungen, die an den Load Balancer gesendet wurden, einschließlich Anforderungen, die nicht bei den Zielen ankamen. Wenn ein Client beispielsweise eine falsch formatierte Anfrage sendet oder keine fehlerfreien Ziele vorhanden sind, die auf die Anfrage reagieren können, wird die Anfrage dennoch protokolliert. Elastic Load Balancing protokolliert keine Zustandsprüfungsanforderungen.

Jeder Protokolleintrag enthält die Details einer einzelnen Anfrage (oder Verbindung im Fall von WebSockets), die an den Load Balancer gestellt wurde. Denn ein Eintrag wird erst geschrieben WebSockets, nachdem die Verbindung geschlossen wurde. Wenn die erweiterte Verbindung nicht hergestellt werden kann, entspricht der Eintrag dem für eine HTTP- oder HTTPS-Anfrage.

> **Important**
>
> Elastic Load Balancing protokolliert Anforderungen nach bestmöglichem Bemühen. Wir empfehlen, dass Sie die Zugriffsprotokolle verwende, um die Art der Anforderungen zu verstehen, nicht als eine vollständige Buchführung aller Anforderungen.

Inhalt

- Syntax
- Ergriffene Maßnahmen
- Gründe für die Klassifizierung
- Codes für die Fehlerursache

Syntax

Die folgende Tabelle beschreibt die Felder eines Zugriffsprotokolleintrags der Reihe nach. Alle Felder werden durch Leerzeichen voneinander getrennt. Wenn neue Felder eingeführt werden, werden sie am Ende des Protokolleintrags hinzugefügt. Sie sollten alle Felder am Ende des Protokolleintrags ignorieren, die Sie nicht erwartet haben.

Feld	Beschreibung
type	Der Typ der Anfrage oder Verbindung. Die möglichen Werte sind wie folgt (alle anderen Werte ignorieren): • `http` – HTTP • `https` – HTTP über TLS • `h2` – HTTP/2 über TLS • `grpcs` – gRPC über TLS • `ws` — WebSockets • `wss`— WebSockets über TLS
time	Die Zeit, zu der der Load Balancer eine Antwort an den Client generiert hat, im Format ISO 8601. Denn dies ist die Zeit WebSockets, in der die Verbindung geschlossen wird.
elb	Die Ressourcen-ID des Load Balancer. Beachten Sie beim Analysieren von Zugriffs-Logeinträgen, dass Ressourcen Schrägstriche (/) enthalten IDs können.
client:port	Die IP-Adresse und den Port des anfordernden Clients. Wenn sich vor dem Load Balancer ein Proxy befindet, enthält dieses Feld die IP-Adresse des Proxys.
target:port	Die IP-Adresse und der Port des Ziels, das diese Anfrage verarbeitet hat. Wenn der Client keine vollständige Anfrage gesendet hat, kann der Load Balancer die Anfrage keinem Ziel zuteilen, und dieser Wert wird auf - festgelegt. Wenn das Ziel eine Lambda-Funktion ist, ist dieser Wert auf - einstellt.

Feld	Beschreibung
	Wenn die Anfrage von blockiert wird AWS WAF, wird dieser Wert auf - gesetzt.
request_processing_time	Die insgesamt verstrichene Zeit (in Sekunden, mit einer Genauigkeit in Millisekunden) ab dem Zeitpunkt, zu dem der Load Balancer die Anforderung erhalten hat, bis zu dem Zeitpunkt, zu dem er die Anforderung an ein Ziel gesendet hat. Dieser Wert wird auf -1 festgelegt, wenn der Load Balancer die Anfrage keinem Ziel zuteilen kann. Dies kann der Fall sein, wenn das Ziel die Verbindung vor dem Leerlaufzeitlimit schließt, oder wenn der Client eine falsch formatierte Anfrage sendet. Dieser Wert kann auch auf -1 gesetzt werden, wenn keine TCP-Verbindung mit dem Ziel hergestellt werden kann, bevor das 10-Sekunden-Timeout für die TCP-Verbindung erreicht ist. Wenn für Ihren Application Load Balancer aktiviert AWS WAF ist oder der Zieltyp eine Lambda-Funktion ist, wird die Zeit, die der Client benötigt, um die erforderlichen Daten für POST-Anfragen zu senden, angerechnet. `request_processing_time`

Feld	Beschreibung
target_processing_time	Die insgesamt verstrichene Zeit (in Sekunden, mit einer Genauigkeit in Millisekunden) ab dem Zeitpunkt, zu dem der Load Balancer die Anfrage an ein Ziel gesendet hat, bis zu dem Zeitpunkt, zu dem das Ziel begonnen hat, die Antwort-Header zu senden. Dieser Wert wird auf -1 festgelegt, wenn der Load Balancer die Anfrage keinem Ziel zuteilen kann. Dies kann der Fall sein, wenn das Ziel die Verbindung vor dem Leerlaufzeitlimit schließt, oder wenn der Client eine falsch formatierte Anfrage sendet. Dieser Wert kann auch auf -1 gesetzt werden, wenn das registrierte Ziel nicht vor dem Timeoutwert für die Leerlaufzeit antwortet. Wenn es für Ihren Application Load Balancer nicht aktiviert AWS WAF ist, wird die Zeit angerechnet`target_processing_time` , die der Client benötigt, um die erforderlichen Daten für POST-Anfragen zu senden.
response_processing_time	Die insgesamt verstrichene Zeit (in Sekunden, mit einer Genauigkeit in Millisekunden) ab dem Zeitpunkt, zu dem der Load Balancer den Antwort-Header vom Ziel erhalten hat, bis zu dem Zeitpunkt, zu dem er begonnen hat, die Antwort an den Client zu senden. Dies umfasst sowohl die Wartezeit am Load Balancer als auch die Zeit für die Herstellung der Verbindung vom Load Balancer zum Client. Dieser Wert wird auf -1 gesetzt, wenn der Load Balancer keine Antwort von einem Ziel erhält. Dies kann der Fall sein, wenn das Ziel die Verbindung vor dem Leerlaufzeitlimit schließt, oder wenn der Client eine falsch formatierte Anfrage sendet.
elb_status_code	Der Statuscode der Antwort, die vom Load Balancer, der festen Antwortregel oder dem AWS WAF benutzerdefinierten Antwortcode für Blockaktionen generiert wurde.

Feld	Beschreibung
target_status_code	Der Statuscode der Antwort vom Ziel. Dieser Wert wird nur aufgezeic hnet, wenn eine Verbindung zum Ziel hergestellt wurde und das Ziel eine Antwort gesendet hat. Andernfalls lautet der Wert –.
received_bytes	Die Größe der Anforderung, in Byte, die vom Client (Auftraggeber) eingegangen ist. Bei HTTP-Anfragen sind die Header eingeschlossen. Für ist dies die Gesamtzahl der Byte WebSockets, die vom Client über die Verbindung empfangen wurden.
sent_bytes	Die Größe der Antwort, in Byte, die an den Client (Auftraggeber) gesendet wurde. Bei HTTP-Anfragen umfasst dies die Header und den Hauptteil der Antwort. Denn dies ist die Gesamtzahl der Byte WebSocket s, die über die Verbindung an den Client gesendet wurden. Die TCP-Header und die TLS-Handshake-Payload werden nicht gezählt und haben keine Korrelation zu in. `DataTransfer-Out-Bytes` AWS Cost Explorer
„request“	Die Anfragezeile vom Client in Anführungszeichen und protokolliert mit folgendem Format: HTTP-Methode + Protokoll://Host:Port/URI + HTTP-Version. Der Load Balancer behält die vom Client gesendete URL bei der Aufnahme des Anforderungs-URI unverändert bei. Es wird kein Inhaltsty p für die Zugriffsprotokolldatei festgelegt. Berücksichtigen Sie bei der Verarbeitung des Feldes, wie der Client die URL gesendet hat.
„user_agent“	Eine User-Agent-Zeichenfolge, die den Client identifiziert, von dem die Anfrage stammt, in Anführungszeichen. Die Zeichenfolge besteht aus einem oder mehreren Produkt-IDs, Produkt[/Version]. Wenn die Zeichenfolge länger als 8 KB ist, wird sie gekürzt.
ssl_cipher	[HTTPS-Listener] Die SSL-Verschlüsselung. Dieser Wert ist auf „-“ festgelegt, wenn es sich bei dem Listener nicht um einen HTTPS-Lis tener handelt.
ssl_protocol	[HTTPS-Listener] Das SSL-Protokoll. Dieser Wert ist auf „-“ festgelegt, wenn es sich bei dem Listener nicht um einen HTTPS-Listener handelt.

Feld	Beschreibung
target_group_arn	Der Amazon-Ressourcenname (ARN) der Zielgruppe.
"trace_id"	Der Inhalt des X-Amzn-Trace-Id-Headers in Anführungszeichen.
"domain_name"	[HTTPS-Listener] Die vom Client beim TLS-Handshake bereitgestellte SNI-Domain in Anführungszeichen. Dieser Wert wird auf - festgelegt, wenn der Client SNI nicht unterstützt oder die Domain keinem Zertifikat entspricht und dem Client das Standardzertifikat vorgelegt wird.
"chosen_cert_arn"	[HTTPS-Listener] Der ARN des Zertifikats, das dem Client vorgelegt wird, in Anführungszeichen. Dieser Wert ist auf `session-reused` festgelegt, wenn die Sitzung wiederverwendet wird. Dieser Wert ist auf „-“ festgelegt, wenn es sich bei dem Listener nicht um einen HTTPS-Lis tener handelt.
matched_rule_priority	Der Prioritätswert der Regel, die eine Übereinstimmung mit der Anforderung erzeugt. Wenn eine Regel eine Übereinstimmung erzeugt hat, ist dies ein Wert zwischen 1 und 50.000. Hat keine Regel eine Übereinstimmung erzeugt und die Standardaktion wurde ausgeführt, ist dieser Wert 0. Wenn während der Regelauswertung ein Fehler auftritt, beträgt der Wert -1. Für alle anderen Fehler lautet der Wert -.
request_creation_time	Die Uhrzeit, zu der der Load Balancer die Anforderung vom Client erhalten hat, im ISO 8601-Format.
"actions_executed"	Die bei der Verarbeitung der Anfrage ergriffenen Maßnahmen in Anführungszeichen. Dieser Wert ist eine durch Kommas getrennte Liste, die die in Ergriffene Maßnahmen beschriebenen Werte enthalten kann. Wenn keine Maßnahmen ergriffen wurden, beispielsweise bei einer falsch formatierten Anfrage, wird dieser Wert auf - festgelegt.
"redirect_url"	Die URL des Weiterleitungsziels für den Location-Header der HTTP-Antwort in doppelten Anführungszeichen. Wenn keine Weiterleitungsakti onen ausgeführt wurden, wird dieser Wert auf "-" eingestellt.

Feld	Beschreibung
"error_reason"	Der Ursachencode in doppelten Anführungszeichen. Wenn die Anforderung fehlschlug, ist dies einer der in Codes für die Fehlerursache beschriebenen Fehlercodes. Wenn die durchgeführten Aktionen keine Authentifizierungsaktion umfassen oder das Ziel keine Lambda-Funktion ist, wird dieser Wert auf „-“ festgelegt.
„target:port_list“	Eine durch Leerzeichen getrennte Liste von IP-Adressen und Ports für die Ziele, die diese Anforderung verarbeitet haben, eingeschlossen in doppelten Anführungszeichen. Derzeit kann diese Liste ein Element enthalten und es entspricht dem target:port-Feld. Wenn der Client keine vollständige Anfrage gesendet hat, kann der Load Balancer die Anfrage keinem Ziel zuteilen, und dieser Wert wird auf - festgelegt. Wenn das Ziel eine Lambda-Funktion ist, ist dieser Wert auf - einstellt. Wenn die Anfrage von blockiert wird AWS WAF, wird dieser Wert auf - gesetzt.
„target_status_code_list“	Eine durch Leerzeichen getrennte Liste von Statuscodes aus den Antworten der Ziele, die in doppelte Anführungszeichen eingeschlossen sind. Derzeit kann diese Liste ein Element enthalten und entspricht dem target_status_code-Feld. Dieser Wert wird nur aufgezeichnet, wenn eine Verbindung zum Ziel hergestellt wurde und das Ziel eine Antwort gesendet hat. Andernfalls lautet der Wert –.
„classification“	Die Klassifikation für die desynchrone Mitigation in doppelten Anführungszeichen. Wenn die Anforderung nicht den Anforderungen von RFC 7230 entspricht, lauten die möglichen Werte „Acceptable“ (Akzeptabel), „Ambiguous“ (Mehrdeutig) und „Severe“ (Schwerwiegend). Wenn die Anforderung RFC 7230 entspricht, wird dieser Wert auf „-“ gesetzt.

Feld	Beschreibung
„classification_reason“	Der Ursachencode für die Klassifizierung steht in doppelten Anführung szeichen. Wenn die Anforderung nicht RFC 7230 entspricht, ist dies einer der unter Gründe für die Klassifizierung beschriebenen Klassifiz ierungscodes. Wenn die Anforderung RFC 7230 entspricht, wird dieser Wert auf „-“ gesetzt.
conn_trace_id	Die Verbindungsrückverfolgbarkeits-ID ist eine eindeutige undurchsi chtige ID, die zur Identifizierung jeder Verbindung verwendet wird. Nachdem eine Verbindung mit einem Client hergestellt wurde, enthalten nachfolgende Anfragen von diesem Client diese ID in ihren jeweiligen Zugriffsprotokolleinträgen. Diese ID fungiert als Fremdschlüssel, um eine Verbindung zwischen den Verbindungs- und Zugriffsprotokollen herzustel len.

Ergriffene Maßnahmen

Der Load Balancer speichert die ausgeführten Maßnahmen im Feld „actions_executed“ des Zugriffsprotokolls.

- `authenticate` – Der Load Balancer hat die Sitzung validiert, den Benutzer authentifiziert und die Benutzerinformationen den Anforderungs-Headern hinzugefügt, wie in der Regelkonfiguration angegeben.
- `fixed-response` – Der Load Balancer hat eine feste Antwort ausgegeben, wie in der Regelkonfiguration angegeben.
- `forward` – Der Load Balancer hat die Anforderung an ein Ziel weitergeleitet, wie in der Regelkonfiguration angegeben.
- `redirect` – Der Load Balancer hat die Anforderung an eine andere URL weitergeleitet, wie in der Regelkonfiguration angegeben.
- `waf` – Der Load Balancer hat die Anforderung an AWS WAF weitergeleitet, um festzustellen, ob die Anforderung an das Ziel weitergeleitet werden sollte. Wenn dies die letzte Aktion ist, wurde AWS WAF festgestellt, dass die Anfrage abgelehnt werden sollte. Standardmäßig AWS WAF werden Anfragen, die von abgelehnt wurden, im `elb_status_code` Feld als „403“ protokolliert. Wenn AWS WAF es so konfiguriert ist, dass Anfragen mit einem benutzerdefinierten Antwortcode abgelehnt werden, spiegelt das `elb_status_code` Feld den konfigurierten Antwortcode wider.

