



Network Load Balancers

Elastic Load Balancing



Elastic Load Balancing: Network Load Balancers

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

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irreführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist ein Network Load Balancer?	1
Network-Load-Balancer-Komponenten	1
Network Load Balancer im Überblick	2
Vorteile der Migration von einem Classic Load Balancer	3
Erste Schritte	4
Preisgestaltung	4
Network Load Balancers	5
Load Balancer-Status	6
IP-Adresstyp	6
Zeitlimit für Verbindungsleerlauf	7
Load Balancer-Attribute	8
Zonenübergreifendes Load Balancing	9
DNS-Name	9
Zonaler Zustand des Load Balancers	10
Erstellen eines Load Balancers	11
Voraussetzungen	11
Erstellen Sie den Load Balancer	12
Testen Sie den Load Balancer	17
Nächste Schritte	18
Aktualisieren von Availability Zones	18
Aktualisieren Sie den IP-Adresstyp	21
Bearbeiten Sie die Load Balancer-Attribute	23
Löschschutz	23
Zonenübergreifendes Load Balancing	24
DNS-Affinität der Availability Zone	26
Sekundäre IP-Adressen	30
Aktualisieren Sie die Sicherheitsgruppen	32
Überlegungen	33
Beispiel: Filtern des Client-Datenverkehrs	33
Beispiel: Nur Datenverkehr vom Network Load Balancer akzeptieren	34
Aktualisieren der zugeordneten Sicherheitsgruppen	35
Aktualisieren der Sicherheitseinstellungen	36
Überwachen Sie Sicherheitsgruppen	38
Kennzeichnen Sie einen Load Balancer	38

Löschen eines -Load Balancers	40
Sehen Sie sich die Ressourcenübersicht an	42
Komponenten der Ressourcenübersicht	42
CloudWatch Logs	43
Zonale Verschiebung	45
Bevor Sie beginnen	45
Administrative Überschreibung	46
Zonenverschiebung aktivieren	46
Starten einer Zonenverschiebung	48
Aktualisieren einer Zonenverschiebung	49
Abbrechen einer Zonenverschiebung	51
LCU-Reservierungen	51
Reservierung anfragen	53
Reservierung aktualisieren oder stornieren	55
Überwachen Sie die Reservierung	56
Listener	58
Listener-Konfiguration	58
Standardaktionen	60
Listener-Attribute	61
Sichere Zuhörer	61
ALPN-Richtlinien	62
Erstellen eines Listeners	63
Voraussetzungen	63
Hinzufügen eines Listeners	64
Serverzertifikate	69
Unterstützte Schlüsselalgorithmen	70
Standardzertifikat	71
Zertifikatliste	71
Zertifikatserneuerung	72
Sicherheitsrichtlinien	72
TLS-Sicherheitsrichtlinien	75
FIPS-Sicherheitsrichtlinien	105
FS unterstützte Sicherheitsrichtlinien	126
Aktualisieren eines Listeners	132
Aktualisieren Sie das Leerlauf-Timeout	136
Aktualisieren eines TLS-Listeners	137

Ersetzen des Standardzertifikats	138
Hinzufügen von Zertifikaten zu einer Zertifikatliste	139
Entfernen eines Zertifikats aus der Zertifikatliste	141
Aktualisieren der Sicherheitsrichtlinie	142
Aktualisieren der ALPN-Richtlinie	143
Löschen eines Listeners	145
Zielgruppen	146
Weiterleitungskonfiguration	147
Zieltyp	148
Routing- und IP-Adressen anfordern	149
On-Premises-Ressourcen als Ziele	150
IP-Adresstyp	151
Registrierte Ziele	151
Zielgruppenattribute	153
Zustand der Zielgruppe	155
Maßnahmen bei fehlerhaftem Zustand	155
Anforderungen und Überlegungen	156
Beispiel	157
Verwenden des Route-53-DNS-Failover für Ihren Load Balancer	158
Erstellen einer Zielgruppe	159
Aktualisieren Sie die Gesundheitseinstellungen	163
Integritätsprüfungen konfigurieren	165
Zustandsprüfungseinstellungen	167
Zustandsstatus des Ziels	170
Ursachencodes für Zustandsprüfungen	171
Überprüfen Sie den Zustand Ihres Ziels	172
Aktualisieren Sie die Einstellungen für die Integritätsprüfung	174
Zielgruppenattribute bearbeiten	176
Client-IP-Erhaltung	176
Verzögerung der Registrierungsaufhebung	180
Proxy-Protokoll	182
Sticky Sessions	185
Zonenübergreifendes Load Balancing	187
Verbindungsabbruch für fehlerhafte Ziele	189
Ungesundes Entleerungsintervall	190
Ziele registrieren	192

Zielsicherheitsgruppen	193
Netzwerk ACLs	194
Gemeinsam genutzte Subnetze	196
Ziele registrieren	197
Ziele deregistrieren	201
Verwenden Sie Application Load Balancers als Ziele	202
Voraussetzung	203
Schritt 1: Erstellen Sie die Zielgruppe	203
Schritt 2: Erstellen Sie den Network Load Balancer	206
Schritt 3: (Optional) Aktivieren Sie die private Konnektivität	209
Taggen Sie eine Zielgruppe	210
Löschen einer Zielgruppe	212
Überwachen Ihrer Load Balancers	213
CloudWatch Metriken	214
Network Load Balancer-Metriken	215
Metrik-Dimensionen für Network Load Balancers	230
Statistiken für Network-Load-Balancer-Metriken	231
CloudWatch Metriken für Ihren Load Balancer anzeigen	232
Zugriffsprotokolle	234
Zugriffsprotokolldateien	235
Zugriffsprotokolleinträge	236
Verarbeiten von Zugriffsprotokolldateien	240
Aktivieren der Zugriffsprotokolle	240
Deaktivieren der Zugriffsprotokolle	245
Fehlerbehebung	247
Ein registriertes Ziel ist nicht in Betrieb	247
Anfragen werden nicht an Ziele weitergeleitet.	247
Ziele erhalten mehr Zustandsprüfungsanfragen als erwartet.	248
Ziele erhalten weniger Zustandsprüfungsanfragen als erwartet.	248
Fehlerhafte Ziele erhalten Anfragen vom Load Balancer.	249
Am Ziel schlagen HTTP- oder HTTPS-Zustandsprüfungen aufgrund nicht übereinstimmender Host-Header fehl	249
Einem Load Balancer konnte keine Sicherheitsgruppe zugeordnet werden	249
Es konnten nicht alle Sicherheitsgruppen entfernt werden	249
Erhöhung der TCP_ELB_Reset_Count-Metrik	250

Verbindungen überschreiten bei Anfragen von einem Ziel an dessen Load Balancer das Zeitlimit.	250
Die Leistung nimmt beim Verschieben von Zielen an einen Network Load Balancer ab.	251
Fehler bei der Portzuweisung für Back-End-Flows	251
Zeitweise fehlgeschlagener TCP-Verbindungsaufbau oder Verzögerungen beim TCP- Verbindungsaufbau	251
Möglicher Fehler bei der Bereitstellung des Load Balancers	252
Der Verkehr ist ungleichmäßig auf die Ziele verteilt	252
Die DNS-Namensauflösung enthält weniger IP-Adressen als aktivierte Availability Zones	253
IP-fragmentierte Pakete werden nicht an Ziele weitergeleitet	254
Beheben Sie Fehler bei fehlerhaften Zielen mithilfe der Ressourcenübersicht	254
Kontingente	257
Load Balancer	257
Zielgruppen	258
Load Balancer Balancer-Kapazitätseinheiten	258
Dokumentverlauf	260
.....	cclxvi

Was ist ein Network Load Balancer?

Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, z. B. EC2-Instances, Container und IP-Adressen oder eine oder mehrere 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 Network Load Balancers beschrieben. Weitere Informationen zu den anderen Load Balancers finden Sie im [Benutzerhandbuch für Application Load Balancers](#), im [Benutzerhandbuch für Gateway Load Balancers](#) und im [Benutzerhandbuch für Classic Load Balancers](#).

Network-Load-Balancer-Komponenten

Ein Load Balancer dient als zentraler Kontaktpunkt für Clients. Der Load Balancer verteilt den eingehenden Datenverkehr über mehrere Ziele, z. B. Amazon-EC2-Instances. Dies erhöht die Verfügbarkeit Ihrer Anwendung. Sie fügen Ihrem Load Balancer einen oder mehrere Listener hinzu.

Ein Listener prüft Verbindungsanforderungen von Clients unter Verwendung des von Ihnen konfigurierten Protokolls und Ports, und gibt Anforderungen an eine Zielgruppe weiter.

Eine Zielgruppe leitet Anforderungen an ein oder mehrere registrierte Ziele, z. B. EC2-Instances, über das Protokoll und die Port-Nummer, die Sie angeben, weiter. Die Zielgruppen des Network Load Balancer unterstützen die Protokolle TCP, UDP, TCP_UDP, TLS, QUIC und TCP_QUIC. Sie können ein Ziel bei mehreren Zielgruppen registrieren. Sie können Zustandsprüfungen pro Zielgruppe konfigurieren. Integritätsprüfungen werden für alle Ziele durchgeführt, die für die Zielgruppen registriert sind, die in der Standardaktion für Ihren Load Balancer angegeben sind.

Weitere Informationen finden Sie in der folgenden Dokumentation:

- [Load Balancers](#)
- [Listener](#)
- [Zielgruppen](#)

Network Load Balancer im Überblick

Ein Network Load Balancer arbeitet auf der vierten Ebene der OSI-Modells (Open Systems Interconnection). Es können Millionen von Anfragen pro Sekunde verarbeitet werden. Nachdem der Load Balancer eine Anfrage von einem Client erhalten hat, wählt er in der Standardaktion ein Ziel aus einer Zielgruppe aus. Er versucht, die Anfrage mithilfe des von Ihnen angegebenen Protokolls und Ports an das ausgewählte Ziel zu senden.

Wenn Sie eine Availability Zone für den Load Balancer aktivieren, erstellt Elastic Load Balancing einen Load-Balancer-Knoten in der Availability Zone. Standardmäßig verteilt jeder Load Balancer-Knoten Datenverkehr nur auf die registrierten Ziele in seiner Verfügbarkeitszone. Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Load Balancer-Knoten den Datenverkehr gleichmäßig auf die registrierten Ziele in allen aktivierten Availability Zones. Weitere Informationen finden Sie unter [Aktualisieren Sie die Availability Zones für Ihren Network Load Balancer](#).

Um die Fehlertoleranz Ihrer Anwendungen zu erhöhen, können Sie mehrere Availability Zones für Ihren Load Balancer aktivieren und sicherstellen, dass jede Zielgruppe mindestens ein Ziel in jeder aktivierten Availability Zone hat. Wenn beispielsweise eine oder mehrere Zielgruppen in einer Availability Zone kein fehlerfreies Ziel haben, entfernen wir die IP-Adresse für das entsprechende Subnetz vom DNS, aber die Load Balancer-Knoten in den anderen Availability Zones sind weiter verfügbar, um den Datenverkehr weiterzuleiten. Wenn ein Client die time-to-live (TTL) nicht berücksichtigt und Anfragen an die IP-Adresse sendet, nachdem diese aus dem DNS entfernt wurde, schlagen die Anfragen fehl.

Für TCP-Datenverkehr lädt der Load Balancer ein Ziel unter Verwendung eines Flow-Hash-Algorithmus basierend auf dem Protokoll, der Quell-IP-Adresse, dem Quell-Port, der Ziel-IP-Adresse, dem Ziel-Port und der TCP-Sequenznummer aus. Die TCP-Verbindungen von einem Client verfügen über unterschiedliche Quell-Ports und Sequenznummern und können an verschiedene Ziele geleitet werden. Jede einzelne TCP-Verbindung wird für die Dauer der Verbindung an ein einzelnes Ziel geleitet.

Für den UDP-Datenverkehr wählt der Load Balancer ein Ziel unter Verwendung eines Flow-Hash-Algorithmus basierend auf dem Protokoll, der Quell-IP-Adresse, dem Quell-Port, der Ziel-IP-Adresse und des Ziel-Ports aus. Ein UDP-Datenstrom hat die gleiche Quelle und das gleiche Ziel. Folglich wird er während seiner gesamten Lebensdauer konsistent an ein Ziel weitergeleitet. Unterschiedliche UDP-Datenströme verfügen über unterschiedliche Quell-IP-Adressen und -Ports, sodass sie an verschiedene Ziele weitergeleitet werden können.

Für QUIC-Verkehr wählt der Load Balancer anhand der in der Verbindungs-ID (CID) angegebenen Server-ID ein Ziel aus. Für erste Verbindungsversuche ohne Server-ID wird ein Flow-Hash-Algorithmus verwendet, der auf dem Protokoll, der Quell-IP-Adresse, dem Quellport, der Ziel-IP-Adresse und dem Zielport basiert. Sobald eine Verbindungs-ID eingerichtet ist, wird der Verkehr für diese CID für die gesamte Lebensdauer der CID an dasselbe Ziel weitergeleitet.

Elastic Load Balancing erstellt eine Netzwerkschnittstelle für jede Availability Zone, die Sie aktivieren. Jeder Load Balancer-Knoten in der Availability Zone verwendet diese Netzwerkschnittstelle, um eine statische IP-Adresse zu erhalten. Wenn Sie einen Load Balancer erstellen, der mit dem Internet verbunden ist, können Sie optional eine Elastic IP-Adresse pro Subnetz zuordnen.

Wenn Sie eine Zielgruppe erstellen, können Sie ihren Zieltyp angeben, durch den festgelegt wird, wie Sie Ziele registrieren. Sie können beispielsweise eine Instanz IDs, IP-Adressen oder einen Application Load Balancer registrieren. Der Zieltyp wirkt sich auch darauf aus, ob die Client-IP-Adressen beibehalten werden. Weitere Informationen finden Sie unter [the section called “Client-IP-Erhaltung”](#).

Sie können Ziele zu Ihrem Load Balancer hinzufügen und wieder entfernen, wenn sich Ihr Bedarf ändert, ohne den allgemeinen Fluss von Anforderungen 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 Network Load Balancers anstelle eines Classic Load Balancers hat die folgenden Vorteile:

- Möglichkeit, temporäre Verarbeitungslasten zu verarbeiten und eine Skalierung auf Millionen Anfragen pro Sekunde durchzuführen.
- Unterstützung statischer IP-Adressen für den Load Balancer. Sie können auch eine Elastic IP-Adresse pro Subnetz zuweisen, die für den Load Balancer aktiviert wird.

- Unterstützung einer Registrierung von Zielen unter Verwendung von IP-Adressen, auch für Ziele, die außerhalb der VPC für den Load Balancer liegen.
- Unterstützung von Weiterleitungsanfragen an mehrere Anwendungen auf einer einzelnen EC2-Instance. Sie können jede Instance oder IP-Adresse mit derselben Zielgruppe unter Verwendung mehrerer Ports registrieren.
- 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 Amazon-Metriken auf Zielgruppenebene gemeldet werden. Wenn Sie eine Zielgruppe einer Auto-Scaling-Gruppe zuweisen, können Sie jeden Service je nach Bedarf dynamisch skalieren.
- Support für die Protokolle QUIC und TCP_QUIC mit erweiterter Überlastungskontrolle, weniger Roundtrip-Verbindungsaufbau, integriertem TLS und Verbindungsmigration zwischen Netzwerken.

Weitere Informationen zu den von den einzelnen Load-Balancer-Typen unterstützten Features finden Sie unter [Produktvergleich](#) für Elastic Load Balancing.

Erste Schritte

Informationen zum Erstellen eines Network Load Balancer mithilfe von AWS-Managementkonsole AWS CLI AWS CloudFormation, oder finden Sie unter [Erstellen eines Network Load Balancers](#).

Demos häufiger Load-Balancer-Konfigurationen finden Sie unter [Elastic-Load-Balancing-Demos](#).

Preisgestaltung

Weitere Informationen finden Sie unter [Elastic Load Balancing Pricing](#).

Network Load Balancers

Ein Network Load Balancer dient als zentrale Anlaufstelle für Kunden. Clients senden Anfragen an den Network Load Balancer, und der Network Load Balancer sendet sie an Ziele wie EC2 Instances in einer oder mehreren Availability Zones.

Um Ihren Network Load Balancer zu konfigurieren, erstellen Sie [Zielgruppen](#) und registrieren dann Ziele bei Ihren Zielgruppen. Ihr Network Load Balancer ist am effektivsten, wenn Sie sicherstellen, dass jede aktivierte Availability Zone über mindestens ein registriertes Ziel verfügt. Außerdem erzeugen Sie [Listener](#) für Verbindungsanforderungen von Clients und Listener-Regeln zum Weiterleiten von Anforderungen von Clients an Ziele in Ihren Zielgruppen.

Network Load Balancer unterstützen Verbindungen von Clients über VPC-Peering, AWS verwaltetes VPN und Direct Connect VPN-Lösungen von Drittanbietern.

Inhalt

- [Load Balancer-Status](#)
- [IP-Adresstyp](#)
- [Zeitlimit für Verbindungsleerlauf](#)
- [Load Balancer-Attribute](#)
- [Zonenübergreifendes Load Balancing](#)
- [DNS-Name](#)
- [Zonaler Zustand des Load Balancers](#)
- [Erstellen eines Network Load Balancers](#)
- [Aktualisieren Sie die Availability Zones für Ihren Network Load Balancer](#)
- [Aktualisieren Sie die IP-Adresstypen für Ihren Network Load Balancer](#)
- [Attribute für Ihren Network Load Balancer bearbeiten](#)
- [Aktualisieren Sie die Sicherheitsgruppen für Ihren Network Load Balancer](#)
- [Einen Network Load Balancer taggen](#)
- [Löschen eines Network Load Balancers](#)
- [Sehen Sie sich die Network Load Balancer Balancer-Ressourcenübersicht an](#)
- [CloudWatch Logs für Ihren Network Load Balancer](#)
- [Zonenverschiebung für Ihren Network Load Balancer](#)

- [Kapazitätsreservierungen für Ihren Network Load Balancer](#)

Load Balancer-Status

Ein Network Load Balancer kann sich in einem der folgenden Zustände befinden:

provisioning

Der Network Load Balancer wird eingerichtet.

active

Der Network Load Balancer ist vollständig eingerichtet und bereit, den Datenverkehr weiterzuleiten.

failed

Der Network Load Balancer konnte nicht eingerichtet werden.

IP-Adresstyp

Sie können die Typen von IP-Adressen festlegen, die Clients mit Ihrem Network Load Balancer verwenden können.

Network Load Balancer unterstützen die folgenden IP-Adresstypen:

ipv4

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

dualstack

Clients können mit dem Network Load Balancer 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) verbinden.

Überlegungen

- Der Network Load Balancer kommuniziert mit Zielen auf der Grundlage des IP-Adresstyps der Zielgruppe.
- Um die Erhaltung der Quell-IP für IPv6 UDP-Listener zu unterstützen, stellen Sie sicher, dass die Option Präfix für IPv6 Quell-NAT aktiviert ist.

- Wenn Sie den Dual-Stack-Modus für den Network Load Balancer aktivieren, stellt Elastic Load Balancing einen AAAA-DNS-Eintrag für den Network Load Balancer bereit. Clients, die über IPv4 Adressen mit dem Network Load Balancer kommunizieren, lösen den A-DNS-Eintrag auf. Clients, die über IPv6 Adressen mit dem Network Load Balancer kommunizieren, lösen den AAAA-DNS-Eintrag auf.
- Der Zugriff auf Ihren internen Dualstack Network Load Balancer über das Internet-Gateway ist blockiert, um einen unbeabsichtigten Internetzugang zu verhindern. Dies verhindert jedoch nicht den Zugriff auf andere Internetzugänge (z. B. über Peering, Transit Gateway AWS Direct Connect, oder Site-to-Site VPN).

Weitere Informationen finden Sie unter [Aktualisieren Sie die IP-Adresstypen für Ihren Network Load Balancer](#).

Zeitlimit für Verbindungsleerlauf

Für jede TCP-Anforderung, die ein Client über einen Network Load Balancer sendet, wird der Zustand dieser Verbindung nachverfolgt. Wenn weder vom Client noch vom Ziel länger als das Leerlauf-Timeout Daten über die Verbindung gesendet werden, wird die Verbindung nicht mehr nachverfolgt. Wenn ein Client oder ein Ziel nach Ablauf des Timeouts im Leerlauf Daten sendet, erhält der Client ein TCP-RST-Paket, das angibt, dass die Verbindung nicht mehr gültig ist.

Der Standardwert für das Leerlauf-Timeout für TCP-Datenflüsse beträgt 350 Sekunden, kann aber auf einen beliebigen Wert zwischen 60 und 6000 Sekunden aktualisiert werden. Clients oder Ziele können TCP-Keepalive-Pakete verwenden, um das Leerlauf-Timeout neu zu starten. Keepalive-Pakete, die zur Aufrechterhaltung von TLS-Verbindungen gesendet werden, dürfen keine Daten oder Nutzlast enthalten.

Das Timeout im Verbindungsleerlauf für TLS-Listener beträgt 350 Sekunden und kann nicht geändert werden. Wenn ein TLS-Listener ein TCP-Keepalive-Paket von einem Client oder einem Ziel empfängt, generiert der Load Balancer TCP-Keepalive-Pakete und sendet sie alle 20 Sekunden sowohl an die Front-End- als auch an die Back-End-Verbindungen. Sie können dieses Verhalten nicht ändern.

Während UDP verbindungslos ist, behält der Load Balancer den UDP-Datenstromstatus basierend auf den Quell- und Ziel-IP-Adressen und -Ports bei. Dadurch wird sichergestellt, dass Pakete, die zu demselben Flow gehören, konsistent an dasselbe Ziel gesendet werden. Nachdem der Timeoutwert für die Leerlaufzeit abgelaufen ist, betrachtet der Load Balancer das eingehende UDP-Paket als

neuen Flow und leitet es an ein neues Ziel weiter. Elastic Load Balancing legt den Leerlauf-Timeout-Wert für UDP-Flows auf 120 Sekunden fest. Dies können nicht geändert werden.

EC2 Instanzen müssen innerhalb von 30 Sekunden auf eine neue Anfrage antworten, um einen Rückpfad einzurichten.

Weitere Informationen finden Sie unter [Aktualisieren Sie das Leerlauf-Timeout](#).

Load Balancer-Attribute

Sie können Ihren Network Load Balancer konfigurieren, indem Sie seine Attribute bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten Sie die Load Balancer-Attribute](#).

Im Folgenden sind die Load Balancer-Attribute für Network Load Balancer aufgeführt:

`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 [Bucket-Anforderungen](#).

`access_logs.s3.prefix`

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

`deletion_protection.enabled`

Gibt an, ob der [Löschschutz](#) aktiviert ist. Der Standardwert ist `false`.

`ipv6.deny_all_igw_traffic`

Sperrt den Zugriff des Internet-Gateways (IGW) auf den Network Load Balancer und verhindert so den unbeabsichtigten Zugriff auf Ihren internen Network Load Balancer über ein Internet-Gateway. Es ist auf `false` für mit dem Internet verbundene Network Load Balancer und für interne Network Load Balancer eingestellt. `true` Dieses Attribut verhindert nicht den Internetzugriff außerhalb von IGW (z. B. über Peering, Transit Gateway AWS Direct Connect, oder). Site-to-Site VPN

`load_balancing.cross_zone.enabled`

Gibt an, ob [zonenübergreifendes Load Balancing](#) aktiviert ist. Der Standardwert ist `false`.

`dns_record.client_routing_policy`

Gibt an, wie der Verkehr auf die Availability Zones des Network Load Balancers verteilt wird. Die möglichen Werte sind `availability_zone_affinity` bei 100 Prozent zonaler Affinität, `partial_availability_zone_affinity` bei 85 Prozent zonaler Affinität und `any_availability_zone` bei 0 Prozent zonaler Affinität.

`secondary_ips.auto_assigned.per_subnet`

Die Anzahl der zu [konfigurierenden sekundären IP-Adressen](#). Wird verwendet, um Fehler bei der Portzuweisung zu beheben, wenn Sie keine Ziele hinzufügen können. Der gültige Bereich liegt zwischen 0 und 7. Der Standardwert ist 0. Nachdem Sie diesen Wert festgelegt haben, können Sie ihn nicht verringern.

`zonal_shift.config.enabled`

Gibt an, ob [Zonal Shift](#) aktiviert ist. Der Standardwert ist `false`.

Zonenübergreifendes Load Balancing

Standardmäßig verteilt jeder Network Load Balancer Balancer-Knoten den Verkehr nur auf die registrierten Ziele in seiner Availability Zone. Wenn Sie zonenübergreifendes Load Balancing aktivieren, verteilt jeder Network Load Balancer Balancer-Knoten den Verkehr auf die registrierten Ziele in allen aktivierten Availability Zones. Sie können das zonenübergreifende Load Balancing auch auf Zielgruppenebene aktivieren. Weitere Informationen finden Sie unter [the section called “Zonenübergreifendes Load Balancing”](#) und [Zonenübergreifendes Load Balancing](#) im Benutzerhandbuch für Elastic Load Balancing.

DNS-Name

Jeder Network 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 Network Load Balancer verknüpfen. Wenn ein Client eine Anfrage mit diesem benutzerdefinierten Domänennamen stellt, löst der DNS-Server sie in den DNS-Namen für Ihren Network Load Balancer auf.

Registrieren Sie zunächst einen Domainnamen bei einer akkreditierten Domainnamenvergabestelle. Verwenden Sie als Nächstes Ihren DNS-Dienst, z. B. Ihren Domain-Registrierer, um einen DNS-Eintrag zu erstellen, um Anfragen an Ihren Network 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 Network Load Balancer verweist. Weitere Informationen finden Sie unter [Weiterleiten von Datenverkehr an einen ELB Load Balancer](#) im Entwicklerhandbuch von Amazon Route 53.

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

Linux oder Mac

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

Windows

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

Der Network Load Balancer hat DNS-Einträge für seine Knoten. Sie können DNS-Namen mit der folgenden Syntax verwenden, um die IP-Adressen der Network 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
```

Zonaler Zustand des Load Balancers

Network Load Balancer verfügen über zonale DNS-Einträge und IP-Adressen in Route 53 für jede aktivierte Availability Zone. Wenn ein Network Load Balancer eine zonale Zustandsprüfung

für eine bestimmte Availability Zone nicht besteht, wird sein DNS-Eintrag aus Route 53 entfernt. Der zonale Zustand des Load Balancers wird mithilfe der CloudWatch Amazon-Metrik überwacht. Dadurch erhalten Sie mehr Einblick in Ereignisse `ZonalHealthStatus`, die zu einem Ausfall führen, sodass Sie präventive Maßnahmen ergreifen können, um eine optimale Anwendungsverfügbarkeit sicherzustellen. Weitere Informationen finden Sie unter [Network Load Balancer-Metriken](#).

Network Load Balancer können zonale Zustandsprüfungen aus verschiedenen Gründen nicht bestehen, wodurch sie fehlerhaft werden. Im Folgenden finden Sie die häufigsten Ursachen für fehlerhafte Network Load Balancer, die auf fehlgeschlagene zonale Integritätsprüfungen zurückzuführen sind.

Suchen Sie nach den folgenden möglichen Ursachen:

- Es gibt keine fehlerfreien Ziele für den Load Balancer
- Die Anzahl fehlerfreier Ziele liegt unter dem konfigurierten Minimum
- Eine zonale Verschiebung oder eine zonale automatische Verschiebung ist im Gange
- Aufgrund festgestellter Probleme wird der Verkehr automatisch in fehlerfreie Zonen verlagert

Erstellen eines Network Load Balancers

Ein Network Load Balancer nimmt Anfragen von Clients entgegen und verteilt sie auf Ziele in einer Zielgruppe, z. B. EC2 auf Instanzen. Weitere Informationen hierzu finden Sie unter [the section called "Network Load Balancer im Überblick"](#).

Aufgaben

- [Voraussetzungen](#)
- [Erstellen Sie den Load Balancer](#)
- [Testen Sie den Load Balancer](#)
- [Nächste Schritte](#)

Voraussetzungen

- Entscheiden Sie, welche Availability Zones und IP-Adresstypen Ihre Anwendung unterstützen soll. Konfigurieren Sie Ihre Load Balancer-VPC mit Subnetzen in jeder dieser Availability Zones. Wenn die Anwendung sowohl als auch IPv4 IPv6 Datenverkehr unterstützt, stellen Sie sicher, dass die

Subnetze sowohl als auch enthalten. IPv4 IPv6 CIDRs Stellen Sie mindestens ein Ziel in jeder Availability Zone bereit.

- Stellen Sie sicher, dass die Sicherheitsgruppen für Ziel-Instances Datenverkehr auf dem Listener-Port von Client-IP-Adressen (wenn Ziele durch die Instanz-ID angegeben werden) oder Load Balancer-Knoten (wenn Ziele anhand der IP-Adresse angegeben werden) zulassen. Weitere Informationen finden Sie unter [the section called “Zielsicherheitsgruppen”](#).
- Stellen Sie sicher, dass die Sicherheitsgruppen für Ziel-Instances mithilfe des Health Check-Protokolls Datenverkehr vom Load Balancer auf dem Health Check-Port zulassen.
- Wenn Sie planen, Ihren Load Balancer mit statischen IP-Adressen auszustatten, stellen Sie sicher, dass jede Elastic IP-Adresse aus dem Adresspool von IPv4 Amazon stammt und dass sie dieselbe Netzwerkrenzgruppe wie der Load Balancer hat.
- Wenn Sie QUIC- oder TCP_QUIC-Listener verwenden möchten, stellen Sie sicher, dass der Network Load Balancer den `ipv4` Adresstyp verwendet und ihm keine Sicherheitsgruppen zugeordnet sind.

Erstellen Sie den Load Balancer

Im Rahmen der Erstellung eines Network Load Balancer erstellen Sie den Load Balancer, mindestens einen Listener und mindestens eine Zielgruppe. Ihr Load Balancer ist bereit, Client-Anfragen zu bearbeiten, wenn in jeder seiner aktivierten Availability Zones mindestens ein fehlerfreies registriertes Ziel vorhanden ist.

Console

So erstellen Sie einen Network Load Balancer

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 Load Balancer erstellen aus.
4. Wählen Sie im Bereich Network Load Balancer die Option Erstellen.
5. Basiskonfiguration
 - a. Geben Sie unter Load Balancer name einen Namen für Ihren Network Load Balancer ein. Der Name muss innerhalb Ihrer Gruppe von Load Balancern in der Region eindeutig sein. Er darf maximal 32 Zeichen lang sein und nur alphanumerische Zeichen und

Bindestriche enthalten. Er darf nicht mit einem Bindestrich oder mit `internal-` beginnen oder enden.

- b. Wählen Sie für Scheme (Schema) entweder Internet-facing (Mit dem Internet verbunden) oder Internal (Intern) aus. Ein mit dem Internet verbundener Network Load Balancer leitet Anfragen von Clients über das Internet an Ziele weiter. Ein interner Network Load Balancer leitet Anfragen über private IP-Adressen an Ziele weiter.
- c. Wählen Sie für den Load Balancer-IP-Adresstyp aus, IPv4ob Ihre Clients IPv4 Adressen für die Kommunikation mit dem Network Load Balancer oder Dualstack verwenden, wenn Ihre Clients beide verwenden, IPv4 und IPv6 Adressen für die Kommunikation mit dem Network Load Balancer verwenden.

6. Netzwerkzuordnung

- a. Wählen Sie für VPC die VPC aus, die Sie für Ihren Load Balancer vorbereitet haben. Bei einem mit dem Internet verbundenen Load Balancer stehen nur Load Balancer VPCs mit Internet-Gateway zur Auswahl.
- b. Bei einem Dual-Stack-Load Balancer können Sie keinen UDP-Listener hinzufügen, es sei denn, das Enable-Präfix für IPv6 Quell-NAT ist On (Quell-NAT-Präfixe pro Subnetz).
- c. Wählen Sie für Availability Zones und Subnetze mindestens eine Availability Zone und wählen Sie ein Subnetz pro Zone aus. Beachten Sie, dass Subnetze, die mit Ihnen geteilt wurden, zur Auswahl stehen.

Wenn Sie mehrere Availability Zones auswählen und sicherstellen, dass Sie in jeder ausgewählten Zone Ziele registriert haben, erhöht dies die Fehlertoleranz Ihrer Anwendung.

- d. Bei einem mit dem Internet verbundenen Load Balancer können Sie für jede Availability Zone eine Elastic IP-Adresse auswählen. Auf diese Weise erhält Ihr Load Balancer statische IP-Adressen.


Bei einem internen Load Balancer können Sie eine private IPv4 Adresse aus dem Adressbereich jedes Subnetzes eingeben oder eine für Sie auswählen lassen AWS .

Bei einem Dual-Stack-Loadbalancer können Sie eine IPv6 Adresse aus dem Adressbereich jedes Subnetzes eingeben oder eine für Sie auswählen lassen. AWS


Bei einem Load Balancer mit aktiviertem Quell-NAT können Sie ein benutzerdefiniertes IPv6 Präfix eingeben oder eines für Sie auswählen lassen AWS .

7. Sicherheitsgruppen

Wir wählen die Standardsicherheitsgruppe für die Load Balancer-VPC vorab aus. Sie können bei Bedarf zusätzliche Sicherheitsgruppen auswählen. Wenn Sie keine Sicherheitsgruppe haben, die Ihren Anforderungen entspricht, wählen Sie Neue Sicherheitsgruppe erstellen, um jetzt eine zu erstellen. Weitere Informationen finden Sie unter [Erstellen einer Sicherheitsgruppe](#) im Amazon-VPC-Benutzerhandbuch.

 Warning

Wenn Sie Ihrem Network Load Balancer jetzt keine Sicherheitsgruppen zuordnen, können Sie sie später nicht mehr zuordnen.

 Warning

Um QUIC- oder TCP_QUIC-Listener verwenden zu können, darf Ihr Network Load Balancer keine Sicherheitsgruppen haben.

8. Listener und Routing

- a. Es ist standardmäßig ein Listener eingestellt, der über Port 80 TCP-Datenverkehr annimmt. Sie können die Standard-Listener-Einstellungen beibehalten oder bei Bedarf das Protokoll oder den Port ändern.
- b. Wählen Sie unter Standardaktion eine Zielgruppe aus, an die der Datenverkehr weitergeleitet werden soll.

Um eine weitere Zielgruppe hinzuzufügen, wählen Sie Zielgruppe hinzufügen und aktualisieren Sie die Gewichtungen nach Bedarf.

Wenn Sie keine Zielgruppe haben, die Ihren Bedürfnissen entspricht, wählen Sie Zielgruppe erstellen, um jetzt eine zu erstellen. Weitere Informationen finden Sie unter [Erstellen einer Zielgruppe](#).

- c. (Optional) Wählen Sie Listener-Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
- d. (Optional) Wählen Sie „Listener hinzufügen“, um einen weiteren Listener hinzuzufügen (z. B. einen TLS-Listener).

9. Secure listener settings (Sichere Listener-Einstellungen)

Dieser Abschnitt wird nur angezeigt, wenn Sie einen TLS-Listener hinzufügen.

- a. Wählen Sie unter Sicherheitsrichtlinie eine Sicherheitsrichtlinie aus, die Ihren Anforderungen entspricht. Weitere Informationen finden Sie unter [Sicherheitsrichtlinien](#).
- b. Wählen Sie für SSL/TLS Standardserverzertifikat die Option Von ACM als Zertifikatsquelle aus. Wählen Sie ein Zertifikat aus, mit dem Sie bereitgestellt oder importiert haben. AWS Certificate Manager Wenn in ACM kein Zertifikat verfügbar ist, Sie aber über ein Zertifikat zur Verwendung mit Ihrem Load Balancer verfügen, wählen Sie Zertifikat importieren aus und geben Sie die erforderlichen Informationen ein. Wählen Sie andernfalls Neues ACM-Zertifikat anfordern aus. Weitere Informationen finden Sie unter [AWS Certificate Manager Zertifikate](#) im AWS Certificate Manager Benutzerhandbuch.
- c. (Optional) Wählen Sie für die ALPN-Richtlinie eine Richtlinie aus, um ALPN zu aktivieren. Weitere Informationen finden Sie unter [the section called “ALPN-Richtlinien”](#).

10. Load Balancer-Tags

(Optional) Erweitern Sie die Load Balancer-Tags. Wählen Sie Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein. Weitere Informationen finden Sie unter [Tags](#).

11. Übersicht

Überprüfen Sie Ihre Konfiguration und wählen Sie Load Balancer erstellen aus. Während der Erstellung werden einige Standardattribute auf Ihren Network Load Balancer angewendet. Sie können sie anzeigen und bearbeiten, nachdem Sie den Network Load Balancer erstellt haben. Weitere Informationen finden Sie unter [Load Balancer-Attribute](#).

AWS CLI

So erstellen Sie einen Network Load Balancer

Verwenden Sie den Befehl [create-load-balancer](#).

Im folgenden Beispiel wird ein mit dem Internet verbundener Load Balancer mit zwei aktivierten Availability Zones und einer Sicherheitsgruppe erstellt.