- `waf-failed`— Der Load Balancer hat versucht, die Anfrage weiterzuleiten AWS WAF, aber dieser Vorgang ist fehlgeschlagen.

Gründe für die Klassifizierung

Wenn eine Anforderung nicht RFC 7230 entspricht, speichert der Load Balancer einen der folgenden Codes im Feld „classification_reason“ des Zugriffsprotokolls. Weitere Informationen finden Sie unter Desynchroner Mitigationsmodus.

Code	Beschreibung	Klassifizierung
`AmbiguousUri`	Der Anforderungs-URI enthält Steuerzeichen.	Mehrdeutig
`BadContentLength`	Der Content-Length-Header enthält einen Wert, der nicht analysiert werden kann oder der keine gültige Zahl ist.	Schwerwiegend
`BadHeader`	Ein Header enthält ein Nullzeichen oder einen Zeilenumbuch.	Schwerwiegend
`BadTransferEncoding`	Der Transfer-Encoding-Header enthält einen ungültigen Wert.	Schwerwiegend
`BadUri`	Die Anforderungs-URI enthält ein Nullzeichen oder ein Zeilenumkehrzeichen.	Schwerwiegend
`BadMethod`	Die Anforderungsmethode ist falsch formatiert.	Schwerwiegend
`BadVersion`	Die Anforderungsversion ist falsch formatiert.	Schwerwiegend
`BothTeClPresent`	Die Anforderung enthält sowohl einen Transfer-Encoding-Header als auch einen Content-Length-Header.	Mehrdeutig
`DuplicateContentLength`	Es gibt mehrere Content-Length-Header mit demselben Wert.	Mehrdeutig
`EmptyHeader`	Eine Kopfzeile ist leer oder es gibt eine Zeile, die nur Leerzeichen enthält.	Mehrdeutig

Code	Beschreibung	Klassifizierung
`GetHeadZeroContentLength`	Es gibt einen Content-Length-Header mit dem Wert 0 für eine GET- oder HEAD-Anforderung.	Akzeptabel
`MultipleContentLength`	Es gibt mehrere Content-Length-Header mit verschiedenen Werten.	Schwerwiegend
`MultipleTransferEncodingChunked`	Es gibt mehrere „Transfer-Encoding: chunked“-Header.	Schwerwiegend
`NonCompliantHeader`	Ein Header enthält ein Nicht-ASCII- oder Steuerzeichen.	Akzeptabel
`NonCompliantVersion`	Die Anforderungsversion enthält einen ungültigen Wert.	Akzeptabel
`SpaceInUri`	Die Anforderungs-URI enthält ein Leerzeichen, das nicht URL-codiert ist.	Akzeptabel
`SuspiciousHeader`	Es gibt einen Header, der mithilfe gängiger Textnormalisierungstechniken auf Transfer-Encoding oder Content-Length normalisiert werden kann.	Mehrdeutig
`SuspiciousTeClPresent`	Die Anfrage enthält sowohl einen Transfer-Encoding-Header als auch einen Content-Length-Header, von denen mindestens einer verdächtig ist.	Schwerwiegend
`UndefinedContentLengthSemantics`	Für eine GET- oder HEAD-Anforderung ist ein Content-Length-Header definiert.	Mehrdeutig

Code	Beschreibung	Klassifizierung
`UndefinedTransferEncodingSemantics`	Für eine GET- oder HEAD-Anforderung ist ein Transfer-Encoding-Header definiert.	Mehrdeutig

Codes für die Fehlerursache

Wenn der Load Balancer keine Authentifizierungsaktion abschließen kann, speichert er einen der folgenden Ursachencodes im Feld „error_reason“ im Aktionsprotokoll. Der Load Balancer erhöht auch die entsprechende Metrik. CloudWatch Weitere Informationen finden Sie unter Authentifizieren von Benutzern mithilfe eines Application Load Balancers.

Code	Beschreibung	Metrik
`AuthInvalidCookie`	Das Authenitfizierungs-Cookie ist ungültig.	`ELBAuthFailure`
`AuthInvalidGrantError`	Der Code zur Gewährung der Authentifizierungs vom Token-Endpunkt ist ungültig.	`ELBAuthFailure`
`AuthInvalidIdToken`	Das ID-Token ist ungültig.	`ELBAuthFailure`
`AuthInvalidStateParam`	Der Zustandsparameter ist ungültig.	`ELBAuthFailure`
`AuthInvalidTokenResponse`	Die Antwort vom Token-Endpunkt ist ungültig.	`ELBAuthFailure`
`AuthInvalidUserinfoResponse`	Die Antwort vom Benutzerinformationsendpunkt ist ungültig.	`ELBAuthFailure`

Code	Beschreibung	Metrik
`AuthMissingCodeParam`	Der Authentifizierungsantwort vom Authentifizierungsendpunkt fehlt ein Abfrageparameter namens „code“.	`ELBAuthFailure`
`AuthMissingHostHeader`	Der Authentifizierungsantwort vom Authentifizierungsendpunkt fehlt ein Host-Header-Feld.	`ELBAuthError`
`AuthMissingStateParam`	Der Authentifizierungsantwort vom Authentifizierungsendpunkt fehlt ein Abfrageparameter namens „state“.	`ELBAuthFailure`
`AuthTokenEpRequestFailed`	Es liegt eine Fehlerantwort (non-2XX) vom Token-Endpunkt vor.	`ELBAuthError`
`AuthTokenEpRequestTimeout`	Der Load Balancer kann nicht mit dem Token-Endpunkt kommunizieren, oder der Token-Endpunkt reagiert nicht innerhalb von 5 Sekunden.	`ELBAuthError`
`AuthUnhandledException`	Der Load Balancer hat eine unbehandelte Ausnahme festgestellt.	`ELBAuthError`
`AuthUserinfoEpRequestFailed`	Es liegt eine Fehlerantwort (non-2XX) vom Identitätsanbieter-Benutzerinformationsendpunkt vor.	`ELBAuthError`
`AuthUserinfoEpRequestTimeout`	Der Load Balancer kann nicht mit dem IdP-Benutzerinfo-Endpunkt kommunizieren, oder der Benutzerinfo-Endpunkt reagiert nicht innerhalb von 5 Sekunden.	`ELBAuthError`
`AuthUserinfoResponseSizeExceeded`	Die Größe der vom Identitätsanbieter zurückgegebenen Ansprüche übersteigt 11 K Byte.	`ELBAuthUserClaimsSizeExceeded`

Wenn eine Anforderung an eine gewichtete Zielgruppe fehlschlägt, speichert der Load Balancer einen der folgenden Fehlercodes im Feld „error_reason“ des Zugriffsprotokolls.

Code	Beschreibung
`AWSALBTGCookieInvalid`	Das AWSALBTG Cookie, das für gewichtete Zielgruppen verwendet wird, ist nicht gültig. Beispielsweise gibt der Load Balancer diesen Fehler zurück, wenn Cookie-Werte URL-codiert sind.
`WeightedTargetGroupsUnhandledException`	Der Load Balancer hat eine unbehandelte Ausnahme festgestellt.

Wenn eine Anforderung an eine Lambda-Funktion fehlschlägt, speichert der Load Balancer eine der folgenden Ursachencodes im Feld "error_reason" des Zugriffsprotokolls. Der Load Balancer erhöht auch die entsprechende CloudWatch Metrik. Weitere Informationen finden Sie unter der Lambda-Aktion Invoke.

Code	Beschreibung	Metrik
`LambdaAccessDenied`	Der Load Balancer war nicht zum Aufrufen der Lambda-Funktion berechtigt.	`LambdaUserError`
`LambdaBadRequest`	Der Lambda-Aufruf ist fehlgeschlagen, da die Clientanforderungsheader oder der Hauptteil nicht nur UTF-8-Zeichen enthalten.	`LambdaUserError`
`LambdaConnectionError`	Der Load Balancer kann keine Verbindung mit Lambda herstellen.	`LambdaInternalError`
`LambdaConnectionTimeout`	Bei dem Versuch, eine Verbindung mit Lambda herzustellen, ist eine Zeitüberschreitung aufgetreten.	`LambdaInternalError`

Code	Beschreibung	Metrik
`LambdaEC2AccessDeniedException`	Amazon EC2 hat während der Funktionsinitialisierung den Zugriff auf Lambda verweigert.	`LambdaUserError`
`LambdaEC2ThrottledException`	Amazon hat Lambda während der EC2 Funktionsinitialisierung gedrosselt.	`LambdaUserError`
`LambdaEC2UnexpectedException`	Amazon EC2 ist bei der Funktionsinitialisierung auf eine unerwartete Ausnahme gestoßen.	`LambdaUserError`
`LambdaENILimitReachedException`	Lambda konnte in der VPC, die in der Konfiguration der Lambda-Funktion angegeben wird, keine Netzwerkschnittstelle erstellen, da das Limit für Netzwerkschnittstellen überschritten wurde.	`LambdaUserError`
`LambdaInvalidResponse`	Die Antwort von der Lambda-Funktion ist falsch formatiert oder enthält nicht alle erforderlichen Felder.	`LambdaUserError`
`LambdaInvalidRuntimeException`	Die angegebene Version der Lamda-Laufzeit wird nicht unterstützt.	`LambdaUserError`
`LambdaInvalidSecurityGroupIDException`	Die angegebene Sicherheitsgruppen-ID in der Konfiguration der Lambda-Funktion ist nicht gültig.	`LambdaUserError`
`LambdaInvalidSubnetIDException`	Die angegebene Subnetz-ID in der Konfiguration der Lambda-Funktion ist nicht gültig.	`LambdaUserError`

Code	Beschreibung	Metrik
`LambdaInvalidZipFileException`	Lambda konnte die angegebene Funktions-Zip-Datei nicht entpacken.	`LambdaUserError`
`LambdaKMSAccessDeniedException`	Lambda konnte die Umgebungsvariablen nicht entschlüsseln, da der Zugriff auf den KMS-Schlüssel abgelehnt wurde. Überprüfen Sie die KMS-Berechtigungen der Lambda-Funktion.	`LambdaUserError`
`LambdaKMSDisabledException`	Lambda konnte die Umgebungsvariablen nicht entschlüsseln, da der angegebene KMS-Schlüssel deaktiviert ist. Überprüfen Sie die Einstellungen des KMS-Schlüssels der Lambda-Funktion.	`LambdaUserError`
`LambdaKMSInvalidStateException`	Lambda konnte die Umgebungsvariablen nicht entschlüsseln, da der Zustand des KMS-Schlüssels nicht gültig ist. Überprüfen Sie die Einstellungen des KMS-Schlüssels der Lambda-Funktion.	`LambdaUserError`
`LambdaKMSNotFoundException`	Lambda konnte die Umgebungsvariablen nicht entschlüsseln, da der KMS-Schlüssel nicht gefunden wurde. Überprüfen Sie die Einstellungen des KMS-Schlüssels der Lambda-Funktion.	`LambdaUserError`
`LambdaRequestTooLarge`	Die Größe des Anfragetextes überschritt 1 MB.	`LambdaUserError`
`LambdaResourceNotFound`	Die Lambda-Funktion konnte nicht gefunden werden.	`LambdaUserError`
`LambdaResponseTooLarge`	Die Größe der Antwort überschritt 1 MB.	`LambdaUserError`

Code	Beschreibung	Metrik
`LambdaServiceException`	Bei Lambda trat ein interner Fehler auf.	`LambdaInternalError`
`LambdaSubnetIPAddressLimitReachedException`	Lambda konnte den VPC-Zugriff für die Lambda-Funktion nicht einrichten, da ein oder mehrere konfigurierte Subnetze keine verfügbaren IP-Adressen haben.	`LambdaUserError`
`LambdaThrottling`	Die Lambda-Funktion wurde gedrosselt, da es zu viele Anfragen gab.	`LambdaUserError`
`LambdaUnhandled`	Bei der Lambda-Funktion trat eine unbehandelte Ausnahme auf.	`LambdaUserError`
`LambdaUnhandledException`	Der Load Balancer hat eine unbehandelte Ausnahme festgestellt.	`LambdaInternalError`
`LambdaWebsocketNotSupported`	WebSockets werden von Lambda nicht unterstützt.	`LambdaUserError`

Wenn der Load Balancer bei der Weiterleitung von Anfragen an einen Fehler AWS WAF feststellt, speichert er einen der folgenden Fehlercodes im Feld error_reason des Zugriffsprotokolls.

Code	Beschreibung
`WAFConnectionError`	Der Load Balancer kann keine Verbindung zu herstellen. AWS WAF
`WAFConnectionTimeout`	Bei der Verbindung wurde das AWS WAF Zeitlimit überschritten.
`WAFResponseReadTimeout`	Eine Anfrage zum AWS WAF Timeout.

Code	Beschreibung
`WAFServiceError`	AWS WAF hat einen 5XX-Fehler zurückgegeben.
`WAFUnhandledException`	Der Load Balancer hat eine unbehandelte Ausnahme festgestellt.

Beispiel-Protokolleinträge

Es folgen beispielhafte Protokolleinträge. Beachten Sie, dass der Beispieltext nur aus Gründen der besseren Lesbarkeit in mehreren Zeilen erscheint.

Beispiel für HTTP-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen HTTP-Listener (Port 80 zu Port 80):

```
http 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337262-36d228ad5d99923122bbe354" "-" "-"
0 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.0.1:80" "200" "-" "-"
 TID_1234abcd5678ef90
```

Beispiel für HTTPS-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen HTTPS-Listener (Port 443 zu Port 80):

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256
 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com" "arn:aws:acm:us-
east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" "10.0.0.1:80" "200" "-"
 "-" TID_1234abcd5678ef90
```

Beispiel für HTTP/2-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen HTTP/2-Stream.

```
h2 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.1.252:48160 10.0.0.66:9000 0.000 0.002 0.000 200 200 5 257
"GET https://10.0.2.105:773/ HTTP/2.0" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256
 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337327-72bd00b0343d75b906739c42" "-" "-"
1 2018-07-02T22:22:48.364000Z "redirect" "https://example.com:80/" "-" "10.0.0.66:9000"
 "200" "-" "-" TID_1234abcd5678ef90
```

Beispiel für einen WebSockets Eintrag

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für eine WebSockets Verbindung.

```
ws 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.0.140:40914 10.0.1.192:8010 0.001 0.003 0.000 101 101 218 587
"GET http://10.0.0.30:80/ HTTP/1.1" "-" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
1 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.1.192:8010" "101" "-" "-"
 TID_1234abcd5678ef90
```

Beispiel für einen gesicherten WebSockets Eintrag

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für eine sichere WebSockets Verbindung.

```
wss 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.0.140:44244 10.0.0.171:8010 0.000 0.001 0.000 101 101 218 786
"GET https://10.0.0.30:443/ HTTP/1.1" "-" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
1 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.0.171:8010" "101" "-" "-"
 TID_1234abcd5678ef90
```

Beispieleinträge für Lambda-Funktionen

Es folgt ein Beispiel eines Protokolleintrags für eine Anfrage an eine Lambda-Funktion, die erfolgreich war:

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "-" "-" "-" "-" "-" TID_1234abcd5678ef90
```

Es folgt ein Beispiel eines Protokolleintrags für eine Anfrage an eine Lambda-Funktion, die fehlgeschlagen ist:

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 502 - 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "LambdaInvalidResponse" "-" "-" "-" "-"
 TID_1234abcd5678ef90
```

Verarbeiten von Zugriffsprotokolldateien

Die Zugriffsprotokolldateien werden komprimiert. Wenn Sie die Dateien herunterladen, müssen Sie sie dekomprimieren, um die Informationen anzuzeigen.

Falls es viele Zugriff auf Ihre Website gibt, kann der Load Balancer Protokolldateien mit mehreren Gigabyte an Daten generieren. Möglicherweise sind Sie nicht in der Lage, eine so große Datenmenge mithilfe von line-by-line Processing zu verarbeiten. Daher müssen Sie möglicherweise Tools zur Datenanalyse verwenden, die parallele Verarbeitungslösungen bieten. Beispielsweise können Sie die folgenden analytischen Tools zum Analysieren und Verarbeiten von Zugriffsprotokollen verwenden:

- Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mit Standard-SQL erleichtert. Weitere Informationen finden Sie unter Abfragen von Application-Load-Balancer-Protokollen im Benutzerhandbuch zu Amazon Athena.
- Loggly
- Splunk

- Sumo Logic

Aktivieren der Zugriffsprotokolle für Ihren Application Load Balancer

Wenn Sie die Zugriffsprotokolle für Ihren Load Balancer aktivieren, müssen Sie den Namen des S3-Bucket angeben, in dem der Load Balancer die Protokolle speichert. Der Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Berechtigung zum Schreiben in den Bucket gewährt.

Aufgaben

- Schritt 1: Einen S3-Bucket erstellen
- Schritt 2: Hinzufügen von Richtlinien zu Ihrem S3-Bucket
- Schritt 3: Konfigurieren von Zugriffsprotokollen
- Schritt 4: Überprüfen der Bucket-Berechtigungen
- Fehlerbehebung

Schritt 1: Einen S3-Bucket erstellen

Wenn Sie Zugriffsprotokolle aktivieren, müssen Sie einen S3-Bucket für die Zugriffsprotokolle angeben. Sie können einen vorhandenen Bucket verwenden oder einen Bucket speziell für Zugriffsprotokolle erstellen. Der Bucket muss die folgenden Anforderungen erfüllen.

Voraussetzungen

- Der Bucket muss sich in derselben Region wie der Load Balancer befinden. Der Bucket und der Load Balancer können verschiedenen Konten gehören.
- Die einzige serverseitige Verschlüsselungsoption, die unterstützt wird, sind von Amazon S3 verwaltete Schlüssel (SSE-S3). Weitere Informationen finden Sie unter Amazon-S3-verwaltete Verschlüsselungsschlüssel (SSE-S3).

Erstellen eines S3-Buckets mithilfe der Amazon-S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Create Bucket (Bucket erstellen) aus.
3. Führen Sie auf der Seite Create bucket (Bucket erstellen) die folgenden Schritte aus:

a. Geben Sie unter Bucket Name (Bucket-Name) einen Namen für den Bucket ein. Dieser Name muss unter den in Amazon S3 vorhandenen Bucket-Namen eindeutig sein. In einigen Regionen kann es zusätzliche Einschränkungen für Bucket-Namen geben. Weitere Informationen finden Sie unter Bucket-Einschränkungen und Einschränkungen im Amazon S3 S3-Benutzerhandbuch.
b. Wählen Sie unter AWS -Region die Region aus, in der Sie Ihren Load Balancer erstellt haben.
c. Wählen Sie für Standardverschlüsselung die Option Von Amazon S3 verwaltete Schlüssel (SSE-S3) aus.
d. Wählen Sie Create Bucket (Bucket erstellen) aus.

Schritt 2: Hinzufügen von Richtlinien zu Ihrem S3-Bucket

Der S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Berechtigung zum Schreiben von Zugriffsprotokollen in den Bucket gewährt. Bucket-Richtlinien sind eine Sammlung von JSON-Anweisungen, die in der Sprache der Zugriffsrichtlinie geschrieben sind, um Zugriffsberechtigungen für Ihre Buckets zu definieren. Jeder Anweisung enthält Informationen über eine einzelne Berechtigung und besteht aus einer Reihe von Elementen.

Wenn Sie einen vorhandenen Bucket verwenden, dem bereits eine Richtlinie angehängt ist, können Sie die Anweisung für Zugriffsprotokolle von Elastic Load Balancing zu der Richtlinie hinzufügen. Wenn Sie dies tun, empfehlen wir, dass Sie eine Beurteilung der daraus resultierenden Berechtigungen vornehmen, um sicherzustellen, dass sie für die Benutzer geeignet sind, die Zugriff auf die Bucket-Zugriffsprotokolle benötigen.

Verfügbare Bucket-Richtlinien

Die Bucket-Richtlinie, die Sie verwenden, hängt von der AWS-Region und der Art der Zone ab.

Regionen, die ab August 2022 oder später verfügbar sind

Diese Richtlinie erteilt Berechtigungen für den angegebenen Protokoll-Bereitstellungsdienst. Verwenden Sie diese Richtlinie für Load Balancer in den folgenden Regionen:

- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Melbourne)

- Asien-Pazifik (Taipeh)
- Asien-Pazifik (Thailand)
- Kanada West (Calgary)
- Europa (Spain)
- Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (VAE)
- Mexiko (Zentral)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Regionen, die vor August 2022 verfügbar sind

Diese Richtlinie gewährt Berechtigungen für die angegebene Konto-ID von Elastic Load Balancing. Verwenden Sie diese Richtlinie für Load Balancer in den unten aufgeführten Regionen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

*elb-account-id*Ersetzen Sie für `Principal` durch die ID des Elastic Load Balancing Balancing-Kontos für die Region des Load Balancers:

- USA Ost (Nord-Virginia) – 127311923021
- USA Ost (Ohio) – 033677994240
- USA West (Nordkalifornien) – 027434742980

- USA West (Oregon) – 797873946194
- Afrika (Kapstadt) – 098369216593
- Asien-Pazifik (Hongkong) – 754344448648
- Asien-Pazifik (Jakarta) – 589379963580
- Asien-Pazifik (Mumbai) – 718504428378
- Asien-Pazifik (Osaka) – 383597477331
- Asien-Pazifik (Seoul) – 600734575887
- Asien-Pazifik (Singapur) – 114774131450
- Asien-Pazifik (Sydney) – 783225319266
- Asien-Pazifik (Tokio) – 582318560864
- Kanada (Zentral) – 985666609251
- Europa (Frankfurt) – 054676820928
- Europa (Irland) – 156460612806
- Europa (London) – 652711504416
- Europa (Mailand) – 635631232127
- Europa (Paris) – 009996457667
- Europa (Stockholm) – 897822967062
- Naher Osten (Bahrain) – 076674570225
- Südamerika (São Paulo) – 507241528517

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regionen

Diese Richtlinie gewährt Berechtigungen für die angegebene Konto-ID von Elastic Load Balancing. Verwenden Sie diese Richtlinie für Load Balancer in den AWS GovCloud (US) Regionen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/123456789012/*"
    }
  ]
}
```

*elb-account-id*Ersetzen Sie für `Principal` durch die ID des Elastic Load Balancing Balancing-Kontos für die Region des Load Balancers:

- AWS GovCloud (US-West) — 048591011584
- AWS GovCloud (US-Ost) — 190560391635

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt,

dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der S3-Bucket-ARN, den Sie angeben, hängt davon ab, ob Sie planen, ein Präfix einzubeziehen, wenn Sie den Link für Zugriffsprotokolle aktivieren, Schritt 3.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Outposts-Zonen

Die folgende Richtlinie erteilt Berechtigungen für den angegebenen Protokoll-Bereitstellungsdienst. Verwenden Sie diese Richtlinie für Load Balancer in Outposts-Zonen.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
```

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos

beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene S3-Bucket-ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

⚠ Sicherheit erhöhen

Verwenden Sie die folgenden Vorschläge, um die Sicherheit Ihres S3-Buckets zu verbessern.

Überprüfen Sie Ihre Bucket-Richtlinie

- Verwenden Sie den vollständigen Ressourcenpfad, einschließlich des Konto-ID-Teils des S3-Bucket-ARN. Verwenden Sie keine Platzhalter (*) im Konto-ID-Teil des S3-Bucket-ARN.

  ```
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
  ```

- Verwenden Sie diese Option, `aws:SourceArn` um sicherzustellen, dass nur Load Balancer aus der angegebenen Region und dem angegebenen Konto Ihren Bucket verwenden können.

  ```
  "Condition": {
      "ArnLike": {
          "aws:SourceArn":
   "arn:aws:elasticloadbalancing:region:123456789012:loadbalancer/*"
      }
  ```

```
}
```

- Verwenden Sie `aws:SourceOrgId` with`aws:SourceArn`, um sicherzustellen, dass nur Load Balancer der angegebenen Organisation Ihren Bucket verwenden können.

```
"Condition": {
    "StringEquals": {
        "aws:SourceOrgId": "o-1234567890"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    }
}
```

- Wenn Sie über eine `Deny` Anweisung verfügen, die den Zugriff auf Service Principals mit Ausnahme der ausdrücklich erlaubten verhindert, sollten Sie dies der Liste der erlaubten Service Principals hinzufügen`logdelivery.elasticloadbalancing.amazonaws.com`. Wenn Sie beispielsweise die `aws:PrincipalServiceNamesList` Bedingung verwendet haben, fügen Sie Folgendes hinzu`logdelivery.elasticloadbalancing.amazonaws.com`:

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Condition": {
      "StringNotEqualsIfExists": {
          "aws:PrincipalServiceNamesList": [
              "logdelivery.elasticloadbalancing.amazonaws.com",
              "service.amazonaws.com"
          ]
      }
  }
}
```

  Wenn Sie das `NotPrincipal` Element verwendet haben, fügen Sie es `logdelivery.elasticloadbalancing.amazonaws.com` wie folgt hinzu. Beachten Sie, dass wir empfehlen, den `aws:PrincipalServiceNamesList` Bedingungsschlüssel `aws:PrincipalServiceName` oder zu verwenden, um Serviceprinzipale explizit zuzulassen, anstatt das `NotPrincipal` Element zu verwenden. Weitere Informationen finden Sie unter NotPrincipal.

```
{
```

```
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "service.amazonaws.com"
    ]
  }
},
```

So fügen Sie Ihrem Bucket über die Amazon S3-Konsole eine Bucket-Richtlinie für Zugriffsprotokolle hinzu

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, um seine Detailseite zu öffnen.
3. Wählen Sie Berechtigungen und anschließend Bucket-Richtlinie, Bearbeiten aus.
4. Aktualisieren Sie die Bucket-Richtlinie, um die erforderlichen Berechtigungen zu gewähren.
5. Wählen Sie Änderungen speichern aus.

Schritt 3: Konfigurieren von Zugriffsprotokollen

Gehen Sie wie folgt vor, um Zugriffsprotokolle zur Erfassung von Anforderungsinformationen und zur Übermittlung von Protokolldateien an Ihren S3-Bucket zu konfigurieren.

Voraussetzungen

Der Bucket muss die in Schritt 1 beschriebenen Anforderungen erfüllen und Sie müssen eine Bucket-Richtlinie wie in Schritt 2 beschrieben anhängen. Wenn Sie ein Präfix angeben, darf es die Zeichenfolge "AWSLogs“ nicht enthalten.

So aktivieren Sie die Zugriffsprotokolle für Ihren Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen Ihres Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren Sie für die Überwachung die Option Zugriffsprotokolle.

6. Geben Sie für S3-URI den S3-URI für Ihre Protokolldateien ein. Der URI, den Sie angeben, hängt davon ab, ob Sie ein Präfix verwenden.

   - URI mit einem Präfix: s3://*amzn-s3-demo-logging-bucket*/*logging-prefix*
   - URI ohne Präfix: s3://*amzn-s3-demo-logging-bucket*

7. Wählen Sie Änderungen speichern aus.

Um Zugriffsprotokolle zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-load-balancer-attributes-Befehl.

So verwalten Sie den S3-Bucket für Ihre Zugriffsprotokolle

Stellen Sie sicher, dass Sie die Zugriffsprotokolle deaktivieren, bevor Sie den Bucket löschen, den Sie für Zugriffsprotokolle konfiguriert haben. Andernfalls kann Elastic Load Balancing keine Zugriffsprotokolle für Ihren Load Balancer in diesem neuen Bucket schreiben, wenn es einen neuen Bucket mit demselben Namen und den erforderlichen Bucket-Richtlinien in einem AWS-Konto gibt, dessen Eigentümer nicht Sie sind.

Schritt 4: Überprüfen der Bucket-Berechtigungen

Nachdem Zugriffsprotokolle für den Load Balancer aktiviert ist, überprüft Elastic Load Balancing den S3-Bucket und erstellt eine Testdatei, um sicherzustellen, dass die Bucket-Richtlinie die erforderlichen Berechtigungen angibt. Sie können die Amazon-S3-Konsole verwenden, um sicherzustellen, dass die Testdatei erstellt wurde. Die Testdatei ist keine tatsächliche Zugriffsprotokolldatei; sie enthält keine Beispieldatensätze.

Um zu überprüfen, ob mit der Amazon S3 S3-Konsole eine Testdatei in Ihrem Bucket erstellt wurde

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, den Sie für Zugriffsprotokolle angegeben haben.
3. Navigieren Sie zur Testdatei, `ELBAccessLogTestFile`. Der Standort hängt davon ab, ob Sie ein Präfix verwenden.