```
aws elbv2 create-load-balancer \  
  --name my-load-balancer \  
  --type network \  
  --
```

```
--subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \  
--security-groups sg-1111222233334444
```

So erstellen Sie einen internen Network Load Balancer

Fügen Sie die `--scheme` Option ein, wie im folgenden Beispiel gezeigt.

```
aws elbv2 create-load-balancer \  
  --name my-load-balancer \  
  --type network \  
  --scheme internal \  
  --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \  
  --security-groups sg-1111222233334444
```

So erstellen Sie einen Dual-Stack-Network-Load-Balancer

Fügen Sie die `--ip-address-type` Option ein, wie im folgenden Beispiel gezeigt.

```
aws elbv2 create-load-balancer \  
  --name my-load-balancer \  
  --type network \  
  --ip-address-type dualstack \  
  --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \  
  --security-groups sg-1111222233334444
```

So fügen Sie einen Listener hinzu

Verwenden Sie den Befehl [create-listener](#). Beispiele finden Sie unter [Erstellen eines Listeners](#).

CloudFormation

So erstellen Sie einen Network Load Balancer

Definieren Sie eine Ressource des Typs [AWS::ElasticLoadBalancingV2::LoadBalancer](#)

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network  
      Scheme: internal
```

```
IpAddressType: dualstack
Subnets:
  - !Ref subnet-AZ1
  - !Ref subnet-AZ2
SecurityGroups:
  - !Ref mySecurityGroup
Tags:
  - Key: 'department'
    Value: '123'
```

So fügen Sie einen Listener hinzu

Definieren Sie eine Ressource des Typs [AWS::ElasticLoadBalancingV2::Listener](#). Beispiele finden Sie unter [Erstellen eines Listeners](#).

Testen Sie den Load Balancer

Nachdem Sie Ihren Network Load Balancer erstellt haben, können Sie überprüfen, ob Ihre EC2 Instances die erste Zustandsprüfung bestanden haben, und dann testen, ob der Network Load Balancer Traffic an Ihre EC2 Instances sendet. Informationen zum Löschen des Network Load Balancer finden Sie unter [Löschen eines Network Load Balancers](#).

So testen Sie den Network Load Balancer

1. Nachdem der Network Load Balancer erstellt wurde, wählen Sie Schließen.
2. Wählen Sie im Navigationsbereich Zielgruppen aus.
3. Wählen Sie die neue 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 mindestens einer Instance fehlerfrei ist, können Sie Ihren Network Load Balancer testen. Weitere Informationen finden Sie unter [Zustandsstatus des Ziels](#).
5. Klicken Sie im Navigationsbereich auf Load Balancers.
6. Wählen Sie den neuen Network Load Balancer aus.
7. Kopieren Sie den DNS-Namen des Network Load Balancer (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.

Nächste Schritte

Nachdem Sie Ihren Load Balancer erstellt haben, möchten Sie möglicherweise Folgendes tun:

- Konfigurieren Sie die [Load Balancer-Attribute](#).
- Konfigurieren Sie [Zielgruppenattribute](#).
- [TLS-Listener] Fügen Sie der [optionalen Zertifikatsliste](#) Zertifikate hinzu.
- Konfigurieren Sie die [Überwachungsfunktionen](#).

Aktualisieren Sie die Availability Zones für Ihren Network Load Balancer

Sie können die Availability Zones für Ihren Network Load Balancer jederzeit aktivieren oder deaktivieren. Wenn Sie eine Availability Zone aktivieren, müssen Sie ein Subnetz aus dieser Availability Zone angeben. Nachdem Sie eine Availability Zone aktiviert haben, beginnt der Load Balancer, Anforderungen an die registrierten Ziele in der Availability Zone weiterzuleiten. Ihr Load Balancer ist am effektivsten, wenn Sie dafür sorgen, dass jede aktivierte Availability Zone mindestens ein registriertes Ziel hat. Die Aktivierung mehrerer Availability Zones trägt zur Verbesserung der Fehlertoleranz Ihrer Anwendungen bei.

Elastic Load Balancing erstellt einen Network Load Balancer Balancer-Knoten in der von Ihnen ausgewählten Availability Zone und eine Netzwerkschnittstelle für das ausgewählte Subnetz in dieser Availability Zone. Jeder Network Load Balancer Balancer-Knoten in der Availability Zone verwendet die Netzwerkschnittstelle, um eine IPv4 Adresse abzurufen. Sie können diese Netzwerkschnittstellen anzeigen, sie können jedoch nicht geändert werden.

Überlegungen

- Bei Network Load Balancers mit Internetzugriff müssen die von Ihnen angegebenen Subnetze über mindestens 8 verfügbare IP-Adressen verfügen. Für interne Network Load Balancer ist dies nur erforderlich, wenn Sie eine private IPv4 Adresse aus dem Subnetz AWS auswählen lassen.
- Sie können kein Subnetz in einer eingeschränkten Availability Zone angeben. Sie können jedoch ein Subnetz in einer Availability Zone ohne Einschränkungen angeben und den

zonenübergreifenden Lastenausgleich verwenden, um den Verkehr auf Ziele in der eingeschränkten Availability Zone zu verteilen.

- Sie können kein Subnetz in einer lokalen Zone angeben.
- Sie können ein Subnetz nicht entfernen, wenn der Network Load Balancer über aktive Amazon VPC-Endpunktzuordnungen verfügt.
- Wenn Sie ein zuvor entferntes Subnetz wieder hinzufügen, wird eine neue Netzwerkschnittstelle mit einer anderen ID erstellt.
- Subnetzänderungen innerhalb derselben Availability Zone müssen unabhängige Aktionen sein. Sie schließen zunächst das Entfernen des vorhandenen Subnetzes ab und können dann das neue Subnetz hinzufügen.
- Das Entfernen des Subnetzes kann bis zu 3 Minuten dauern.

Wenn Sie einen mit dem Internet verbundenen Network Load Balancer erstellen, können Sie wählen, ob Sie für jede Availability Zone eine Elastic IP-Adresse angeben möchten. Elastic IP-Adressen versorgen Ihren Network Load Balancer mit statischen IP-Adressen. Wenn Sie sich dafür entscheiden, keine Elastic IP-Adresse anzugeben, AWS wird jeder Availability Zone eine Elastic IP-Adresse zugewiesen.

Wenn Sie einen internen Network Load Balancer erstellen, können Sie wählen, ob Sie für jedes Subnetz eine private IP-Adresse angeben möchten. Private IP-Adressen stellen Ihrem Network Load Balancer statische IP-Adressen zur Verfügung. Wenn Sie keine private IP-Adresse angeben möchten, AWS weisen Sie Ihnen eine zu.

Bevor Sie die Availability Zones für Ihren Network Load Balancer aktualisieren, empfehlen wir Ihnen, mögliche Auswirkungen auf bestehende Verbindungen, Datenverkehrsflüsse oder Produktionsworkloads zu prüfen.

 Die Aktualisierung einer Availability Zone kann zu Störungen führen

- Wenn ein Subnetz entfernt wird, wird das zugehörige Elastic Network Interface (ENI) gelöscht. Dadurch werden alle aktiven Verbindungen in der Availability Zone beendet.
- Nachdem ein Subnetz entfernt wurde, werden alle Ziele innerhalb der Availability Zone, der es zugeordnet war, als unused markiert. Dies führt dazu, dass diese Ziele aus dem verfügbaren Zielpool entfernt werden und alle aktiven Verbindungen zu diesen Zielen beendet werden. Dies schließt alle Verbindungen ein, die aus anderen Availability Zones stammen, wenn zonenübergreifendes Load Balancing verwendet wird.

- Network Load Balancer haben für ihren vollqualifizierten Domainnamen (FQDN) eine Gültigkeitsdauer von 60 Sekunden. Wenn eine Availability Zone, die aktive Ziele enthält, entfernt wird, kann es bei bestehenden Client-Verbindungen zu Timeouts kommen, bis die DNS-Auflösung erneut erfolgt und der Datenverkehr in alle verbleibenden Availability Zones verlagert wird.

Console

Um die Availability Zones zu ändern

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.

AWS CLI

Um die Availability Zones zu ändern

Verwenden Sie den Befehl [set-subnets](#).

```
aws elbv2 set-subnets \  
  --load-balancer-arn load-balancer-arn \  
  --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890
```

CloudFormation

Um die Availability Zones zu ändern

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#)Ressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref new-subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Aktualisieren Sie die IP-Adresstypen für Ihren Network Load Balancer

Sie können Ihren Network Load Balancer so konfigurieren, dass Clients mit dem Network Load Balancer nur über IPv4 Adressen oder über beide IPv4 Adressen kommunizieren können (IPv6 Dualstack). Der Network 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-Adresstyp bei der Erstellung des Network Load Balancer festlegen und ihn jederzeit aktualisieren.
- Der Virtual Private Cloud (VPC) und den Subnetzen, die Sie für den Network Load Balancer angeben, müssen zugeordnete IPv6 CIDR-Blöcke haben. Weitere Informationen finden Sie unter [IPv6Adressen](#) im EC2 Amazon-Benutzerhandbuch.
- Die Routing-Tabellen für die Network Load Balancer Balancer-Subnetze müssen den Verkehr weiterleiten IPv6 .
- Das Netzwerk ACLs für die Network Load Balancer Balancer-Subnetze muss Datenverkehr zulassen IPv6 .
- An den Network Load Balancer sind keine QUIC- oder TCP_QUIC-Listener angeschlossen.

Console

Um den IP-Adresstyp zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Aktivieren Sie das Kontrollkästchen für den Network Load Balancer.
4. Klicken Sie auf Aktionen und anschließend auf IP-Adresstyp bearbeiten.
5. Wählen Sie für den IP-Adresstyp, ob IPv4 nur IPv4 Adressen unterstützt werden sollen oder Dualstack, um beide IPv4 Adressen zu unterstützen. IPv6
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um den IP-Adresstyp zu aktualisieren

Verwenden Sie den Befehl [set-ip-address-type](#).

```
aws elbv2 set-ip-address-type \  
  --load-balancer-arn load-balancer-arn \  
  --ip-address-type dualstack
```

CloudFormation

Um den IP-Adresstyp zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network  
      Scheme: internal  
      IpAddressType: dualstack  
      Subnets:  
        - !Ref subnet-AZ1  
        - !Ref subnet-AZ2  
      SecurityGroups:
```

- !Ref mySecurityGroup

Attribute für Ihren Network Load Balancer bearbeiten

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

Load Balancer-Attribute

- [Löschschutz](#)
- [Zonenübergreifendes Load Balancing](#)
- [DNS-Affinität der Availability Zone](#)
- [Sekundäre IP-Adressen](#)

Löschschutz

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

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

Console

Um den Löschschutz zu aktivieren oder 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 des Network Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren oder deaktivieren Sie unter Schutz den Löschschutz.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um den Löschschutz zu aktivieren oder zu deaktivieren

Verwenden Sie den Befehl [modify-load-balancer-attributes](#) mit dem Attribut `deletion_protection.enabled`.

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes "Key=deletion_protection.enabled,Value=true"
```

CloudFormation

Um den Löschschutz zu aktivieren oder zu deaktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource so, dass sie das `deletion_protection.enabled` Attribut enthält.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network  
      Scheme: internal  
      Subnets:  
        - !Ref subnet-AZ1  
        - !Ref subnet-AZ2  
      SecurityGroups:  
        - !Ref mySecurityGroup  
      LoadBalancerAttributes:  
        - Key: "deletion_protection.enabled"  
          Value: "true"
```

Zonenübergreifendes Load Balancing

Bei Network Load Balancers ist der zonenübergreifende Load Balancing auf Load-Balancer-Ebene standardmäßig deaktiviert, Sie können ihn jedoch jederzeit aktivieren. Für Zielgruppen wird standardmäßig die Load-Balancer-Einstellung verwendet. Sie können die Standardeinstellung jedoch überschreiben, indem Sie den zonenübergreifenden Load Balancing auf Zielgruppenebene explizit ein- oder ausschalten. Weitere Informationen finden Sie unter [the section called "Zonenübergreifendes Load Balancing"](#).

Console

Um den zonenübergreifenden Load Balancing für einen Load Balancer zu aktivieren oder zu deaktivieren

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, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren oder deaktivieren Sie auf der Seite Load Balancer-Attribute bearbeiten die Option Zonenübergreifendes Load Balancing.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um zonenübergreifendes Load Balancing für einen Load Balancer zu aktivieren oder zu deaktivieren

Verwenden Sie den Befehl [modify-load-balancer-attributes](#) mit dem Attribut `load_balancing.cross_zone.enabled`.

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

So aktivieren oder deaktivieren Sie den zonenübergreifenden Load Balancing für einen Load Balancer

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource so, dass sie das `load_balancing.cross_zone.enabled` Attribut enthält.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network  
      Scheme: internal
```

```
Subnets:
  - !Ref subnet-AZ1
  - !Ref subnet-AZ2
SecurityGroups:
  - !Ref mySecurityGroup
LoadBalancerAttributes:
  - Key: "load_balancing.cross_zone.enabled"
    Value: "true"
```

DNS-Affinität der Availability Zone

Wenn Sie die standardmäßige Client-Routing-Richtlinie verwenden, erhalten Anfragen, die an den DNS-Namen Ihres Network Load Balancers gesendet werden, alle fehlerfreien Network Load Balancer Balancer-IP-Adressen. Dies führt zur Verteilung der Client-Verbindungen auf die Availability Zones des Network Load Balancers. Mit den Availability Zone-Affinitätsrouting-Richtlinien bevorzugen Client-DNS-Abfragen IP-Adressen des Network Load Balancer in ihrer eigenen Availability Zone. Dies trägt dazu bei, sowohl die Latenz als auch die Ausfallsicherheit zu verbessern, da Clients beim Herstellen einer Verbindung zu Zielen keine Grenzen der Availability Zone überschreiten müssen.

Die Affinitätsrouting-Richtlinien für die Availability Zone gelten nur für Clients, die den DNS-Namen des Network Load Balancers mithilfe von Route 53 Resolver auflösen. Weitere Informationen finden Sie unter [Was ist Route 53 Resolver?](#) im Entwicklerhandbuch von Amazon Route 53.

Client-Routing-Richtlinien, die für Network Load Balancers verfügbar sind, die den Route-53-Resolver verwenden:

- Affinität zur Availability Zone – 100-prozentige zonale Affinität

Client-DNS-Abfragen bevorzugen die Network Load Balancer Balancer-IP-Adresse in ihrer eigenen Availability Zone. Abfragen können in andere Zonen weitergeleitet werden, wenn es in ihrer eigenen Zone keine fehlerfreien Network Load Balancer Balancer-IP-Adressen gibt.

- Teilweise Affinität zur Availability Zone – 85-prozentige zonale Affinität

85 Prozent der Client-DNS-Abfragen bevorzugen Network Load Balancer Balancer-IP-Adressen in ihrer eigenen Availability Zone, während die restlichen Abfragen in jede gesunde Zone aufgelöst werden. Abfragen können in andere fehlerfreie Zonen weitergeleitet werden, wenn es in deren Zone keine fehlerfreien IP-Adressen gibt. Wenn es in einer Zone keine fehlerfreien IP-Adressen gibt, werden Abfragen in einer beliebigen Zone aufgelöst.

- Beliebige Availability Zone (Standard) – 0-prozentige zonale Affinität

Client-DNS-Abfragen werden zwischen gesunden Network Load Balancer Balancer-IP-Adressen in allen Network Load Balancer Balancer-Verfügbarkeitszonen aufgelöst.

Die Availability Zone-Affinität hilft dabei, Anfragen vom Client an den Network Load Balancer weiterzuleiten, während zonenübergreifendes Load Balancing verwendet wird, um Anfragen vom Network Load Balancer an die Ziele weiterzuleiten. Bei Verwendung der Availability Zone-Affinität sollte der zonenübergreifende Load Balancing deaktiviert werden, um sicherzustellen, dass der Network Load Balancer Balancer-Verkehr von Clients zu Zielen innerhalb derselben Availability Zone bleibt. Bei dieser Konfiguration wird der Client-Verkehr an dieselbe Network Load Balancer Availability Zone gesendet. Es wird daher empfohlen, Ihre Anwendung so zu konfigurieren, dass sie in jeder Availability Zone unabhängig skaliert wird. Dies ist ein wichtiger Aspekt, wenn die Anzahl der Clients pro Availability Zone oder der Traffic pro Availability Zone nicht identisch sind. Weitere Informationen finden Sie unter [Zonenübergreifendes Load Balancing für Zielgruppen](#).

Wenn eine Availability Zone als fehlerhaft eingestuft wird oder wenn eine Zonenverschiebung gestartet wird, gilt die zonale IP-Adresse als fehlerhaft und wird nicht an die Clients zurückgegeben, es sei denn, Fail-Open ist aktiv. Die Affinität zur Availability Zone bleibt erhalten, wenn der DNS-Eintrag zu einem Fail-Open führt. Dies trägt dazu bei, dass Availability Zones unabhängig bleiben und potenzielle zonenübergreifende Ausfälle vermieden werden.

Bei Verwendung der Availability-Zone-Affinität ist mit Zeiten zu rechnen, in denen ein Ungleichgewicht zwischen den Availability Zones besteht. Es wird empfohlen, sicherzustellen, dass Ihre Ziele auf Zonenebene skaliert werden, um die einzelnen Availability-Zones-Workloads zu unterstützen. In Fällen, in denen diese Ungleichgewichte erheblich sind, wird empfohlen, die Availability-Zone-Affinität zu deaktivieren. Dies ermöglicht eine gleichmäßige Verteilung der Client-Verbindungen zwischen allen Availability Zones des Network Load Balancers innerhalb von 60 Sekunden oder der DNS-TTL.

Bevor Sie Availability-Zone-Affinität verwenden, sollten Sie Folgendes beachten:

- Die Availability-Zone-Affinität führt zu Änderungen bei allen Network-Load-Balancers-Clients, die Route 53 Resolver verwenden.
 - Clients können sich nicht zwischen zonenlokalen und zonenübergreifenden DNS-Auflösungen entscheiden. Die Availability-Zone-Affinität entscheidet für sie.
 - Den Clients steht keine zuverlässige Methode zur Verfügung, um festzustellen, wann sie von der Availability-Zone-Affinität betroffen sind oder wie sie herausfinden können, welche IP-Adresse sich in welcher Availability Zone befindet.

- Wenn die Availability Zone-Affinität mit Network Load Balancern und Route 53 Resolver verwendet wird, empfehlen wir Kunden, den Route 53 Resolver-Eingangsendpunkt in ihrer eigenen Availability Zone zu verwenden.
- Den Clients wird weiterhin ihre zonenlokale IP-Adresse zugewiesen, bis diese laut DNS-Zustandsprüfungen als vollständig fehlerhaft eingestuft und aus DNS entfernt wird.
- Die Verwendung der Availability-Zone-Affinität bei aktiviertem zonenübergreifenden Load Balancing kann zu einer unausgewogenen Verteilung der Client-Verbindungen zwischen den Availability Zones führen. Es wird empfohlen, Ihren Anwendungs-Stack so zu konfigurieren, dass er unabhängig in jeder Availability Zone skaliert, um sicherzustellen, dass er den Datenverkehr von zonalen Clients unterstützt.
- Wenn das zonenübergreifende Load Balancing aktiviert ist, ist der Network Load Balancer zonenübergreifenden Auswirkungen ausgesetzt.
- Die Auslastung der einzelnen Availability Zones des Network Load Balancers ist proportional zu den zonalen Standorten der Client-Anforderungen. Wenn Sie nicht konfigurieren, wie viele Clients in welcher Availability Zone ausgeführt werden, müssen Sie jede Availability Zone unabhängig voneinander reaktiv skalieren.

Überwachen

Es wird empfohlen, die Verteilung der Verbindungen zwischen Availability Zones mithilfe der zonalen Network Load Balancer Balancer-Metriken zu verfolgen. Sie können Metriken verwenden, um die Anzahl der neuen und aktiven Verbindungen pro Zone anzuzeigen.

Wir empfehlen, Folgendes zu verfolgen:

- **ActiveFlowCount** – Die Gesamtzahl der gleichzeitigen Flows (oder Verbindungen) von Clients zu Zielen.
- **NewFlowCount** – Die Gesamtanzahl neuer Flows (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden.
- **HealthyHostCount** – Die Anzahl der als fehlerfrei betrachteten Ziele.
- **UnHealthyHostCount** – Die Anzahl der als fehlerhaft betrachteten Ziele.

Weitere Informationen finden Sie unter [CloudWatch Metriken für Ihren Network Load Balancer](#).

Aktivieren Sie die Affinität zur Availability Zone

Console

Um die Availability Zone-Affinität 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 des Network Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie unter Konfiguration des Availability Zone-Routings, Client-Routing-Richtlinie (DNS-Eintrag) die Option Availability-Zone-Affinität oder Partial-Availability-Zone-Affinität aus.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Availability Zone-Affinität zu aktivieren

Verwenden Sie den Befehl [modify-load-balancer-attributes](#) mit dem Attribut `dns_record.client_routing_policy`.

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes  
  "Key=dns_record.client_routing_policy,Value=partial_availability_zone_affinity"
```

CloudFormation

Um die Availability Zone-Affinität zu aktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource so, dass sie das `dns_record.client_routing_policy` Attribut enthält.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network
```

```
Scheme: internal
Subnets:
  - !Ref subnet-AZ1
  - !Ref subnet-AZ2
SecurityGroups:
  - !Ref mySecurityGroup
LoadBalancerAttributes:
  - Key: "dns_record.client_routing_policy"
    Value: "partial_availability_zone_affinity"
```

Sekundäre IP-Adressen

Wenn [Fehler bei der Portzuweisung auftreten](#) und Sie der Zielgruppe keine Ziele hinzufügen können, um diese zu beheben, können Sie den Netzwerkschnittstellen des Load Balancers sekundäre IP-Adressen hinzufügen. Für jede Zone, in der der Load Balancer aktiviert ist, wählen wir IPv4 Adressen aus dem Load Balancer-Subnetz aus und weisen sie der entsprechenden Netzwerkschnittstelle zu. Diese sekundären IP-Adressen werden verwendet, um Verbindungen zu Zielen herzustellen. Sie werden auch für die Überprüfung des Datenverkehrs verwendet. Es wird empfohlen, zunächst eine sekundäre IP-Adresse hinzuzufügen, die `PortAllocationErrors` Metrik zu überwachen und nur dann eine weitere sekundäre IP-Adresse hinzuzufügen, wenn die Fehler bei der Portzuweisung nicht behoben wurden.

Warning

Nachdem Sie sekundäre IP-Adressen hinzugefügt haben, können Sie sie nicht mehr entfernen. Die einzige Möglichkeit, die sekundären IP-Adressen freizugeben, besteht darin, den Load Balancer zu löschen. Bevor Sie sekundäre IP-Adressen hinzufügen, stellen Sie sicher, dass in den Load Balancer-Subnetzen genügend IPv4 Adressen verfügbar sind.

Console

Um eine sekundäre IP-Adresse hinzuzufügen

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 des Network Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.

5. Erweitern Sie Spezialfallattribute, entsperren Sie die Option Sekundäre IP-Adressen, die auto pro Subnetzattribut zugewiesen werden, und wählen Sie die Anzahl der sekundären IP-Adressen aus.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um eine sekundäre IP-Adresse hinzuzufügen

Verwenden Sie den Befehl [modify-load-balancer-attributes](#) mit dem Attribut `secondary_ips.auto_assigned.per_subnet`.

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes "Key=secondary_ips.auto_assigned.per_subnet,Value=1"
```

Sie können den [describe-network-interfaces](#)Befehl verwenden, um die IPv4 Adressen für die Load Balancer-Netzwerkschnittstellen abzurufen. Der `--filters` Parameter beschränkt die Ergebnisse auf die Netzwerkschnittstellen für Network Load Balancer, und der `--query` Parameter beschränkt die Ergebnisse weiter auf den Load Balancer mit dem angegebenen Namen und zeigt nur die angegebenen Felder an. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws elbv2 describe-network-interfaces \  
  --filters "Name=interface-type,Values=network_load_balancer" \  
  --query "NetworkInterfaces[?contains(Description,'my-nlb')].  
{ID:NetworkInterfaceId,AZ:AvailabilityZone,Addresses:PrivateIpAddresses[*]}"
```

CloudFormation

Um eine sekundäre IP-Adresse hinzuzufügen

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#)Ressource so, dass sie das `secondary_ips.auto_assigned.per_subnet` Attribut enthält.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb
```

```
Type: network
Scheme: internal
Subnets:
  - !Ref subnet-AZ1
  - !Ref subnet-AZ2
SecurityGroups:
  - !Ref mySecurityGroup
LoadBalancerAttributes:
  - Key: "secondary_ips.auto_assigned.per_subnet"
    Value: "1"
```

Aktualisieren Sie die Sicherheitsgruppen für Ihren Network Load Balancer

Sie können Ihrem Network Load Balancer eine Sicherheitsgruppe zuordnen, um den Datenverkehr zu kontrollieren, der den Network Load Balancer erreichen und verlassen darf. Sie geben die Ports, Protokolle und Quellen an, die eingehenden Datenverkehr zulassen, und die Ports, Protokolle und Ziele, die ausgehenden Datenverkehr zulassen sollen. Wenn Sie Ihrem Network Load Balancer keine Sicherheitsgruppe zuweisen, kann der gesamte Client-Verkehr die Network Load Balancer-Listener erreichen und der gesamte Datenverkehr kann den Network Load Balancer verlassen.

Sie können den mit Ihren Zielen verknüpften Sicherheitsgruppen eine Regel hinzufügen, die auf die mit Ihrem Network Load Balancer verknüpfte Sicherheitsgruppe verweist. Auf diese Weise können Clients über Ihren Network Load Balancer Datenverkehr an Ihre Ziele senden, sie können jedoch keinen Datenverkehr direkt an Ihre Ziele senden. Wenn Sie in den mit Ihren Zielen verknüpften Sicherheitsgruppen auf die Ihrem Network Load Balancer zugeordnete Sicherheitsgruppe verweisen, wird sichergestellt, dass Ihre Ziele Datenverkehr von Ihrem Network Load Balancer akzeptieren, auch wenn Sie die [Client-IP-Erhaltung](#) für Ihren Network Load Balancer aktivieren.

Für Datenverkehr, der durch Sicherheitsgruppenregeln für eingehenden Datenverkehr blockiert wird, werden Ihnen keine Gebühren berechnet.

Inhalt

- [Überlegungen](#)
- [Beispiel: Filtern des Client-Datenverkehrs](#)
- [Beispiel: Nur Datenverkehr vom Network Load Balancer akzeptieren](#)
- [Aktualisieren der zugeordneten Sicherheitsgruppen](#)

- [Aktualisieren der Sicherheitseinstellungen](#)
- [Sicherheitsgruppen des Network Load Balancer überwachen](#)

Überlegungen

- Sie können Sicherheitsgruppen einem Network Load Balancer zuordnen, wenn Sie ihn erstellen. Wenn Sie einen Network Load Balancer erstellen, ohne Sicherheitsgruppen zuzuordnen, können Sie sie später nicht mehr mit dem Network Load Balancer verknüpfen. Wir empfehlen, dass Sie Ihrem Network Load Balancer bei der Erstellung eine Sicherheitsgruppe zuordnen.
- Nachdem Sie einen Network Load Balancer mit zugehörigen Sicherheitsgruppen erstellt haben, können Sie die mit dem Network Load Balancer verknüpften Sicherheitsgruppen jederzeit ändern.
- Zustandsprüfungen unterliegen Regeln für ausgehenden Datenverkehr, nicht jedoch für eingehenden. Sie müssen sicherstellen, dass Regeln für ausgehenden Datenverkehr den Zustandsprüfungsdatenverkehr nicht blockieren. Andernfalls betrachtet der Network Load Balancer die Ziele als fehlerhaft.
- Sie können steuern, ob der PrivateLink Datenverkehr Regeln für eingehenden Datenverkehr unterliegt. Wenn Sie Regeln für eingehenden PrivateLink Datenverkehr aktivieren, ist die Quelle des Datenverkehrs die private IP-Adresse des Clients, nicht die Endpunktschnittstelle.

Beispiel: Filtern des Client-Datenverkehrs

Die folgenden Regeln für eingehenden Datenverkehr in der Sicherheitsgruppe, die Ihrem Network Load Balancer zugeordnet ist, lassen nur Datenverkehr zu, der aus dem angegebenen Adressbereich stammt. Wenn es sich um einen internen Network Load Balancer handelt, können Sie einen VPC-CIDR-Bereich als Quelle angeben, um nur Datenverkehr von einer bestimmten VPC zuzulassen. Wenn es sich um einen mit dem Internet verbundenen Network Load Balancer handelt, der Datenverkehr von überall im Internet akzeptieren muss, können Sie 0.0.0.0/0 als Quelle angeben.

Eingehend

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
<i>protocol</i>	<i>client IP address range</i>	<i>listener port</i>	Erlaubt eingehenden Datenverkehr vom Quell-CIDR auf dem Listener-Port

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
ICMP	0.0.0.0/0	Alle	Erlaubt eingehendem ICMP-Datenverkehr die Unterstützung von MTU oder Path MTU Discovery †

† Weitere Informationen finden Sie unter [Path MTU Discovery](#) im EC2 Amazon-Benutzerhandbuch.

Ausgehend

Protocol (Protokoll)	Ziel	Port-Bereich	Comment
Alle	Überall	Alle	Erlaubt allen ausgehenden Datenverkehr

Beispiel: Nur Datenverkehr vom Network Load Balancer akzeptieren

Angenommen, Ihr Network Load Balancer hat eine Sicherheitsgruppe sg-111112222233333. Verwenden Sie die folgenden Regeln in den Sicherheitsgruppen, die Ihren Ziel-Instances zugeordnet sind, um sicherzustellen, dass sie nur Datenverkehr vom Network Load Balancer akzeptieren. Sie müssen sicherstellen, dass die Ziele Datenverkehr vom Network Load Balancer sowohl auf dem Zielport als auch auf dem Health Check-Port akzeptieren. Weitere Informationen finden Sie unter [the section called “Zielsicherheitsgruppen”](#).

Eingehend

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
<i>protocol</i>	sg-111112 222233333	<i>target port</i>	Lässt eingehenden Datenverkehr vom Network Load Balancer auf dem Zielport zu

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
<i>protocol</i>	sg-111112 222233333	<i>health check</i>	Lässt eingehenden Datenverkehr vom Network Load Balancer auf dem Health Check-Port zu

Ausgehend

Protocol (Protokoll)	Ziel	Port-Bereich	Comment
Alle	Überall	Beliebig	Erlaubt allen ausgehenden Datenverkehr

Aktualisieren der zugeordneten Sicherheitsgruppen

Wenn Sie bei der Erstellung mindestens eine Sicherheitsgruppe mit einem Network Load Balancer verknüpft haben, können Sie die Sicherheitsgruppen für diesen Network Load Balancer jederzeit aktualisieren.

Console

Um die Sicherheitsgruppen 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 Load Balancers aus.
3. Wählen Sie den Network Load Balancer aus.
4. Wählen Sie auf der Registerkarte Sicherheit die Option Bearbeiten aus.
5. Um Ihrem Network Load Balancer eine Sicherheitsgruppe zuzuordnen, wählen Sie sie aus.
Um eine Sicherheitsgruppe aus Ihrem Network Load Balancer zu entfernen, löschen Sie sie.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Sicherheitsgruppen zu aktualisieren

Verwenden Sie den Befehl [set-security-groups](#).