   - Standort mit einem Präfix:*amzn-s3-demo-logging-bucket*/*logging-prefix*/AWSLogs/*123456789012*/ELBAccessLogTestFile
   - Standort ohne Präfix:*amzn-s3-demo-logging-bucket*/AWSLogs/*123456789012*/ELBAccessLogTestFile

Fehlerbehebung

Wenn Sie einen Fehler aufgrund Zugriffsverweigerung erhalten, kann dies die folgenden möglichen Ursachen haben.

- Die Bucket-Policy gewährt Elastic Load Balancing nicht die Berechtigung, Zugriffsprotokolle in den Bucket zu schreiben. Stellen Sie sicher, dass Sie die richtige Bucket-Richtlinie für die Region verwenden. Stellen Sie sicher, dass der Ressourcen-ARN denselben Bucket-Namen verwendet, den Sie bei der Aktivierung von Zugriffsprotokollen angegeben haben. Stellen Sie sicher, dass der Ressourcen-ARN kein Präfix enthält, wenn Sie bei der Aktivierung von Zugriffsprotokollen kein Präfix angegeben haben.
- Der Bucket verwendet eine nicht unterstützte serverseitige Verschlüsselungsoption. Der Bucket muss von Amazon S3 verwaltete Schlüssel (SSE-S3) verwenden.

Deaktivieren der Zugriffsprotokolle für Ihren Application Load Balancer

Sie können die Zugriffsprotokolle für Ihren Load Balancer jederzeit deaktivieren. Nachdem Sie Zugriffsprotokolle deaktiviert haben, verbleiben Ihre Zugriffsprotokolle in Ihrem S3-Bucket, bis Sie sie löschen. Weitere Informationen finden Sie unter Erstellen, Konfigurieren und Arbeiten mit S3-Buckets im Amazon S3 S3-Benutzerhandbuch.

So deaktivieren Sie die Zugriffsprotokolle mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen Ihres Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Deaktivieren Sie für die Überwachung die Zugriffsprotokolle.
6. Wählen Sie Änderungen speichern aus.

Um Zugriffsprotokolle zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-load-balancer-attributes-Befehl.

Verbindungsprotokolle für Ihren Application Load Balancer

Elastic Load Balancing stellt Verbindungsprotokolle bereit, die detaillierte Informationen über Anfragen erfassen, die an Ihren Load Balancer gesendet wurden. Jedes Protokoll enthält Informationen wie die IP-Adresse und den Port des Clients, den Listener-Port, die verwendete TLS-Chiffre und das verwendete Protokoll, die TLS-Handshake-Latenz, den Verbindungsstatus und Details zum Client-Zertifikat. Sie können diese Verbindungsprotokolle verwenden, um Anforderungsmuster zu analysieren und Probleme zu beheben.

Verbindungsprotokolle sind eine optionale Funktion von Elastic Load Balancing, die standardmäßig deaktiviert ist. Nachdem Sie Verbindungsprotokolle für Ihren Load Balancer aktiviert haben, erfasst Elastic Load Balancing die Protokolle und speichert sie in dem von Ihnen angegebenen Amazon S3 S3-Bucket als komprimierte Dateien. Sie können Verbindungsprotokolle jederzeit deaktivieren.

Sie zahlen Speicherkosten für Amazon S3, aber Sie zahlen nicht für die Bandbreite, die von Elastic Load Balancing zum Senden von Protokolldateien an Amazon S3 verwendet wird. Weitere Information zu Speicherkosten finden Sie unter Amazon S3 – Preise.

Inhalt

- Verbindungsprotokolldateien
- Verbindungsprotokolleinträge
- Beispiel-Protokolleinträge
- Verbindungsprotokolldateien werden verarbeitet
- Verbindungsprotokolle für Ihren Application Load Balancer aktivieren
- Verbindungsprotokolle für Ihren Application Load Balancer deaktivieren

Verbindungsprotokolldateien

Elastic Load Balancing veröffentlicht alle 5 Minuten eine Protokolldatei für jeden Load-Balancer-Knoten. Die Protokollbereitstellung ist letztendlich konsistent. Der Load Balancer kann mehrere Protokolle für denselben Zeitraum bereitstellen. Dies passiert in der Regel, wenn die Website hohen Datenverkehr aufweist.

Die Dateinamen der Verbindungsprotokolle verwenden das folgende Format:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/
conn_log_aws-account-id_elasticloadbalancing_region_app.load-balancer-id_end-time_ip-
address_random-string.log.gz
```

bucket

Der Name des S3-Buckets.

prefix

(Optional) Das Präfix (logische Hierarchie) für den Bucket. Das von Ihnen angegebene Präfix darf die Zeichenfolge `AWSLogs` nicht enthalten. Weitere Informationen finden Sie unter Organisieren von Objekten mit Präfixen.

`AWSLogs`

Wir fügen den Teil des Dateinamens hinzu, der mit `AWSLogs` nach dem von Ihnen angegebenen Bucket-Namen und dem optionalen Präfix beginnt.

aws-account-id

Die AWS Konto-ID des Besitzers.

Region

Die Region für Ihren Load Balancer und den S3-Bucket.

JJJJ/MM/TT

Das Datum, an dem das Protokoll übermittelt wurde.

load-balancer-id

Die Ressourcen-ID des Load Balancer. Wenn die Ressourcen-ID Schrägstriche (/) enthält, werden sie durch Punkte (.) ersetzt.

end-time

Das Datum und die Uhrzeit, an dem das Protokollierungsintervall endete. Beispiel: Die Endzeit 20140215T2340Z enthält Einträge für Anforderungen, die zwischen 23:35 und 23:40 in UTC- oder Zulu-Zeit durchgeführt wurden.

ip-address

Die IP-Adresse des Load Balancer-Knotens, der die Anforderung verarbeitet hat. Für einen internen Load Balancer handelt es sich hierbei um eine private IP-Adresse.

random-string

Eine vom System generierte zufällige Zeichenfolge.

Im Folgenden finden Sie ein Beispiel für einen Protokolldateinamen mit Präfix:

```
s3://amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/
elasticloadbalancing/us-east-2/2022/05/01/
conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Im Folgenden finden Sie ein Beispiel für einen Protokolldateinamen ohne Präfix:

```
s3://amzn-s3-demo-logging-bucket/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Sie können Ihre Protokolldateien beliebig lange im Bucket speichern. Sie können aber auch Amazon S3-Lebenszyklusregeln aufstellen, anhand derer die Protokolldateien automatisch archiviert oder gelöscht werden. Weitere Informationen finden Sie unter Object Lifecycle Management im Amazon S3 S3-Benutzerhandbuch.

Verbindungsprotokolleinträge

Jeder Verbindungsversuch hat einen Eintrag in einer Verbindungsprotokolldatei. Wie Client-Anfragen gesendet werden, hängt davon ab, ob die Verbindung persistent oder nicht persistent ist. Nicht persistente Verbindungen haben eine einzige Anfrage, wodurch ein einziger Eintrag im Zugriffs- und Verbindungsprotokoll erstellt wird. Persistente Verbindungen haben mehrere Anfragen, wodurch mehrere Einträge im Zugriffslog und ein einziger Eintrag im Verbindungsprotokoll erstellt werden.

Inhalt

- Syntax
- Codes für die Fehlerursache

Syntax

In der folgenden Tabelle werden die Felder eines Verbindungsprotokolleintrags der Reihe nach beschrieben. Alle Felder werden durch Leerzeichen voneinander getrennt. Wenn neue Felder

eingeführt werden, werden sie am Ende des Protokolleintrags hinzugefügt. Sie sollten alle Felder am Ende des Protokolleintrags ignorieren, die Sie nicht erwartet haben.

Feld	Beschreibung
timestamp	Der Zeitpunkt im ISO 8601-Format, zu dem der Load Balancer erfolgrei ch eine Verbindung hergestellt hat oder nicht.
client_ip	Die IP-Adresse des anfragenden Clients.
client_port	Der Port des anfragenden Clients.
listener_port	Der Port des Load Balancer-Listeners, der die Client-Anfrage empfängt.
tls_protocol	[HTTPS-Listener] Das SSL/TLS Protokoll, das bei Handshakes verwendet wird. Dieses Feld ist auf „Keine Anfragen“ gesetzt-. SSL/TLS
tls_cipher	[HTTPS-Listener] Das bei SSL/TLS Handshakes verwendete Protokoll. Dieses Feld ist auf „Keine Anfragen“ gesetzt-. SSL/TLS
tls_handshake_late ncy	[HTTPS-Listener] Die Gesamtzeit in Sekunden, mit einer Genauigkeit von Millisekunden, die beim Aufbau eines erfolgreichen Handshakes verstrichen ist. Dieses Feld ist auf Folgendes gesetzt: - • Die eingehende Anfrage ist keine SSL/TLS Anfrage. • Der Handshake wurde nicht erfolgreich eingerichtet.
leaf_client_cert_s ubject	[HTTPS-Listener] Der Betreffname des Leaf-Client-Zertifikats. Dieses Feld ist auf Folgendes gesetzt-: • Die eingehende Anfrage ist keine SSL/TLS Anfrage. • Der Load Balancer-Listener ist nicht mit aktiviertem mTLS konfiguriert. • Der Server ist nicht in der Lage, das load/parse Leaf-Client-Zertifikat zu erstellen.
leaf_client_cert_v alidity	[HTTPS-Listener] Die Gültigkeit des Leaf-Client-Zertifikats mit `not-before` und `not-after` im ISO 8601-Format. Dieses Feld ist auf Folgendes gesetzt-:

Feld	Beschreibung
	• Die eingehende Anfrage ist keine SSL/TLS Anfrage. • Der Load Balancer-Listener ist nicht mit aktiviertem mTLS konfiguriert. • Der Server ist nicht in der Lage, das load/parse Leaf-Client-Zertifikat zu erstellen.
leaf_client_cert_serial_number	[HTTPS-Listener] Die Seriennummer des Leaf-Client-Zertifikats. Dieses Feld ist auf den Zeitpunkt gesetzt, - wenn: • Die eingehende Anfrage ist keine SSL/TLS Anfrage. • Der Load Balancer-Listener ist nicht mit aktiviertem mTLS konfiguriert. • Der Server ist nicht in der Lage, das load/parse Leaf-Client-Zertifikat zu erstellen.
tls_verify_status	[HTTPS-Listener] Der Status der Verbindungsanfrage. Dieser Wert gibt an`Success`, ob die Verbindung erfolgreich hergestellt wurde. Bei einer erfolglosen Verbindung ist der Wert`Failed:$error_code` .
conn_trace_id	Die Verbindungsrückverfolgbarkeits-ID ist eine eindeutige undurchsichtige ID, die zur Identifizierung jeder Verbindung verwendet wird. Nachdem eine Verbindung mit einem Client hergestellt wurde, enthalten nachfolgende Anfragen von diesem Client diese ID in ihren jeweiligen Zugriffsprotokolleinträgen. Diese ID fungiert als Fremdschlüssel, um eine Verbindung zwischen der Verbindung und den Zugriffsprotokollen herzustellen.

Codes für die Fehlerursache

Wenn der Load Balancer keine Verbindung herstellen kann, speichert der Load Balancer einen der folgenden Ursachencodes im Verbindungsprotokoll.

Code	Beschreibung
`ClientCertMaxChainDepthExceeded`	Die maximale Tiefe der Client-Zertifikatskette wurde überschritten

Code	Beschreibung	
`ClientCertMaxSizeExceeded`	Die maximale Größe des Client-Zertifikats wurde überschritten	
`ClientCertCrlHit`	Das Client-Zertifikat wurde von der CA gesperrt	
`ClientCertCrlProcessingError`	Fehler bei der CRL-Verarbeitung	
`ClientCertUntrusted`	Das Client-Zertifikat ist nicht vertrauenswürdig	
`ClientCertNotYetValid`	Das Client-Zertifikat ist noch nicht gültig	
`ClientCertExpired`	Das Client-Zertifikat ist abgelaufen	
`ClientCertTypeUnsupported`	Der Typ des Client-Zertifikats wird nicht unterstützt	
`ClientCertInvalid`	Das Client-Zertifikat ist ungültig	
`ClientCertPurposeInvalid`	Der Zweck des Client-Zertifikats ist ungültig	
`ClientCertRejected`	Das Client-Zertifikat wurde durch die benutzerdefinierte Servervalidierung abgelehnt	
`UnmappedConnectionError`	Fehler bei der Verbindung zur Laufzeit bei nicht zugeordneter Zuordnung	

Beispiel-Protokolleinträge

Im Folgenden finden Sie Beispiele für Verbindungsprotokolleinträge. Beachten Sie, dass der Beispieltext nur aus Gründen der besseren Lesbarkeit in mehreren Zeilen erscheint.

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für eine erfolgreiche Verbindung mit einem HTTPS-Listener, bei dem der Modus für die gegenseitige TLS-Überprüfung auf Port 443 aktiviert ist.

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
 4.036
"CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z
FEF257372D5C14D4 Success TID_3180a73013c8ca4bac2f731159d4b0fe
```

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für eine fehlgeschlagene Verbindung mit einem HTTPS-Listener, bei dem der Modus für die gegenseitige TLS-Überprüfung auf Port 443 aktiviert ist.