```
aws elbv2 set-security-groups \  
  --load-balancer-arn load-balancer-arn \  
  --security-groups sg-1234567890abcdef0 sg-0abcdef0123456789
```

CloudFormation

Um die Sicherheitsgruppen zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#)Ressource.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network  
      Scheme: internal  
      Subnets:  
        - !Ref subnet-AZ1  
        - !Ref subnet-AZ2  
      SecurityGroups:  
        - !Ref mySecurityGroup  
        - !Ref myNewSecurityGroup
```

Aktualisieren der Sicherheitseinstellungen

Standardmäßig wenden wir die Sicherheitsgruppenregeln für eingehenden Datenverkehr auf den gesamten Datenverkehr an, der an den Network Load Balancer gesendet wird. Möglicherweise möchten Sie diese Regeln jedoch nicht auf den Datenverkehr anwenden, der an den Network Load Balancer gesendet wird und der von überlappenden IP-Adressen stammen kann. AWS PrivateLink
In diesem Fall können Sie den Network Load Balancer so konfigurieren, dass wir die Regeln für eingehenden Datenverkehr, über den an den Network Load Balancer gesendet wird, nicht anwenden.
AWS PrivateLink

Console

Um die Sicherheitseinstellungen 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 Load Balancers aus.
3. Wählen Sie den Network Load Balancer aus.
4. Wählen Sie auf der Registerkarte Sicherheit die Option Bearbeiten aus.
5. Deaktivieren Sie unter Sicherheitseinstellungen die Option Regeln für eingehenden Datenverkehr durchsetzen. PrivateLink
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Sicherheitseinstellungen zu aktualisieren

Verwenden Sie den Befehl [set-security-groups](#).

```
aws elbv2 set-security-groups \  
  --load-balancer-arn load-balancer-arn \  
  --enforce-security-group-inbound-rules-on-private-link-traffic off
```

CloudFormation

Um die Sicherheitseinstellungen zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#)Ressource.

```
Resources:  
  myLoadBalancer:  
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
    Properties:  
      Name: my-nlb  
      Type: network  
      Scheme: internal  
      EnforceSecurityGroupInboundRulesOnPrivateLinkTraffic: off  
      Subnets:  
        - !Ref subnet-AZ1  
        - !Ref subnet-AZ2  
      SecurityGroups:  
        - !Ref mySecurityGroup
```

Sicherheitsgruppen des Network Load Balancer überwachen

Verwenden Sie die `SecurityGroupBlockedFlowCount_Outbound` CloudWatch Metriken `SecurityGroupBlockedFlowCount_Inbound` und, um die Anzahl der Datenflüsse zu überwachen, die von den Network Load Balancer Balancer-Sicherheitsgruppen blockiert werden. Blockierter Datenverkehr spiegelt sich nicht in anderen Metriken wider. Weitere Informationen finden Sie unter [the section called “CloudWatch Metriken”](#).

Verwenden Sie VPC-Flussprotokolle, um den Datenverkehr zu überwachen, der von den Network Load Balancer Balancer-Sicherheitsgruppen akzeptiert oder abgelehnt wird. Weitere Informationen finden Sie unter [VPC-Flow-Protokolle](#) im Amazon-VPC-Benutzerhandbuch.

Einen Network Load Balancer taggen

Mithilfe von Tags können Sie Ihre Network Load Balancer auf unterschiedliche Weise kategorisieren. Sie können Ressourcen beispielsweise nach Zweck, Inhaber oder Umgebung taggen.

Sie können jedem Network Load Balancer mehrere Tags hinzufügen. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der bereits mit dem Network Load Balancer verknüpft ist, wird der Wert dieses Tags aktualisiert.

Wenn Sie mit einem Tag fertig sind, können Sie es aus Ihrem Network 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 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.

Console

Um die Tags für einen Load Balancer zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Aktivieren Sie das Kontrollkästchen für den Network Load Balancer.
4. Wählen Sie auf der Registerkarte Tags die Option Manage tags (Tags verwalten).
5. Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann den Tagschlüssel und -Wert 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.
6. Um ein Tag zu aktualisieren, geben Sie neue Werte in das Feld Schlüssel oder Wert ein.
7. Um ein Tag zu löschen, wählen Sie Entfernen neben dem Tag.
8. Wählen Sie Änderungen speichern aus.

AWS CLI

So fügen Sie -Tags hinzu

Verwenden Sie den Befehl [add-tags](#). Im folgenden Beispiel werden zwei Tags hinzugefügt.

```
aws elbv2 add-tags \  
  --resource-arns load-balancer-arn \  
  --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

So entfernen Sie Tags

Verwenden Sie den Befehl [remove-tags](#). Im folgenden Beispiel werden die Tags mit den angegebenen Schlüsseln entfernt.

```
aws elbv2 remove-tags \  
  --resource-arns load-balancer-arn \  
  --tag-keys project department
```

CloudFormation

So fügen Sie -Tags hinzu

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource, die die Tags Eigenschaft einschließt.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'project'
          Value: 'Lima'
        - Key: 'department'
          Value: 'digital-media'
```

Löschen eines Network Load Balancers

Sobald Ihr Network Load Balancer verfügbar ist, wird Ihnen jede Stunde oder Teilstunde in Rechnung gestellt, in der Sie ihn am Laufen halten. Wenn Sie den Network Load Balancer nicht mehr benötigen, können Sie ihn löschen. Sobald der Network Load Balancer gelöscht ist, fallen keine Gebühren mehr für ihn an.

Sie können einen Network Load Balancer nicht löschen, wenn der Löschschutz aktiviert ist. Weitere Informationen finden Sie unter [Löschschutz](#).

Sie können einen Network Load Balancer nicht löschen, wenn er von einem anderen Dienst verwendet wird. Wenn der Network Load Balancer beispielsweise einem VPC-Endpunktdienst zugeordnet ist, müssen Sie die Endpunktdienstkonfiguration löschen, bevor Sie den zugehörigen Network Load Balancer löschen können.

Beim Löschen eines Network Load Balancer werden auch seine Listener gelöscht. Das Löschen eines Network Load Balancer hat keine Auswirkungen auf seine registrierten Ziele. Beispielsweise laufen Ihre EC2 Instances weiter und sind weiterhin für ihre Zielgruppen registriert. Informationen

zum Löschen Ihrer Zielgruppen finden Sie unter [Löschen Sie eine Zielgruppe für Ihren Network Load Balancer](#).

Console

So löschen Sie einen Network Load Balancer

1. Wenn Sie einen DNS-Eintrag für Ihre Domain haben, der auf Ihren Network Load Balancer verweist, verweisen Sie ihn auf einen neuen Standort und warten Sie, bis die DNS-Änderung wirksam wird, bevor Sie Ihren Network 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. Klicken Sie im Navigationsbereich auf Load Balancers.
4. Aktivieren Sie das Kontrollkästchen für den Network Load Balancer.
5. Wählen Sie den Load Balancer aus und klicken Sie auf Aktionen und dann auf Load Balancer löschen.
6. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **confirm** ein und wählen Sie Löschen aus.

AWS CLI

So löschen Sie einen Network Load Balancer

Verwenden Sie den Befehl [delete-load-balancer](#).

```
aws elbv2 delete-load-balancer \  
  --load-balancer-arn load-balancer-arn
```

Sehen Sie sich die Network Load Balancer Balancer-Ressourcenübersicht an

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

Um die Ressourcenübersicht für Ihren Load Balancer anzuzeigen

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 Network Load Balancer aus.
4. Wählen Sie die Registerkarte Ressourcenübersicht aus.

Komponenten der Ressourcenübersicht

Kartenansichten

In der Network Load Balancer Balancer-Ressourcenübersicht sind zwei Ansichten verfügbar: Overview und Unhealthy Target Map. Die Option „Übersicht“ ist standardmäßig ausgewählt und zeigt alle Ressourcen Ihres Network 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 zur Fehlerbehebung bei Zielen verwendet werden, bei denen die Zustandsprüfungen nicht bestanden haben. Weitere Informationen finden Sie unter [Beheben Sie Fehler bei fehlerhaften Zielen mithilfe der Ressourcenübersicht](#).

Ressourcenspalten

Die Network Load Balancer Balancer-Ressourcenübersicht enthält drei Ressourcenspalten, eine für jeden Ressourcentyp. Die Ressourcengruppen sind Listener, Zielgruppen und Ziele.

Ressourcenkacheln

Jede Ressource in einer Spalte hat ihre eigene Kachel, in 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.
 - Zusammenfassung des Zustands der Zielgruppe: Die Anzahl der registrierten Ziele für jeden Gesundheitsstatus.
 - Gesundheitsstatus der Zielperson: Der aktuelle Gesundheitsstatus und die Beschreibung der Zielperson.

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: TCP:80
 - 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 Network Load Balancers als PDF zu exportieren.

CloudWatch Logs für Ihren Network Load Balancer

Amazon CloudWatch Logs unterstützt Network Load Balancer Balancer-Zugriffsprotokolle als verkaufte Protokolle, wodurch die Beobachtbarkeit verbessert und das Debuggen von Netzwerkverkehrsmustern vereinfacht wird. Sie können die Network Load Balancer Balancer-Zugriffsprotokolle direkt analysieren, CloudWatch um Einblicke in die Client-Verbindungen, die Verkehrsverteilung und den Verbindungsstatus zu erhalten, sodass Sie Netzwerkprobleme schneller identifizieren und beheben können.

Sie können die Übermittlung von Network Load Balancer Balancer-Zugriffsprotokollen an Amazon CloudWatch Logs, Amazon Data Firehose und Amazon Simple Storage Service (Amazon S3) mit Unterstützung für das Apache Parquet-Format konfigurieren.

⚠ Important

Zugriffsprotokolle werden nur erstellt, wenn der Load Balancer über einen TLS-Listener verfügt, und die Protokolle enthalten nur Informationen über TLS-Anfragen. In den Zugriffsprotokollen werden Anfragen nach bestem Wissen und Gewissen aufgezeichnet. Wir empfehlen, dass Sie die Zugriffsprotokolle verwenden, um die Art der Anforderungen zu verstehen, nicht als eine vollständige Buchführung aller Anforderungen.

⚠ Important

Herkömmliche „ältere“ Zugriffsprotokolle bleiben für Network Load Balancer verfügbar. Um Konfigurationen für ältere Zugriffsprotokolle zu verwalten, besuchen Sie den Tab Attribute Ihres Load Balancers. Weitere Informationen zu „älteren“ Zugriffsprotokollen finden Sie unter [Zugriffsprotokolle für Ihren Network Load Balancer](#).

Mit dieser CloudWatch Logs-Integration können Sie mithilfe von CloudWatch Logs Insights-Abfragen detaillierte Zugriffsmuster verfolgen, Metrikfilter für die Überwachung erstellen und Verkehrsmuster mit Live Tail in Echtzeit überprüfen.

Sie können CloudWatch Logs for Network Load Balancer Balancer-Zugriffsprotokolle auf der Registerkarte Integrationen des Load Balancers in der Konsole aktivieren. Um die Protokollierung zu aktivieren, müssen Sie als Benutzer mit bestimmten Berechtigungen angemeldet sein. Darüber hinaus müssen Sie Berechtigungen erteilen, AWS um das Senden der Protokolle zu ermöglichen.

Informationen zu den erforderlichen Berechtigungen für jedes Protokollierungsziel finden Sie unter [Protokollierung von AWS Diensten aktivieren](#).

Weitere Informationen finden Sie unter [Was ist Amazon CloudWatch Logs?](#) .

Preisinformationen finden Sie unter [CloudWatch Amazon-Preise](#).

Zonenverschiebung für Ihren Network Load Balancer

Die Zonenverschiebung ist eine Funktion in Amazon Application Recovery Controller (ARC). Mit Zonal Shift können Sie eine Network Load Balancer Balancer-Ressource mit einer einzigen Aktion aus einer beeinträchtigten Availability Zone verlagern. Auf diese Weise können Sie den Betrieb von anderen fehlerfreien Availability Zones in einer AWS-Region fortsetzen.

Wenn Sie eine Zonenverschiebung starten, stoppt Ihr Network Load Balancer die Weiterleitung von Datenverkehr zu Zielen in der betroffenen Availability Zone. Bestehende Verbindungen zu Zielen in der betroffenen Availability Zone werden durch die Zonenverschiebung nicht beendet. Es kann mehrere Minuten dauern, bis diese Verbindungen ordnungsgemäß abgeschlossen sind.

Inhalt

- [Bevor Sie mit einer Zonenverschiebung beginnen](#)
- [Administrative Überschreibung von Zonenschichten](#)
- [Aktivieren Sie Zonal Shift für Ihren Network Load Balancer](#)
- [Starten Sie eine Zonenschicht für Ihren Network Load Balancer](#)
- [Aktualisieren Sie eine Zonenverschiebung für Ihren Network Load Balancer](#)
- [Stornieren Sie eine Zonenverschiebung für Ihren Network Load Balancer](#)

Bevor Sie mit einer Zonenverschiebung beginnen

- Zonal Shift ist standardmäßig deaktiviert und muss auf jedem Network Load Balancer aktiviert werden. Weitere Informationen finden Sie unter [Aktivieren Sie Zonal Shift für Ihren Network Load Balancer](#).
- Sie können eine Zonenverschiebung für einen bestimmten Network Load Balancer nur für eine einzelne Availability Zone starten. Eine Zonenverschiebung lässt sich nicht für mehrere Availability Zones starten.
- AWS entfernt proaktiv zonale IP-Adressen des Network Load Balancer aus DNS, wenn sich mehrere Infrastrukturprobleme auf Dienste auswirken. Prüfen Sie immer die aktuelle Kapazität der Availability Zone, bevor Sie mit einer Zonenverschiebung beginnen. Wenn Sie auf Ihrem Network Load Balancer eine Zonenverschiebung verwenden, verliert die Availability Zone, die von der Zonenverschiebung betroffen ist, ebenfalls an Zielkapazität.
- Bei einer zonalen Verschiebung auf Network Load Balancern mit aktiviertem zonenübergreifendem Load Balancing werden die IP-Adressen des zonalen Load Balancers aus DNS entfernt.

Bestehende Verbindungen zu Zielen in der beeinträchtigten Availability Zone bleiben bestehen, bis sie organisch geschlossen werden, während neue Verbindungen nicht mehr an Ziele in der beeinträchtigten Availability Zone weitergeleitet werden.

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

Administrative Überschreibung von Zonenschichten

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

Wenn eine Zonenverschiebung für einen Network Load Balancer gestartet wird, gelten alle Ziele innerhalb der Zone, von der aus sie verschoben werden, als administrativ außer Kraft gesetzt. Der Network Load Balancer beendet die Weiterleitung von neuem Datenverkehr an vom Administrator überschriebene Ziele. Bestehende Verbindungen bleiben intakt, bis sie organisch geschlossen werden.

Die möglichen `AdministrativeOverride` Zustände sind:

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

`zonal_shift_delegated_to_dns`

Der zonale Verschiebungsstatus dieses Ziels ist nicht verfügbar, kann aber direkt über die API oder Konsole eingesehen werden. `DescribeTargetHealth` AWS ARC - Zonal Shift

Aktivieren Sie Zonal Shift für Ihren Network Load Balancer

Zonal Shift ist standardmäßig deaktiviert und muss auf jedem Network Load Balancer aktiviert werden. Dadurch wird sichergestellt, dass Sie eine Zonenverschiebung starten können, indem Sie

nur die von Ihnen gewünschten Network Load Balancer verwenden. Weitere Informationen finden Sie unter [the section called “Zonale Verschiebung”](#).

Voraussetzungen

Wenn Sie zonenübergreifendes Load Balancing für den Load Balancer aktivieren, muss jede dem Load Balancer zugeordnete Zielgruppe die folgenden Anforderungen erfüllen, bevor Sie Zonal Shift aktivieren können.

- Das Zielgruppenprotokoll muss oder sein. TCP TLS
- Der Zielgruppentyp darf nicht sein alb.
- Der [Verbindungsabbruch für fehlerhafte Ziele](#) muss deaktiviert sein.
- Das `load_balancing.cross_zone.enabled` Zielgruppenattribut muss `true` oder sein `use_load_balancer_configuration` (Standard).

Console

Um Zonal Shift 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 Load Balancers aus.
3. Wählen Sie den Network Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie unter Availability Zone-Routing-Konfiguration für ARC Zonal Shift Integration die Option Enable aus.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um Zonal Shift zu aktivieren

Verwenden Sie den Befehl [modify-load-balancer-attributes](#) mit dem Attribut `zonal_shift.config.enabled`.

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes "Key=zonal_shift.config.enabled,Value=true"
```

CloudFormation

Um Zonal Shift zu aktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource so, dass sie das `zonal_shift.config.enabled` Attribut enthält.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        -Key: "zonal_shift.config.enabled"
          Value: "true"
```

Starten Sie eine Zonenschicht für Ihren Network Load Balancer

Die Zonenverschiebung in ARC ermöglicht es Ihnen, den Datenverkehr für unterstützte Ressourcen vorübergehend von einer Availability Zone weg zu verlagern, sodass Ihre Anwendung weiterhin normal mit anderen Availability Zones in einer Region arbeiten kann. AWS

Voraussetzung

Bevor Sie beginnen, stellen Sie sicher, dass Sie [Zonal Shift für den Load Balancer aktiviert](#) haben.

Console

In diesem Verfahren wird erklärt, wie Sie mit der EC2 Amazon-Konsole eine Zonenschicht starten. Schritte zum Starten einer Zonenschicht mithilfe der ARC-Konsole finden Sie unter [Starting a Zonal Shift](#) im Amazon Application Recovery Controller (ARC) Developer Guide.

So starten Sie eine Zonenschicht

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 Network Load Balancer aus.
4. Erweitern Sie auf der Registerkarte Integrationen den Amazon Application Recovery Controller (ARC) und wählen Sie Start Zonal Shift aus.
5. Wählen Sie die Availability Zone, von der Sie den Datenverkehr wegleiten möchten.
6. Wählen Sie ein Ablaufdatum für die Zonenverschiebung aus oder geben Sie es ein. Eine Zonenverschiebung kann zunächst auf eine Dauer von 1 Minute bis zu 3 Tagen (72 Stunden) festgelegt werden.

Alle Zonenverschiebungen sind temporär. Sie müssen ein Ablaufdatum festlegen, aber Sie können aktive Verschiebungen später aktualisieren, um ein neues Ablaufdatum festzulegen.

7. Geben Sie einen Kommentar ein. Sie können die Zonenverschiebung später aktualisieren, um den Kommentar zu bearbeiten.
8. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass der Start einer Zonenverschiebung die Kapazität Ihrer Anwendung reduziert, da der Datenverkehr von der Availability Zone weg verlagert wird.
9. Wählen Sie Bestätigen aus.

AWS CLI

Um eine Zonenschicht zu starten

Verwenden Sie den [start-zonal-shift](#) Befehl Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift start-zonal-shift \  
  --resource-identifier load-balancer-arn \  
  --away-from use2-az2 \  
  --expires-in 2h \  
  --comment "zonal shift due to scheduled maintenance"
```

Aktualisieren Sie eine Zonenverschiebung für Ihren Network Load Balancer

Sie können eine zonale Schicht aktualisieren, um ein neues Ablaufdatum festzulegen, oder den Kommentar für die zonale Schicht bearbeiten oder ersetzen.

Console

In diesem Verfahren wird erklärt, wie Sie eine Zonenschicht mithilfe der EC2 Amazon-Konsole aktualisieren. Schritte zum Aktualisieren einer zonalen Schicht mithilfe der Amazon Application Recovery Controller (ARC) -Konsole finden Sie unter [Aktualisieren einer zonalen Schicht](#) im Amazon Application Recovery Controller (ARC) Developer Guide.

So aktualisieren Sie eine Zonenschicht

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 einen Application Load Balancer mit einer aktiven Zonenverschiebung aus.
4. Erweitern Sie auf der Registerkarte Integrationen den Amazon Application Recovery Controller (ARC) und wählen Sie Update Zonal Shift aus.

Dadurch wird die ARC-Konsole geöffnet, um den Aktualisierungsvorgang fortzusetzen.

5. (Optional) Wählen Sie unter Ablauf der Zonenschicht festlegen eine Gültigkeitsdauer aus, oder geben Sie sie ein.
6. (Optional) Bearbeiten Sie unter Kommentar optional den vorhandenen Kommentar oder geben Sie einen neuen Kommentar ein.
7. Wählen Sie Aktualisieren aus.

AWS CLI

Um eine zonale Schicht zu aktualisieren

Verwenden Sie den [update-zonal-shift](#) Befehl Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift update-zonal-shift \  
  --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE \  
  --expires-in 1h \  
  --comment "extending zonal shift for scheduled maintenance"
```

Stornieren Sie eine Zonenverschiebung für Ihren Network Load Balancer

Sie können eine zonale Schicht jederzeit stornieren, bevor sie abläuft. Sie können Zonenverschiebungen, die Sie initiiert haben, oder Zonenverschiebungen, die für eine Ressource AWS beginnen, für einen Übungslauf für zonale automatische Verschiebung stornieren.

Console

In diesem Verfahren wird erklärt, wie Sie eine Zonenschicht mithilfe der EC2 Amazon-Konsole stornieren. Schritte zum Stornieren einer zonalen Schicht mithilfe der Amazon Application Recovery Controller (ARC) -Konsole finden Sie unter [Stornieren einer zonalen Schicht](#) im Amazon Application Recovery Controller (ARC) Developer Guide.

So stornieren Sie eine Zonenschicht

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 einen Network Load Balancer mit einer aktiven Zonenverschiebung aus.
4. Wählen Sie auf der Registerkarte Integrationen unter Amazon Application Recovery Controller (ARC) die Option Zonal Shift stornieren aus.

Dadurch wird die ARC-Konsole geöffnet, um den Kündigungsvorgang fortzusetzen.

5. Wählen Sie Zonenverschiebung abbrechen.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Confirm (Bestätigen).

AWS CLI

Um eine Zonenschicht abzurechnen

Verwenden Sie den [cancel-zonal-shift](#) Befehl Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift cancel-zonal-shift \  
  --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE
```

Kapazitätsreservierungen für Ihren Network Load Balancer

Mit Reservierungen für Load Balancer Capacity Unit (LCU) können Sie eine statische Mindestkapazität für Ihren Load Balancer reservieren. Network Load Balancer skalieren automatisch,

um erkannte Workloads zu unterstützen und den Kapazitätsbedarf zu decken. Wenn die Mindestkapazität konfiguriert ist, skaliert Ihr Load Balancer je nach empfangenem Datenverkehr weiter nach oben oder unten, verhindert aber auch, dass die Kapazität unter die konfigurierte Mindestkapazität fällt.

Erwägen Sie die Verwendung der LCU-Reservierung in 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 migrieren Workloads zwischen Load Balancern und möchten das Ziel so konfigurieren, dass es der Größe 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 anhand einer CloudWatch Metrik ProcessedBytes das richtige Kapazitätsniveau ermitteln. Die Kapazität für Ihren Load Balancer ist reserviert LCUs, wobei jede LCU 2,2 Mbit/s entspricht. Sie können die Max (ProcessedBytes) -Metrik verwenden, um den maximalen Datendurchsatz pro Minute auf dem Load Balancer zu ermitteln. Anschließend können Sie diesen Durchsatz so umrechnen, dass eine Konversionsrate von 2,2 LCUs Mbit/s einer LCU entspricht.

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](#).

Unterstützte Regionen

Diese Funktion ist nur in den folgenden Regionen verfügbar:

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (Stockholm)

Mindest- und Höchstwerte für eine LCU-Reservierung

Die gesamte Reservierungsanfrage muss mindestens 2.750 LCU pro Availability Zone betragen. Der Höchstwert wird durch die Kontingente für Ihr Konto bestimmt. Weitere Informationen finden Sie unter [the section called "Load Balancer Balancer-Kapazitätseinheiten"](#).

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

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

- Die LCU-Reservierung wird auf Network Load Balancern, die TLS-Listener verwenden, nicht unterstützt.
- Die LCU-Reservierung unterstützt nur die Reservierung von Durchsatzkapazität für Network Load Balancer. Wenn Sie eine LCU-Reservierung beantragen, rechnen Sie Ihren Kapazitätsbedarf von Mbit/s auf LCUs die Umrechnungsrate von 1 LCU auf 2,2 Mbit/s um.
- Die Kapazität wird auf regionaler Ebene reserviert und gleichmäßig auf die Verfügbarkeitszonen 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 einer Stunde 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.

Console

Um eine LCU-Reservierung anzufordern

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 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.

AWS CLI

Um eine LCU-Reservierung anzufordern

Verwenden Sie den Befehl [modify-capacity-reservation](#).

```
aws elbv2 modify-capacity-reservation \  
  --load-balancer-arn load-balancer-arn \  
  --minimum-load-balancer-capacity CapacityUnits=3000
```

CloudFormation

Um eine LCU-Reservierung anzufordern

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#)Ressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-alb
      Type: application
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      MinimumLoadBalancerCapacity:
        CapacityUnits: 3000
```

Load Balancer Capacity Unit-Reservierungen für Ihren Network Load Balancer aktualisieren oder stornieren

Wenn sich die Verkehrsmuster für Ihren Load Balancer ändern, können Sie die LCU-Reservierung für Ihren Load Balancer aktualisieren oder stornieren.

Console

Um eine LCU-Reservierung zu aktualisieren oder zu stornieren

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. Führen Sie auf der Registerkarte Kapazität einen der folgenden Schritte aus:
 - a. Um die LCU-Reservierung zu aktualisieren, wählen Sie LCU-Reservierung bearbeiten.
 - b. Um die LCU-Reservierung zu stornieren, wählen Sie Kapazität stornieren.

AWS CLI

Um eine LCU-Reservierung zu stornieren

Verwenden Sie den Befehl [modify-capacity-reservation](#).

```
aws elbv2 modify-capacity-reservation \  
  --load-balancer-arn load-balancer-arn \  
  --reset-capacity-reservation
```

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

Status der Reservierung

Im Folgenden sind die möglichen Statuswerte für eine LCU-Reservierung aufgeführt:

- **pending-** Zeigt an, dass die Reservierung gerade bereitgestellt wird.
- **provisioned-** Zeigt an, dass die reservierte Kapazität bereit und nutzbar ist.
- **failed-** Zeigt an, dass die Anfrage derzeit nicht abgeschlossen werden kann.
- **rebalancing-** Zeigt an, dass eine Availability Zone hinzugefügt oder entfernt wurde und der Load Balancer die Kapazität neu verteilt.

LCU-Auslastung

Um die reservierte LCU-Auslastung zu ermitteln, können Sie die Metrik pro Minute mit der ProcessedBytes Metrik pro Stunde vergleichen. $\text{Sum(ReservedLCUs)} \times (\text{Byte pro Minute}) \times 8/60 / (10^6) / 2.2$, um Byte pro Minute in LCU pro Stunde umzurechnen.

Console

Um den Status einer LCU-Reservierung einzusehen

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.

AWS CLI

Um den Status einer LCU-Reservierung zu überwachen

Verwenden Sie den Befehl [describe-capacity-reservation](#).

```
aws elbv2 describe-capacity-reservation \  
  --load-balancer-arn load-balancer-arn
```

Listener für Ihre Network Load Balancers

Ein Listener ist ein Prozess, der mit dem Protokoll und dem Port, das bzw. den Sie konfigurieren, Verbindungsanforderungen prüft. Bevor Sie Ihren Network 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 Regel, die Sie für einen Listener definieren, bestimmt, wie der Load Balancer Anforderungen an die Ziele weiterleitet, die Sie registrieren, z. B. EC2-Instances.

Inhalt

- [Listener-Konfiguration](#)
- [Standardaktionen](#)
- [Listener-Attribute](#)
- [Sichere Zuhörer](#)
- [ALPN-Richtlinien](#)
- [Erstellen Sie einen Listener für Ihren Network Load Balancer.](#)
- [Serverzertifikate für Ihren Network Load Balancer](#)
- [Sicherheitsrichtlinien für Ihren Network Load Balancer](#)
- [Aktualisieren eines Listeners für Ihren Network Load Balancer.](#)
- [Aktualisieren Sie das TCP-Leerlauf-Timeout für Ihren Network Load Balancer Balancer-Listener](#)
- [Aktualisieren eines TLS-Listeners für Ihren Network Load Balancer](#)
- [Löschen eines TLS-Listeners für Ihren Network Load Balancer](#)

Listener-Konfiguration

Listener unterstützen die folgenden Protokolle und Ports:

- Protokolle: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- Ports: 1-65535

Mit einem TLS-Listener können Sie die Ver- und Entschlüsselung auf Ihren Load Balancer auslagern, damit sich Ihre Anwendungen auf die Geschäftslogik konzentrieren können. Wenn das Listener-

Protokoll TLS ist, müssen Sie mindestens ein SSL-Serverzertifikat auf dem Listener bereitstellen. Weitere Informationen finden Sie unter [Serverzertifikate](#).

Wenn Sie sicherstellen müssen, dass die Ziele den TLS-Datenverkehr anstelle des Load Balancers entschlüsseln, können Sie einen TCP-Listener auf Port 443 erstellen, anstatt einen TLS-Listener zu erstellen. Bei einem TCP-Listener leitet der Load Balancer verschlüsselten Datenverkehr an die Ziele weiter, ohne ihn zu entschlüsseln.

Sie können einen QUIC-Listener verwenden, um QUIC-Verkehr zu akzeptieren. [Der Network Load Balancer fungiert als Pass-Through-Load Balancer gemäß RFC9000](#). Verwenden Sie einen QUIC-Listener und QUIC-fähige Backends, um eine nahtlose Verbindungsmigration für mobile Geräte zu ermöglichen.

Erstellen Sie zur Unterstützung von TCP und UDP auf demselben Port einen TCP_UDP-Listener. Die Zielgruppen für einen TCP_UDP-Listener müssen das TCP_UDP-Protokoll verwenden.

Um sowohl TCP als auch QUIC auf demselben Port zu unterstützen, erstellen Sie einen TCP_QUIC-Listener. Die Zielgruppen für einen TCP_QUIC-Listener müssen das TCP_QUIC-Protokoll verwenden.

Ein UDP-Listener für einen Dual-Stack-Load Balancer benötigt IPv6-Zielgruppen.

WebSockets wird nur auf TCP-, TLS-, TCP_UDP- und TCP_QUIC-Listnern unterstützt.

QUIC-Verkehr unterstützt keine Versionsaushandlung. QUIC v1 ist die einzige unterstützte QUIC-Version.

Der gesamte an einen konfigurierten Listener gesendete Netzwerkdatenverkehr wird als beabsichtigter Datenverkehr klassifiziert. Netzwerkdatenverkehr, der keinem konfigurierten Listener entspricht, wird als unbeabsichtigter Datenverkehr klassifiziert. Andere ICMP-Anfragen als Typ 3 gelten ebenfalls als unbeabsichtigter Datenverkehr. Network Load Balancers lassen unbeabsichtigten Datenverkehr fallen, ohne ihn an Ziele weiterzuleiten. TCP-Datenpakete, die an den Listener-Port für konfigurierte Listener gesendet werden, bei denen es sich nicht um neue Verbindungen oder Teile einer aktiven TCP-Verbindung handelt, werden mit einer TCP-Zurücksetzung (Reset, RST) abgewiesen.

Weitere Informationen finden Sie unter [Weiterleitung von Anforderungen](#) im Benutzerhandbuch zu Elastic Load Balancing.

Standardaktionen

Wenn Sie einen Listener erstellen, geben Sie eine Standardaktion für das Routing von Anfragen an. Die Standardaktion leitet Anfragen an die von Ihnen angegebenen Zielgruppen weiter.

Verteilen Sie den Traffic auf mehrere Zielgruppen

Wenn Sie mehrere Zielgruppen für eine Standardaktion angeben, werden Anfragen auf der Grundlage ihrer relativen Gewichtung an diese Zielgruppen verteilt. Sie müssen für jede Zielgruppe eine Gewichtung zwischen 0 und 999 angeben. Eine Zielgruppe mit einer Gewichtung von 0 erhält keinen Traffic. Nachdem Sie eine Zielgruppe hinzugefügt oder die Zielgruppengewichte aktualisiert haben, werden neue Verbindungen auf der Grundlage der neuen Zielgruppengewichte weitergeleitet. Bestehende Verbindungen sind davon nicht betroffen und bestehen, bis sie wie gewohnt geschlossen werden.

Wenn Sie beispielsweise zwei Zielgruppen mit einer Gewichtung von jeweils 10 angeben, erhält jede Zielgruppe die Hälfte der Anfragen. Wenn Sie zwei Zielgruppen angeben, eine mit einer Gewichtung von 10 und die andere mit einer Gewichtung von 20, erhält die Zielgruppe mit einer Gewichtung von 20 doppelt so viele Anfragen wie die Zielgruppe mit einer Gewichtung von 10.

Ein häufiger Anwendungsfall ist die Migration von Traffic von einer Zielgruppe zur anderen. Das bedeutet, dass Sie das Gewicht der neuen Zielgruppe schrittweise erhöhen und gleichzeitig das Gewicht der ursprünglichen Zielgruppe verringern, bis es 0 ist. Wenn Sie die Gewichtung einer Zielgruppe nach kurzer Zeit auf 0 aktualisieren, erhält sie keine neuen Verbindungen und bestehende Verbindungen werden geschlossen.

Wichtige Sessions und gewichtete Zielgruppen

Mit Weiterleitungsaktionen für Zuhörer können Sie festlegen, ob die Zielgruppenbindung aktiviert werden soll. Wenn diese Option aktiviert ist, führt die Zielgruppenbindung dazu, dass nachfolgende Verbindungen von derselben Quell-IP-Adresse aus die zuvor gewählte Zielgruppe bevorzugen.

Überlegungen

- Bei TLS-Listnern können Sie der Listener-Regel nicht sowohl TCP-Zielgruppen als auch TLS-Zielgruppen hinzufügen. Alle Zielgruppen müssen dasselbe Protokoll verwenden.
- Für TLS-Listener wird die Zielgruppenbindung nicht unterstützt.
- Bei Dualstack-Loadbalancern können Sie derselben Standardaktion nicht sowohl IPv4-Zielgruppen als auch IPv6-Zielgruppen hinzufügen. Alle Zielgruppen in der Standardaktion müssen denselben IP-Adresstyp verwenden.

- Für Zuhörer gilt: Wenn eine Weiterleitungsaktion mehrere Zielgruppen enthält und für eine von ihnen die Option „Klebrigkeit“ aktiviert ist, muss für die Weiterleitungsaktion auch die Zielgruppen-Klebrigkeit aktiviert sein.

Listener-Attribute

Im Folgenden sind die Listener-Attribute für Network Load Balancer aufgeführt:

`tcp.idle_timeout.seconds`

Der TCP-Leerlauf-Timeout-Wert in Sekunden. Der gültige Bereich liegt zwischen 60 und 6000 Sekunden. Die Standardeinstellung ist 350 Sekunden.

Weitere Informationen finden Sie unter [Aktualisieren Sie das Leerlauf-Timeout](#).

Sichere Zuhörer

Um einen TLS-Listener zu verwenden, müssen Sie auf dem Load Balancer mindestens ein Serverzertifikat 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. Beachten Sie, dass Sie, wenn Sie verschlüsselten Datenverkehr an die Ziele weiterleiten müssen, ohne dass der Load Balancer ihn entschlüsselt, einen TCP-Listener auf Port 443 erstellen, anstatt einen TLS-Listener zu erstellen. Der Load Balancer leitet die Anforderung unverändert an das Ziel weiter, ohne sie zu entschlüsseln.

Elastic Load Balancing verwendet eine TLS-Aushandlungskonfiguration, die als Sicherheitsrichtlinie bezeichnet wird, um TLS-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. Eine Chiffre ist ein Verschlüsselungsalgorithmus, der Verschlüsselungsschlüssel verwendet, um eine codierte Nachricht zu erstellen. Protokolle verwenden mehrere Chiffren, um Daten über das Internet zu verschlüsseln. Während der Verbindungsaushandlung präsentieren der Client und der Load Balancer eine Liste von Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Als sichere Verbindung wird die erste Verschlüsselung auf der Liste des Servers ausgewählt, die mit einem der Verschlüsselungsverfahren des Clients übereinstimmt.

Network Load Balancer unterstützen keine gegenseitige TLS-Authentifizierung (mTLS). Für mTLS-Unterstützung erstellen Sie einen TCP-Listener anstelle eines TLS-Listeners. Der Load Balancer leitet die Anforderung unverändert weiter, sodass Sie mTLS auf dem Ziel implementieren können.

Network Load Balancer unterstützen die TLS-Wiederaufnahme mit PSK für TLS 1.3 und Sitzungstickets für TLS 1.2 und älter. Wiederaufnahmen mit Sitzungs-ID oder wenn mehrere Zertifikate im Listener mithilfe von SNI konfiguriert sind, werden nicht unterstützt. Die 0-RTT-Datenfunktion und die Erweiterung `early_data` sind nicht implementiert.

Verwandte Demos finden Sie unter [TLS-Unterstützung für Network Load Balancer](#) und [SNI-Unterstützung für Network Load Balancer](#).

ALPN-Richtlinien

Application-Layer Protocol Negotiation (ALPN) ist eine TLS-Erweiterung, die bei den ersten TLS-Handshake-Hello-Nachrichten gesendet wird. ALPN ermöglicht es der Anwendungsebene, auszuhandeln, welche Protokolle über eine sichere Verbindung verwendet werden sollen, z. B. und HTTP/1 HTTP/2

Wenn der Client eine ALPN-Verbindung initiiert, vergleicht der Load Balancer die ALPN-Einstellungsliste des Clients mit der ALPN-Richtlinie. Wenn der Client ein Protokoll aus der ALPN-Richtlinie unterstützt, stellt der Load Balancer die Verbindung basierend auf der Einstellungsliste der ALPN-Richtlinie her. Andernfalls verwendet der Load Balancer ALPN nicht.

Unterstützte ALPN-Richtlinien

Im Folgenden werden die unterstützten ALPN-Richtlinien aufgeführt:

HTTP1only

Nur verhandeln HTTP/1 .* . Die ALPN-Einstellungsliste lautet `http/1 .1`, `http/1 .0`.

HTTP2only

Nur verhandeln. HTTP/2 Die ALPN-Einstellungsliste lautet `h2`.

HTTP2optional

Bevorzugen Sie HTTP/1 .* gegenüber HTTP/2 (was zum HTTP/2 Testen nützlich sein kann). Die ALPN-Einstellungsliste lautet `http/1 .1`, `http/1 .0`, `h2`.

HTTP2Preferred

Lieber HTTP/2 als *. HTTP/1 Die ALPN-Einstellungsliste lautet h2, http/1 .1, http/1 .0.

None

ALPN nicht aushandeln. Dies ist die Standardeinstellung.

ALPN-Verbindungen aktivieren

Sie können ALPN-Verbindungen aktivieren, wenn Sie einen TLS-Listener erstellen oder ändern. Weitere Informationen erhalten Sie unter [Hinzufügen eines Listeners](#) und [Aktualisieren der ALPN-Richtlinie](#).

Erstellen Sie einen Listener für Ihren Network Load Balancer.

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Sie definieren einen Listener, wenn Sie Ihren Load Balancer erstellen, und Sie können Listener jederzeit zu Ihrem Load Balancer hinzufügen.

Voraussetzungen

- Sie müssen eine Zielgruppe für die Standardaktion angeben. Weitere Informationen finden Sie unter [Erstellen einer Zielgruppe für Ihren Network Load Balancer](#).
- Sie müssen ein SSL-Zertifikat für einen TLS-Listener angeben. Der Load Balancer verwendet ein Zertifikat, um die Verbindung zu beenden und Anforderungen von Clients zu entschlüsseln, bevor er sie an Ziele weiterleitet. Weitere Informationen finden Sie unter [Serverzertifikate für Ihren Network Load Balancer](#).
- Sie können keine IPv4-Zielgruppe mit einem UDP-Listener für einen dualstack Load Balancer verwenden.
- QUIC- und TCP_QUIC-Listener sind auf Load Balancern oder dualstack Load Balancern mit zugehörigen Sicherheitsgruppen nicht zulässig.
- QUIC- und TCP_QUIC-Listener sind auf Load Balancern mit zugehörigen Sicherheitsgruppen nicht zulässig.
- Auf einem Network Load Balancer ist jeweils nur ein QUIC- oder TCP_QUIC-Listener zulässig.
- QUIC- und TCP_QUIC-Listener sind auf einem Network Load Balancer, der über UDP- oder TCP_UDP-Listener verfügt, nicht zulässig.

Hinzufügen eines 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](#).

Console

So fügen Sie einen Listener hinzu

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listeners Option Listener hinzufügen aus.
5. Wählen Sie als Protokoll TCP, UDP, TCP_UDP, TLS, QUIC oder TCP_QUIC aus. Übernehmen Sie den Standardport oder geben Sie einen anderen Port ein.
6. Wählen Sie unter Standardaktion eine Zielgruppe aus, an die der Datenverkehr weitergeleitet werden soll.

Um eine weitere Zielgruppe hinzuzufügen, wählen Sie Zielgruppe hinzufügen und aktualisieren Sie die Gewichtungen nach Bedarf.

Wenn Sie keine Zielgruppe haben, die Ihren Bedürfnissen entspricht, wählen Sie Zielgruppe erstellen, um jetzt eine zu erstellen. Weitere Informationen finden Sie unter [Erstellen einer Zielgruppe](#).

7. [TLS-Listener] Wir empfehlen Ihnen, für Sicherheitsrichtlinie die Standardsicherheitsrichtlinie beizubehalten.
8. [TLS-Listener] Wählen Sie für SSL/TLS Standardserverzertifikat das Standardzertifikat aus. 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 Datei mit dem privaten Schlüssel () PEM-encoded

und fügen Sie ihn ein. Kopieren Sie für Certificate Body den Inhalt der Zertifikatsdatei mit dem öffentlichen Schlüssel (PEM-encoded) und fügen Sie ihn ein. Kopieren Sie für Certificate Chain den Inhalt der Zertifikatskettendatei (PEM-encoded) und fügen Sie ihn ein, es sei denn, Sie verwenden ein selbstsigniertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.

9. [TLS-Listener] Wählen Sie für die ALPN-Richtlinie eine Richtlinie aus, um ALPN zu aktivieren, oder wählen Sie None (Keine), um ALPN zu deaktivieren. Weitere Informationen finden Sie unter [ALPN-Richtlinien](#).
10. (Optional) Um Tags hinzuzufügen, erweitern Sie Listener-Tags. Wählen Sie Neues Tag hinzufügen und geben Sie den Tag-Schlüssel und den Tag-Wert ein.
11. Wählen Sie Hinzufügen aus.
12. [TLS-Listener] Informationen zum Hinzufügen von Zertifikaten zur Liste der optionalen Zertifikate finden Sie unter [Hinzufügen von Zertifikaten zu einer Zertifikatliste](#).

AWS CLI

Erstellen einer Zielgruppe

Wenn Sie keine Zielgruppe haben, die Sie für die Standardaktion verwenden können, verwenden Sie jetzt den Befehl [create-target-group](#), um eine zu erstellen. Beispiele finden Sie unter [Erstellen einer Zielgruppe](#).

Um einen TCP-Listener hinzuzufügen

Verwenden Sie den Befehl [create-listener](#) und geben Sie das TCP-Protokoll an.

```
aws elbv2 create-listener \  
  --load-balancer-arn load-balancer-arn \  
  --protocol TCP \  
  --port 80 \  
  --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Um einen TCP-Listener mit mehreren Zielgruppen hinzuzufügen

Verwenden Sie den Befehl [create-listener](#) und geben Sie das TCP-Protokoll, die Zielgruppen und die Gewichte an.

```
aws elbv2 create-listener \  
  --load-balancer-arn load-balancer-arn \  
  --protocol TCP \  
  --port 80 \  
  --default-actions Type=forward,TargetGroupArns=[target-group-arn,target-group-arn],Weights=[1,1]
```

```

--protocol TCP \
--port 80 \
--default-actions '[{
  "Type":"forward",
  "ForwardConfig":{
    "TargetGroups":[
      {"TargetGroupArn":"target-group-1-arn","Weight":10},
      {"TargetGroupArn":"target-group-2-arn","Weight":30}
    ]
  }
}]'
```

Um einen TLS-Listener hinzuzufügen

Verwenden Sie den Befehl [create-listener](#), der das TLS-Protokoll angibt.

```

aws elbv2 create-listener \
  --load-balancer-arn load-balancer-arn \
  --protocol TLS \
  --port 443 \
  --certificates CertificateArn=certificate-arn \
  --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06 \
  --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Um einen UDP-Listener hinzuzufügen

Verwenden Sie den Befehl [create-listener](#), der das UDP-Protokoll angibt.

```

aws elbv2 create-listener \
  --load-balancer-arn load-balancer-arn \
  --protocol UDP \
  --port 53 \
  --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Um einen QUIC-Listener hinzuzufügen

Verwenden Sie den Befehl [create-listener](#), der das QUIC-Protokoll angibt.

```

aws elbv2 create-listener \
  --load-balancer-arn load-balancer-arn \
  --protocol QUIC \
  --port 443 \
```

```
--default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Um einen TCP-Listener hinzuzufügen

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::Listener](#) mithilfe des TCP-Protokolls.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Um einen TCP-Listener mit mehreren Zielgruppen hinzuzufügen

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::Listener](#) mithilfe des TCP-Protokolls.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          ForwardConfig:
            TargetGroups:
              - TargetGroupArn: !Ref myTargetGroup1,
                Weight: 10
              - TargetGroupArn: !Ref myTargetGroup2,
                Weight: 30
            TargetGroupStickinessConfig:
              Enabled: true
```

Um einen TLS-Listener hinzuzufügen

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::Listener](#) mithilfe des TLS-Protokolls.

```
Resources:
  myTLSTListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Um einen UDP-Listener hinzuzufügen

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::Listener](#) mithilfe des UDP-Protokolls.

```
Resources:
  myUDPLListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: UDP
      Port: 53
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Um einen QUIC-Listener hinzuzufügen

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::Listener](#) mithilfe des QUIC-Protokolls.

```
Resources:
  myQUICListener:
```

```
Type: 'AWS::ElasticLoadBalancingV2::Listener'  
Properties:  
  LoadBalancerArn: !Ref myLoadBalancer  
  Protocol: QUIC  
  Port: 443  
  DefaultActions:  
    - Type: forward  
      TargetGroupArn: !Ref myTargetGroup
```

Serverzertifikate für Ihren Network Load Balancer

Wenn Sie einen sicheren Listener für Ihren Network Load Balancer erstellen, müssen Sie mindestens ein Zertifikat auf dem Load Balancer bereitstellen. Der Load Balancer benötigt X.509 Zertifikate (Serverzertifikat). 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 zum Anfordern öffentlicher Zertifikate finden Sie unter [Anfordern eines öffentlichen Zertifikats](#) im AWS Certificate Manager -Benutzerhandbuch.

Wir empfehlen, Zertifikate für Ihre Load Balancers mit [AWS Certificate Manager \(ACM\)](#) zu erstellen. 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 TLS-Tools verwenden, um eine 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 IAM hochladen. Weitere Informationen finden Sie unter [Importieren von Zertifikaten](#) im AWS Certificate Manager -Benutzerhandbuch oder [Arbeiten mit Serverzertifikaten](#) im IAM-Benutzerhandbuch.

Unterstützte Schlüsselalgorithmen

- RSA 1024-Bit
- RSA 2048-Bit
- RSA 3072-Bit
- ECDSA 256-Bit
- ECDSA 384 Bit
- ECDSA 521-Bit

Wichtig — Verhalten bei der Verwendung von Zertifikaten IAM-imported

Wenn Sie ein Zertifikat in AWS Identity and Access Management (IAM) importieren und es an einen NLB-TLS-Listener anhängen, werden die Schlüsselgröße und der Algorithmus des Zertifikats zum Zeitpunkt des Anhangs nicht validiert. Die Validierung erfolgt asynchron, nachdem das Zertifikat dem Listener zugeordnet wurde. Wenn das Zertifikat eine nicht unterstützte Schlüsselgröße verwendet (z. B. RSA 4096-Bit), wechselt der Listener in einen nicht funktionierenden Zustand und Sie erhalten eine Benachrichtigung über AWS das Personal Health Dashboard (PHD).

Beachten Sie, dass, wenn Ihr Listener zuvor ein funktionierendes Zertifikat konfiguriert hat, der Datenverkehr möglicherweise weiterhin über dieses Zertifikat bedient wird, während das nicht unterstützte Zertifikat abgelehnt wird. Die PHD-Benachrichtigung gibt an, dass der Listener mit einem nicht unterstützten Zertifikat konfiguriert ist, bestätigt jedoch nicht, ob der Datenverkehr noch über ein früheres Zertifikat bedient wird.

Um dies zu vermeiden, überprüfen Sie die Schlüsselgröße Ihres Zertifikats, bevor Sie es in IAM importieren. Bei RSA-Zertifikaten beträgt die maximal unterstützte Schlüsselgröße für NLB-TLS-Listener 3072-Bit.

Wenn Sie AWS Certificate Manager (ACM) zum Bereitstellen oder Importieren von Zertifikaten verwenden, werden nicht unterstützte Schlüsselgrößen zum Zeitpunkt des Anhangs zurückgewiesen, sodass Sie sofort Feedback erhalten.

Standardzertifikat

Wenn Sie einen TLS-Listener erstellen, müssen Sie mindestens ein Zertifikat angeben. Dieses Zertifikat wird als Standardzertifikat bezeichnet. Sie können das Standardzertifikat ersetzen, nachdem Sie den TLS-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

Nach der Erstellung eines TLS-Listeners verfügt dieser über ein Standardzertifikat und eine leere Zertifikatliste. Optional können Sie der Zertifikatliste für den Listener Zertifikate hinzufügen. 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)
- Hash-Algorithmus (SHA gegenüber MD5 bevorzugt)
- 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 Network Load Balancer

Wenn Sie einen TLS-Listener erstellen, müssen Sie eine Sicherheitsrichtlinie auswählen. Eine Sicherheitsrichtlinie legt fest, welche Verschlüsselungen und Protokolle bei SSL-Verhandlungen zwischen Ihrem Load Balancer und den Clients unterstützt werden. Sie können die Sicherheitsrichtlinie für Ihren Load Balancer aktualisieren, falls sich Ihre Anforderungen ändern oder wenn wir eine neue Sicherheitsrichtlinie veröffentlichen. Weitere Informationen finden Sie unter [Aktualisieren der Sicherheitsrichtlinie](#).

Überlegungen

- Ein TLS-Listener erfordert eine Sicherheitsrichtlinie. Wenn Sie bei der Erstellung des Listeners keine Sicherheitsrichtlinie angeben, verwenden wir die Standard-Sicherheitsrichtlinie. Die Standardsicherheitsrichtlinie hängt davon ab, wie Sie den TLS-Listener erstellt haben:
 - Konsole — Die Standard-Sicherheitsrichtlinie lautet `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09`.
 - Andere Methoden (z. B. die AWS CLI, AWS CloudFormation, und die AWS CDK) — Die Standard-Sicherheitsrichtlinie ist `ELBSecurityPolicy-2016-08`.
- Sicherheitsrichtlinien, deren Namen PQ enthalten, bieten einen hybriden Schlüsselaustausch nach dem Quantum-Verfahren. Aus Kompatibilitätsgründen unterstützen sie sowohl klassische Algorithmen als auch Algorithmen für den ML-KEM Schlüsselaustausch nach dem Quantenaustausch. Kunden müssen den ML-KEM Schlüsselaustausch unterstützen, um hybrides Post-Quantum-TLS für den Schlüsselaustausch verwenden zu können. Die hybriden Post-Quantum-Richtlinien unterstützen die Algorithmen SECP256R1MLKEM768, SECP384R1MLKEM1024 und X25519MLKEM768. Weitere Informationen [Post-quantum finden Sie unter Kryptografie](#).
- AWS empfiehlt die Implementierung der neuen Post-Quantum-Sicherheitsrichtlinie auf Basis von TLS (PQ-TLS) `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09` oder `ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09`. Diese Richtlinie gewährleistet die Abwärtskompatibilität, indem sie Kunden unterstützt, die in der Lage sind PQ-TLS, hybride Lösungen, nur TLS 1.3 oder nur TLS 1.2 auszuhandeln, wodurch Serviceunterbrechungen beim Übergang zur Post-Quanten-Kryptografie minimiert werden. Sie können schrittweise auf restriktivere Sicherheitsrichtlinien umsteigen, wenn Ihre Client-Anwendungen die Fähigkeit entwickeln, Schlüsselaustauschvorgänge auszuhandeln PQ-TLS .
- Sie können Zugriffsprotokolle für Informationen über die an Ihren Network Load Balancer gesendeten TLS-Anfragen aktivieren, TLS-Datenverkehrsmuster analysieren, Sicherheitsrichtlinien-Upgrades verwalten und Probleme beheben. Aktivieren Sie die Zugriffsprotokollierung für Ihren Load Balancer und überprüfen Sie die entsprechenden Zugriffsprotokolleinträge. Weitere Informationen finden Sie unter [Zugriffsprotokolle](#) und [Network Load Balancer Balancer-Beispielabfragen](#).
- Um die TLS-Protokollversion (Protokollfeldposition 5) und den Schlüsselaustausch (Protokollfeldposition 13) für Zugriffsanforderungen an Ihren Load Balancer anzuzeigen, aktivieren Sie die Zugriffsprotokollierung und überprüfen Sie die entsprechenden Protokolleinträge. Weitere Informationen finden Sie unter [Zugriffsprotokolle](#).

- 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 Policies (SCPs) verwenden. Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien \(SCPs\)](#) 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.
- Network Load Balancers unterstützen die Erweiterung Extended Master Secret (EMS) für TLS 1.2.

Backend-Verbindungen

Sie können die Sicherheitsrichtlinie wählen, die für Front-End-Verbindungen verwendet wird, aber nicht für Back-End-Verbindungen. Die Sicherheitsrichtlinie für Backend-Verbindungen hängt von der Sicherheitsrichtlinie des Listeners ab. Wenn einer Ihrer Zuhörer Folgendes verwendet:

- FIPS-Post-Quantum-TLS-Richtlinie — Verwendung von Backend-Verbindungen `ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09`
- FIPS-Richtlinie — Verwendung von Backend-Verbindungen `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`
- Post-quantum TLS-Richtlinie — Verwendung von Backend-Verbindungen `ELBSecurityPolicy-TLS13-1-0-PQ-2025-09`
- TLS 1.3-Richtlinie — Verwendung von Backend-Verbindungen `ELBSecurityPolicy-TLS13-1-0-2021-06`
- Alle anderen TLS-Richtlinien, die Backend-Verbindungen verwenden `ELBSecurityPolicy-2016-08`

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

Sicherheitsrichtlinien

- [TLS-Sicherheitsrichtlinien](#)
 - [Protokolle nach Richtlinie](#)
 - [Verschlüsselungen nach Richtlinien](#)
 - [Richtlinien nach Chiffre](#)

- [FIPS-Sicherheitsrichtlinien](#)
 - [Protokolle nach Richtlinien](#)
 - [Verschlüsselungen nach Richtlinien](#)
 - [Richtlinien nach Chiffre](#)
- [FS unterstützte Sicherheitsrichtlinien](#)
 - [Protokolle nach Richtlinie](#)
 - [Verschlüsselungen nach Richtlinien](#)
 - [Richtlinien nach Chiffre](#)

TLS-Sicherheitsrichtlinien

Sie können die TLS-Sicherheitsrichtlinien verwenden, um Compliance- 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](#)
- [Verschlüsselungen 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
ELBSecurityPolicy-TLS13-1-3-2021-06	Ja	Nein	Nein	Nein
ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	Ja	Nein	Nein	Nein

Sicherheitsrichtlinien	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-2-2021-06	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Res-2021-06	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-1-2021-06	Ja	Ja	Ja	Nein
ELBSecurityPolicy-TLS13-1-0-2021-06	Ja	Ja	Ja	Ja
ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	Ja	Ja	Ja	Ja
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	Nein	Ja	Nein	Nein
ELBSecurityPolicy-TLS-1-2-2017-01	Nein	Ja	Nein	Nein
ELBSecurityPolicy-TLS-1-1-2017-01	Nein	Ja	Ja	Nein
ELBSecurityPolicy-2016-08	Nein	Ja	Ja	Ja
ELBSecurityPolicy-2015-05	Nein	Ja	Ja	Ja

Verschlüsselungen nach Richtlinien

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

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-3-2021-06	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256
ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	<ul style="list-style-type: none"> • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256
ELBSecurityPolicy-TLS13-1-2-2021-06	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	<ul style="list-style-type: none"> • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-2021-06	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	<ul style="list-style-type: none"> • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	<ul style="list-style-type: none"> • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256

Sicherheitsrichtlinie	Verschlüsselungen
	<ul style="list-style-type: none">• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES128-SHA• ECDHE-RSA-AES128-SHA• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES256-SHA384• ECDHE-RSA-AES256-SHA384• ECDHE-ECDSA-AES256-SHA• ECDHE-RSA-AES256-SHA• AES128-GCM-SHA256• AES128-SHA256• AES128-SHA• AES256-GCM-SHA384• AES256-SHA256• AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06	• TLS_AES_128_GCM_SHA256
ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-	• TLS_AES_256_GCM_SHA384
2025-09	• TLS_CHACHA20_POLY1305_SHA256
	• ECDHE-ECDSA-AES128-GCM-SHA256
	• ECDHE-RSA-AES128-GCM-SHA256
	• ECDHE-ECDSA-AES128-SHA256
	• ECDHE-RSA-AES128-SHA256
	• ECDHE-ECDSA-AES256-GCM-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
ELBSecurityPolicy-TLS13-1-1-2021-06	<ul style="list-style-type: none">• TLS_AES_128_GCM_SHA256• TLS_AES_256_GCM_SHA384• TLS_CHACHA20_POLY1305_SHA256• ECDHE-ECDSA-AES128-GCM-SHA256• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES128-SHA256• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES128-SHA• ECDHE-RSA-AES128-SHA• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES256-SHA384• ECDHE-RSA-AES256-SHA384• ECDHE-ECDSA-AES256-SHA• ECDHE-RSA-AES256-SHA• AES128-GCM-SHA256• AES128-SHA256• AES128-SHA• AES256-GCM-SHA384• AES256-SHA256• AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-0-2021-06	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256
ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	<ul style="list-style-type: none"> • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	<ul style="list-style-type: none">• ECDHE-ECDSA-AES128-GCM-SHA256• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES128-SHA256• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES128-SHA• ECDHE-RSA-AES128-SHA• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES256-SHA384• ECDHE-RSA-AES256-SHA384• ECDHE-ECDSA-AES256-SHA• ECDHE-RSA-AES256-SHA• AES128-GCM-SHA256• AES128-SHA256• AES128-SHA• AES256-GCM-SHA384• AES256-SHA256• AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS-1-2-2017-01	<ul style="list-style-type: none">• ECDHE-ECDSA-AES128-GCM-SHA256• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES128-SHA256• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES256-GCM-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
ELBSecurityPolicy-TLS-1-1-2017-01	<ul style="list-style-type: none">• ECDHE-ECDSA-AES128-GCM-SHA256• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES128-SHA256• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES128-SHA• ECDHE-RSA-AES128-SHA• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES256-SHA384• ECDHE-RSA-AES256-SHA384• ECDHE-ECDSA-AES256-SHA• ECDHE-RSA-AES256-SHA• AES128-GCM-SHA256• AES128-SHA256• AES128-SHA• AES256-GCM-SHA384• AES256-SHA256• AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-2016-08	<ul style="list-style-type: none">• ECDHE-ECDSA-AES128-GCM-SHA256• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES128-SHA256• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES128-SHA• ECDHE-RSA-AES128-SHA• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES256-SHA384• ECDHE-RSA-AES256-SHA384• ECDHE-ECDSA-AES256-SHA• ECDHE-RSA-AES256-SHA• AES128-GCM-SHA256• AES128-SHA256• AES128-SHA• AES256-GCM-SHA384• AES256-SHA256• AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-2015-05	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

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	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-2021-06 	1301

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
IANA — TLS_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — TLS_AES_256_GCM_SHA384 IANA — TLS_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 	1302

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — TLS_CHACHA20_POLY1305_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-2021-06 	1303
IANA — TLS_CHACHA20_POLY1305_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c02b

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 	c02f
IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c023

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c027

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c009
OpenSSL — ECDHE-RSA-AES128-SHA IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c013

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c02c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 	c030
IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c024

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c028

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	c014

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES128-GCM-SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	9 c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES128-SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	3c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES128-SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none">• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06• ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09• ELBSecurityPolicy-TLS13-1-1-2021-06• ELBSecurityPolicy-TLS13-1-0-2021-06• ELBSecurityPolicy-TLS13-1-0-PQ-2025-09• ELBSecurityPolicy-TLS-1-2-Ext-2018-06• ELBSecurityPolicy-TLS-1-1-2017-01• ELBSecurityPolicy-2016-08	2f

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES256-GCM-SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	9 d

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES256-SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	3d

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES256-SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 	35
IANA — TLS_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08 	

FIPS-Sicherheitsrichtlinien

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 AWS-LC FIPS-validierte kryptografische Modul. 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 FIPS140-Modul, entsprechen aber möglicherweise nicht den neuesten NIST-Richtlinien für die TLS-Konfiguration.

Inhalt

- [Protokolle nach Richtlinien](#)
- [Verschlüsselungen nach Richtlinien](#)
- [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
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	Ja	Nein	Nein	Nein
ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09	Ja	Nein	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04	Ja	Ja	Nein	Nein

Sicherheitsrichtlinien	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09	Ja	Ja	Nein	Nein
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	Ja	Ja	Ja	Nein
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	Ja	Ja	Ja	Ja
ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	Ja	Ja	Ja	Ja

Verschlüsselungen nach Richtlinien

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

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09	
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09	
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
<p>ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04</p> <p>ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09</p>	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256
<p>ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04</p> <p>ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09</p>	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	<ul style="list-style-type: none">• TLS_AES_128_GCM_SHA256• TLS_AES_256_GCM_SHA384• ECDHE-ECDSA-AES128-GCM-SHA256• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES128-SHA256• ECDHE-RSA-AES128-SHA256• ECDHE-ECDSA-AES128-SHA• ECDHE-RSA-AES128-SHA• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES256-SHA384• ECDHE-RSA-AES256-SHA384• ECDHE-RSA-AES256-SHA• ECDHE-ECDSA-AES256-SHA• AES128-GCM-SHA256• AES128-SHA256• AES128-SHA• AES256-GCM-SHA384• AES256-SHA256• AES256-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

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	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 	1301
IANA — TLS_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — TLS_AES_256_GCM_SHA384 IANA — TLS_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 	1302

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	
<p>OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256</p> <p>IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</p>	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c02b

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c02f

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 	c023

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c027

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c009
OpenSSL — ECDHE-RSA-AES128-SHA IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c013

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 	c02c
IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c030

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES256-SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 	c024
IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c028

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 	c014

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES128-GCM-SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	9 c
OpenSSL — AES128-SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	3c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES128-SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	2f
OpenSSL — AES256-GCM-SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	9 d

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — AES256-SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	3d
OpenSSL — AES256-SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 	35

FS unterstützte Sicherheitsrichtlinien

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, stellen auch FS bereit.

Inhalt

- [Protokolle nach Richtlinie](#)
- [Verschlüsselungen 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
ELBSecurityPolicy-FS-1-2-Res-2020-10	Nein	Ja	Nein	Nein
ELBSecurityPolicy-FS-1-2-Res-2019-08	Nein	Ja	Nein	Nein
ELBSecurityPolicy-FS-1-2-2019-08	Nein	Ja	Nein	Nein
ELBSecurityPolicy-FS-1-1-2019-08	Nein	Ja	Ja	Nein
ELBSecurityPolicy-FS-2018-06	Nein	Ja	Ja	Ja

Verschlüsselungen nach Richtlinien

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

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolicy-FS-1-2-Res-2020-10	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-FS-1-2-Res-2019-08	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-FS-1-2-2019-08	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA
ELBSecurityPolicy-FS-1-1-2019-08	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256

Sicherheitsrichtlinie	Verschlüsselungen
	<ul style="list-style-type: none"> • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA
ELBSecurityPolicy-FS-2018-06	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

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-AES128-GCM-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c02b
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c02f
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c023
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c027
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 	c009

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-2018-06 	
OpenSSL — ECDHE-RSA-AES128-SHA IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c013
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c02c
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c030
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	c024

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES256-SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-Res-2019-08 	c028
IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06 	
OpenSSL — ECDHE-ECDSA-AES256-SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 	c00a
IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-2018-06 	
OpenSSL — ECDHE-RSA-AES256-SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 	c014
IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> • ELBSecurityPolicy-FS-2018-06 	

Aktualisieren eines Listeners für Ihren Network Load Balancer.

Sie können das Listener-Protokoll, den Listener-Port oder die Zielgruppe aktualisieren, die Datenverkehr von der Weiterleitungsaktion empfängt. Die Standardaktion, auch Standardregel genannt, leitet Anfragen an die ausgewählte Zielgruppe weiter.

Wenn Sie das Protokoll von TCP, UDP oder QUIC auf TLS ändern, müssen Sie eine Sicherheitsrichtlinie und ein Serverzertifikat angeben. Wenn Sie das Protokoll von TLS auf TCP, UDP oder QUIC ändern, werden die Sicherheitsrichtlinie und das Serverzertifikat entfernt.

Wenn die Zielgruppe für die Standardaktion eines TCP-, TLS- oder QUIC-Listeners aktualisiert wird, werden neue Verbindungen an die neu konfigurierte Zielgruppe weitergeleitet. Dies hat jedoch keine Auswirkungen auf aktive Verbindungen, die vor dieser Änderung erstellt wurden. Diese aktiven Verbindungen bleiben bis zu einer Stunde mit dem Ziel in der ursprünglichen Zielgruppe verknüpft, wenn Datenverkehr gesendet wird, oder bis zu dem Zeitpunkt, an dem das Leerlauf-Timeout abläuft,


```
--default-actions Type=forward,TargetGroupArn=new-target-group-arn
```

Das folgende Beispiel aktualisiert einen Listener mit mehreren Zielgruppen.