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
 -
"CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z
FEF257372D5C14D4 Failed:ClientCertUntrusted TID_1c71a68d70587445ad5127ff8b2687d7
```

Verbindungsprotokolldateien werden verarbeitet

Die Verbindungsprotokolldateien sind komprimiert. Wenn Sie die Dateien mithilfe der Amazon-S3-Konsole öffnen, werden sie dekomprimiert und die Informationen werden angezeigt. Wenn Sie die Dateien herunterladen, müssen Sie sie dekomprimieren, um die Informationen anzuzeigen.

Falls es viele Zugriff auf Ihre Website gibt, kann der Load Balancer Protokolldateien mit mehreren Gigabyte an Daten generieren. Möglicherweise sind Sie nicht in der Lage, eine so große Datenmenge mithilfe von line-by-line Processing zu verarbeiten. Daher müssen Sie möglicherweise Tools zur Datenanalyse verwenden, die parallele Verarbeitungslösungen bieten. Sie können beispielsweise die folgenden Analysetools verwenden, um Verbindungsprotokolle zu analysieren und zu verarbeiten:

- Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mit Standard-SQL erleichtert.
- Loggly

- Splunk
- Sumo Logic

Verbindungsprotokolle für Ihren Application Load Balancer aktivieren

Wenn Sie Verbindungsprotokolle für Ihren Load Balancer aktivieren, müssen Sie den Namen des S3-Buckets angeben, in dem der Load Balancer die Protokolle speichert. Der Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Berechtigung zum Schreiben in den Bucket gewährt.

Aufgaben

- Schritt 1: Einen S3-Bucket erstellen
- Schritt 2: Hinzufügen von Richtlinien zu Ihrem S3-Bucket
- Schritt 3: Verbindungsprotokolle konfigurieren
- Schritt 4: Überprüfen der Bucket-Berechtigungen
- Fehlerbehebung

Schritt 1: Einen S3-Bucket erstellen

Wenn Sie Verbindungsprotokolle aktivieren, müssen Sie einen S3-Bucket für die Verbindungsprotokolle angeben. Sie können einen vorhandenen Bucket verwenden oder einen Bucket speziell für Verbindungsprotokolle erstellen. Der Bucket muss die folgenden Anforderungen erfüllen.

Voraussetzungen

- Der Bucket muss sich in derselben Region wie der Load Balancer befinden. Der Bucket und der Load Balancer können verschiedenen Konten gehören.
- Die einzige serverseitige Verschlüsselungsoption, die unterstützt wird, sind von Amazon S3 verwaltete Schlüssel (SSE-S3). Weitere Informationen finden Sie unter Amazon-S3-verwaltete Verschlüsselungsschlüssel (SSE-S3).

Erstellen eines S3-Buckets mithilfe der Amazon-S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Create Bucket (Bucket erstellen) aus.

3. Führen Sie auf der Seite Create bucket (Bucket erstellen) die folgenden Schritte aus:

   a. Geben Sie unter Bucket Name (Bucket-Name) einen Namen für den Bucket ein. Dieser Name muss unter den in Amazon S3 vorhandenen Bucket-Namen eindeutig sein. In einigen Regionen kann es zusätzliche Einschränkungen für Bucket-Namen geben. Weitere Informationen finden Sie unter Bucket-Einschränkungen und Einschränkungen im Amazon S3 S3-Benutzerhandbuch.

   b. Wählen Sie unter AWS -Region die Region aus, in der Sie Ihren Load Balancer erstellt haben.

   c. Wählen Sie für Standardverschlüsselung die Option Von Amazon S3 verwaltete Schlüssel (SSE-S3) aus.

   d. Wählen Sie Create Bucket (Bucket erstellen) aus.

Schritt 2: Hinzufügen von Richtlinien zu Ihrem S3-Bucket

Ihr S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Erlaubnis erteilt, die Verbindungsprotokolle in den Bucket zu schreiben. Bucket-Richtlinien sind eine Sammlung von JSON-Anweisungen, die in der Sprache der Zugriffsrichtlinie geschrieben sind, um Zugriffsberechtigungen für Ihre Buckets zu definieren. Jeder Anweisung enthält Informationen über eine einzelne Berechtigung und besteht aus einer Reihe von Elementen.

Wenn Sie einen vorhandenen Bucket verwenden, dem bereits eine Richtlinie angehängt ist, können Sie der Richtlinie die Anweisung für Elastic Load Balancing Balancing-Verbindungsprotokolle hinzufügen. Wenn Sie dies tun, empfehlen wir Ihnen, die resultierenden Berechtigungen auszuwerten, um sicherzustellen, dass sie für die Benutzer geeignet sind, die Zugriff auf den Bucket für Verbindungsprotokolle benötigen.

Verfügbare Bucket-Richtlinien

Welche Bucket-Richtlinie Sie verwenden, hängt von der AWS-Region und der Art der Zone ab.

⚠ Verbessern Sie die Sicherheit, indem Sie einen präzisen S3-Bucket verwenden ARNs.

- Verwenden Sie den vollständigen Ressourcenpfad, nicht nur den S3-Bucket-ARN.
- Geben Sie den Konto-ID-Teil des S3-Bucket-ARN an.
- Verwenden Sie keine Platzhalter (*) im Konto-ID-Teil des S3-Bucket-ARN.

Regionen, die ab August 2022 oder später verfügbar sind

Diese Richtlinie erteilt Berechtigungen für den angegebenen Protokoll-Bereitstellungsdienst. Verwenden Sie diese Richtlinie für Load Balancer in den folgenden Regionen:

- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Thailand)
- Kanada West (Calgary)
- Europa (Spain)
- Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (VAE)
- Mexiko (Zentral)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt,

dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene S3-Bucket-ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

NotPrincipalWenn verwendet Effect wird, ist Deny

Wenn die Amazon S3 S3-Bucket-Richtlinie `Effect` mit dem Wert `Deny` und dem Include-Wert verwendet, `NotPrincipal` wie im Beispiel unten gezeigt, stellen Sie sicher, dass dieser Wert in der `Service` Liste enthalten `logdelivery.elasticloadbalancing.amazonaws.com` ist.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
  }
},
```

Regionen, die vor August 2022 verfügbar sind

Diese Richtlinie gewährt dem angegebenen Elastic Load Balancing Balancing-Konto Berechtigungen. Verwenden Sie diese Richtlinie für Load Balancer in den unten aufgeführten Regionen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
       "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

*elb-account-id*Ersetzen Sie für `Principal` durch die ID des Elastic Load Balancing Balancing-Kontos für die Region des Load Balancers:

- USA Ost (Nord-Virginia) – 127311923021
- USA Ost (Ohio) – 033677994240
- USA West (Nordkalifornien) – 027434742980
- USA West (Oregon) – 797873946194
- Afrika (Kapstadt) – 098369216593
- Asien-Pazifik (Hongkong) – 754344448648
- Asien-Pazifik (Jakarta) – 589379963580
- Asien-Pazifik (Mumbai) – 718504428378
- Asien-Pazifik (Osaka) – 383597477331
- Asien-Pazifik (Seoul) – 600734575887
- Asien-Pazifik (Singapur) – 114774131450
- Asien-Pazifik (Sydney) – 783225319266
- Asien-Pazifik (Tokio) – 582318560864
- Kanada (Zentral) – 985666609251

- Europa (Frankfurt) – 054676820928
- Europa (Irland) – 156460612806
- Europa (London) – 652711504416
- Europa (Mailand) – 635631232127
- Europa (Paris) – 009996457667
- Europa (Stockholm) – 897822967062
- Naher Osten (Bahrain) – 076674570225
- Südamerika (São Paulo) – 507241528517

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene S3-Bucket-ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regionen

Diese Richtlinie gewährt dem angegebenen Elastic Load Balancing Balancing-Konto Berechtigungen. Verwenden Sie diese Richtlinie für Load Balancer in Availability Zones oder Local Zones in den AWS GovCloud (US) Regionen in der folgenden Liste.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/123456789012/*"
    }
  ]
}
```

Um *elb-account-id* durch die ID des Elastic Load Balancing Balancing-Kontos für die Region des Load Balancers zu `Principal` ersetzen:

- AWS GovCloud (US-West) — 048591011584
- AWS GovCloud (US-Ost) — 190560391635

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass Sie Load Balancer vom angegebenen Konto aus Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene S3-Bucket-ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Outposts-Zonen

Die folgende Richtlinie erteilt Berechtigungen für den angegebenen Protokoll-Bereitstellungsdienst. Verwenden Sie diese Richtlinie für Load Balancer in Outposts-Zonen.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
```

Geben Sie für `Resource` den ARN des Standorts für die Zugriffsprotokolle ein. Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

NotPrincipalWenn verwendet Effect wird, ist Deny

Wenn die Amazon S3 S3-Bucket-Richtlinie `Effect` mit dem Wert `Deny` und dem Include-Wert verwendet, `NotPrincipal` wie im Beispiel unten gezeigt, stellen Sie sicher, dass dieser Wert in der `Service` Liste enthalten `logdelivery.elasticloadbalancing.amazonaws.com` ist.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
  }
},
```

So hängen Sie mithilfe der Amazon S3 S3-Konsole eine Bucket-Richtlinie für Verbindungsprotokolle an Ihren Bucket an

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, um seine Detailseite zu öffnen.
3. Wählen Sie Berechtigungen und anschließend Bucket-Richtlinie, Bearbeiten aus.
4. Aktualisieren Sie die Bucket-Richtlinie, um die erforderlichen Berechtigungen zu gewähren.
5. Wählen Sie Änderungen speichern aus.

Schritt 3: Verbindungsprotokolle konfigurieren

Gehen Sie wie folgt vor, um Verbindungsprotokolle für die Erfassung und Übermittlung von Protokolldateien an Ihren S3-Bucket zu konfigurieren.

Voraussetzungen

Der Bucket muss die in Schritt 1 beschriebenen Anforderungen erfüllen und Sie müssen eine Bucket-Richtlinie wie in Schritt 2 beschrieben anhängen. Wenn Sie ein Präfix angeben, darf es die Zeichenfolge "AWSLogs“ nicht enthalten.

Um Verbindungsprotokolle für Ihren Load Balancer mithilfe der Konsole zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen Ihres Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren Sie für die Überwachung die Verbindungsprotokolle.
6. Geben Sie für S3 URI (S3-URI) den S3-URI für Ihre Protokolldateien ein. Der URI, den Sie angeben, hängt davon ab, ob Sie ein Präfix verwenden.
   - URI mit einem Präfix: `s3://bucket-name/prefix`
   - URI ohne Präfix: `s3://bucket-name`
7. Wählen Sie Änderungen speichern aus.

Um Verbindungsprotokolle zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-load-balancer-attributes-Befehl.

Um den S3-Bucket für Ihre Verbindungsprotokolle zu verwalten

Stellen Sie sicher, dass Sie die Verbindungsprotokolle deaktivieren, bevor Sie den Bucket löschen, den Sie für Verbindungsprotokolle konfiguriert haben. Andernfalls könnte Elastic Load Balancing die Verbindungsprotokolle für Ihren Load Balancer in AWS-Konto diesen neuen Bucket schreiben, wenn es einen neuen Bucket mit demselben Namen und der erforderlichen Bucket-Richtlinie gibt, aber in einem Bucket erstellt wurde, den Sie nicht besitzen.

Schritt 4: Überprüfen der Bucket-Berechtigungen

Nachdem die Verbindungsprotokolle für Ihren Load Balancer aktiviert wurden, validiert Elastic Load Balancing den S3-Bucket und erstellt eine Testdatei, um sicherzustellen, dass die Bucket-Richtlinie die erforderlichen Berechtigungen festlegt. Sie können die Amazon-S3-Konsole verwenden, um sicherzustellen, dass die Testdatei erstellt wurde. Die Testdatei ist keine eigentliche Verbindungsprotokolldatei; sie enthält keine Beispieldatensätze.

So überprüfen Sie, ob Elastic Load Balancing eine Testdatei in Ihrem S3-Bucket erstellt hat

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, den Sie für Verbindungsprotokolle angegeben haben.

3. Navigieren Sie zur Testdatei, `ELBConnectionLogTestFile`. Der Standort hängt davon ab, ob Sie ein Präfix verwenden.

   - Standort mit einem Präfix:*amzn-s3-demo-logging-bucket*/*prefix*/AWSLogs/*123456789012*/ELBConnectionLogTestFile
   - Standort ohne Präfix:*amzn-s3-demo-logging-bucket*/AWSLogs/*123456789012*/ELBConnectionLogTestFile

Fehlerbehebung

Wenn Sie einen Fehler aufgrund Zugriffsverweigerung erhalten, kann dies die folgenden möglichen Ursachen haben.

- Die Bucket-Richtlinie gewährt Elastic Load Balancing nicht die Erlaubnis, Verbindungsprotokolle in den Bucket zu schreiben. Stellen Sie sicher, dass Sie die richtige Bucket-Richtlinie für die Region verwenden. Stellen Sie sicher, dass der Ressourcen-ARN denselben Bucket-Namen verwendet, den Sie bei der Aktivierung von Verbindungsprotokollen angegeben haben. Stellen Sie sicher, dass der Ressourcen-ARN kein Präfix enthält, wenn Sie bei der Aktivierung von Verbindungsprotokollen kein Präfix angegeben haben.
- Der Bucket verwendet eine nicht unterstützte serverseitige Verschlüsselungsoption. Der Bucket muss von Amazon S3 verwaltete Schlüssel (SSE-S3) verwenden.

Verbindungsprotokolle für Ihren Application Load Balancer deaktivieren

Sie können die Verbindungsprotokolle für Ihren Load Balancer jederzeit deaktivieren. Nachdem Sie die Verbindungsprotokolle deaktiviert haben, verbleiben Ihre Verbindungsprotokolle in Ihrem S3-Bucket, bis Sie sie löschen. Weitere Informationen finden Sie unter Buckets erstellen, konfigurieren und damit arbeiten im Amazon S3 S3-Benutzerhandbuch.

Um Verbindungsprotokolle mit der Konsole zu deaktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen Ihres Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Schalten Sie für die Überwachung die Verbindungsprotokolle aus.

6. Wählen Sie Änderungen speichern aus.

Um Verbindungsprotokolle zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den modify-load-balancer-attributes-Befehl.

Anfragenachverfolgung für Ihren Application Load Balancer

Wenn der Load Balancer eine Anfrage von einem Client erhält, fügt er die Kopfzeile X-Amzn-Trace-Id hinzu oder aktualisiert diese, bevor er die Anfrage an das Ziel sendet. Jeder Service oder jede Anwendung zwischen dem Load Balancer und dem Ziel kann diese Kopfzeile ebenfalls hinzufügen oder aktualisieren.

Sie können Anfragenachverfolgung verwenden, um HTTP-Anfragen von Clients an Ziele oder andere Services nachzuverfolgen. Wenn Sie Zugriffsprotokolle aktivieren, wird der Inhalt der Kopfzeile X-Amzn-Trace-Id protokolliert. Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihre Application Load Balancer.

Syntax

Die Kopfzeile X-Amzn-Trace-Id enthält Felder mit folgendem Format:

```
Field=version-time-id
```

Feld

Der Name des Felds. Die unterstützten Werte sind `Root` und `Self`.

Eine Anwendung kann beliebige Felder für eigene Zwecke hinzufügen. Der Load Balancer behält diese Felder bei, verwendet sie jedoch nicht.

version

Die Versionsnummer. Dieser Wert ist 1.

time

Die Epoch-Zeit in Sekunden. Dieser Wert ist 8 Hexadezimalziffern lang.

id

Die Nachverfolgungskennung. Dieser Wert besteht aus 24 Hexadezimalziffern.

Beispiele

Wenn die Kopfzeile X-Amzn-Trace-Id in einer eingehenden Anfrage nicht vorhanden ist, generiert der Load Balancer eine Kopfzeile mit einem `Root`-Feld und leitet die Anfrage weiter. Zum Beispiel:

```
X-Amzn-Trace-Id: Root=1-67891233-abcdef012345678912345678
```

Wenn die X-Amzn-Trace-Id-Kopfzeile vorhanden ist und ein `Root`-Feld aufweist, fügt der Load Balancer ein `Self`-Feld ein und leitet die Anfrage weiter. Zum Beispiel:

```
X-Amzn-Trace-Id: Self=1-67891233-12456789abcdef012345678;Root=1-67891233-
abcdef012345678912345678
```

Wenn eine Anwendung eine Kopfzeile mit einem `Root`-Feld und ein benutzerdefiniertes Feld hinzufügt, behält der Load Balancer beide Felder bei, fügt ein `Self`-Feld hinzu und leitet die Anfrage weiter:

```
X-Amzn-Trace-Id: Self=1-67891233-12456789abcdef012345678;Root=1-67891233-
abcdef012345678912345678;CalledFrom=app
```

Wenn die X-Amzn-Trace-Id-Kopfzeile vorhanden ist und ein `Self`-Feld aufweist, aktualisiert der Load Balancer den Wert des `Self`-Felds.

Einschränkungen

- Der Load Balancer aktualisiert die Kopfzeile, wenn er eine eingehende Anfrage erhält, nicht wenn er eine Antwort erhält.
- Wenn die HTTP-Header größer als 7 KB sind, schreibt der Load Balancer die Kopfzeile X-Amzn-Trace-Id neu mit einem `Root`-Feld.
- Mit können Sie nur so lange nachverfolgen WebSockets, bis die Upgrade-Anfrage erfolgreich ist.

Fehlerbehebung bei Ihren Application Load Balancern

Die folgenden Informationen können Ihnen helfen, Probleme bei Ihren Application Load Balancer zu beheben.

Problembereiche

- Ein registriertes Ziel ist nicht in Betrieb
- Clients können keine Verbindung zu einem mit dem Internet verbundenen Load Balancer herstellen
- Anfragen, die an eine benutzerdefinierte Domain gesendet werden, werden vom Load Balancer nicht empfangen
- An den Load Balancer gesendete HTTPS-Anfragen geben „NET::ERR_CERT_COMMON_NAME_INVALID“ zurück
- Der Load Balancer zeigt erhöhte Verarbeitungszeiten an
- Der Load Balancer sendet als Antwortcode „000“.
- Der Load Balancer generiert einen HTTP-Fehler
- Ein Ziel generiert einen HTTP-Fehler
- Ein AWS Certificate Manager Zertifikat steht nicht zur Verwendung zur Verfügung
- Header mit mehreren Zeilen werden nicht unterstützt
- Beheben Sie fehlerhafte Ziele mithilfe der Ressourcenübersicht

Ein registriertes Ziel ist nicht in Betrieb

Wenn es länger als erwartet dauert, bis ein Ziel den Zustand `InService` aufweist, besteht es möglicherweise Zustandsprüfungen nicht. Ihr Ziel ist erst betriebsbereit, wenn es eine Zustandsprüfung besteht. Weitere Informationen finden Sie unter Gesundheitschecks für Application Load Balancer Balancer-Zielgruppen.

Überprüfen Sie, ob Ihre Instance Zustandsprüfungen nicht besteht und prüfen Sie dann Folgendes:

Eine Sicherheitsgruppe erlaubt keinen Datenverkehr

> Die mit einer Instance verbundene Sicherheitsgruppe muss mithilfe des Zustandsprüfungs-Ports und Zustandsprüfungs-Protokolls Datenverkehr vom Load Balancer zulassen. Sie können eine Regel zur Sicherheitsgruppe der Instance hinzufügen, um den gesamten Datenverkehr von der

Load Balancer-Sicherheitsgruppe zuzulassen. Außerdem muss die Sicherheitsgruppe für Ihren Load Balancer Datenverkehr zu den Instances zulassen.

Eine Netzwerk-Zugriffskontrollliste (ACL) erlaubt keinen Datenverkehr

Die mit den Subnetzen verbundene Netzwerk-ACL für Ihre Instances muss eingehenden Datenverkehr am Zustandsprüfungs-Port und ausgehenden Datenverkehr an den flüchtigen Ports (1024-65535) zuzulassen. Die mit den Subnetzen verbundene Netzwerk-ACL für Ihre Load Balancer-Knoten muss eingehenden Datenverkehr an den flüchtigen Ports und ausgehenden Datenverkehr am Zustandsprüfungs-Port und an den flüchtigen Ports zulassen.

Der Ping-Pfad ist nicht vorhanden

Erstellen Sie eine Zielseite für die Zustandsprüfung und geben Sie den Pfad als den Ping-Pfad an.

Die Verbindung läuft ab

Vergewissern Sie sich zunächst, dass Sie mithilfe der privaten IP-Adresse des Ziels und des Zustandsprüfungs-Protokolls im Netzwerk eine direkt Verbindung zum Ziel herstellen können. Wenn Sie keine Verbindung herstellen können, prüfen Sie, ob die Instance überlastet ist, und fügen Sie weitere Ziele zu Ihrer Zielgruppe hinzu, wenn sie zu stark ausgelastet ist, um zu reagieren. Wenn Sie eine Verbindung herstellen können, ist es möglich, dass die Zielseite vor Ablauf des Zeitüberschreitungszeitraums der Zustandsprüfung nicht reagiert. Wählen Sie eine einfachere Zielseite für die Zustandsprüfung aus oder passen Sie die Zustandsprüfungseinstellungen an.

Das Ziel hat keinen Erfolgsmeldungscode zurückgegeben

Der Erfolgscode lautet standardmäßig 200. Sie können jedoch optional zusätzliche Erfolgscodes angeben, wenn Sie Zustandsprüfungen konfigurieren. Überprüfen Sie die Erfolgscodes, die der Load Balancer erwartet, und stellen Sie sicher, dass Ihre Anwendung so konfiguriert ist, dass sie diese Codes bei Erfolg zurückgibt.

Der Antwortcode des Ziels war fehlerhaft oder bei der Verbindung zum Ziel ist ein Fehler aufgetreten

Überprüfen Sie, ob Ihre Anwendung auf die Zustandsprüfungsanfragen des Load Balancers antwortet. Einige Anwendungen benötigen zusätzliche Konfigurationen, um auf Zustandsprüfungen zu reagieren, z. B. eine Konfiguration des virtuellen Hosts, um auf den vom Load Balancer gesendeten HTTP-Host-Header zu reagieren. Der Host-Header-Wert enthält die private IP-Adresse des Ziels, gefolgt vom Health Check-Port, wenn kein Standardport verwendet wird. Wenn das Ziel einen standardmäßigen Port für die Integritätsprüfung verwendet, enthält der Host-Header-Wert nur die private IP-Adresse des Ziels. Wenn die private IP-Adresse Ihres

Ziels beispielsweise lautet `10.0.0.10` und der Port für die Zustandsprüfung lautet, lautet der HTTP-Host-Header`8080`, der vom Load Balancer bei Integritätsprüfungen gesendet wird`Host: 10.0.0.10:8080`. Wenn die private IP-Adresse Ihres Ziels lautet `10.0.0.10` und der Port für die Zustandsprüfung der HTTP-Host-Header ist, ist `80` dies der HTTP-Host-Header, der vom Load Balancer bei Integritätsprüfungen gesendet wird. `Host: 10.0.0.10` Möglicherweise ist eine virtuelle Hostkonfiguration, die auf diesen Host reagiert, oder eine Standardkonfiguration erforderlich, um den Zustand Ihrer Anwendung zu überprüfen. Anfragen für Zustandsprüfungen haben die folgenden Attribute: `User-Agent` ist auf `ELB-HealthChecker/2.0` gesetzt, das Zeilenende für die Felder des Nachrichtenkopfes ist die Sequenz CRLF und der Header endet an der ersten leeren Zeile, gefolgt von einem CRLF.

Clients können keine Verbindung zu einem mit dem Internet verbundenen Load Balancer herstellen

Wenn der Load Balancer auf Anfragen nicht reagiert, überprüfen Sie Folgendes:

Ihr mit dem Internet verbundener Load Balancer ist mit einem privaten Subnetz verbunden.

Sie müssen öffentliche Subnetze für Ihren Load Balancer angeben. Ein öffentliches Subnetz verfügt über einen Zugang zum Internet-Gateway für Ihre Virtual Private Cloud (VPC).

Eine Sicherheitsgruppe oder Netzwerk-ACL erlaubt keinen Datenverkehr

Die Sicherheitsgruppe für den Load Balancer und alle Netzwerke ACLs für die Load Balancer-Subnetze müssen eingehenden Datenverkehr von den Clients und ausgehenden Verkehr zu den Clients an den Listener-Ports zulassen.

Anfragen, die an eine benutzerdefinierte Domain gesendet werden, werden vom Load Balancer nicht empfangen

Wenn der Load Balancer keine Anfragen empfängt, die an eine benutzerdefinierte Domain gesendet werden, überprüfen Sie Folgendes:

Der benutzerdefinierte Domainname kann nicht in die IP-Adresse des Load Balancers aufgelöst werden

- Bestätigen Sie mithilfe einer Befehlszeilenschnittstelle, auf welche IP-Adresse der benutzerdefinierte Domainname aufgelöst wird.

    - Linux, macOS oder Unix: Sie können den `dig`-Befehl im Terminal verwenden. Beispiel: `dig example.com`
    - Windows: Sie können den `nslookup`-Befehl in der Eingabeaufforderung verwenden. Beispiel: `nslookup example.com`
  - Bestätigen Sie die IP-Adresse, zu der der DNS-Name des Load Balancers über eine Befehlszeilenschnittstelle aufgelöst wird.
  - Vergleichen Sie die Ergebnisse der beiden Ausgaben. Die IP-Adressen müssen übereinstimmen.

Weitere Informationen zur Verwendung von Route 53 zum Hosten Ihrer benutzerdefinierten Domain finden Sie unter Meine Domain ist im Internet nicht verfügbar im Entwicklerhandbuch zu Amazon Route 53.

An den Load Balancer gesendete HTTPS-Anfragen geben „NET::ERR_CERT_COMMON_NAME_INVALID“ zurück

Wird auf HTTPS-Anfragen vom Load Balancer `NET::ERR_CERT_COMMON_NAME_INVALID` zurückgegeben, überprüfen Sie die folgenden möglichen Ursachen:

- Der in der HTTPS-Anfrage verwendete Domainname stimmt nicht mit dem im ACM-Zertifikat des Listeners angegebenen alternativen Namen überein.
- Der Standard-DNS-Name des Load Balancers wird verwendet. Der Standard-DNS-Name kann nicht für HTTPS-Anfragen verwendet werden, da für die `*.amazonaws.com`-Domain kein öffentliches Zertifikat angefordert werden kann.

Der Load Balancer zeigt erhöhte Verarbeitungszeiten an

Der Load Balancer berechnet die Verarbeitungszeit je nach Konfiguration unterschiedlich.

- Wenn mit Ihrem Application Load Balancer verknüpft AWS WAF ist und ein Client eine HTTP-POST-Anfrage sendet, wird die Zeit zum Senden der Daten für POST-Anfragen in dem `request_processing_time` Feld in den Load Balancer-Zugriffsprotokollen wiedergegeben. Dieses Verhalten wird für HTTP-POST-Anfragen erwartet.
- Wenn AWS WAF es nicht mit Ihrem Application Load Balancer verknüpft ist und ein Client eine HTTP-POST-Anforderung sendet, wird die Zeit zum Senden der Daten für POST-Anfragen in

dem `target_processing_time` Feld in den Load Balancer-Zugriffsprotokollen wiedergegeben. Dieses Verhalten wird für HTTP-POST-Anfragen erwartet.

Der Load Balancer sendet als Antwortcode „000“.

Wenn bei HTTP/2-Verbindungen die Anzahl der Anfragen, die über eine Verbindung bedient werden, 10.000 übersteigt, sendet der Load Balancer einen GOAWAY-Frame und schließt die Verbindung mit einer TCP-FIN.

Der Load Balancer generiert einen HTTP-Fehler

Die folgenden HTTP-Fehler werden vom Load Balancer generiert. Der Load Balancer sendet den HTTP-Code an den Client, speichert die Anforderung im Zugriffsprotokoll und erhöht die `HTTPCode_ELB_4XX_Count`- oder `HTTPCode_ELB_5XX_Count`-Metrik schrittweise.

Fehler

- HTTP 400: Schlechte Anfrage
- HTTP 401: Unauthorized (Nicht autorisiert)
- HTTP 403: Forbidden (Verboten)
- HTTP 405: Methode nicht erlaubt
- HTTP 408: Anfrage-Timeout
- HTTP 413: Nutzlast zu hoch
- HTTP 414: URI zu lang
- HTTP 460
- HTTP 463
- HTTP 464
- HTTP 500: Interner Serverfehler
- HTTP 501: Nicht implementiert
- HTTP 502: Schlechtes Gateway
- HTTP 503: Service Unavailable
- HTTP 504: Gateway-Timeout
- HTTP 505: Version wird nicht unterstützt
- HTTP 507: Nicht genügend Speicherplatz

- HTTP 561: Unauthorized (Nicht autorisiert)

HTTP 400: Schlechte Anfrage

Mögliche Ursachen:

- Der Client hat eine falsch formatierte Anforderung gesendet, die die HTTP-Spezifikation nicht erfüllt.
- Der Anforderungsheader hat 16 K pro Anforderungszeile, 16 K pro einzelnem Header oder 64 K pro gesamtem Anfrage-Header überschritten.
- Der Client hat die Verbindung beendet, bevor er den vollständigen Anfragetext gesendet hat.

HTTP 401: Unauthorized (Nicht autorisiert)

Sie haben eine Listener-Regel zum Authentifizieren von Benutzern konfiguriert, es trifft aber eine der folgenden Bedingungen zu:

- Entweder haben Sie `OnUnauthenticatedRequest` so konfiguriert, dass nicht authentifizierte Benutzer abgelehnt werden, oder der Identitätsanbieter hat den Zugriff abgelehnt.
- Die Größe der vom Identitätsanbieter zurückgegebenen Ansprüche überschreitet die maximale Größe, die vom Load Balancer unterstützt wird.
- Ein Client hat eine HTTP/1.0-Anfrage ohne Host-Header eingereicht und der Load Balancer konnte keine Umleitungs-URL generieren.
- Der angeforderte Bereich gibt kein ID-Token zurück.
- Sie schließen den Anmeldevorgang nicht ab, bevor das Client-Login-Timeout abgelaufen ist. Weitere Informationen finden Sie unter Client-Login-Timeout.

HTTP 403: Forbidden (Verboten)

Sie haben eine AWS WAF Web Access Control List (Web ACL) konfiguriert, um Anfragen an Ihren Application Load Balancer zu überwachen, und dieser hat eine Anfrage blockiert.