```
aws elbv2 modify-listener \
  --listener-arn listener-arn \
  --default-actions '[{
    "Type":"forward",
    "ForwardConfig":{
      "TargetGroups":[
        {"TargetGroupArn":"target-group-1-arn","Weight":10},
        {"TargetGroupArn":"target-group-2-arn","Weight":30}
      ]
    }
  }]'
```

So fügen Sie -Tags hinzu

Verwenden Sie den Befehl [add-tags](#). Im folgenden Beispiel werden zwei Tags hinzugefügt.

```
aws elbv2 add-tags \
  --resource-arns listener-arn \
  --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

So entfernen Sie Tags

Verwenden Sie den Befehl [remove-tags](#). Im folgenden Beispiel werden die Tags mit den angegebenen Schlüsseln entfernt.

```
aws elbv2 remove-tags \
  --resource-arns listener-arn \
  --tag-keys project department
```

CloudFormation

Um die Standardaktion zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::Listener-Ressource](#), sodass sie die neue Zielgruppe einschließt.

```
Resources:
```

```

myTCPListener:
  Type: 'AWS::ElasticLoadBalancingV2::Listener'
  Properties:
    LoadBalancerArn: !Ref myLoadBalancer
    Protocol: TCP
    Port: 80
    DefaultActions:
      - Type: forward
        TargetGroupArn: !Ref newTargetGroup

```

Um den Traffic auf mehrere Zielgruppen zu verteilen, definieren Sie alternativ DefaultActions wie folgt.

```

DefaultActions:
  - Type: forward
  ForwardConfig:
    TargetGroups:
      - TargetGroupArn: !Ref TargetGroup1
        Weight: 10
      - TargetGroupArn: !Ref TargetGroup2
        Weight: 30

```

So fügen Sie -Tags hinzu

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::Listener-Ressource](#) so, dass sie die Eigenschaft Tags enthält.

```

Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'

```

Aktualisieren Sie das TCP-Leerlauf-Timeout für Ihren Network Load Balancer Listener

Für jede TCP-Anfrage, die über einen Network Load Balancer gestellt wird, wird der Status dieser Verbindung verfolgt. Werden länger als die vorgegebene Leerlaufzeit weder vom Client noch vom Ziel Daten über die Verbindung gesendet, wird die Verbindung beendet.

Überlegungen

- Der Standardwert für das Leerlauf-Timeout für TCP-Datenflüsse beträgt 350 Sekunden.
- Das Timeout bei Verbindungsinaktivität für TLS-Listener beträgt 350 Sekunden und kann nicht geändert werden.

Console

Um das TCP-Leerlauf-Timeout zu aktualisieren

1. Öffnen Sie die Amazon-EC2-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 Network Load Balancer.
4. Aktivieren Sie auf der Registerkarte Listener das Kontrollkästchen für den TCP-Listener und wählen Sie dann Aktionen, Listener-Details anzeigen aus.
5. Wählen Sie auf der Listener-Detailseite auf der Registerkarte Attribute die Option Bearbeiten aus. Wenn der Listener ein anderes Protokoll als TCP verwendet, ist diese Registerkarte nicht vorhanden.
6. Geben Sie einen Wert für das TCP-Leerlauf-Timeout zwischen 60 und 6000 Sekunden ein.
7. Wählen Sie Änderungen speichern aus.

AWS CLI

Um das TCP-Leerlauf-Timeout zu aktualisieren

Verwenden Sie den Befehl [modify-listener-attributes](#) mit dem Attribut `tcp.idle_timeout.seconds`

```
aws elbv2 modify-listener-attributes \  
  --listener-arn listener-arn \  
  --tcp-idle-timeout-seconds seconds
```

```
--attributes Key=tcp.idle_timeout.seconds,Value=500
```

Es folgt eine Beispielausgabe.

```
{
  "Attributes": [
    {
      "Key": "tcp.idle_timeout.seconds",
      "Value": "500"
    }
  ]
}
```

CloudFormation

Um das TCP-Leerlauf-Timeout zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::Listener-Ressource](#) so, dass sie das [tcp.idle_timeout.seconds Listener-Attribut](#) enthält.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      ListenerAttributes:
        - Key: "tcp.idle_timeout.seconds"
          Value: "500"
```

Aktualisieren eines TLS-Listeners für Ihren Network Load Balancer

Nachdem Sie einen TLS-Listener erstellt haben, können Sie das Standardzertifikat ersetzen, Zertifikate aus der Zertifikatliste hinzufügen oder entfernen, die Sicherheitsrichtlinie aktualisieren oder die ALPN-Richtlinie aktualisieren.

Aufgaben


```
--certificates CertificateArn=new-default-certificate-arn
```

CloudFormation

Um das Standardzertifikat zu ersetzen

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::Listener-Ressource](#) mit dem neuen Standardzertifikat.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "new-default-certificate-arn"
```

Hinzufügen von Zertifikaten zu einer Zertifikatliste

Sie können der Zertifikatliste für den Listener mit den folgenden Schritten Zertifikate hinzufügen. Wenn Sie zum ersten Mal einen TLS-Listener erstellen, ist die Zertifikatliste leer. Sie können das Standardzertifikat zur Zertifikatsliste hinzufügen, um sicherzustellen, dass dieses Zertifikat mit dem SNI-Protokoll verwendet wird, auch wenn es als Standardzertifikat ersetzt wird. Weitere Informationen finden Sie unter [Zertifikatliste](#).

Console

Um Zertifikate zur Zertifikatsliste hinzuzufügen

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listener den Text in der Protocol:PortSpalte aus, um die Detailseite für den Listener zu öffnen.

5. Wählen Sie die Registerkarte Certificates (Zertifikate) aus.
6. Um das Standardzertifikat zur Liste hinzuzufügen, wählen Sie Standard zur Liste hinzufügen aus.
7. Gehen Sie wie folgt vor, um der Liste nicht standardmäßige Zertifikate hinzuzufügen:
 - a. Wählen Sie Zertifikat hinzufügen aus.
 - b. Um Zertifikate hinzuzufügen, die bereits von ACM oder IAM verwaltet werden, wählen Sie die Kontrollkästchen für die Zertifikate und dann die Option Schließen Sie die unten angeführten als ausstehend ein aus.
 - c. Um ein Zertifikat hinzuzufügen, das nicht von ACM oder IAM verwaltet wird, wählen Sie Zertifikat importieren, füllen Sie das Formular aus und wählen Sie Importieren.
 - d. Wählen Sie Ausstehende Zertifikate hinzufügen aus.

AWS CLI

Um Zertifikate zur Zertifikatsliste hinzuzufügen

Verwenden Sie den Befehl [add-listener-certificates](#).

```
aws elbv2 add-listener-certificates \  
  --listener-arn listener-arn \  
  --certificates \  
    CertificateArn=certificate-arn-1 \  
    CertificateArn=certificate-arn-2 \  
    CertificateArn=certificate-arn-3
```

CloudFormation

Um Zertifikate zur Zertifikatsliste hinzuzufügen

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::ListenerCertificate](#).

```
Resources:  
  myCertificateList:  
    Type: 'AWS::ElasticLoadBalancingV2::ListenerCertificate'  
    Properties:  
      ListenerArn: !Ref myTLSEListener  
      Certificates:  
        - CertificateArn: "certificate-arn-1"  
        - CertificateArn: "certificate-arn-2"
```

```
- CertificateArn: "certificate-arn-3"

myTLSTListener:
  Type: AWS::ElasticLoadBalancingV2::Listener
  Properties:
    LoadBalancerArn: !Ref myLoadBalancer
    Protocol: TLSS
    Port: 443
    SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
    Certificates:
      - CertificateArn: "certificate-arn-1"
    DefaultActions:
      - Type: forward
        TargetGroupArn: !Ref myTargetGroup
```

Entfernen eines Zertifikats aus der Zertifikatliste

Sie können mit den folgenden Schritten Zertifikate aus der Zertifikatliste für einen TLS-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](#).

Console

Um Zertifikate aus der Zertifikatsliste zu entfernen

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listener den Text in der Protocol:PortSpalte 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.

AWS CLI

Um Zertifikate aus der Zertifikatsliste zu entfernen

Verwenden Sie den Befehl [remove-listener-certificates](#).

```
aws elbv2 remove-listener-certificates \  
  --listener-arn listener-arn \  
  --certificates CertificateArn=certificate-arn
```

Aktualisieren der Sicherheitsrichtlinie

Wenn Sie einen TLS-Listener erstellen, können Sie die Sicherheitsrichtlinie auswählen, die Ihre Anforderungen erfüllt. Wenn eine neue Sicherheitsrichtlinie hinzugefügt wird, können Sie Ihren TLS-Listener aktualisieren, sodass die neue Sicherheitsrichtlinie verwendet wird. Network Load Balancers unterstützen keine benutzerdefinierten Sicherheitsrichtlinien. Weitere Informationen finden Sie unter [Sicherheitsrichtlinien für Ihren Network Load Balancer](#).

Die Aktualisierung der Sicherheitsrichtlinie kann zu Störungen führen, wenn der Load Balancer ein hohes Datenverkehrsvolumen 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.

Console

Um die Sicherheitsrichtlinie zu aktualisieren

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listener den Text in der Protocol:PortSpalte aus, um die Detailseite für den Listener zu öffnen.
5. Wählen Sie Aktionen, Listener bearbeiten.
6. Wählen Sie im Abschnitt Sichere Listener-Einstellungen unter Sicherheitsrichtlinie eine neue Sicherheitsrichtlinie aus.
7. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Sicherheitsrichtlinie zu aktualisieren

Verwenden Sie den Befehl [modify-listener](#).

```
aws elbv2 modify-listener \  
  --listener-arn listener-arn \  
  --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06
```

CloudFormation

Um die Sicherheitsrichtlinie zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::Listener-Ressource](#) mit der neuen Sicherheitsrichtlinie.

```
Resources:  
  myTLSTListener:  
    Type: 'AWS::ElasticLoadBalancingV2::Listener'  
    Properties:  
      LoadBalancerArn: !Ref myLoadBalancer  
      Protocol: TLS  
      Port: 443  
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"  
      Certificates:  
        - CertificateArn: "default-certificate-arn"  
      DefaultActions:  
        - Type: forward  
          TargetGroupArn: !Ref myTargetGroup
```

Aktualisieren der ALPN-Richtlinie

Sie können die ALPN-Richtlinie für Ihren TLS-Listener nach Bedarf aktualisieren. Weitere Informationen finden Sie unter [ALPN-Richtlinien](#).

Console

Um die ALPN-Richtlinie zu aktualisieren

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

2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listener den Text in der Protocol:PortSpalte aus, um die Detailseite für den Listener zu öffnen.
5. Wählen Sie Aktionen, Listener bearbeiten.
6. Wählen Sie im Abschnitt Sichere Listener-Einstellungen für ALPN-Richtlinie eine Richtlinie aus, um ALPN zu aktivieren, oder wählen Sie Keine, um ALPN zu deaktivieren.
7. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die ALPN-Richtlinie zu aktualisieren

Verwenden Sie den Befehl [modify-listener](#).

```
aws elbv2 modify-listener \  
  --listener-arn listener-arn \  
  --alpn-policy HTTP2Preferred
```

CloudFormation

Um die ALPN-Richtlinie zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::Listener-Ressource](#), sodass sie die ALPN-Richtlinie enthält.

```
Resources:  
  myTLSListener:  
    Type: 'AWS::ElasticLoadBalancingV2::Listener'  
    Properties:  
      LoadBalancerArn: !Ref myLoadBalancer  
      Protocol: TLS  
      Port: 443  
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"  
      AlpnPolicy:  
        - HTTP2Preferred  
      Certificates:  
        - CertificateArn: "certificate-arn"  
      DefaultActions:  
        - Type: forward
```

```
TargetGroupArn: !Ref myTargetGroup
```

Löschen eines TLS-Listeners für Ihren Network Load Balancer

Bevor Sie einen Listener löschen, sollten Sie die Auswirkungen auf Ihre Anwendung berücksichtigen:

- [TCP- und TLS-Listener] Der Load Balancer akzeptiert sofort keine neuen Verbindungen auf dem Listener mehr. Alle laufenden TLS-Handshakes schlagen möglicherweise fehl. Bestehende Verbindungen bleiben geöffnet, bis sie auf natürliche Weise geschlossen werden oder ein Timeout auftritt. In-flight-Anfragen für bestehende Verbindungen wurden erfolgreich abgeschlossen.
- [UDP- und QUIC-Listener] Alle Pakete, die gerade übertragen werden, erreichen ihr Ziel möglicherweise nicht.

Console

So löschen Sie einen Listener

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Aktivieren Sie das Kontrollkästchen für den Load Balancer.
4. Wählen Sie Listener, markieren Sie das Kontrollkästchen für den Listener, und wählen Sie dann Aktionen, Listener löschen.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **confirm** ein und wählen Sie Löschen aus.

AWS CLI

So löschen Sie einen Listener

Verwenden Sie den Befehl [delete-listener](#).

```
aws elbv2 delete-listener \  
  --listener-arn listener-arn
```

Zielgruppen für Ihre Network Load Balancers

Jede Zielgruppe wird verwendet, um Anfragen an ein oder mehrere registrierte Ziele weiterzuleiten. Wenn Sie einen Listener erstellen, geben Sie eine Zielgruppe für die Standardaktion an. Der Datenverkehr wird an die in der Listener-Regel angegebene 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. Weitere Informationen finden Sie unter [Network-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. Weitere Informationen finden Sie unter [Zustandsprüfungen für Zielgruppen von Network Load Balancer](#).

Inhalt

- [Weiterleitungskonfiguration](#)
- [Zieltyp](#)
- [IP-Adresstyp](#)
- [Registrierte Ziele](#)
- [Zielgruppenattribute](#)
- [Zustand der Zielgruppe](#)
- [Erstellen einer Zielgruppe für Ihren Network Load Balancer](#)
- [Aktualisieren Sie die Gesundheitseinstellungen für Ihre Zielgruppe für Ihren Network Load Balancer](#)
- [Zustandsprüfungen für Zielgruppen von Network Load Balancer](#)
- [Zielgruppenattribute für Ihren Network Load Balancer bearbeiten](#)
- [Registrieren Sie Ziele für Ihren Network Load Balancer](#)
- [Verwenden Sie einen Application Load Balancer als Ziel eines Network Load Balancer](#)
- [Kennzeichnen Sie eine Zielgruppe für Ihren Network Load Balancer](#)
- [Löschen Sie eine Zielgruppe für Ihren Network Load Balancer](#)

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 für Network Load Balancers unterstützen die folgenden Protokolle und Ports:

- Protokolle: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- Ports: 1-65535

Wenn eine Zielgruppe mit dem TLS-Protokoll konfiguriert ist, stellt der Load Balancer 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 in einer Virtual Private Cloud (VPC) befindet, 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.

In der folgenden Tabelle finden Sie eine Zusammenfassung der unterstützten Kombinationen der Einstellungen für Listener-Protokoll und Zielgruppe.

Listener-Protokoll	Protokoll der Zielgruppe	Zielgruppentyp	Zustandsprüfungsprotokoll
TCP	TCP TCP_UDP TCP_QUIC	instance ip	HTTP HTTPS TCP
TCP	TCP	alb	HTTP HTTPS
TLS	TCP TLS	instance ip	HTTP HTTPS TCP
UDP	UDP TCP_UDP	instance ip	HTTP HTTPS TCP
TCP_UDP	TCP_UDP	instance ip	HTTP HTTPS TCP
SCHNELL	SCHNELL TCP_QUIC	instance ip	HTTP HTTPS TCP

Listener-Protokoll	Protokoll der Zielgruppe	Zielgruppentyp	Zustandsprüfungsprotokoll
TCP_QUIC	TCP_QUIC	instance ip	HTTP HTTPS TCP

Zieltyp

Wenn Sie eine Zielgruppe erstellen, können Sie ihren Zieltyp angeben, der bestimmt, wie Sie ihre Ziele 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 werden nach IP-Adresse angegeben.

`alb`

Das Ziel ist ein Application Load Balancer.

Wenn der Zieltyp `ip` ist, können Sie IP-Adressen von einem der folgenden CIDR-Blöcke angeben:

- Die Subnetze der Zielgruppe VPC
- 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:

- AWS Ressourcen, die über IP-Adresse und Port adressierbar sind (z. B. Datenbanken).
- Lokale Ressourcen, mit denen AWS über eine VPN-Verbindung Direct Connect oder eine Site-to-Site VPN-Verbindung verbunden ist.

Wenn die Client-IP-Erhaltung für Ihre Zielgruppen deaktiviert ist, kann der Load Balancer rund 55 000 Verbindungen pro Minute für jede Kombination aus Network-Load-Balancer-IP-Adresse und eindeutigem Ziel (IP-Adresse und Port) unterstützen. Werden diese Verbindungen überschritten, steigt das Risiko von Port-Zuordnungsfehlern. Falls Port-Zuordnungsfehlern auftreten, fügen Sie der Zielgruppe mehrere Ziele hinzu.

Wenn Sie einen Network Load Balancer in einer gemeinsam genutzten VPC (als Teilnehmer) starten, können Sie nur Ziele in Subnetzen registrieren, die für Sie freigegeben wurden.

Wenn der Zieltyp `a1b` ist, können Sie einen einzelnen Application Load Balancer als Ziel registrieren. Weitere Informationen finden Sie unter [Verwenden Sie einen Application Load Balancer als Ziel eines Network Load Balancer](#).

Network Load Balancers unterstützen den Zieltyp `lambda` nicht. Application Load Balancers sind die einzigen Load Balancers, die den Zieltyp `lambda` unterstützen. Weitere Informationen finden Sie unter [Lambda-Funktionen als Ziele](#) im Benutzerhandbuch für Application Load Balancers.

Wenn Sie Microservices auf Instances haben, die bei einem Network Load Balancer registriert sind, können Sie den Load Balancer nicht für die Kommunikation zwischen den Instances verwenden, es sei denn, der Load Balancer ist mit dem Internet verbunden oder die Instances sind nach IP-Adresse registriert. Weitere Informationen finden Sie unter [Verbindungen überschreiten bei Anfragen von einem Ziel an dessen Load Balancer das Zeitlimit](#).

Routing- und IP-Adressen anfordern

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. Der Load Balancer schreibt die Ziel-IP-Adresse aus dem Datenpaket neu, bevor er sie an die Ziel-Instance weiterleitet.

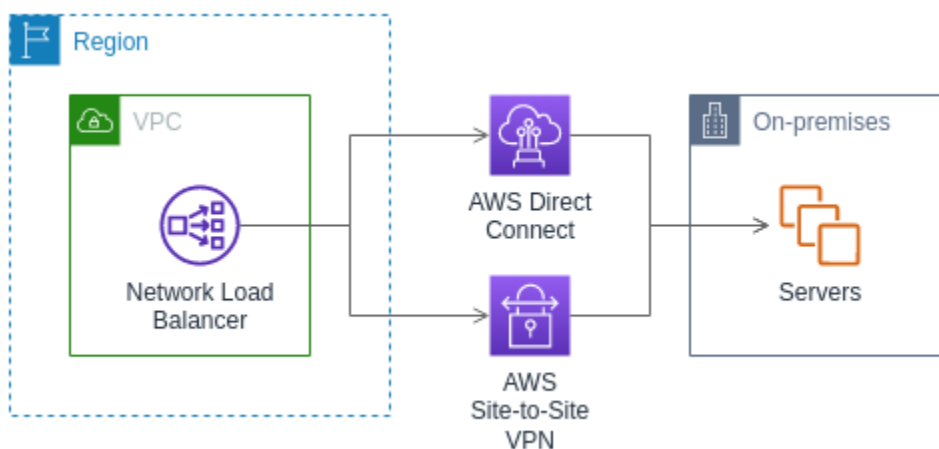
Wenn Sie Ziele unter Verwendung von IP-Adressen angeben, können Sie den Datenverkehr über eine beliebige private IP-Adresse aus einer oder mehreren Netzwerkschnittstellen an eine Instance

weiterleiten. Auf diese Weise können mehrere Anwendungen auf eine Instance denselben Port verwenden. Beachten Sie, dass jede Netzwerkschnittstelle eine eigene Sicherheitsgruppe haben kann. Der Load Balancer schreibt die Ziel-IP-Adresse neu, bevor sie an das Ziel weitergeleitet wird.

Weitere Informationen zum Ermöglichen von Datenverkehr zu Ihren Instances finden Sie unter [Zielsicherheitsgruppen](#).

On-Premises-Ressourcen als Ziele

Lokale Ressourcen, die über eine VPN-Verbindung Direct Connect oder eine Site-to-Site VPN-Verbindung verknüpft sind, können als Ziel dienen, wenn der Zieltyp ist. `ip`



Bei der Verwendung von On-Premises-Ressourcen müssen die IP-Adressen dieser Ziele dennoch aus einem der folgenden CIDR-Blöcke stammen:

- 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)

Weitere Informationen zu finden Sie Direct Connect unter [Was ist? Direct Connect](#)

Weitere Informationen zu AWS Site-to-Site VPN finden Sie unter [Was ist AWS Site-to-Site VPN?](#)

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 Network 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 keine IPv4 Zielgruppe mit einem UDP-Listener für einen `dualstack` Load Balancer verwenden.
- Sie können einen Application Load Balancer nicht bei einer IPv6 Zielgruppe registrieren.
- Sie können keine IPv6 Zielgruppe mit den Protokollen QUIC oder TCP_QUIC verwenden.

Registrierte Ziele

Ihr Load Balancer dient als zentraler Kontaktpunkt für Clients und verteilt eingehenden Datenverkehr an die fehlerfreien registrierten Ziele. Jede Zielgruppe muss mindestens ein registriertes Ziel in jeder Availability Zone haben, die für den Load Balancer aktiviert ist. 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 Datenverkehr 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 Datenverkehr 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 [Anhängen eines Load Balancers an Ihre Auto-Scaling-Gruppe](#) im Benutzerhandbuch zu Auto Scaling in Amazon EC2.

Anforderungen und Überlegungen

- Sie können Instances nicht anhand der Instanz-ID registrieren, wenn sie einen der folgenden Instance-Typen verwenden: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, H1, HS1, M1, M2, M3 oder T1.
- Bei der Registrierung von Zielen anhand der Instanz-ID für eine IPv6 Zielgruppe müssen die Ziele über eine zugewiesene primäre IPv6 Adresse verfügen. Weitere Informationen finden Sie unter [IPv6 Adressen](#) im Amazon EC2 EC2-Benutzerhandbuch
- Bei der Registrierung von Zielen anhand der Instanz-ID müssen sich die Instances in derselben VPC wie der Network Load Balancer befinden. Sie können Instances nicht nach Instance-ID registrieren, wenn sie sich in einer VPC befinden, die mit der Load-Balancer-VPC gekoppelt ist (dieselbe Region oder eine andere Region). Sie können diese Instances nach IP-Adresse registrieren.
- Wenn Sie ein Ziel nach IP-Adresse registrieren und sich die IP-Adresse in derselben VPC wie der Load Balancer befindet, überprüft der Load Balancer, ob das Ziel zu einem Subnetz gehört, das es erreichen kann.
- Der Load Balancer leitet Datenverkehr nur an Ziele in aktivierten Availability Zones weiter. Ziele in Zonen, die nicht aktiviert sind, werden nicht verwendet.
- Registrieren Sie Instances für die Zielgruppen UDP, TCP_UDP, QUIC und TCP_QUIC nicht anhand der IP-Adresse, wenn sie sich außerhalb der Load Balancer-VPC befinden oder einen

der folgenden Instance-Typen verwenden: C1,,,,,,, G1, G2, CC1, CC2, M1 CG1 CG2, M2 CR1, M3 oder T1. H11 HS1 Ziele, die sich außerhalb der Load-Balancer-VPC befinden oder einen nicht unterstützten Instance-Typ verwenden, können möglicherweise Datenverkehr vom Load Balancer empfangen, dann aber nicht antworten.

Zielgruppenattribute

Sie können eine Zielgruppe konfigurieren, indem Sie ihre Attribute bearbeiten. Weitere Informationen finden Sie unter [Zielgruppenattribute bearbeiten](#).

Die folgenden Zielgruppenattribute werden unterstützt. Sie können diese Attribute nur ändern, wenn der Zielgruppentyp `instance` oder `ip` ist. Wenn der Zielgruppentyp `alb` ist, verwenden diese Attribute immer ihre Standardwerte.

`deregistration_delay.timeout_seconds`

Die Zeitspanne, wie lange Elastic Load Balancing wartet, bevor der Status eines deregistrierten Ziels von `draining` in `unused` geändert wird. Der Bereich liegt zwischen 0 und 3 600 Sekunden. Der Standardwert beträgt 300 Sekunden. Für QUIC-Verkehr beträgt der Wert immer 300 Sekunden.

`deregistration_delay.connection_termination.enabled`

Gibt an, ob der Load Balancer Verbindungen am Ende des Timeouts der Abmeldung beendet. Der Wert ist entweder `true` oder `false`. Für neue UDP/TCP_UDP-Zielgruppen ist die Standardeinstellung `true`. Andernfalls ist die Standardeinstellung `false`. Dieses Attribut gilt nicht für QUIC-Verkehr.

`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`.

`preserve_client_ip.enabled`

Zeigt an, ob die IP-Erhaltung des Clients aktiviert ist. Der Wert ist entweder `true` oder `false`. Der Standardwert ist deaktiviert, wenn der Zielgruppentyp die IP-Adresse ist und das Zielgruppenprotokoll TCP oder TLS ist. Andernfalls ist die Standardeinstellung aktiviert. Die Client-IP-Erhaltung kann für die Zielgruppen UDP, TCP_UDP, QUIC und TCP_QUIC nicht deaktiviert werden.

`proxy_protocol_v2.enabled`

Gibt an, ob die Proxy-Protokoll-Version 2 aktiviert ist. Das Proxy-Protokoll ist standardmäßig deaktiviert.

`stickiness.enabled`

Gibt an, ob Sticky Sessions aktiviert sind. Der Wert ist entweder `true` oder `false`. Der Standardwert ist `false`. Dieses Attribut gilt nicht für QUIC-Verkehr.

`stickiness.type`

Die Art der „Sticky Sessions“. Der mögliche Wert ist `source_ip`.

`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 die Zone im DNS als fehlerhaft, sodass der Datenverkehr nur an fehlerfreie Zonen 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 die Zone nicht aus 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 Mindestprozentsatz der Ziele, die fehlerfrei sein müssen. Wenn der Prozentsatz fehlerfreier Ziele unter diesem Wert liegt, markieren Sie die Zone im DNS als fehlerhaft, sodass der Datenverkehr nur an fehlerfreie Zonen weitergeleitet wird. Die möglichen Werte sind `off` oder eine Ganzzahl von 1 bis 100. Wenn `off` DNS-Failaway deaktiviert ist, was bedeutet, dass die Zone nicht aus 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. Mögliche Werte sind 1 bis zur maximalen Anzahl von Zielen. Der Standardwert ist 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

Der Mindestprozentsatz 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`.

`target_health_state.unhealthy.connection_termination.enabled`

Gibt an, ob der Load Balancer Verbindungen mit fehlerhaften Zielen beendet. Der Wert ist entweder `true` oder `false`. Der Standardwert ist `true`.

`target_health_state.unhealthy.draining_interval_seconds`

Die Wartezeit von Elastic Load Balancing, bevor der Status eines fehlerhaften Ziels von `unhealthy.draining` zu `unhealthy` geändert wird. Der Bereich liegt zwischen 0 und 360000 Sekunden. Der Standardwert ist 0 Sekunden.

Hinweis: Dieses Attribut kann nur konfiguriert werden, wenn `target_health_state.unhealthy.connection_termination.enabled` es ist. `false`

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](#)
- [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

- 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](#).
- 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).
- Beim DNS-Failover tritt ein DNS-Failover auf, wenn mehrere Zielgruppen an einen Network Load Balancer angeschlossen sind und eine Zielgruppe in einer Zone fehlerhaft ist, auch wenn 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.

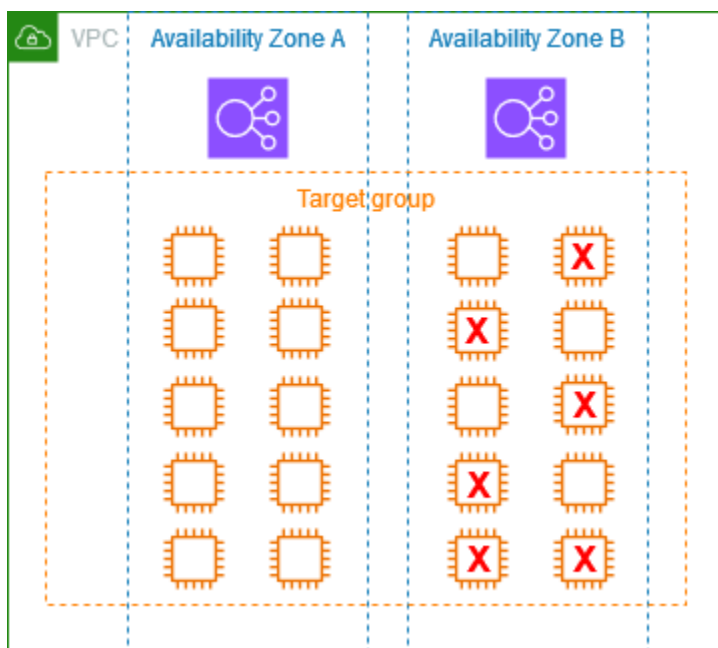
- Neben der Frage, ob genügend fehlerfreie Ziele vorhanden sind, die zu einem DNS-Failover führen könnten, gibt es noch andere Faktoren, z. B. den Zustand der Zone.

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 Balancern 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 Network 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 Network 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 alle Zielgruppen, die an einen Network Load Balancer angeschlossen sind, fehlerhaft sind, besteht der Aliaseintrag die Route 53-Zustandsprüfung (Fail-Open) nicht. Wenn Sie die Option Zielintegrität auswerten verwenden, führt dies dazu, dass die Failover-Routing-Richtlinie den Datenverkehr an die sekundäre Ressource umleitet.
- Wenn alle Zielgruppen in einem Network Load Balancer leer sind (keine Ziele), betrachtet Route 53 den Datensatz als fehlerhaft (Fail-Open). Wenn Sie den Status des Ziels evaluieren verwenden, führt dies dazu, dass die Failover-Routing-Richtlinie den Datenverkehr zur sekundären Ressource umleitet.

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 einer Zielgruppe für Ihren Network Load Balancer

Sie registrieren Ziele für Ihren Network Load Balancer 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.

Um Datenverkehr an die Ziele in einer Zielgruppe weiterzuleiten, erstellen Sie einen Listener und geben Sie die Zielgruppe in der Standardaktion für den Listener an. Weitere Informationen finden Sie unter [Standardaktionen](#). Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Network 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 für Ihren Network Load Balancer](#). Sie können auch die Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern. Weitere Informationen finden Sie unter [Aktualisieren Sie die Einstellungen für die Zustandsprüfung einer Network Load Balancer-Balancer-Zielgruppe](#).

Voraussetzungen

- Nachdem Sie eine Zielgruppe erstellt haben, können Sie ihren Zieltyp oder ihren IP-Adresstyp nicht mehr ändern.
- Alle Ziele in einer Zielgruppe müssen denselben IP-Adresstyp wie die Zielgruppe haben: IPv4 oder IPv6.
- Sie müssen eine IPv6 Zielgruppe mit einem Dual-Stack-Loadbalancer verwenden.
- Sie können keine IPv4 Zielgruppe mit einem UDP-Listener für einen Load Balancer verwenden. `duallstack`
- Sie können keine IPv6 Zielgruppe mit den Protokollen QUIC oder TCP_QUIC verwenden.

Console

Erstellen einer Zielgruppe

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich Target Groups aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Führen Sie unter Grundlegende Konfiguration die folgenden Schritte aus:
 - a. 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 Application Load Balancer, um einen Application Load Balancer als Ziel zu registrieren.

- b. Geben Sie unter Zielgruppenname einen Namen für die 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.
- c. Wählen Sie unter Protocol (Protokoll) wie folgt ein Protokoll aus:
 - Wenn das Listener-Protokoll TCP ist, wählen Sie TCP oder TCP_UDP.
 - Wenn das Listener-Protokoll TLS ist, wählen Sie TCP oder TLS.
 - Wenn das Listener-Protokoll UDP ist, wählen Sie UDP oder TCP_UDP.
 - Wenn das Listener-Protokoll TCP_UDP ist, wählen Sie TCP_UDP.
 - Wenn das Listener-Protokoll QUIC ist, wählen Sie QUIC.
 - Wenn das Listener-Protokoll TCP_QUIC ist, wählen Sie TCP_QUIC.
 - Wenn der Zieltyp Application Load Balancer ist, muss das Protokoll TCP sein.
- d. Ändern Sie für Port den Standardwert nach Bedarf.

Wenn der Zieltyp Application Load Balancer ist, muss der Port mit dem Listener-Port des Application Load Balancer übereinstimmen.

- e. Wählen Sie als IP-Adresstyp oder IPv4IPv6 Diese Option ist nur verfügbar, wenn der Zieltyp Instances oder IP-Adressen ist.
 - f. Wählen Sie für VPC die Virtual Private Cloud (VPC) mit den zu registrierenden Zielen aus.
5. Ändern Sie für den Bereich Zustandsprüfungen die Standardeinstellungen nach Bedarf. 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 [???](#).
 6. (Optional) Um ein Tag hinzuzufügen, erweitern Sie Tags, wählen Sie Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
 7. Wählen Sie Weiter aus.

8. (Optional) Registrieren Sie Ziele. Der Zieltyp der Zielgruppe bestimmt die Informationen, die Sie bereitstellen. Wenn Sie noch nicht bereit sind, Ziele zu registrieren, können Sie sie später registrieren.
 - Instances — Wählen Sie die EC2-Instances aus, geben Sie die Ports ein und wählen Sie unten Include as pending aus.
 - IP-Adressen — Wählen Sie die VPC aus, die die IP-Adressen oder Andere private IP-Adressen enthält, geben Sie die IP-Adressen und Ports ein und wählen Sie unten Als ausstehend einbeziehen aus.
 - Application Load Balancer — Wählen Sie den Application Load Balancer aus. Weitere Informationen finden Sie unter [Verwenden Sie Application Load Balancers als Ziele](#).
9. Wählen Sie Zielgruppe erstellen aus.

AWS CLI

Erstellen einer Zielgruppe

Verwenden Sie den Befehl [create-target-group](#). Im folgenden Beispiel wird eine Zielgruppe mit dem TCP-Protokoll, nach IP-Adresse registrierten Zielen, einem Tag und Standardeinstellungen für die Integritätsprüfung erstellt.

```
aws elbv2 create-target-group \  
  --name my-target-group \  
  --protocol TCP \  
  --port 80 \  
  --target-type ip \  
  --vpc-id vpc-1234567890abcdef0 \  
  --tags Key=department,Value=123
```

Um Ziele zu registrieren

Verwenden Sie den Befehl [register-targets](#), um Ziele bei der Zielgruppe zu registrieren. Beispiele finden Sie unter [the section called “Ziele registrieren”](#).

CloudFormation

Erstellen einer Zielgruppe

Definieren Sie eine Ressource des Typs [AWS::ElasticLoadBalancingV2::TargetGroup](#) Im folgenden Beispiel wird eine Zielgruppe mit dem TCP-Protokoll, nach IP-Adresse registrierten

Zielen, einem Tag, Standardeinstellungen für die Integritätsprüfung und zwei registrierten Zielen erstellt.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: 10.0.50.10
          Port: 80
        - Id: 10.0.50.20
          Port: 80
```

Aktualisieren Sie die Gesundheitseinstellungen für Ihre Zielgruppe für Ihren Network Load Balancer

Standardmäßig überwachen Network Load Balancer den Zustand von Zielen und leiten Anfragen an fehlerfreie Ziele weiter. Wenn der Load Balancer jedoch nicht über genügend fehlerfreie Ziele verfügt, sendet er automatisch Traffic an alle registrierten Ziele (Fail-Open). Sie können die Gesundheitseinstellungen für Ihre Zielgruppe ändern, um die Schwellenwerte für DNS-Failover und Routing-Failover zu definieren. Weitere Informationen finden Sie unter [the section called “Zustand der Zielgruppe”](#).

Console

Um die Gesundheitseinstellungen der Zielgruppe zu aktualisieren

1. Öffnen Sie die Amazon-EC2-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.


```
--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"
```

CloudFormation

Um die Gesundheitseinstellungen für Zielgruppen zu ändern

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource. Im folgenden Beispiel wird der Schwellenwert für den fehlerfreien Zustand für beide Aktionen mit einem fehlerhaften Zustand auf 50 % festgelegt.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - 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"
```

Zustandsprüfungen für Zielgruppen von Network Load Balancer

Sie können Ihre Ziele bei einer oder mehreren Zielgruppen registrieren. Der Load Balancer leitet Anfragen an ein neu registriertes Ziel weiter, sobald der Registrierungsprozess abgeschlossen ist und die Ziele die ersten Zustandsprüfungen bestanden haben. Es kann einige Minuten dauern, bis der Registrierungsvorgang abgeschlossen ist und die Zustandsprüfungen gestartet werden.

Network Load Balancers verwenden aktive und passive Zustandsprüfungen, um zu ermitteln, ob ein Ziel für die Verarbeitung von Anforderungen verfügbar ist. Standardmäßig leitet jeder Load

Balancer-Knoten Anfragen nur an störungsfreie Ziele in seiner Availability Zone weiter. Wenn das zonenübergreifende Load Balancing aktiviert ist, leitet jeder Load Balancer-Knoten Anforderungen an störungsfreie Ziele in allen aktivierten Availability Zones weiter. Weitere Informationen finden Sie unter [Zonenübergreifendes Load Balancing](#).

Mit passiven Zustandsprüfungen beobachtet der Load Balancer, wie Ziele auf Verbindungen reagieren. Passive Zustandsprüfungen ermöglichen dem Load Balancer, ein fehlerhaftes Ziel zu erkennen, bevor es von den aktiven Zustandsprüfungen als fehlerhaft gemeldet wird. Sie können passive Zustandsprüfungen nicht deaktivieren, konfigurieren oder überwachen. Passive Zustandsprüfungen werden für UDP-Verkehr und Zielgruppen mit aktivierter Sperrfunktion nicht unterstützt. Weitere Informationen finden Sie unter [Sticky Sessions](#).

Wenn ein Ziel fehlerhaft wird, sendet der Load Balancer ein TCP RST für Pakete, die auf den mit dem Ziel verknüpften Client-Verbindungen empfangen werden, es sei denn, das fehlerhafte Ziel veranlasst den Load Balancer zum Fail-Open.

Wenn Zielgruppen in einer aktivierten Availability Zone kein fehlerfreies Ziel haben, entfernen wir die IP-Adresse für das entsprechende Subnetz vom DNS, so dass in dieser Availability Zone keine Anfragen an Ziele weitergeleitet werden können. Beim Load Balancer erfolgt ein Fail-Open, wenn alle Ziele gleichzeitig die Zustandsprüfungen in allen aktivierten Availability Zones nicht bestehen. Network Load Balancers können auch nicht geöffnet werden, wenn Sie eine leere Zielgruppe haben. Der Effekt des Fail-Open ist, dass der Datenverkehr zu allen Zielen in allen aktivierten Availability Zones zugelassen wird, unabhängig von ihrem Zustand.

Wenn eine Zielgruppe mit HTTPS-Zustandsprüfungen konfiguriert ist, schlagen ihre registrierten Ziele Zustandsprüfungen fehl, wenn sie nur TLS 1.3 unterstützen. Diese Ziele müssen eine frühere Version von TLS unterstützen, z. B. TLS 1.2.

Bei HTTP- oder HTTPS-Zustandsprüfungsanforderungen enthält der Host-Header anstelle der IP-Adresse des Ziels und des Zustandsprüfungs-Ports die IP-Adresse des Load Balancer-Knotens und des Listener-Ports.

Wenn Sie Ihrem Network Load Balancer einen TLS-Listener hinzufügen, führen wir einen Test der Listener-Konnektivität durch. Da das Beenden von TLS auch eine TCP-Verbindung beendet, wird eine neue TCP-Verbindung zwischen Ihrem Load Balancer und Ihren Zielen hergestellt. Daher werden die TCP-Verbindungen für diesen Test möglicherweise von Ihrem Load Balancer an die Ziele gesendet, die bei Ihrem TLS-Listener registriert sind. Sie können diese TCP-Verbindungen identifizieren, da sie die Quell-IP-Adresse Ihres Network Load Balancer haben und die Verbindungen keine Datenpakete enthalten.

Bei UDP- und QUIC-Diensten kann die Zielverfügbarkeit mithilfe von Zustandsprüfungen, die nicht auf UDP basieren, an Ihrer Zielgruppe getestet werden. Sie können jede verfügbare Zustandsprüfung (TCP, HTTP oder HTTPS) und jeden Port auf Ihrem Ziel verwenden, um die Verfügbarkeit Ihres Dienstes zu überprüfen. Wenn der Service, der die Zustandsprüfung empfängt, fehlschlägt, wird Ihr Ziel als nicht verfügbar betrachtet. Um die Genauigkeit der Zustandsprüfungen für Ihren Dienst zu verbessern, konfigurieren Sie den Dienst, der den Health Check-Port überwacht, so, dass er den Status Ihres UDP- oder QUIC-Dienstes verfolgt und die Zustandsprüfung nicht besteht, wenn der Dienst nicht verfügbar ist.

Weitere Informationen finden Sie unter [the section called “Zustand der Zielgruppe”](#).

Inhalt

- [Zustandsprüfungseinstellungen](#)
- [Zustandsstatus des Ziels](#)
- [Ursachencodes für Zustandsprüfungen](#)
- [Überprüfen Sie den Zustand Ihrer Network Load Balancer Balancer-Ziele](#)
- [Aktualisieren Sie die Einstellungen für die Zustandsprüfung einer Network Load Balancer Balancer-Zielgruppe](#)

Zustandsprüfungseinstellungen

Sie können aktive Zustandsprüfungen für die Ziele in einer Zielgruppe mit den folgenden Einstellungen konfigurieren. Wenn die Integritätsprüfungen `UnhealthyThresholdCount` aufeinanderfolgende Fehler überschreiten, nimmt der Load Balancer das Ziel außer Betrieb. Wenn die Zustandsprüfungen `HealthyThresholdCount` aufeinanderfolgende Erfolge überschreiten, nimmt der Load Balancer das Ziel wieder in Betrieb.

Einstellung	Description	Standard
<code>HealthCheckProtocol</code>	Das Protokoll, das der Load Balancer für die Zustandsprüfungen der Ziele verwendet. Möglichen Protokolle sind HTTP, HTTPS und TCP. Das Standardprotokoll ist TCP. Wenn der Zieltyp <code>alb</code> ist, sind die unterstützten Zustandsprüfungsprotokolle HTTP und HTTPS.	TCP

Einstellung	Description	Standard
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.	Port, auf dem jedes Ziel Datenverkehr vom Load Balancer empfängt.
HealthCheckPath	[HTTP/HTTPS-Zustandsprüfungen] Der Pfad zur Integritätsprüfung, der das Ziel auf den Zielen für Zustandsprüfungen ist. Der Standardwert ist /.	/
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. Die Standardwerte sind 6 Sekunden für HTTP- und 10 Sekunden für TCP- und HTTPS-Zustandsprüfungen.	6 Sekunden für HTTP- und 10 Sekunden für TCP- und HTTPS-Zustandsprüfungen.

Einstellung	Description	Standard
HealthCheckIntervalSeconds	<p>Der etwaige Zeitraum in Sekunden zwischen den Zustandsprüfungen der einzelnen Ziele. Der Bereich liegt zwischen 5 und 300 Sekunden. Standardmäßig ist ein Zeitraum von 30 Sekunden festgelegt.</p> <p>Zustandsprüfungen für Network Load Balancers sind verteilt und verwenden einen Konsensmechanismus, um den Zustand des Ziels zu bestimmen. Daher erhalten Ziele mehr als die konfigurierte Anzahl von Zustandsprüfungen. Wenn Sie die Auswirkungen auf Ihre Ziele bei HTTP-Zustandsprüfungen reduzieren möchten, verwenden Sie ein einfacheres Ziel bei den Zielen, z. B. eine statische HTML-Datei, oder wechseln Sie zu TCP-Zustandsprüfungen.</p>	30 Sekunden
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.	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.	2
Matcher	[HTTP/HTTPS-Zustandsprüfungen] Die HTTP-Codes, die verwendet werden, um ein Ziel auf eine erfolgreiche Antwort zu überprüfen. Der Bereich liegt zwischen 200 und 599. Der Standard ist 200–399.	200-399

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.

Die folgende Tabelle beschreibt die möglichen Werte für den Zustandsstatus eines registrierten Ziels.

Wert	Description
<code>initial</code>	<p>Der Load Balancer befindet sich im Prozess der Registrierung eines Ziels oder der Durchführung der anfänglichen Zustandsprüfungen für das Ziel.</p> <p>Zugehörige Ursachencodes: <code>Elb.RegistrationInProgress</code> <code>Elb.InitialHealthChecking</code></p>
<code>healthy</code>	<p>Das Ziel ist fehlerfrei.</p> <p>Zugehörige Ursachencodes: Keine</p>
<code>unhealthy</code>	<p>Das Ziel hat auf eine Integritätsprüfung nicht geantwortet, hat die Integritätsprüfung nicht bestanden oder das Ziel befindet sich im Status „Gestoppt“.</p> <p>Zugehöriger Ursachencode: <code>Target.FailedHealthChecks</code></p>
<code>draining</code>	<p>Die Registrierung für das Ziel wird aufgehoben, und Connection Draining wird durchgeführt.</p> <p>Zugehöriger Ursachencode: <code>Target.DeregistrationInProgress</code></p>
<code>unhealthy.draining</code>	<p>Das Ziel hat auf die Zustandsprüfungen nicht geantwortet oder hat die Zustandsprüfungen nicht bestanden und tritt in eine Übergangsfrist ein. Das Ziel unterstützt bestehende Verbindungen und akzeptiert während dieser Übergangszeit keine neuen Verbindungen.</p>

Wert	Description
	Zugehöriger Ursachencode: <code>Target.FailedHealthChecks</code>
<code>unavailable</code>	Die Zielintegrität ist nicht verfügbar. Zugehöriger Ursachencode: <code>Elb.InternalError</code>
<code>unused</code>	Das Ziel ist nicht bei einer Zielgruppe registriert, die Zielgruppe wird nicht in einer Listener-Regel verwendet oder das Ziel befindet sich in einer Availability Zone, die nicht aktiviert ist. Zugehörige Ursachencodes: <code>Target.NotRegistered</code> <code>Target.NotInUse</code> <code>Target.InvalidState</code> <code>Target.IpUnusable</code>

Ursachencodes für Zustandsprüfungen

Wenn der Status eines Ziels einen anderen Wert als `Healthy` aufweist, gibt die API einen Ursachencode und eine Beschreibung des Problems zurück und die Konsole zeigt die gleiche Beschreibung in einer QuickInfo an. Beachten Sie, dass Ursachencodes, die mit `Elb` beginnen, ihren Ursprung auf dem Load Balancer und Grundcodes, die mit `Target` beginnen, ihren Ursprung auf der Ziel-Seite haben.

Ursachencode	Description
<code>Elb.InitialHealthChecking</code>	Anfängliche Zustandsprüfungen in Bearbeitung
<code>Elb.InternalError</code>	Zustandsprüfungen aufgrund eines internen Fehles fehlgeschlagen
<code>Elb.RegistrationInProgress</code>	Zielregistrierung wird durchgeführt
<code>Target.DeregistrationInProgress</code>	Zielregistrierung wird aufgehoben

Ursachencode	Description
Target.FailedHealthChecks	Zustandsprüfungen fehlgeschlagen
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 Ziel ist in einer Availability Zone, die nicht für den Load Balancer aktiviert ist
Target.NotRegistered	Ziel ist nicht in der Zielgruppe registriert

Überprüfen Sie den Zustand Ihrer Network Load Balancer Balancer-Ziele

Sie können den Zustand der Ziele, die in Ihren Zielgruppen registriert sind, überprüfen. Hilfe bei fehlgeschlagenen Zustandsprüfungen finden Sie unter [Problembehandlung: Ein registriertes Ziel ist nicht in Betrieb](#).

Console

So überprüfen Sie den Zustand Ihrer Ziele

1. Öffnen Sie die Amazon-EC2-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. Auf der Registerkarte „Details“ werden die Gesamtzahl der Ziele sowie die Anzahl der Ziele für jeden Gesundheitsstatus angezeigt.

5. In der Registerkarte Ziele gibt die Spalte Zustandsstatus den Status der einzelnen Ziele wider.
6. Wenn der Status einen anderen Wert als Healthy hat, enthält die Spalte Details zum Zustand weitere Informationen.

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-step Anweisungen](#) finden Sie im folgenden Blogbeitrag: [Identifizieren fehlerhafter Ziele Ihres Load Balancers](#).

AWS CLI

Um den Zustand Ihrer Ziele zu überprüfen

Verwenden Sie den Befehl [describe-target-health](#). In diesem Beispiel wird die Ausgabe so gefiltert, dass sie nur Ziele enthält, die nicht fehlerfrei sind. Für Ziele, die nicht fehlerfrei sind, enthält die Ausgabe einen Ursachencode.

```
aws elbv2 describe-target-health \
  --target-group-arn target-group-arn \
  --query "TargetHealthDescriptions[?TargetHealth.State!='healthy']" \
  [Target.Id,TargetHealth.State,TargetHealth.Reason]" \
  --output table
```

Es folgt eine Beispielausgabe.

```
-----
|           DescribeTargetHealth           |
+-----+-----+-----+
| 172.31.0.57 | unused | Target.NotInUse |
| 172.31.0.50 | unused | Target.NotInUse |
+-----+-----+-----+
```

Zielstatus und Ursachencodes

Die folgende Liste zeigt die möglichen Ursachencodes für jeden Zielstaat.

Zielstatus ist healthy

Ein Ursachencode ist nicht angegeben.

Zielstatus ist initial

- `Elb.RegistrationInProgress`- Das Ziel wird gerade beim Load Balancer registriert.
- `Elb.InitialHealthChecking`- Der Load Balancer sendet dem Ziel immer noch die Mindestanzahl an Integritätsprüfungen, die zur Bestimmung seines Integritätsstatus erforderlich sind.

Der Zielstatus ist unhealthy

- `Target.FailedHealthChecks`- Der Load Balancer hat beim Herstellen einer Verbindung zum Ziel einen Fehler erhalten, oder die Zielantwort war falsch formatiert.

Der Zielstatus ist unused

- `Target.NotRegistered`- Das Ziel ist nicht bei der Zielgruppe registriert.
- `Target.NotInUse`- Die Zielgruppe wird von keinem Load Balancer verwendet oder das Ziel befindet sich in einer Availability Zone, die für den Load Balancer nicht aktiviert ist.
- `Target.InvalidState`- Das Ziel befindet sich im Status „Gestoppt“ oder „Beendet“.
- `Target.IpUnusable`- Die Ziel-IP-Adresse ist für die Verwendung durch einen Load Balancer reserviert.

Der Zielstatus ist draining

- `Target.DeregistrationInProgress`- Das Ziel wird gerade abgemeldet und die Frist für die Abmeldung ist noch nicht abgelaufen.

Der Zielstatus ist unavailable

- `Elb.InternalError`- Der Zustand des Ziels ist aufgrund eines internen Fehlers nicht verfügbar.

Aktualisieren Sie die Einstellungen für die Zustandsprüfung einer Network Load Balancer Balancer-Zielgruppe

Sie können die Einstellungen für den Gesundheitscheck für Ihre Zielgruppe jederzeit aktualisieren. Eine Liste der Einstellungen für die Gesundheitsprüfung finden Sie unter [the section called „Zustandsprüfungseinstellungen“](#).

Console

So aktualisieren Sie die Einstellungen für die Zustandsprüfung

1. Öffnen Sie die Amazon-EC2-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. Wählen Sie in der Registerkarte Health checks (Zustandsprüfungen) die Option Edit (Bearbeiten) aus.
5. Ändern Sie auf der Seite Einstellungen für die Integritätsprüfung bearbeiten die Einstellungen nach Bedarf.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Einstellungen für die Gesundheitsprüfung zu aktualisieren

Verwenden Sie den Befehl [modify-target-group](#). Im folgenden Beispiel werden die HealthCheckTimeoutSeconds-Einstellungen HealthyThresholdCount und aktualisiert.

```
aws elbv2 modify-target-group \  
  --target-group-arn target-group-arn \  
  --healthy-threshold-count 3 \  
  --health-check-timeout-seconds 20
```

CloudFormation

Um die Einstellungen für die Gesundheitsprüfung zu aktualisieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie die aktualisierten Einstellungen für die Integritätsprüfung enthält. Im folgenden Beispiel werden die HealthCheckTimeoutSeconds-Einstellungen HealthyThresholdCount und aktualisiert.

```
Resources:  
  myTargetGroup:  
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'  
    Properties:  
      Name: my-target-group  
      Protocol: TCP
```

```
Port: 80
TargetType: instance
VpcId: !Ref myVPC
HealthyThresholdCount: 3
HealthCheckTimeoutSeconds: 20
```

Zielgruppenattribute für Ihren Network Load Balancer bearbeiten

Nachdem Sie eine Zielgruppe für Ihren Network Load Balancer erstellt haben, können Sie dessen Zielgruppenattribute bearbeiten.

Zielgruppenattribute

- [Client-IP-Erhaltung](#)
- [Verzögerung der Registrierungsaufhebung](#)
- [Proxy-Protokoll](#)
- [Sticky Sessions](#)
- [Zonenübergreifendes Load Balancing für Zielgruppen](#)
- [Verbindungsabbruch für fehlerhafte Ziele](#)
- [Ungesundes Entleerungsintervall](#)

Client-IP-Erhaltung

Network Load Balancer können die Quell-IP-Adressen von Clients beibehalten, wenn Anfragen an Backend-Ziele weitergeleitet werden. Wenn Sie die Client-IP-Erhaltung deaktivieren, ist die Quell-IP-Adresse die private IP-Adresse des Network Load Balancer.

Standardmäßig ist die Client-IP-Erhaltung für Instance- und IP-Typ-Zielgruppen mit den Protokollen UDP, TCP_UDP, QUIC und TCP_QUIC aktiviert (und kann nicht deaktiviert werden). Sie können jedoch die Client-IP-Erhaltung für TCP- und TLS-Zielgruppen mithilfe des Zielgruppenattributs `preserve_client_ip.enabled` aktivieren oder deaktivieren.

Standardeinstellungen

- Instance-Typ-Zielgruppen: Aktiviert
- Zielgruppen vom Typ IP (UDP, TCP_UDP, QUIC, TCP_QUIC): Aktiviert
- IP-Typ-Zielgruppen (TCP, TLS): Deaktiviert

Wenn die Client-IP-Erhaltung aktiviert ist

In der folgenden Tabelle werden die IP-Adressen beschrieben, die Ziele erhalten, wenn die Client-IP-Erhaltung aktiviert ist.

Ziele	IPv4 Client-Anfragen	IPv6 Kundenanfragen
Instanztyp (IPv4)	IPv4 Adresse des Kunden	Adresse des Load Balancers IPv4
IP-Typ () IPv4	IPv4 Adresse des Kunden	Adresse des Load Balancers IPv4
IP-Typ () IPv6	Adresse des Load Balancers IPv6	Adresse des Kunden IPv6

Wenn die Client-IP-Erhaltung deaktiviert ist

In der folgenden Tabelle werden die IP-Adressen beschrieben, die Ziele erhalten, wenn die Client-IP-Erhaltung deaktiviert ist.

Ziele	IPv4 Client-Anfragen	IPv6 Kundenanfragen
Instanztyp (IPv4)	Adresse des Load Balancers IPv4	Adresse des Load Balancers IPv4
IP-Typ () IPv4	Adresse des Load Balancers IPv4	Adresse des Load Balancers IPv4
IP-Typ () IPv6	Adresse des Load Balancers IPv6	Adresse des Load Balancers IPv6

Anforderungen und Überlegungen

- Änderungen an der Client-IP-Erhaltung werden nur für neue TCP-Verbindungen wirksam.
- Wenn die Client-IP-Erhaltung aktiviert ist, muss der Datenverkehr direkt vom Network Load Balancer zum Ziel fließen. Das Ziel muss sich in derselben VPC wie der Load Balancer oder in einer Peer-VPC in derselben Region befinden.

- Die Beibehaltung der Client-IP wird nicht unterstützt, wenn Ziele über ein Transit-Gateway erreicht werden.
- Client-IP-Erhaltung wird nicht unterstützt, wenn ein Gateway Load Balancer-Endpunkt verwendet wird, um den Verkehr zwischen dem Network Load Balancer und dem Ziel (Instanz oder IP-Adresse) zu untersuchen, auch wenn sich das Ziel in derselben VPC wie der Network Load Balancer befindet.
- Die folgenden Instance-Typen unterstützen die Aufbewahrung von Client-IP nicht: C1,,, CC1, CC2, CG1, G1 CG2 CR1, G2,,, M1 HI1 HS1, M2, M3 und T1. Wir empfehlen, diese Instance-Typen als IP-Adressen zu registrieren, wobei die Client-IP-Erhaltung deaktiviert ist.
- Die Client-IP-Erhaltung hat keine Auswirkung auf den eingehenden Datenverkehr von AWS PrivateLink. Die Quell-IP-Adresse des AWS PrivateLink Datenverkehrs ist immer die private IP-Adresse des Network Load Balancer.
- Client-IP-Erhaltung wird nicht unterstützt, wenn eine Zielgruppe AWS PrivateLink Netzwerkschnittstellen oder die Netzwerkschnittstelle eines anderen Network Load Balancer enthält. Dies führt zu einem Verlust der Kommunikation mit diesen Zielen.
- Die Beibehaltung der Client-IP hat keine Auswirkung auf den Verkehr, der von IPv6 in konvertiert wurde IPv4. Die Quell-IP-Adresse dieses Verkehrstyps ist immer die private IP-Adresse des Network Load Balancer.
- Wenn Sie Ziele nach Application-Load-Balancer-Typ angeben, wird die Client-IP des gesamten eingehenden Datenverkehrs vom Network Load Balancer beibehalten und an den Application Load Balancer gesendet. Der Application Load Balancer fügt dann die Client-IP an den Header der X-Forwarded-For-Anforderung an, bevor er sie an das Ziel sendet.
- NAT-Loopback, auch bekannt als Hairpinning, wird nicht unterstützt, wenn die Client-IP-Erhaltung aktiviert ist. Dies tritt auf, wenn interne Network Load Balancer verwendet werden und das hinter einem Network Load Balancer registrierte Ziel Verbindungen zu demselben Network Load Balancer herstellt. Die Verbindung kann an das Ziel weitergeleitet werden, das versucht, die Verbindung herzustellen, was zu Verbindungsfehlern führt. Wir empfehlen, keine Verbindung zu einem Network Load Balancer von Zielen aus herzustellen, die sich hinter demselben Network Load Balancer befinden. Alternativ können Sie diese Art von Verbindungsfehlern auch verhindern, indem Sie die Client-IP-Erhaltung deaktivieren. Wenn Sie die Client-IP-Adresse benötigen, können Sie sie mithilfe des Proxyprotokolls v2 abrufen verwenden. Weitere Informationen finden Sie unter [Proxy-Protokoll](#).
- Wenn die Client-IP-Erhaltung deaktiviert ist, unterstützt ein Network Load Balancer 55 000 gleichzeitige Verbindungen oder etwa 55 000 Verbindungen pro Minute zu jedem einzelnen Ziel (IP-Adresse und Port). Wenn Sie diese Anzahl an Verbindungen überschreiten, besteht ein erhöhtes Risiko von Fehlern bei der Portzuweisung, was dazu führt, dass neue Verbindungen nicht

hergestellt werden können. Weitere Informationen finden Sie unter [Fehler bei der Portzuweisung für Back-End-Flows](#).