HTTP 405: Methode nicht erlaubt

Der Client hat die TRACE-Methode verwendet, die von Application Load Balancern nicht unterstützt wird.

HTTP 408: Anfrage-Timeout

Der Client hat vor Ablauf des Zeitraums der Leerlaufzeitüberschreitung keine Daten gesendet. Durch Senden eines TCP-Keepalive-Pakets wird dieses Timeout nicht verhindert. Senden Sie mindestens 1 Datenbyte vor Ablauf jeder Leerlaufzeitüberschreitung. Erhöhen Sie bei Bedarf die Länge des Timeout-Limits.

HTTP 413: Nutzlast zu hoch

Mögliche Ursachen:

- Das Ziel ist eine Lambda-Funktion und der Anfragekörper übersteigt 1 MB.
- Der Anforderungsheader hat 16 K pro Anforderungszeile, 16 K pro einzelnem Header oder 64 K pro gesamtem Anfrage-Header überschritten.

HTTP 414: URI zu lang

Die Anfrage-URL oder Abfragezeichenfolgen-Parameter sind zu groß.

HTTP 460

Der Load Balancer hat eine Anforderung von einem Client erhalten, aber der Client hat die Verbindung mit dem Load Balancer getrennt, bevor die Leerlaufzeitüberschreitung abgelaufen war.

Überprüfen Sie, ob der Zeitraum der Client-Zeitüberschreitung größer ist als der Zeitraum der Leerlaufzeitüberschreitung für den Load Balancer. Stellen Sie sicher, dass Ihr Ziel eine Antwort an den Client liefert, bevor der Zeitraum der Client-Zeitüberschreitung verstreicht, oder erhöhen Sie den Zeitraum der Client-Zeitüberschreitung entsprechend der Leerlaufzeitüberschreitung des Load Balancer, wenn dies vom Client unterstützt wird.

HTTP 463

Der Load Balancer hat einen X-Forwarded-For-Anfrage-Header mit zu vielen IP-Adressen erhalten. Die Obergrenze für IP-Adressen liegt bei 30.

HTTP 464

Der Load Balancer hat ein eingehendes Anfrageprotokoll erhalten, das mit der Versionskonfiguration des Zielgruppenprotokolls nicht kompatibel ist.

Mögliche Ursachen:

- Das Anfrageprotokoll ist ein HTTP/1.1, während die Zielgruppenprotokollversion ein gRPC oder HTTP/2 ist.
- Das Anfrageprotokoll ist ein gRPC, während die Zielgruppenprotokollversion ein HTTP/1.1 ist.
- Das Anfrageprotokoll ist ein HTTP/2 und die Anfrage ist nicht POST, während die Zielgruppenprotokollversion ein gRPC ist.

HTTP 500: Interner Serverfehler

Mögliche Ursachen:

- Sie haben eine AWS WAF Web-Zugriffskontrollliste (Web-ACL) konfiguriert und bei der Ausführung der Web-ACL-Regeln ist ein Fehler aufgetreten.
- Der Load Balancer kann nicht mit dem Identitätsanbieter-Tokenendpunkt oder mit dem Endpunkt mit den Benutzerinformationen des Identitätsanbieters kommunizieren.
  - Überprüfen Sie, ob der DNS des IdP öffentlich auflösbar ist.
  - Stellen Sie sicher, dass die Sicherheitsgruppen für Ihren Load Balancer und das Netzwerk ACLs für Ihre VPC ausgehenden Zugriff auf diese Endpunkte zulassen.
  - Stellen Sie sicher, dass Ihre VPC auf das Internet zugreifen kann. Wenn Sie einen internen Load Balancer verwenden, aktivieren Sie den Internetzugriff mithilfe eines NAT-Gateways.
- Der vom IdP erhaltene Benutzeranspruch ist größer als 11 KB.
- Die Antwort des IdP-Token-Endpunkts oder des IdP-Benutzerinformationsendpunkts dauert länger als 5 Sekunden.

HTTP 501: Nicht implementiert

Der Load Balancer erhielt einen Transfer-Encoding (Transferverschlüsselung)-Header mit einem nicht unterstützten Wert. Die unterstützten Werte für Transfer-Encoding (Transferverschlüsselung) sind `chunked` und `identity`. Als Alternative können Sie den Content-Encoding (Inhaltsverschlüsselung)-Header verwenden.

HTTP 502: Schlechtes Gateway

Mögliche Ursachen:

- Der Load Balancer erhielt beim Versuch, eine Verbindung herzustellen, einen TCP-RST vom Ziel.
- Der Load Balancer hat beim Versuch, eine Verbindung herzustellen, eine unerwartete Antwort vom Ziel empfangen, z. B. "ICMP Destination unreachable (Host unreachable)" (ICMP-Ziel nicht erreichbar (Host nicht erreichbar)). Überprüfen Sie, ob Datenverkehr von den Subnetzen des Load Balancers an die Ziele im Ziel-Port zugelassen wird.
- Das Ziel hat die Verbindung mit einem TCP-RST oder einem TCP-FIN geschlossen, während der Load Balancer eine ausstehende Anforderung an das Ziel hatte. Überprüfen Sie, ob die Keep-Alive-Dauer des Ziels kürzer ist als der Timeoutwert für die Leerlaufzeit des Load Balancers.
- Die Zielantwort ist falsch formatiert oder enthält ungültige HTTP-Header.
- Der Ziel-Antwort-Header hat für den gesamten Antwort-Header 32 K überschritten.
- Die Verzögerungszeit der Registrierungsaufhebung einer Anfrage, die von einem Ziel verarbeitet wird, dessen Registrierung aufgehoben wurde, ist abgelaufen. Erhöhen Sie die Verzögerungszeit, sodass langwierige Vorgänge abgeschlossen werden können.
- Das Ziel ist eine Lambda-Funktion und der Anfragekörper übersteigt 1 MB.
- Das Ziel ist eine Lambda-Funktion, die nicht geantwortet hat, bevor die Zeitüberschreitung erreicht wurde.
- Das Ziel ist eine Lambda-Funktion, die einen Fehler zurückgegeben hat, oder die Funktion wurde vom Lambda-Service gedrosselt.
- Der Load Balancer ist beim Herstellen einer Verbindung zu einem Ziel auf einen SSL-Handshake-Fehler gestoßen.

Weitere Informationen finden Sie im AWS Support Knowledge Center unter Wie behebe ich HTTP 502-Fehler im Application Load Balancer?

HTTP 503: Service Unavailable

Die Zielgruppen für den Load Balancer haben keine registrierten Ziele, oder alle registrierten Ziele befinden sich in einem `unused` bestimmten Status.

HTTP 504: Gateway-Timeout

Mögliche Ursachen:

- Der Load Balancer konnte vor Ablauf des Verbindungstimeouts (10 Sekunden) keine Verbindung zum Ziel herstellen.

- Der Load Balancer hat eine Verbindung zum Ziel hergestellt, aber das Ziel hat nicht vor Ablauf des Verbindungstimeouts reagiert.
- Die Netzwerk-ACL oder die SecurityGroup Netzwerkrichtlinien erlaubten keinen Datenverkehr von den Zielen zu den Load Balancer-Knoten an den kurzlebigen Ports (1024-65535).
- Das Ziel gibt einen Inhaltslängen-Header zurück, der größer ist als der Entitätskörper. Beim Warten auf die fehlenden Byte wurde das Zeitlimit des Load Balancer überschritten.
- Das Ziel ist eine Lambda-Funktion und der Lambda-Service hat vor Ablauf des Verbindungszeitlimits nicht reagiert.
- Der Load Balancer hat beim Herstellen einer Verbindung zu einem Ziel ein SSL-Handshake-Timeout (10 Sekunden) festgestellt.

HTTP 505: Version wird nicht unterstützt

Der Load Balancer hat eine unerwartete HTTP-Versionsanfrage erhalten. Beispielsweise hat der Load Balancer eine HTTP/1-Verbindung hergestellt, aber eine HTTP/2-Anfrage erhalten.

HTTP 507: Nicht genügend Speicherplatz

Die Weiterleitungs-URL ist zu lang.

HTTP 561: Unauthorized (Nicht autorisiert)

Sie haben eine Listener-Regel zum Authentifizieren von Benutzern konfiguriert, aber der Identitätsanbieter hat beim Authentifizieren des Benutzers einen Fehlercode zurückgegeben. Suchen Sie in Ihren Zugriffsprotokollen nach dem entsprechenden Fehlerursachencode.

Ein Ziel generiert einen HTTP-Fehler

Der Load Balancer leitet gültige HTTP-Antworten von Zielen an den Client weiter, einschließlich HTTP-Fehlern. Die von einem Ziel generierten HTTP-Fehler werden in der `HTTPCode_Target_4XX_Count`- und der `HTTPCode_Target_5XX_Count`-Metrik aufgezeichnet.

Ein AWS Certificate Manager Zertifikat steht nicht zur Verwendung zur Verfügung

Wenn Sie sich für die Verwendung eines HTTPS-Listeners mit Ihrem Application Load Balancer entscheiden, AWS Certificate Manager müssen Sie vor der Ausstellung eines Zertifikats den Domainbesitz überprüfen. Wenn dieser Schritt bei der Einrichtung versäumt wird, verbleibt das Zertifikat im Status `Pending Validation` und kann erst verwendet werden, wenn es validiert wurde.

- Wenn Sie die E-Mail-Validierung verwenden, finden Sie weitere Informationen unter E-Mail-Validierung im AWS Certificate Manager -Benutzerhandbuch.
- Weitere Informationen zur DNS-Validierung finden Sie unter DNS-Validierung im AWS Certificate Manager -Benutzerhandbuch.

Header mit mehreren Zeilen werden nicht unterstützt

Application Load Balancer unterstützen keine mehrzeiligen Header, einschließlich des `message/http`-Medientyp-Headers. Wenn ein mehrzeiliger Header bereitgestellt wird, hängt der Application Load Balancer einen Doppelpunkt „`:`“ an, bevor er ihn an das Ziel weitergibt.

Beheben Sie fehlerhafte Ziele mithilfe der Ressourcenübersicht

Wenn Ihre Application Load Balancer Balancer-Ziele die Integritätsprüfungen nicht bestehen, können Sie die Ressourcenübersicht verwenden, um fehlerhafte Ziele zu finden und auf der Grundlage des Fehlerursachencodes Maßnahmen zu ergreifen. Weitere Informationen finden Sie unter Sehen Sie sich die Application Load Balancer Balancer-Ressourcenübersicht an.

Die Ressourcenübersicht bietet zwei Ansichten: „Übersicht“ und „Ungesunde Zielübersicht“. Overview ist standardmäßig ausgewählt und zeigt alle Ressourcen Ihres Load Balancers an. Wenn Sie die Ansicht Unhealthy Target Map auswählen, werden nur die fehlerhaften Ziele in jeder Zielgruppe angezeigt, die dem Application Load Balancer zugeordnet ist.

> **Note**
>
> Sie müssen die Option „Ressourcendetails anzeigen“ aktivieren, um die Zusammenfassung der Integritätsprüfung und die Fehlermeldungen für alle entsprechenden Ressourcen in der

Ressourcenübersicht anzuzeigen. Wenn diese Option nicht aktiviert ist, müssen Sie jede Ressource auswählen, um ihre Details anzuzeigen.

In der Spalte Zielgruppen wird eine Zusammenfassung der gesunden und ungesunden Ziele für jede Zielgruppe angezeigt. Auf diese Weise kann festgestellt werden, ob alle Ziele die Zustandsprüfungen nicht bestehen oder ob nur bestimmte Ziele fehlschlagen. Wenn alle Ziele in einer Zielgruppe die Integritätsprüfungen nicht bestehen, überprüfen Sie die Konfiguration der Zielgruppe. Wählen Sie den Namen einer Zielgruppe aus, um deren Detailseite in einem neuen Tab zu öffnen.

In der Spalte Ziele werden die TargetID und der aktuelle Status der Integritätsprüfung für jedes Ziel angezeigt. Wenn ein Ziel fehlerhaft ist, wird der Code für die Ursache des Fehlers bei der Integritätsprüfung angezeigt. Wenn ein einzelnes Ziel eine Integritätsprüfung nicht besteht, stellen Sie sicher, dass das Ziel über ausreichende Ressourcen verfügt, und stellen Sie sicher, dass die auf dem Ziel ausgeführten Anwendungen verfügbar sind. Wählen Sie die ID eines Ziels aus, um die zugehörige Detailseite in einer neuen Registerkarte zu öffnen.

Wenn Sie Exportieren auswählen, haben Sie die Möglichkeit, die aktuelle Ansicht der Ressourcenübersicht Ihres Application Load Balancers als PDF zu exportieren.

Stellen Sie sicher, dass Ihre Instance die Integritätsprüfungen nicht besteht, und überprüfen Sie dann anhand des Fehlerursachencodes auf die folgenden Probleme:

- Fehlerhaft: Die HTTP-Antwort stimmt nicht überein
  - Stellen Sie sicher, dass die auf dem Ziel ausgeführte Anwendung die richtige HTTP-Antwort auf die Integritätsprüfanforderungen des Application Load Balancers sendet.
  - Alternativ können Sie die Integritätsprüfanforderung des Application Load Balancers so aktualisieren, dass sie mit der Antwort der Anwendung übereinstimmt, die auf dem Ziel ausgeführt wird.
- Fehlerhaft: Das Zeitlimit für die Anfrage wurde überschritten
  - Stellen Sie sicher, dass die Sicherheitsgruppen und Network Access Control Lists (ACL), die Ihren Zielen und dem Application Load Balancer zugeordnet sind, die Konnektivität nicht blockieren.
  - Stellen Sie sicher, dass das Ziel über ausreichende Ressourcen verfügt, um Verbindungen vom Application Load Balancer anzunehmen.
  - Überprüfen Sie den Status aller Anwendungen, die auf dem Ziel ausgeführt werden.

  - Die Antworten des Application Load Balancers auf die Integritätsprüfung können in den Anwendungsprotokollen der einzelnen Ziele eingesehen werden. Weitere Informationen finden Sie unter Ursachencodes für Gesundheitschecks.
- Ungesund: FailedHealthChecks
  - Überprüfen Sie den Status aller Anwendungen, die auf dem Ziel ausgeführt werden.
  - Stellen Sie sicher, dass das Ziel auf dem Health Check-Port auf Datenverkehr wartet.

    > **Wenn Sie einen HTTPS-Listener verwenden**
    >