Console

Um die Aufbewahrung der Client-IP zu ändern

1. Öffnen Sie die Amazon-EC2-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 Attribute die Option Bearbeiten aus und suchen Sie den Bereich zur Konfiguration des Datenverkehrs.
5. Um die Client-IP-Erhaltung zu aktivieren, aktivieren Sie die Option Client-IP-Adressen beibehalten. Um die Client-IP-Erhaltung zu deaktivieren, deaktivieren Sie die Option Client-IP-Adressen beibehalten.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die IP-Erhaltung für den Client zu aktivieren

Verwenden Sie den Befehl [modify-target-group-attributes](#) mit dem Attribut `preserve_client_ip.enabled`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes "Key=preserve_client_ip.enabled,Value=true"
```

CloudFormation

Um die Erhaltung der Client-IP zu aktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie das `preserve_client_ip.enabled` Attribut enthält.

```
Resources:
```

```
myTargetGroup:
  Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
  Properties:
    Name: my-target-group
    Protocol: TCP
    Port: 80
    TargetType: ip
    VpcId: !Ref myVPC
    TargetGroupAttributes:
      - Key: "preserve_client_ip.enabled"
        Value: "true"
```

Verzögerung der Registrierungsaufhebung

Wenn die Registrierung eines Ziels aufgehoben wird, stellt der Load Balancer keine neuen Verbindungen zum Ziel her. Der Load Balancer stellt mit Connection Draining sicher, dass in Übertragung befindlicher Datenverkehr auf den vorhandenen Verbindungen abgeschlossen wird. Wenn das Ziel mit aufgehobener Registrierung fehlerfrei bleibt und sich eine vorhandene Verbindung nicht im Leerlauf befindet, kann der Load Balancer mit dem Senden von Datenverkehr an das Ziel fortfahren. Um sicherzustellen, dass bestehende Verbindungen geschlossen werden, können Sie eine der folgenden Maßnahmen ergreifen: Aktivieren Sie das Zielgruppenattribut für die Beendigung von Verbindungen, stellen Sie sicher, dass die Instance fehlerbehaftet ist, bevor Sie sie deregistrieren, oder schließen Sie regelmäßig Client-Verbindungen.

Der Ausgangszustand eines Ziels, dessen Registrierung aufgehoben wird `draining`, ist, dass das Ziel keine neuen Verbindungen mehr empfängt. Aufgrund von Verzögerungen bei der Übertragung der Konfiguration kann das Ziel jedoch weiterhin Verbindungen empfangen. Standardmäßig ändert der Load Balancer den Status eines Ziels, dessen Registrierung aufgehoben wird, nach 300 Sekunden in `unused`. Wenn Sie die Zeitspanne ändern möchten, die der Load Balancer wartet, bevor er den Status eines Ziels, dessen Registrierung aufgehoben wird, in `unused` ändert, aktualisieren Sie den Wert für die Verzögerung der Registrierungsaufhebung. Wir empfehlen, einen Wert von mindestens 120 Sekunden anzugeben, um sicherzustellen, dass die Anfragen abgeschlossen sind. Für QUIC-Verkehr beträgt der Wert immer 300 Sekunden und kann nicht angepasst werden.

Wenn Sie das Zielgruppenattribut für den Verbindungsabbruch aktivieren, werden Verbindungen zu abgemeldeten Zielen kurz nach Ablauf des Abmelde-Timeouts geschlossen.

Console

Um die Attribute für die Verzögerung bei der Abmeldung zu ändern

1. Öffnen Sie die Amazon-EC2-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 Attribute auf Bearbeiten.
5. Um das Zeitlimit für die Abmeldung zu ändern, geben Sie einen neuen Wert für die Abmeldeverzögerung ein. Um sicherzustellen, dass bestehende Verbindungen geschlossen werden, nachdem Sie Ziele abgemeldet haben, wählen Sie Verbindungen bei Aufhebung der Registrierung beenden aus.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Attribute für die Verzögerung bei der Abmeldung zu ändern

Verwenden Sie den [modify-target-group-attributes](#) Befehl mit den Attributen `deregistration_delay.timeout_seconds` und `deregistration_delay.connection_termination.enabled`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes \  
    "Key=deregistration_delay.timeout_seconds,Value=60" \  
    "Key=deregistration_delay.connection_termination.enabled,Value=true"
```

CloudFormation

Um die Attribute für die Verzögerung bei der Abmeldung zu ändern

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie die Attribute `deregistration_delay.timeout_seconds` und `deregistration_delay.connection_termination.enabled` enthält.

```
Resources:
```

```
myTargetGroup:
  Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
  Properties:
    Name: my-target-group
    Protocol: TCP
    Port: 80
    TargetType: ip
    VpcId: !Ref myVPC
    TargetGroupAttributes:
      - Key: "deregistration_delay.timeout_seconds"
        Value: "60"
      - Key: "deregistration_delay.connection_termination.enabled"
        Value: "true"
```

Proxy-Protokoll

Network Load Balancers verwenden die Proxy-Protokoll-Version 2 zum Senden zusätzlicher Verbindungsinformationen, z. B. Quell- und Zieladresse. Proxy-Protokoll-Version 2 bietet eine binäre Codierung des Proxy-Protokoll-Headers.

Mit TCP-Listeners stellt der Load Balancer den TCP-Daten einen Proxy-Protokoll-Header voran. Es werden keine vorhandenen Daten verworfen oder überschreiben, auch keine eingehenden, vom Client gesendeten Proxy-Protokoll-Header oder andere Proxys, Load Balancers oder Server im Netzwerkpfad. Deshalb kann mehr als ein Proxy-Protokoll-Header empfangen werden. Auch wenn es außerhalb Ihres Network Load Balancers einen anderen Netzwerkpfad zu Ihren Zielen gibt, ist der erste Proxyprotokoll-Header möglicherweise nicht der vom Load Balancer.

TLS-Listener unterstützen keine eingehenden Verbindungen mit Proxyprotokoll-Headern, die vom Client oder anderen Proxys gesendet werden.

QUIC-Verkehr unterstützt die Version 2 des Proxyprotokolls nicht.

Wenn Sie Ziele nach IP-Adressen angeben, hängen die Quell-IP-Adressen, die Ihren Anwendungen zur Verfügung gestellt werden, wie folgt vom Protokoll der Zielgruppe ab:

- TCP und TLS: Standardmäßig ist die Client-IP-Erhaltung deaktiviert, und die Quell-IP-Adressen, die Ihren Anwendungen zur Verfügung gestellt werden, sind die privaten IP-Adressen der Load Balancer-Knoten. Um die IP-Adresse des Clients beizubehalten, stellen Sie sicher, dass sich das Ziel innerhalb derselben VPC oder einer Peer-VPC befindet, und aktivieren Sie die Client-IP-Erhaltung. Wenn Sie die IP-Adresse des Clients benötigen und diese Bedingungen nicht erfüllt

sind, aktivieren Sie das Proxyprotokoll und rufen Sie die Client-IP-Adresse aus dem Proxyprotokoll-Header ab.

- **UDP und TCP_UDP:** Die Quell-IP-Adressen sind die IP-Adressen der Clients, da die Client-IP-Erhaltung für diese Protokolle standardmäßig aktiviert ist und nicht deaktiviert werden kann. Wenn Sie Ziele unter Verwendung der Instance-ID angeben, sind die für Ihre Anwendungen bereitgestellten Quell-IP-Adressen die Client-IP-Adressen. Wenn Sie dies bevorzugen, können Sie jedoch auch das Proxy-Protokoll aktivieren und die Client-IP-Adressen aus dem Proxy-Protokoll-Header abrufen.

Zustandsprüfungsverbindungen

Nachdem Sie das Proxy-Protokoll aktiviert haben, ist der Proxy-Protokoll-Header auch in Zustandsprüfungsverbindungen vom Load Balancer enthalten. Bei Zustandsprüfungsverbindungen werden die Client-Verbindungsinformationen jedoch nicht im Proxy-Protokoll-Header gesendet.

Ziele können die Integritätsprüfungen nicht bestehen, wenn sie den Proxyprotokoll-Header nicht analysieren können. Sie könnten beispielsweise den folgenden Fehler zurückgeben: HTTP 400: Schlechte Anfrage.

VPC-Endpunkt-Services

Für Datenverkehr, der von Servicenutzern über einen [VPC-Endpunkt-Service](#) eingeht, sind die für Ihre Anwendungen bereitgestellten Quell-IP-Adressen die privaten IP-Adressen der Load Balancer-Knoten. Wenn Ihre Anwendungen die IP-Adressen der Servicenutzer benötigen, aktivieren Sie das Proxy-Protokoll und rufen Sie sie aus dem Proxy-Protokoll-Header ab.

Der Proxy-Protokoll-Header enthält außerdem die ID des Endpunkts. Diese Informationen werden mithilfe eines benutzerdefinierten Vektors Type-Length-Value (TLV) wie folgt codiert.

Feld	Länge (in Oktetten)	Description
Typ	1	PP2_TYPE_AWS (0xEA)
Länge	2	Die Länge des Wertes
Wert	1	PP2_UNTERTYP_ (0x01) AWS_VPCE_ID

Feld	Länge (in Oktetten)	Description
	variabel (Wertlänge minus 1)	Die ID des Endpunkts

Ein Beispiel, das den TLV-Typ 0xEA analysiert, finden Sie unter/. <https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot>

Aktivierung des Proxy-Protokolls

Bevor Sie das Proxy-Protokoll bei einer Zielgruppe aktivieren, stellen Sie sicher, dass Ihre Anwendungen den Proxy-Protokoll-Header Version 2 erwarten und parsen können, da die Aktion andernfalls fehlschlagen kann. Weitere Informationen finden Sie unter [PROXY-Protokoll-Versionen 1 und 2](#).

Console

Um die Version 2 des Proxyprotokolls zu aktivieren

1. Öffnen Sie die Amazon-EC2-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, um deren Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie auf der Seite Attribute bearbeiten die Option Proxyprotokoll v2 aus.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um die Version 2 des Proxyprotokolls zu aktivieren

Verwenden Sie den Befehl [modify-target-group-attributes](#) mit dem Attribut `proxy_protocol_v2.enabled`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes "Key=proxy_protocol_v2.enabled,Value=true"
```

CloudFormation

Um die Version 2 des Proxyprotokolls zu aktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie das `proxy_protocol_v2.enabled` Attribut enthält.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "proxy_protocol_v2.enabled"
          Value: "true"
```

Sticky Sessions

Sticky Sessions sind ein Mechanismus, um Clientdatenverkehr an dasselbe Ziel in einer Zielgruppe weiterzuleiten. Dies ist nützlich für Server, die Zustandsinformationen verwalten, um Clients eine kontinuierliche Erfahrung zu bieten.

Überlegungen

- Die Verwendung von Sticky Sessions kann zu einer ungleichmäßigen Verteilung der Verbindungen und Flows führen, was sich auf die Verfügbarkeit Ihrer Ziele auswirken kann. Beispielsweise haben alle Clients hinter demselben NAT-Gerät dieselbe Quell-IP-Adresse. Daher wird der gesamte Datenverkehr von diesen Clients an dasselbe Ziel weitergeleitet.
- Der Load Balancer kann die Sticky Sessions für eine Zielgruppe zurücksetzen, wenn sich der Integritätsstatus eines seiner Ziele ändert oder wenn Sie Ziele für die Zielgruppe registrieren oder abmelden.
- Wenn das Stickiness-Attribut für eine Zielgruppe aktiviert ist, werden passive Zustandsprüfungen nicht unterstützt. Weitere Informationen finden Sie unter [Gesundheitschecks für Ihre Zielgruppen](#).
- Sticky Sessions werden für TLS- oder QUIC-Listener nicht unterstützt.

Console

Um Sticky Sessions zu aktivieren

1. Öffnen Sie die Amazon-EC2-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 in der Registerkarte Attribute auf Bearbeiten.
5. Aktivieren Sie unter Konfiguration der Zielauswahl die Option Stickiness.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um Sticky Sessions zu aktivieren

Verwenden Sie den Befehl [modify-target-group-attributes](#) mit dem Attribut `stickiness.enabled`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes "Key=stickiness.enabled,Value=true"
```

CloudFormation

Um Sticky Sessions zu aktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie das `stickiness.enabled` Attribut enthält.

```
Resources:  
  myTargetGroup:  
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'  
    Properties:  
      Name: my-target-group  
      Protocol: TCP  
      Port: 80  
      TargetType: ip  
      VpcId: !Ref myVPC  
      TargetGroupAttributes:
```

```
- Key: "stickiness.enabled"  
  Value: "true"
```

Zonenübergreifendes Load Balancing für 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 Ausfalldomains regionalen vorzuziehen sind, um sicherzustellen, dass eine fehlerfreie Zone nicht von einer fehlerhaften Zone beeinträchtigt wird, oder um die allgemeine Latenz zu verbessern.

Bei Network Load Balancers ist der zonenübergreifende Load Balancing standardmäßig auf Load Balancer-Ebene deaktiviert, Sie können ihn jedoch jederzeit aktivieren. Für Zielgruppen wird standardmäßig die Load Balancer-Einstellung verwendet. Sie können die Standardeinstellung jedoch überschreiben, indem Sie den zonenübergreifenden Load Balancing auf Zielgruppenebene explizit aktivieren oder deaktivieren.

Überlegungen

- Wenn Sie den zonenübergreifenden Load Balancing für einen Network Load Balancer aktivieren, fallen EC2-Datenübertragungsgebühren an. Weitere Informationen finden Sie im [Data Exports User Guide unter Grundlegendes zu AWS Datenübertragungsgebühren](#)
- Die Zielgruppeneinstellung bestimmt das Load-Balancing-Verhalten für die Zielgruppe. Wenn beispielsweise zonenübergreifendes Load Balancing auf Load-Balancer-Ebene aktiviert und auf Zielgruppenebene deaktiviert ist, wird der an die Zielgruppe gesendete Datenverkehr nicht über Availability Zones geleitet.
- Wenn der zonenübergreifende Lastenausgleich deaktiviert ist, stellen Sie sicher, dass Sie in jeder der Availability Zones des Load Balancers über genügend Zielkapazität verfügen, damit jede Zone ihre zugeordnete Arbeitslast bedienen kann.
- Wenn der zonenübergreifende Lastenausgleich deaktiviert ist, stellen Sie sicher, dass alle Zielgruppen denselben Availability Zones angehören. Eine leere Availability Zone wird als fehlerhaft angesehen.
- Sie können den zonenübergreifenden Load Balancing auf Zielgruppenebene aktivieren oder deaktivieren, wenn der Zielgruppentyp `alb` ist.

erbt die Zielgruppe immer die Einstellung für das zonenübergreifende Load Balancing vom Load Balancer.

Weitere Informationen zur Aktivierung des zonenübergreifenden Load Balancing auf Load Balancer-Ebene finden Sie unter. [the section called “Zonenübergreifendes Load Balancing”](#)

Console

So aktivieren Sie den zonenübergreifenden Load Balancing für eine Zielgruppe

1. Öffnen Sie die Amazon-EC2-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 in der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie auf der Seite Zielgruppenattribute bearbeiten die Option An für zonenübergreifendes Load Balancing aus.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um den zonenübergreifenden Lastenausgleich für eine Zielgruppe zu aktivieren

Verwenden Sie den Befehl [modify-target-group-attributes](#) mit dem Attribut `load_balancing.cross_zone.enabled`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Um den zonenübergreifenden Lastenausgleich für eine Zielgruppe zu aktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie das `load_balancing.cross_zone.enabled` Attribut enthält.

```
Resources :
```

```
myTargetGroup:
  Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
  Properties:
    Name: my-target-group
    Protocol: TCP
    Port: 80
    TargetType: ip
    VpcId: !Ref myVPC
    TargetGroupAttributes:
      - Key: "load_balancing.cross_zone.enabled"
        Value: "true"
```

Verbindungsabbruch für fehlerhafte Ziele

Der Verbindungsabbruch ist standardmäßig aktiviert. Wenn das Ziel eines Network Load Balancer die konfigurierten Integritätsprüfungen nicht besteht und als fehlerhaft eingestuft wird, beendet der Load Balancer bestehende Verbindungen und beendet das Routing neuer Verbindungen zum Ziel. Wenn der Verbindungsabbruch deaktiviert ist, gilt das Ziel immer noch als fehlerhaft und empfängt keine neuen Verbindungen. Etablierte Verbindungen bleiben jedoch aktiv, sodass sie problemlos geschlossen werden können.

Der Verbindungsabbruch für fehlerhafte Ziele wird auf Zielgruppenebene konfiguriert.

Console

Um das Attribut für den Verbindungsabbruch zu ändern

1. Öffnen Sie die Amazon-EC2-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 in der Registerkarte Attribute auf Bearbeiten.
5. Wählen Sie unter Verwaltung des fehlerhaften Zustands von Zielen aus, ob die Option Verbindungen beenden, wenn Ziele fehlerhaft werden aktiviert oder deaktiviert sein soll.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Um das Attribut für den Verbindungsabbruch zu deaktivieren

Verwenden Sie den Befehl [modify-target-group-attributes](#) mit dem Attribut `target_health_state.unhealthy.connection_termination.enabled`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes  
  "Key=target_health_state.unhealthy.connection_termination.enabled,Value=false"
```

CloudFormation

Um das Verbindungsabbruchattribut zu deaktivieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource, sodass sie das `target_health_state.unhealthy.connection_termination.enabled` Attribut enthält.

```
Resources:  
  myTargetGroup:  
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'  
    Properties:  
      Name: my-target-group  
      Protocol: TCP  
      Port: 80  
      TargetType: ip  
      VpcId: !Ref myVPC  
      TargetGroupAttributes:  
        - Key: "target_health_state.unhealthy.connection_termination.enabled"  
          Value: "false"
```

Ungesundes Entleerungsintervall

Ziele in diesem `unhealthy.draining` Status gelten als fehlerhaft, empfangen keine neuen Verbindungen, behalten aber bestehende Verbindungen für das konfigurierte Intervall bei. Das Verbindungsintervall für fehlerhafte Verbindungen bestimmt, wie lange das Ziel in dem `unhealthy.draining` Status verbleibt, bevor dieser Status erreicht wird. `unhealthy` Wenn das Ziel während des Verbindungsintervalls für fehlerhafte Verbindungen die Zustandsprüfungen bestanden hat, wird `healthy` es wieder in den Status versetzt. Wenn eine Abmeldung ausgelöst wird, wird der Status des Ziels geändert `draining` und das Zeitlimit für die Abmeldeverzögerung beginnt.

Anforderung

Der Verbindungsabbruch muss deaktiviert werden, bevor ein fehlerhaftes Entladeintervall aktiviert wird.

Console

Um das Intervall für fehlerhafte Entleerungen zu ändern

1. Öffnen Sie die Amazon-EC2-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. Vergewissern Sie sich, dass unter Verwaltung von fehlerhaftem Zielstatus die Option Verbindungen beenden, wenn Ziele fehlerhaft werden deaktiviert ist.
6. Geben Sie einen Wert für Intervall für fehlerhafte Entleerung ein.
7. Wählen Sie Änderungen speichern aus.

AWS CLI

Um das Intervall für fehlerhafte Entleerungen zu ändern

Verwenden Sie den Befehl [modify-target-group-attributes](#) mit dem Attribut `target_health_state.unhealthy.draining_interval_seconds`.

```
aws elbv2 modify-target-group-attributes \  
  --target-group-arn target-group-arn \  
  --attributes  
  "Key=target_health_state.unhealthy.draining_interval_seconds,Value=60"
```

CloudFormation

Um das Intervall für fehlerhafte Entleerungen zu ändern

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie das `target_health_state.unhealthy.draining_interval_seconds` Attribut enthält.

```
Resources:  
  myTargetGroup:  
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'  
    Properties:  
      Name: my-target-group
```

```
Protocol: TCP
Port: 80
TargetType: ip
VpcId: !Ref myVPC
TargetGroupAttributes:
  - Key: "target_health_state.unhealthy.draining_interval_seconds"
    Value: "60"
```

Registrieren Sie Ziele für Ihren Network Load Balancer

Wenn Ihr Ziel dazu bereit ist, Anforderungen zu bearbeiten, registrieren Sie es bei mindestens einer Zielgruppe. Der Zieltyp der Zielgruppe legt fest, wie Sie Ziele registrieren. Sie können beispielsweise eine Instanz IDs, IP-Adressen oder einen Application Load Balancer registrieren. Ihr Network Load Balancer beginnt mit der Weiterleitung von Anforderungen an die Ziele, sobald der Registrierungsprozess abgeschlossen ist und die Ziele die ersten Zustandsprüfungen bestanden haben. Es kann einige Minuten dauern, bis der Registrierungsprozess abgeschlossen ist und die Zustandsprüfungen gestartet werden. Weitere Informationen finden Sie unter [Zustandsprüfungen für Zielgruppen von Network Load Balancer](#).

Wenn die Nachfrage nach Ihren aktuell registrierten Zielen steigt, können Sie zusätzliche Ziele registrieren, um die Nachfrage zu bewältigen. Wenn der Bedarf an Ihren registrierten Zielen abnimmt, können Sie Ziele aus Ihrer Zielgruppe abmelden. Es kann einige Minuten dauern, bis der Abmeldevorgang abgeschlossen ist und der Load Balancer Routinganfragen an das Ziel einstellt. Wenn der Bedarf nachträglich steigt, können Sie Ziele, die Sie bei der Zielgruppe abgemeldet haben, erneut registrieren. Muss ein Ziel gewartet werden, können Sie es abmelden und dann erneut registrieren, wenn die Wartung abgeschlossen ist.

Wenn Sie die Registrierung eines Ziels aufheben, wartet Elastic Load Balancing, bis die laufenden Anforderungen abgeschlossen sind. Dies wird als Connection Draining bezeichnet. Der Status eines Ziels ist `draining`, während Connection Draining erfolgt. Nach Aufheben der Registrierung ändert sich der Status des Ziels in `unused`. Weitere Informationen finden Sie unter [Verzögerung der Registrierungsaufhebung](#).

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 den Load Balancer von der Auto-Scaling-Gruppe trennen, wird die Registrierung der Instances bei der Zielgruppe automatisch

aufgehoben. Weitere Informationen finden Sie unter [Anhängen eines Load Balancers an Ihre Auto-Scaling-Gruppe](#) im Benutzerhandbuch zu Auto Scaling in Amazon EC2.

Inhalt

- [Zielsicherheitsgruppen](#)
- [Netzwerk ACLs](#)
- [Gemeinsam genutzte Subnetze](#)
- [Ziele registrieren](#)
- [Ziele deregistrieren](#)

Zielsicherheitsgruppen

Bevor Sie Ziele zu Ihrer Zielgruppe hinzufügen, konfigurieren Sie die mit den Zielen verknüpften Sicherheitsgruppen so, dass sie Datenverkehr von Ihrem Network Load Balancer akzeptieren.

Empfehlungen für Zielsicherheitsgruppen, wenn dem Load Balancer eine Sicherheitsgruppe zugeordnet ist

- Um Client-Datenverkehr zuzulassen: Fügen Sie eine Regel hinzu, die auf die Sicherheitsgruppe verweist, die dem Load Balancer zugeordnet ist.
- Um PrivateLink Datenverkehr zuzulassen: Wenn Sie den Load Balancer so konfiguriert haben, dass er eingehende Regeln für den durchgehenden Datenverkehr auswertet AWS PrivateLink, fügen Sie eine Regel hinzu, die den Datenverkehr von der Load Balancer-Sicherheitsgruppe am Verkehrsport akzeptiert. Fügen Sie andernfalls eine Regel hinzu, die Datenverkehr von den privaten IP-Adressen des Load Balancers am Datenverkehrsport akzeptiert.
- Um Load Balancer-Zustandsprüfungen zu akzeptieren: Fügen Sie eine Regel hinzu, die Zustandsprüfungsverkehr von den Load-Balancer-Sicherheitsgruppen am Zustandsprüfport akzeptiert.

Empfehlungen für Zielsicherheitsgruppen, wenn dem Load Balancer keine Sicherheitsgruppe zugeordnet ist

- Um Client-Datenverkehr zuzulassen: Wenn Ihr Load Balancer Client-IP-Adressen beibehält, fügen Sie eine Regel hinzu, die Datenverkehr von den IP-Adressen zugelassener Clients am Datenverkehrsport akzeptiert. Fügen Sie andernfalls eine Regel hinzu, die Datenverkehr von den privaten IP-Adressen des Load Balancers am Datenverkehrsport akzeptiert.

- Um PrivateLink Datenverkehr zuzulassen: Fügen Sie eine Regel hinzu, die Datenverkehr von den privaten IP-Adressen des Load Balancers am Verkehrsport akzeptiert.
- Um Load-Balancer-Zustandsprüfungen zu akzeptieren: Fügen Sie eine Regel hinzu, die Zustandsprüfungsverkehr von privaten Adressen des Load Balancers am Zustandsprüfport akzeptiert.

So funktioniert die Beibehaltung von Client-IP-Adressen

Network Load Balancers behalten Client-IP-Adressen nur bei, wenn Sie das `preserve_client_ip.enabled`-Attribut auf `true` setzen. Außerdem funktioniert bei Dual-Stack-Netzwerk-Loadbalancern die Beibehaltung der Client-IP-Adressen nicht, wenn Adressen in oder in IPv4 Adressen übersetzt werden. IPv6 IPv6 IPv4 Die Beibehaltung von Client-IP-Adressen funktioniert nur, wenn Client- und Ziel-IP-Adressen beide oder beide sind. IPv4 IPv6

So finden Sie die privaten IP-Adressen des Load Balancers mithilfe der Konsole

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Geben Sie in das Suchfeld den Namen Ihres Network Load Balancer ein. Es gibt eine Netzwerkschnittstelle pro Load Balancer-Subnetz.
4. Kopieren Sie auf der Registerkarte Details für jede Netzwerkschnittstelle die Adresse aus Private IPv4 Adresse.

Weitere Informationen finden Sie unter [Aktualisieren Sie die Sicherheitsgruppen für Ihren Network Load Balancer](#).

Netzwerk ACLs

Wenn Sie EC2-Instances als Ziele registrieren, müssen Sie sicherstellen, dass das Netzwerk ACLs für die Subnetze Ihrer Instances Datenverkehr sowohl auf dem Listener-Port als auch auf dem Health Check-Port zulässt. Die standardmäßige Netzwerkzugriffskontrollliste (ACL) für eine VPC erlaubt den gesamten ein- und ausgehenden Datenverkehr. Wenn Sie ein benutzerdefiniertes Netzwerk erstellen ACLs, stellen Sie sicher, dass diese den entsprechenden Datenverkehr zulassen.

Das mit den Subnetzen für Ihre Instances ACLs verknüpfte Netzwerk muss den folgenden Datenverkehr für einen mit dem Internet verbundenen Load Balancer zulassen.

Empfohlene Regeln für Instance-Subnetze

Inbound

Quelle	Protocol (Protokoll)	Port Range (Port-Bereich)	Kommentar
<i>Client IP addresses</i>	<i>listener</i>	<i>target port</i>	Client-Verkehr zulassen (IP-Erhaltung:) ON
<i>VPC CIDR</i>	<i>listener</i>	<i>target port</i>	Client-Verkehr zulassen (IP-Erhaltung:OFF)
<i>VPC CIDR</i>	<i>health check</i>	<i>health check</i>	Zustandsüberprüfungsverkehr zulassen

Outbound

Ziel	Protocol (Protokoll)	Port Range (Port-Bereich)	Kommentar
<i>Client IP addresses</i>	<i>listener</i>	1024 - 65535	Rückverkehr zum Client zulassen (IP-Erhaltung:ON)
<i>VPC CIDR</i>	<i>listener</i>	1024 - 65535	Rückverkehr zum Client zulassen (IP-Erhaltung:OFF)
<i>VPC CIDR</i>	<i>health check</i>	1024 - 65535	Zustandsüberprüfungsverkehr zulassen

Das mit den Subnetzen für Ihren Load Balancer ACLs verknüpfte Netzwerk muss den folgenden Datenverkehr für einen mit dem Internet verbundenen Load Balancer zulassen.

Empfohlene Regeln für Load Balancer-Subnetze

Inbound

Quelle	Protocol (Protokoll)	Port Range (Port-Bereich)	Kommentar
<i>Client IP addresses</i>	<i>listener</i>	<i>listener</i>	Client-Verkehr zulassen
<i>VPC CIDR</i>	<i>listener</i>	1024 - 65535	Antwort vom Ziel zulassen
<i>VPC CIDR</i>	<i>health check</i>	1024 - 65535	Zustandsüberprüfungsverkehr zulassen
Outbound			
Ziel	Protocol (Protokoll)	Port Range (Port-Bereich)	Kommentar
<i>Client IP addresses</i>	<i>listener</i>	1024 - 65535	Antworten an Kunden zulassen
<i>VPC CIDR</i>	<i>listener</i>	<i>target port</i>	Anfragen an Ziele zulassen
<i>VPC CIDR</i>	<i>health check</i>	<i>health check</i>	Lassen Sie Ziele einen Gesundheitscheck zu

Bei einem internen Load Balancer muss das Netzwerk ACLs für die Subnetze für Ihre Instances und Load Balancer-Knoten sowohl eingehenden als auch ausgehenden Datenverkehr zum und vom VPC CIDR auf dem Listener-Port und den ephemeren Ports zulassen.

Gemeinsam genutzte Subnetze

Teilnehmer können einen Network 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.

Gemeinsam genutzte Subnetze für Network Load Balancer werden in allen Regionen unterstützt, mit Ausnahme von: AWS

- Asien-Pazifik (Osaka) ap-northeast-3
- Asien-Pazifik (Hongkong) ap-east-1
- Naher Osten (Bahrain) me-south-1
- AWS China (Peking) cn-north-1
- AWS China (Ningxia) cn-northwest-1

Ziele registrieren

Jede Zielgruppe muss mindestens ein registriertes Ziel in jeder Availability Zone haben, die für den Load Balancer aktiviert ist.

Der Zieltyp Ihrer Zielgruppe bestimmt, welche Ziele Sie registrieren können. Weitere Informationen finden Sie unter [Zieltyp](#). Verwenden Sie die folgenden Informationen, um Ziele für eine Zielgruppe vom Typ `instance` oder `ip` zu registrieren. Wenn der Zieltyp `alb` ist, finden Sie weitere Informationen unter [Verwenden Sie Application Load Balancers als Ziele](#).

Anforderungen und Überlegungen

- Die Instance muss sich bei der Registrierung im Status „running“ befinden.
- Sie können Instances nicht anhand der Instanz-ID registrieren, wenn sie einen der folgenden Instance-Typen verwenden: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, H1, HS1, M1, M2, M3 oder T1.
- Bei der Registrierung von Zielen anhand der Instanz-ID müssen sich die Instances in derselben VPC wie der Network Load Balancer befinden. Sie können Instances nicht nach Instance-ID registrieren, wenn sie sich in einer VPC befinden, die mit der Load-Balancer-VPC gekoppelt ist (dieselbe Region oder eine andere Region). Sie können diese Instances nach IP-Adresse registrieren.
- Bei der Registrierung von Zielen anhand der Instanz-ID für eine IPv6 Zielgruppe müssen die Ziele über eine zugewiesene IPv6 Primäradresse verfügen. Weitere Informationen finden Sie unter [IPv6 Adressen](#) im Amazon EC2 EC2-Benutzerhandbuch
- Wenn Sie Ziele anhand der IP-Adresse für eine IPv4 Zielgruppe registrieren, müssen die IP-Adressen, die Sie registrieren, aus einem der folgenden CIDR-Blöcke stammen:
 - Die Subnetze der Zielgruppe VPC
 - 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)
- Wenn Sie Ziele nach IP-Adresse für eine IPv6 Zielgruppe registrieren, müssen sich die IP-Adressen, die Sie registrieren, innerhalb des IPv6 VPC-CIDR-Blocks oder innerhalb des IPv6 CIDR-Blocks einer Peer-VPC befinden.
- Wenn Sie ein Ziel nach IP-Adresse registrieren und sich die IP-Adresse in derselben VPC wie der Load Balancer befindet, überprüft der Load Balancer, ob das Ziel zu einem Subnetz gehört, das es erreichen kann.
- Registrieren Sie Instances für die Zielgruppen UDP, TCP_UDP, QUIC und TCP_QUIC nicht anhand der IP-Adresse, wenn sie sich außerhalb der Load Balancer-VPC befinden oder einen der folgenden Instance-Typen verwenden: C1,,,,,,, G1, G2, CC1, CC2, M1 CG1 CG2, M2 CR1, M3 oder T1. H11 HS1 Ziele, die sich außerhalb der Load-Balancer-VPC befinden oder einen nicht unterstützten Instance-Typ verwenden, können möglicherweise Datenverkehr vom Load Balancer empfangen, dann aber nicht antworten.