    > Sie wählen aus, welche Sicherheitsrichtlinie für Front-End-Verbindungen verwendet wird. Die für Back-End-Verbindungen verwendete Sicherheitsrichtlinie wird automatisch auf der Grundlage der verwendeten Front-End-Sicherheitsrichtlinie ausgewählt.
    >
    > - Wenn Ihr HTTPS-Listener eine TLS 1.3-Sicherheitsrichtlinie für Front-End-Verbindungen verwendet, wird die `ELBSecurityPolicy-TLS13-1-0-2021-06` Sicherheitsrichtlinie für Back-End-Verbindungen verwendet.
    > - Wenn Ihr HTTPS-Listener keine TLS 1.3-Sicherheitsrichtlinie für Front-End-Verbindungen verwendet, wird die `ELBSecurityPolicy-2016-08` Sicherheitsrichtlinie für Back-End-Verbindungen verwendet.
    >
    > Weitere Informationen finden Sie unter Sicherheitsrichtlinien.

  - Stellen Sie sicher, dass das Ziel ein Serverzertifikat und einen Schlüssel im richtigen Format bereitstellt, das in der Sicherheitsrichtlinie angegeben ist.
  - Stellen Sie sicher, dass das Ziel eine oder mehrere übereinstimmende Chiffren und ein vom Application Load Balancer bereitgestelltes Protokoll zur Einrichtung von TLS-Handshakes unterstützt.

Kontingente für Ihre Application Load Balancer

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für Ihre Application Load Balancer anzuzeigen, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS services (Dienste) und wählen Sie Elastic Load Balancing aus. Sie können auch den Befehl describe-account-limits(AWS CLI) für Elastic Load Balancing verwenden.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent noch nicht unter Servicekontingente verfügbar ist, reichen Sie einen Antrag auf Erhöhung des Servicekontingents ein.

Kontingente

- Load Balancers
- Zielgruppen
- Regeln
- Vertraue Geschäften
- Zertifikate
- HTTP-Header
- Load Balancer Balancer-Kapazitätseinheiten

Load Balancers

Ihr AWS Konto hat die folgenden Kontingente für Application Load Balancers.

Name	Standard	Anpassbar
Application Load Balancer pro Region	50	Ja
Zertifikate pro Application Load Balancer (ausgenommen Standardzertifikate)	25	Ja

Name	Standard	Anpassbar
Listener pro Application Load Balancer	50	Ja
Zielgruppen pro Aktion und Application Load Balancer	5	Nein
Zielgruppen pro Application Load Balancer	100	Nein
Ziele pro Application Load Balancer	1.000	Ja

Zielgruppen

Die folgenden Kontingente gelten für Zielgruppen.

Name	Standard	Anpassbar
Zielgruppen pro Region	3.000*	Ja
Ziele pro Zielgruppe pro Region (Instances oder IP-Adressen)	1.000	Ja
Ziele pro Zielgruppe (Lambda-Funktionen)	1	Nein
Load Balancer pro Zielgruppe	1	Nein

* Dieses Kontingent wird von Application Load Balancers und Network Load Balancers geteilt.

Regeln

Die folgenden Kontingente gelten für Regeln.

Name	Standard	Anpassbar
Regeln pro Application Load Balancer (ohne Standardregeln)	100	Ja

Name	Standard	Anpassbar
Bedingungswerte pro Regel	5	Nein
Bedingungsplatzhalter pro Regel	5	Nein
Übereinstimmungsauswertungen pro Regel	5	Nein

Vertraue Geschäften

Die folgenden Kontingente gelten für Trust Stores.

Name	Standard	Anpassbar
Trust Stores pro Konto	20	Ja
Anzahl der Listener, die mTLS im Überprüfungsmodus verwenden, pro Load Balancer.	2	Nein

Zertifikate

Die folgenden Kontingente gelten für Zertifikate, einschließlich der Namen von Zertifizierungsstellenzertifikaten und Zertifikatssperrlisten.

Name	Standard	Anpassbar
Größe des CA-Zertifikats	16 KB	Nein
CA-Zertifikate pro Trust Store	25	Ja
Größe des Betreffs von CA-Zertifikaten pro Trust Store	10.000	Ja
Maximale Tiefe der Zertifikatskette	4	Nein
Sperreinträge pro Trust Store	500 000	Ja

Name	Standard	Anpassbar
Dateigröße der Sperrliste	50 MB	Nein
Sperrlisten pro Trust Store	30	Ja
Größe der TLS-Nachricht	64 K	Nein

HTTP-Header

Für HTTP-Header gilt die folgende Größenbeschränkung.

Name	Standard	Anpassbar
Anforderungszeile	16 K	Nein
Einzelner Header	16 K	Nein
Gesamter Antwort-Header	32 K	Nein
Gesamter Anfrage-Header	64 K	Nein

Load Balancer Balancer-Kapazitätseinheiten

Die folgenden Kontingente gelten für Load Balancer Capacity Units (LCU).

Name	Standard	Anpassbar
Reservierte Kapazitätseinheiten für den Application Load Balancer (LCUs) pro Application Load Balancer	15 000	Ja
Reservierte Application Load Balancer Balancer-Kapazitätseinheiten (LCU) pro Region	0	Ja

Dokumentverlauf für Application Load Balancer

In der folgenden Tabelle werden die Versionen für Application Load Balancer beschrieben.

Änderung	Beschreibung	Datum
Änderung des HTTP-Headers	Diese Version bietet Unterstützung für die Änderung von HTTP-Headern für alle Antwortcodes. Bisher war diese Funktion auf die Antwortcodes 2xx und 3xx beschränkt.	28. Februar 2025
Reservierung von Kapazitätseinheiten	Diese Version bietet Unterstützung für die Festlegung einer Mindestkapazität für Ihren Load Balancer.	20. November 2024
Karte der Ressourcen	Diese Version bietet Unterstützung für die Anzeige Ihrer Load Balancer-Ressourcen und -Beziehungen in einem visuellen Format.	8. März 2024
WAF mit einem Klick	Diese Version bietet Unterstützung für die Konfiguration des Verhaltens Ihres Load Balancers, wenn er mit einem Klick integriert wird. AWS WAF	6. Februar 2024
Gegenseitiges TLS	Diese Version bietet Unterstützung für die gegenseitige TLS-Authentifizierung.	26. November 2023

Automatische Zielgewichte	Diese Version bietet Unterstützung für den Algorithmus für automatische Zielgewichte.	26. November 2023
FIPS 140-3 TLS-Terminierung	Diese Version fügt Sicherheitsrichtlinien hinzu, die beim Beenden von TLS-Verbindungen kryptografische FIPS 140-3-MODULE verwenden.	20. November 2023
Registrieren Sie Ziele mit IPv6	Diese Version bietet Unterstützung für die Registrierung von Instances als Ziele, wenn sie von adressiert werden IPv6.	2. Oktober 2023
Sicherheitsrichtlinien, die TLS 1.3 unterstützen	Diese Version bietet Unterstützung für vordefinierte Sicherheitsrichtlinien mit TLS 1.3.	22. März 2023
Zonale Verschiebung	Diese Version bietet Unterstützung für die Weiterleitung von Datenverkehr von einer einzelnen beeinträchtigten Availability Zone weg durch die Integration mit der Amazon Anwendungswiederherstellungs-Controller (ARC).	28. November 2022
Schalten Sie den zonenübergreifenden Lastenausgleich aus	Diese Version bietet Unterstützung für die Deaktivierung des zonenübergreifenden Lastenausgleichs.	28. November 2022

Zustand der Zielgruppe	Mit dieser Version lässt sich die Mindestanzahl oder der Prozentsatz der Ziele konfigurieren, die fehlerfrei sein müssen. Außerdem können Sie festlegen, welche Maßnahmen der Load Balancer ergreift, wenn der Schwellenwert nicht erreicht wird.	28. November 2022
Zonenübergreifendes Load Balancing	Diese Version bietet Unterstützung für die Konfiguration des zonenübergreifenden Lastenausgleichs auf Zielgruppenebene.	17. November 2022
IPv6 Zielgruppen	Diese Version bietet Unterstützung für die Konfiguration von IPv6 Zielgruppen für Application Load Balancers.	23. November 2021
IPv6 interne Load Balancer	Diese Version bietet Unterstützung für die Konfiguration von IPv6 Zielgruppen für Application Load Balancers.	23. November 2021
AWS PrivateLink und statische IP-Adressen	Diese Version bietet Unterstützung für die Verwendung AWS PrivateLink und Offenlegung statischer IP-Adressen, indem der Datenverkehr direkt von Network Load Balancers an Application Load Balancers weitergeleitet wird.	27. September 2021

Erhaltung des Client-Ports	In dieser Version wurde ein Attribut hinzugefügt, um den Quellport zu erhalten, den der Client zur Verbindung mit dem Load Balancer verwendet hat.	29. Juli 2021
TLS-Header	In dieser Version wird ein Attribut hinzugefügt, das angibt, dass die TLS-Header, die Informationen über die ausgehandelte TLS-Version und die Verschlüsselungssuite enthalten, der Client-Anfrage hinzugefügt werden, bevor sie an das Ziel gesendet wird.	21. Juli 2021
Zusätzliche ACM-Zertifikate	Diese Version unterstützt RSA-Zertifikate mit Schlüssellängen von 2048, 3072 und 4096 Bit sowie alle ECDSA-Zertifikate.	14. Juli 2021
Anwendungsbasierte Sticky Sessions	Diese Version fügt ein anwendungsbasiertes Cookie hinzu, um Sticky Sessions für Ihren Load Balancer zu unterstützen.	8. Februar 2021
Sicherheitsrichtlinie für FS mit Unterstützung für TLS Version 1.2	Diese Version umfasst eine Sicherheitsrichtlinie für Forward Secrecy (FS) mit Unterstützung für TLS Version 1.2.	24. November 2020

Unterstützung für WAF Fail Open	Diese Version bietet Unterstützung für die Konfiguration des Verhaltens Ihres Load Balancers, wenn dieser mit integriert wird. AWS WAF	13. November 2020
Unterstützung für gRPC und HTTP/2	Diese Version bietet Unterstützung für gRPC-Workloads und end-to-end HTTP/2.	29. Oktober 2020
Outpost-Unterstützung	Sie können einen Application Load Balancer auf Ihrem AWS Outposts bereitstellen.	8. September 2020
Desynchroner Mitigationsmodus	Diese Version bietet Unterstützung für den desynchronen Mitigationsmodus.	17. August 2020
Am wenigsten ausstehende Anfragen	Mit dieser Version wird die Unterstützung für den Algorithmus „Am wenigsten ausstehende Anfragen“ hinzugefügt.	25. November 2019
Gewichtete Zielgruppen	Diese Version bietet neue Unterstützung für Weiterleitungsaktionen mit mehreren Zielgruppen. Anforderungen werden basierend auf der Gewichtung, die Sie für jede Zielgruppe angeben, an diese Zielgruppen verteilt.	19. November 2019
New Attribute	Diese Version bietet neue Unterstützung für das Attribut routing.http.drop_invalid_header_fields.enabled.	15. November 2019

Sicherheitsrichtlinien für FS	Diese Version bietet Unterstützung für drei weitere vordefinierte Forward Secrecy-Sicherheitsrichtlinien.	8. Oktober 2019
Erweiterte Anfrageweiterleitung	In dieser Version wurde Unterstützung für weitere Bedingungstypen für Ihre Listener-Regeln hinzugefügt.	27. März 2019
Lambda-Funktionen als Ziel	Diese Version fügt Unterstützung für die Registrierung von Lambda-Funktionen als Ziel hinzu.	29. November 2018
Weiterleitungsaktionen	In dieser Version wurde Support für den Load Balancer zum Weiterleiten von Anfragen an eine andere URL hinzugefügt.	25. Juli 2018
Aktionen mit feststehender Antwort	In dieser Version wurde Support für den Load Balancer zum Zurückgeben benutzerdefinierter HTTP-Antworten hinzugefügt.	25. Juli 2018
Sicherheitsrichtlinien für FS und TLS 1.2	Mit dieser Version wird die Unterstützung für zwei zusätzliche vordefinierte Sicherheitsrichtlinien hinzugefügt.	6. Juni 2018

Benutzerauthentifizierung	Mit dieser Version wird für den Load Balancer die Unterstützung zum Authentifizieren von Benutzern Ihrer Anwendungen mit ihren Unternehmensidentitäten oder Social Identities vor dem Weiterleiten von Anfragen hinzugefügt.	30. Mai 2018
Berechtigungen auf Ressourcenebene	Mit dieser Version wird Unterstützung für Berechtigungen auf Ressourcenebene und Bedingungsschlüssel für das Markieren hinzugefügt.	10. Mai 2018
Langsamer Startmodus	Diese Version bietet Unterstützung für den Modus des langsamen Hochfahrens, der den Anteil an Anfragen, die vom Load Balancer an ein neu registriertes Ziel gesendet werden, während dieses warmläuft, schrittweise erhöht.	24. März 2018
SNI-Unterstützung	In dieser Version wurde SNI-Unterstützung (Server Name Indication) hinzugefügt.	10. Oktober 2017
IP-Adressen als Ziele	Diese Version bietet Unterstützung für die Registrierung von IP-Adressen als Ziele.	31. August 2017
Host-basiertes Routing	Mit dieser Version wird Unterstützung für Weiterleitungsanfragen basierend auf den Host-Namen im Host-Header hinzugefügt.	5. April 2017

Sicherheitsrichtlinien für TLS 1.1 und TLS 1.2	Mit dieser Version werden Sicherheitsrichtlinien für TLS 1.1 und TLS 1.2 eingeführt.	6. Februar 2017
IPv6 Unterstützung	Diese Version bietet Unterstützung für IPv6 Adressen.	25. Januar 2017
Rückverfolgung anfordern	Diese Version bietet Unterstützung für Anfragenachverfolgung.	22. November 2016
Unterstützung von Perzentilen für die Metrik TargetResponseTime	Diese Version bietet Unterstützung für die neuen Perzentilstatistiken, die von Amazon unterstützt werden. CloudWatch	17. November 2016
Neuer Typ von Load Balancern	In dieser Version von Elastic Load Balancing werden Application Load Balancer eingeführt.	11. August 2016

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.