Spezifische Anforderungen und Überlegungen zu QUIC

- Für alle Ziele, die für eine QUIC- oder TCP_QUIC-Zielgruppe registriert sind, muss eine Server-ID angegeben werden.
- IDs Der Server muss für alle Ziele, die in einem Network Load Balancer Balancer-Listener existieren, eindeutig sein.
- QUIC-Server IDs sind immer 8 Byte groß. Bei der Registrierung des Ziels muss die Server-ID in der Form angegeben werden, 0x gefolgt von 16 Hexadezimalzeichen.
- Sobald ein Ziel mit einer Server-ID registriert ist, ist die ID unveränderlich. Um eine Zielsever-ID zu ändern, muss sie zuerst deregistriert und dann mit der neuen Server-ID registriert werden.
- Eine Kombination aus Ziel-ID und Port muss eine Server-ID haben. Die Verwendung einer anderen Server-ID für dieselbe IP- oder Instance-ID- und Port-Kombination innerhalb derselben VPC wird nicht unterstützt.
- Vermeiden Sie es, dieselbe Server-ID innerhalb von 6 Stunden für ein anderes Ziel wiederzuverwenden.

Console

Um Ziele zu registrieren

1. Öffnen Sie die Amazon-EC2-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. Klicken Sie auf Register Targets (Ziele registrieren).
6. Wenn der Zieltyp der Zielgruppe wie folgt lautet `instance`, wählen Sie verfügbare Instances aus, überschreiben Sie bei Bedarf den Standardport und wählen Sie dann im Folgenden die Option Als ausstehend einbeziehen aus.
7. Wenn der Zieltyp der Zielgruppe lautet `ip`, wählen Sie für jede IP-Adresse das Netzwerk aus, geben Sie die IP-Adresse und die Ports ein und wählen Sie unten Als ausstehend einbeziehen aus.
8. Wenn der Zieltyp der Zielgruppe ist `alb`, überschreiben Sie bei Bedarf den Standardport und wählen Sie den Application Load Balancer aus. Weitere Informationen finden Sie unter [Verwenden Sie Application Load Balancers als Ziele](#).
9. Wenn das Protokoll der Zielgruppe QUIC oder TCP_QUIC ist, stellen Sie sicher, dass eine Server-ID angegeben ist.
10. Wählen Sie Ausstehende Ziele registrieren aus.

AWS CLI

Um Ziele zu registrieren

Verwenden Sie den Befehl [register-targets](#). Im folgenden Beispiel werden Ziele anhand der Instanz-ID registriert. Da der Port nicht angegeben ist, verwendet der Load Balancer den Zielgruppenport.

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

Im folgenden Beispiel werden Ziele anhand der IP-Adresse registriert. Da der Port nicht angegeben ist, verwendet der Load Balancer den Zielgruppenport.

```
aws elbv2 register-targets \
  --target-group-arn target-group-arn \
  --targets Id=10.0.50.10 Id=10.0.50.20
```

Im folgenden Beispiel wird ein Application Load Balancer als Ziel registriert.

```
aws elbv2 register-targets \
  --target-group-arn target-group-arn \
  --targets Id=application-load-balancer-arn
```

Im folgenden Beispiel werden Ziele in einer QUIC- oder TCP_QUIC-Zielgruppe registriert.

```
aws elbv2 register-targets \
  --target-group-arn target-group-arn \
  --targets Id=10.0.50.10,QuicServerId=0xa1b2c3d4e5f65890
  Id=10.0.50.20,QuicServerId=0xa1b2c3d4e5f65999
```

CloudFormation

Um Ziele zu registrieren

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie die neuen Ziele enthält. Im folgenden Beispiel werden zwei Ziele anhand der Instanz-ID registriert.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
```

Im folgenden Beispiel werden zwei Ziele anhand der Instanz-ID in einer QUIC- oder TCP_QUIC-Protokollzielgruppe registriert.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65999
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65000
```

Ziele deregistrieren

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 Datenverkehr an ein Ziel, sobald die Registrierung des Ziels aufgehoben wird. Das Ziel wechselt in den Zustand `draining`, bis laufende Anfragen abgeschlossen wurden.

Console

Um Ziele abzumelden

1. Öffnen Sie die Amazon-EC2-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 Ziele die Ziele aus, die Sie entfernen möchten.
5. Wählen Sie Deregister.

AWS CLI

Um Ziele zu deregistrieren

Verwenden Sie den Befehl [deregister-targets](#). Im folgenden Beispiel werden zwei Ziele, die anhand der Instanz-ID registriert wurden, deregistriert.

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

Verwenden Sie einen Application Load Balancer als Ziel eines Network Load Balancer

Sie können eine Zielgruppe mit einem einzigen Application Load Balancer als Ziel erstellen und Ihren Network Load Balancer so konfigurieren, dass er Datenverkehr an diese weiterleitet. In diesem Szenario übernimmt der Application Load Balancer die Entscheidung über das Load Balancing, sobald der Datenverkehr ihn erreicht. Diese Konfiguration kombiniert die Features beider Load Balancers und bietet die folgenden Vorteile:

- Sie können das anforderungsbasierte Layer-7-Routing-Feature des Application Load Balancer in Kombination mit Funktionen verwenden, die der Network Load Balancer unterstützt, wie Endpunktservices (AWS PrivateLink) und statische IP-Adressen.
- Sie können diese Konfiguration für Anwendungen verwenden, die einen einzigen Endpunkt für Multiprotokolle benötigen, z. B. Medienservices, die HTTP für die Signalisierung und RTP für das Streamen von Inhalten verwenden.

Sie können dieses Feature mit einem internen oder mit dem Internet verbundenen Application Load Balancer als Ziel eines internen oder mit dem Internet verbundenen Network Load Balancers verwenden.

Überlegungen

- Sie können nur einen Application Load Balancer pro Zielgruppe registrieren.
- Um einen Application Load Balancer als Ziel eines Network Load Balancer zuzuordnen, müssen sich die Load Balancer in derselben VPC innerhalb desselben Kontos befinden.

- Sie können einen Application Load Balancer als Ziel von bis zu zwei Network Load Balancern zuordnen. Registrieren Sie dazu den Application Load Balancer mit einer eigenen Zielgruppe für jeden Network Load Balancer.
- Jeder Application Load Balancer, den Sie bei einem Network Load Balancer registrieren, verringert die maximale Anzahl von Zielen pro Availability Zone pro Network Load Balancer um 50. Sie können zonenübergreifendes Load Balancing in beiden Load Balancern deaktivieren, um die Latenz zu minimieren und regionale Datenübertragungsgebühren zu vermeiden. Weitere Informationen finden Sie unter [Kontingente für Ihre Network Load Balancers](#).
- Wenn der Zielgruppentyp `alb` ist, können Sie die Zielgruppenattribute nicht ändern. Diese Attribute verwenden immer ihre Standardwerte.
- Nachdem Sie einen Application Load Balancer als Ziel registriert haben, können Sie den Application Load Balancer erst löschen, wenn Sie ihn für alle Zielgruppen abgemeldet haben.
- Die Kommunikation zwischen einem Network Load Balancer und einem Application Load Balancer verwendet immer IPv4

Aufgaben

- [Voraussetzung](#)
- [Schritt 1: Erstellen Sie eine Zielgruppe des Typs alb](#)
- [Schritt 2: Erstellen Sie einen Network Load Balancer und konfigurieren Sie das Routing](#)
- [Schritt 3: \(Optional\) Erstellen Sie einen VPC-Endpunktdienst](#)

Voraussetzung

Wenn Sie noch keinen Application Load Balancer haben, den Sie als Ziel verwenden können, erstellen Sie den Load Balancer, seine Listener und seine Zielgruppen. Weitere Informationen finden Sie unter [Erstellen eines Application Load Balancer](#) im Benutzerhandbuch für Application Load Balancers.

Schritt 1: Erstellen Sie eine Zielgruppe des Typs alb

Erstellen Sie eine Zielgruppe des Typs `alb`. Sie können Ihren Application Load Balancer bei der Erstellung der Zielgruppe oder zu einem späteren Zeitpunkt als Ziel registrieren.

Console

Um eine Zielgruppe für einen Application Load Balancer als Ziel zu erstellen

1. Öffnen Sie die Amazon-EC2-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 im Bereich Grundkonfiguration unter Zieltyp auswählen die Option Application Load Balancer aus.
5. Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein.
6. Als Protokoll ist nur TCP zulässig. Wählen Sie den Port für Ihre Zielgruppe aus. Der Port für diese Zielgruppe muss mit dem Listener-Port des Application Load Balancer übereinstimmen. Wenn Sie einen anderen Port für diese Zielgruppe wählen, können Sie den Listener-Port auf dem Application Load Balancer entsprechend aktualisieren.
7. Wählen Sie für VPC die Virtual Private Cloud (VPC) für die Zielgruppe aus. Dies muss dieselbe VPC sein, die vom Application Load Balancer verwendet wird.
8. Wählen Sie für Zustandsprüfungen HTTP oder HTTPS als Zustandsprüfungsprotokoll. Zustandsprüfungen werden an den Application Load Balancer gesendet und über den angegebenen Port, das angegebene Protokoll und den angegebenen Ping-Pfad an seine Ziele weitergeleitet. Stellen Sie sicher, dass Ihr Application Load Balancer diese Zustandsprüfungen empfangen kann, indem Sie einen Listener mit einem Port und einem Protokoll verwenden, die dem Port und dem Protokoll für die Zustandsprüfung entsprechen.
9. (Optional) Erweitern Sie Tags. Wählen Sie für jedes Tag die Option Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
10. Wählen Sie Weiter aus.
11. Wenn Sie bereit sind, den Application Load Balancer zu registrieren, wählen Sie Jetzt registrieren, überschreiben Sie bei Bedarf den Standardport und wählen Sie den Application Load Balancer aus. Der Application Load Balancer muss einen Listener auf demselben Port wie die Zielgruppe haben. Sie können auf diesem Load Balancer einen Listener hinzufügen oder bearbeiten, sodass er dem Zielgruppenport entspricht, oder Sie können zum vorherigen Schritt zurückkehren und den Port für die Zielgruppe ändern.

Wenn Sie noch nicht bereit sind, den Application Load Balancer als Ziel zu registrieren, wählen Sie [Später registrieren](#) und registrieren Sie das Ziel später. Weitere Informationen finden Sie unter [the section called "Ziele registrieren"](#).

12. Wählen Sie Zielgruppe erstellen aus.

AWS CLI

Um eine Zielgruppe vom Typ zu erstellen alb

Verwenden Sie den Befehl [create-target-group](#). Das Protokoll muss TCP sein und der Port muss mit dem Listener-Port des Application Load Balancer übereinstimmen.

```
aws elbv2 create-target-group \  
  --name my-target-group \  
  --protocol TCP \  
  --port 80 \  
  --target-type alb \  
  --vpc-id vpc-1234567890abcdef0 \  
  --tags Key=department,Value=123
```

CloudFormation

Um eine Zielgruppe vom Typ zu erstellen alb

Definieren Sie eine Ressource des Typs [AWS::ElasticLoadBalancingV2::TargetGroup](#). Das Protokoll muss TCP sein und der Port muss mit dem Listener-Port des Application Load Balancer übereinstimmen.

```
Resources:  
  myTargetGroup:  
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'  
    Properties:  
      Name: my-target-group  
      Protocol: TCP  
      Port: 80  
      TargetType: alb  
      VpcId: !Ref myVPC  
      Tags:  
        - Key: 'department'  
          Value: '123'  
    Targets:
```

```
- Id: !Ref myApplicationLoadBalancer
  Port: 80
```

Schritt 2: Erstellen Sie einen Network Load Balancer und konfigurieren Sie das Routing

Wenn Sie den Network Load Balancer erstellen, können Sie die Standardaktion für die Weiterleitung von Datenverkehr an den Application Load Balancer konfigurieren.

Console

So erstellen Sie den Network Load Balancer

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie Load Balancer erstellen aus.
4. Wählen Sie im Bereich Network Load Balancer die Option Erstellen.
5. Basiskonfiguration
 - a. Geben Sie unter Load Balancer name einen Namen für Ihren Network Load Balancer ein.
 - b. Wählen Sie für Scheme (Schema) entweder Internet-facing (Mit dem Internet verbunden) oder Internal (Intern) aus. Ein mit dem Internet verbundener Network Load Balancer leitet Anfragen von Clients über das Internet an Ziele weiter. Ein interner Network Load Balancer leitet Anfragen über private IP-Adressen an Ziele weiter.
 - c. Wählen Sie für den Load Balancer-IP-Adresstyp aus, IPv4 ob Ihre Clients IPv4 Adressen für die Kommunikation mit dem Network Load Balancer oder Dualstack verwenden, wenn Ihre Clients beide verwenden, IPv4 und IPv6 Adressen für die Kommunikation mit dem Network Load Balancer verwenden.
6. Netzwerkzuordnung
 - a. Wählen Sie für VPC dieselbe VPC aus, die Sie für Ihren Application Load Balancer verwendet haben. Bei einem mit dem Internet verbundenen Load Balancer stehen nur Load Balancer VPCs mit Internet-Gateway zur Auswahl.
 - b. Wählen Sie für Availability Zones und Subnetze mindestens eine Availability Zones und wählen Sie ein Subnetz pro Zone aus. Wir empfehlen, dass Sie dieselben Availability

Zones auswählen, die für Ihren Application Load Balancer aktiviert sind. Dadurch werden Verfügbarkeit, Skalierung und Leistung optimiert.

(Optional) Um statische IP-Adressen zu verwenden, wählen Sie in den IPv4-Einstellungen für jede Availability Zone die Option Elastic IP-Adresse verwenden aus. Mit statischen IP-Adressen können Sie bestimmte IP-Adressen zu einer Zulassungsliste für Firewalls hinzufügen, oder Sie können IP-Adressen mit Clients fest codieren.

7. Sicherheitsgruppen

Wir wählen die Standardsicherheitsgruppe für die Load Balancer-VPC vorab aus. Sie können bei Bedarf zusätzliche Sicherheitsgruppen auswählen. Wenn Sie keine Sicherheitsgruppe haben, die Ihren Anforderungen entspricht, wählen Sie Neue Sicherheitsgruppe erstellen, um jetzt eine zu erstellen. Weitere Informationen finden Sie unter [Erstellen einer Sicherheitsgruppe](#) im Amazon-VPC-Benutzerhandbuch.

Warning

Wenn Sie Ihrem Network Load Balancer jetzt keine Sicherheitsgruppen zuordnen, können Sie sie später nicht mehr zuordnen.

Warning

Um QUIC- oder TCP_QUIC-Listener verwenden zu können, darf Ihr Network Load Balancer keine Sicherheitsgruppen haben.

8. Listener und Routing

- a. Es ist standardmäßig ein Listener eingestellt, der über Port 80 TCP-Datenverkehr annimmt. Nur TCP-Listener können den Datenverkehr an eine Application-Load-Balancer-Zielgruppe weiterleiten. Sie müssen das Protokoll als TCP beibehalten, können den Port jedoch nach Bedarf ändern.

Mit dieser Konfiguration können Sie HTTPS-Listener am Application Load Balancer verwenden, um den TLS-Datenverkehr zu beenden.

- b. Wählen Sie für Standardaktion die Zielgruppe aus, die Sie im vorherigen Schritt erstellt haben.

- c. (Optional) Wählen Sie „Listener-Tag hinzufügen“ und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.

9. Load Balancer-Tags

(Optional) Erweitern Sie die Load Balancer-Tags. Wählen Sie Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein. Weitere Informationen finden Sie unter [Tags](#).

10. Übersicht

Überprüfen Sie Ihre Konfiguration und wählen Sie Load Balancer erstellen.

AWS CLI

So erstellen Sie den Network Load Balancer

Verwenden Sie den Befehl [create-load-balancer](#). Wir empfehlen, dass Sie dieselben Availability Zones verwenden, die für Ihren Application Load Balancer aktiviert sind.

```
aws elbv2 create-load-balancer \  
  --name my-load-balancer \  
  --type network \  
  --scheme internal \  
  --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \  
  --security-groups sg-1111222233334444
```

Um einen TCP-Listener hinzuzufügen

Verwenden Sie den Befehl [create-listener](#), um einen TCP-Listener hinzuzufügen. Nur TCP-Listener können den Datenverkehr an einen Application Load Balancer weiterleiten. Verwenden Sie für die Standardaktion die Zielgruppe, die Sie im vorherigen Schritt erstellt haben.

```
aws elbv2 create-listener \  
  --load-balancer-arn load-balancer-arn \  
  --protocol TCP \  
  --port 80 \  
  --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

So erstellen Sie den Network Load Balancer

Definieren Sie eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::LoadBalancer](#) und eine Ressource vom Typ [AWS::ElasticLoadBalancingV2::Listener](#). Nur TCP-Listener können den Datenverkehr an einen Application Load Balancer weiterleiten. Verwenden Sie für die Standardaktion die Zielgruppe, die Sie im vorherigen Schritt erstellt haben.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-load-balancer
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup

  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Schritt 3: (Optional) Erstellen Sie einen VPC-Endpunktdienst

Um den Network Load Balancer, den Sie im vorherigen Schritt eingerichtet haben, als Endpunkt für private Konnektivität zu verwenden, können Sie AWS PrivateLink aktivieren. Dadurch wird eine private Verbindung zu Ihrem Load Balancer als Endpunktservice eingerichtet.

So erstellen Sie einen VPC-Endpunktservice mit Ihrem Network Load Balancer

1. Wählen Sie im Navigationsbereich Load Balancers aus.
2. Wählen Sie den Namen des Network Load Balancers aus, um die Detailseite zu öffnen.
3. Erweitern Sie auf der Registerkarte Integrationen die Option VPC-Endpunktservices (AWS PrivateLink).

4. Klicken Sie auf Endpunktservices erstellen, um die Seite Endpunkt erstellen zu öffnen. Die verbleibenden Schritte finden Sie im Handbuch unter [Erstellen eines Endpunktservices](#) im AWS PrivateLink -Handbuch.

Kennzeichnen Sie eine Zielgruppe für Ihren Network Load Balancer

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 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 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.

Console

Um die Tags für eine Zielgruppe zu verwalten

1. Öffnen Sie die Amazon-EC2-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. Wählen Sie Änderungen speichern aus.

AWS CLI

So fügen Sie -Tags hinzu

Verwenden Sie den Befehl [add-tags](#). Im folgenden Beispiel werden zwei Tags hinzugefügt.

```
aws elbv2 add-tags \  
  --resource-arns target-group-arn \  
  --tags "Key=project,value=lima" "Key=department,Value=digital-media"
```

So entfernen Sie Tags

Verwenden Sie den Befehl [remove-tags](#). Im folgenden Beispiel werden die Tags mit den angegebenen Schlüsseln entfernt.

```
aws elbv2 remove-tags \  
  --resource-arns target-group-arn \  
  --tag-keys project department
```

CloudFormation

So fügen Sie -Tags hinzu

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::TargetGroup](#) Ressource so, dass sie die Tags Eigenschaft enthält.

```
Resources:  
  myTargetGroup:  
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'  
    Properties:  
      Name: my-target-group
```

```
Protocol: TCP
Port: 80
TargetType: ip
VpcId: !Ref myVPC
Tags:
  - Key: 'project'
    Value: 'lima'
  - Key: 'department'
    Value: 'digital-media'
```

Löschen Sie eine Zielgruppe für Ihren Network Load Balancer

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, die bei der Zielgruppe registriert sind. Wenn Sie die registrierte EC2-Instance nicht mehr benötigen, können Sie sie anhalten oder beenden.

Console

So löschen Sie eine Zielgruppe

1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancer aus.
3. Markieren Sie die Zielgruppe und wählen Sie Aktionen, Löschen.
4. Wählen Sie Löschen aus.

AWS CLI

So löschen Sie eine Zielgruppe

Verwenden Sie den Befehl [delete-target-group](#).

```
aws elbv2 delete-target-group \
  --target-group-arn target-group-arn
```

Überwachen Ihrer Network Load Balancers

Sie können die folgenden Funktionen verwenden, um Ihre Load Balancers zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihren Load Balancern 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 Network Load Balancer](#).

VPC-Flow-Protokolle

Sie können VPC-Flow-Protokolle verwenden, um detaillierte Informationen über den Datenverkehr zu und von Ihrem Network Load Balancer zu erfassen. Weitere Informationen finden Sie unter [VPC-Flow-Protokolle](#) im Amazon-VPC-Benutzerhandbuch.

Erstellen Sie ein Ablaufprotokoll für jede Netzwerkschnittstelle Ihres Load Balancers. Es gibt eine Netzwerkschnittstelle pro Load Balancer-Subnetz. Um die Netzwerkschnittstellen für einen Network Load Balancer zu identifizieren, suchen Sie den Namen des Load Balancers im Beschreibungsfeld der Netzwerkschnittstelle.

Es gibt zwei Einträge für jede Verbindung über Ihren Network Load Balancer, eine für die Frontend-Verbindung zwischen dem Client und dem Load Balancer und die andere für die Backend-Verbindung zwischen dem Load Balancer und dem Ziel. Wenn das Client-IP-Erhalt-Attribut der Zielgruppe aktiviert ist, wird die Verbindung der Instance als Verbindung vom Client angezeigt. Andernfalls ist die Quell-IP der Verbindung die private IP-Adresse des Load Balancers. Wenn die Sicherheitsgruppe der Instance keine Verbindungen vom Client zulässt, das Netzwerk ACLs für das Load Balancer-Subnetz sie jedoch zulässt, zeigen die Protokolle für die Netzwerkschnittstelle für den Load Balancer „ACCEPT OK“ für die Frontend- und Backend-Verbindungen an, während die Protokolle für die Netzwerkschnittstelle für die Instance „REJECT OK“ für die Verbindung anzeigen.

Wenn einem Network Load Balancer Sicherheitsgruppen zugeordnet sind, enthalten Ihre Flow-Protokolle Einträge für Datenverkehr, der von den Sicherheitsgruppen zugelassen oder abgelehnt wird. Bei Network Load Balancern mit TLS-Listenern spiegeln Ihre Flow-Protokolleinträge nur die abgelehnten Einträge wider.

Amazon CloudWatch Internetmonitor

Sie können Internet Monitor verwenden, um zu sehen, wie sich Internetprobleme auf die Leistung und Verfügbarkeit zwischen Ihren gehosteten Anwendungen AWS und Ihren Endbenutzern auswirken. Sie können auch nahezu in Echtzeit untersuchen, wie Sie die prognostizierte Latenz Ihrer Anwendung verbessern können, indem Sie auf andere Dienste umsteigen oder den Datenverkehr über andere AWS-Regionen Dienste auf Ihren Workload umleiten. Weitere Informationen finden Sie unter [Amazon CloudWatch Internet Monitor verwenden](#).

Zugriffsprotokolle

Sie können mit Zugriffsprotokollen detaillierte Informationen zu TLS-Anforderungen erfassen, die an Ihren Load Balancer gestellt werden. Die Protokolldateien werden in Amazon S3 gespeichert. Sie können anhand dieser Zugriffsprotokolle Datenverkehrsmuster analysieren und Probleme mit Ihren Zielen beheben. Weitere Informationen finden Sie unter [Zugriffsprotokolle für Ihren Network 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 Network 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 Network Load Balancern mit Sicherheitsgruppen wird der von den Sicherheitsgruppen abgelehnte Datenverkehr nicht in den CloudWatch Metriken erfasst.

Weitere Informationen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

Inhalt

- [Network Load Balancer-Metriken](#)
- [Metrik-Dimensionen für Network Load Balancers](#)
- [Statistiken für Network-Load-Balancer-Metriken](#)
- [CloudWatch Metriken für Ihren Load Balancer anzeigen](#)

Network Load Balancer-Metriken

Der AWS/NetworkELB-Namespace enthält die folgenden Metriken.

Metrik	Description
ActiveFlowCount	<p>Die Gesamtzahl der gleichzeitigen Datenflüsse (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält Verbindungen im Status SYN_SENT und ESTABLISHED. TCP-Verbindungen werden am Load Balancer nicht beendet, ein Client, der eine TCP-Verbindung zu einem Ziel öffnet, zählt also als einziger Datenfluss.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichsten Statistiken sind Average, Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup

Metrik	Description
ActiveFlowCount_TCP	<p>Die Gesamtzahl der gleichzeitigen TCP-Datenflüsse (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält Verbindungen im Status SYN_SENT und ESTABLISHED. TCP-Verbindungen werden am Load Balancer nicht beendet, ein Client, der eine TCP-Verbindung zu einem Ziel öffnet, zählt also als einziger Datenfluss.</p> <p>Berichtskriterien: Ein Wert ungleich Null</p> <p>Statistiken: Die nützlichsten Statistiken sind Average, Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer• TargetGroup
ActiveFlowCount_TLS	<p>Die Gesamtzahl der gleichzeitigen TLS-Datenflüsse (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält Verbindungen im Status SYN_SENT und ESTABLISHED.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichsten Statistiken sind Average, Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer• TargetGroup

Metrik	Description
ActiveFlowCount_UDP	<p>Die Gesamtzahl der gleichzeitigen UDP-Datenflüsse (oder Verbindungen) von Clients zu Zielen.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichsten Statistiken sind Average, Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup
ActiveZonalShiftHostCount	<p>Die Anzahl der Ziele, die derzeit aktiv am Zonenwechsel teilnehmen.</p> <p>Berichtskriterien: Wird gemeldet, wenn sich der Load Balancer für Zonal Shift entschieden hat.</p> <p>Statistiken: Die nützlichsten Statistiken sind Maximum, und. Minimum</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
ClientTLSNegotiationErrorCount	<p>Die Gesamtzahl der TLS-Handshakes, die bei der Aushandlung zwischen einem Client und einem TLS-Listener fehlgeschlagen sind.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer

Metrik	Description
ConsumedLCUs	<p>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. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Alle</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer
ConsumedLCUs_TCP	<p>Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer für TCP verwendet werden. Sie zahlen für die Anzahl der Geräte LCUs , die Sie pro Stunde nutzen. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Alle</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer
ConsumedLCUs_TLS	<p>Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer für TLS verwendet werden. Sie zahlen für die Anzahl der Geräte LCUs , die Sie pro Stunde nutzen. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Alle</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer

Metrik	Description
ConsumedLCUs_UDP	<p>Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer für UDP verwendet werden. Sie zahlen für die Anzahl der Geräte LCUs , die Sie pro Stunde nutzen. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Alle</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer
HealthyHostCount	<p>Anzahl der als stabil betrachteten Ziele. Diese Metrik enthält keine Application Load Balancers, die als Ziele registriert sind.</p> <p>Berichtskriterien: Wird gemeldet, wenn es registrierte Ziele gibt.</p> <p>Statistiken: Die nützlichsten Statistiken sind Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer , TargetGroup• AvailabilityZone , LoadBalancer , TargetGroup
NewFlowCount	<p>Die Gesamtanzahl neuer Datenflüsse (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer• TargetGroup

Metrik	Description
NewFlowCount_TCP	<p>Die Gesamtanzahl neuer TCP-Datenflüsse (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer• TargetGroup
NewFlowCount_TLS	<p>Die Gesamtanzahl neuer TLS-Datenflüsse (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer• TargetGroup

Metrik	Description
NewFlowCount_UDP	<p>Die Gesamtanzahl neuer UDP-Datenflüsse (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup
NewFlowCount_QUIC	<p>Die Gesamtzahl der UDP-Datagramme, für die in dem Zeitraum eine Routing-Entscheidung erforderlich war.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
PeakBytesPerSecond	<p>Die höchste durchschnittliche Anzahl verarbeiteter Byte pro Sekunde, berechnet alle 10 Sekunden während des Sampling-Zeitfensters. In dieser Metrik ist kein Datenverkehr mit Gesundheitschecks enthalten.</p> <p>Berichtskriterien: Always reported</p> <p>Statistiken: Die nützlichste Statistik ist Maximum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Description
PeakPacketsPerSecond	<p>Höchste durchschnittliche Paketrage (pro Sekunde verarbeitete Pakete), berechnet alle 10 Sekunden während des Sampling-Zeitfensters. Diese Metrik enthält den Datenverkehr mit Zustandspürungen.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Maximum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
PortAllocationErrorCount	<p>Die Gesamtzahl der kurzlebigen Fehler bei der Portzuweisung während eines Client-IP-Übersetzungsvorgangs. Ein Wert ungleich Null weist auf unterbrochene Client-Verbindungen hin.</p> <p>Hinweis: Network Load Balancers unterstützen 55 000 gleichzeitige Verbindungen oder etwa 55 000 Verbindungen pro Minute zu jedem einzelnen Ziel (IP-Adresse und Port), wenn sie eine Client-Adressübersetzung durchführen. Um Port-Zuordnungsfehler zu beheben, fügen Sie der Zielgruppe mehr Ziele hinzu.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Metrik	Description
ProcessedBytes	<p>Die Gesamtzahl der vom Load Balancer verarbeiteten Byte, einschließlich TCP/IP Header. Diese Anzahl umfasst Datenverkehr zu und von Zielen, abzüglich des Datenverkehrs für Zustandsprüfungen.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
ProcessedBytes_TCP	<p>Gesamtanzahl der von TCP-Listnern verarbeiteten Bytes.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
ProcessedBytes_TLS	<p>Gesamtanzahl der von TLS-Listnern verarbeiteten Bytes.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Metrik	Description
ProcessedBytes_UDP	<p>Gesamtanzahl der von UDP-Listnern verarbeiteten Bytes.</p> <p>Berichtskriterien: Ein Wert ungleich Null</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
ProcessedBytes_QUIC	<p>Die Gesamtzahl der von QUIC-Listnern verarbeiteten Byte.</p> <p>Berichtskriterien: Ein Wert ungleich Null</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
ProcessedPackets	<p>Gesamtanzahl der von einem Load Balancer verarbeiteten Pakets. Diese Anzahl umfasst Datenverkehr zu und von Zielen, einschließlich des Datenverkehrs für Zustandsprüfungen.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Metrik	Description
RejectedFlowCount	<p>Die Gesamtzahl der vom Load Balancer zurückgewiesenen Datenflüsse (oder Verbindungen).</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichsten Statistiken sind Average, Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
RejectedFlowCount_TCP	<p>Die Anzahl der vom Load Balancer zurückgewiesenen TCP-Flows (oder Verbindungen).</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
ReservedLCUs	<p>Die Anzahl der Load Balancer-Kapazitätseinheiten (LCUs), die mithilfe der LCU-Reservierung für Ihren Load Balancer reserviert wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null</p> <p>Statistiken: Alle</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer

Metrik	Description
SecurityGroupBlockedFlowCount_Inbound_ICMP	<p>Die Anzahl neuer ICMP-Nachrichten, die nach den Regeln für eingehenden Datenverkehr der Load-Balancer-Sicherheitsgruppen zurückgewiesen wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_TCP	<p>Die Anzahl neuer TCP-Flows, die nach den Regeln für eingehenden Datenverkehr der Load-Balancer-Sicherheitsgruppen zurückgewiesen wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_UDP	<p>Die Anzahl neuer UDP-Flows, die nach den Regeln für eingehenden Datenverkehr der Load-Balancer-Sicherheitsgruppen zurückgewiesen wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Description
SecurityGroupBlockedFlowCount_Outbound_ICMP	<p>Die Anzahl neuer ICMP-Nachrichten, die nach den Regeln für ausgehenden Datenverkehr der Load-Balancer-Sicherheitsgruppen zurückgewiesen wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_TCP	<p>Die Anzahl neuer TCP-Flows, die nach den Regeln für ausgehenden Datenverkehr der Load-Balancer-Sicherheitsgruppen zurückgewiesen wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_UDP	<p>Die Anzahl neuer UDP-Flows, die nach den Regeln für ausgehenden Datenverkehr der Load-Balancer-Sicherheitsgruppen zurückgewiesen wurden.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Metrik	Description
TargetTLSNegotiationErrorCount	<p>Die Gesamtzahl der TLS-Handshakes, die bei der Aushandlung zwischen einem TLS-Listener und einem Ziel fehlgeschlagen sind.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer
TCP_Client_Reset_Count	<p>Die Gesamtzahl der Reset-Pakete (RST), die von einem Client an ein Ziel gesendet werden. Diese Resets werden vom Client erzeugt und vom Load Balancer weitergeleitet.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
TCP_ELB_Reset_Count	<p>Die Gesamtanzahl der vom Load Balancer generierten Reset-Pakete (RST). Weitere Informationen finden Sie unter Fehlerbehebung.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Metrik	Description
TCP_Target_Reset_Count	<p>Die Gesamtzahl der Reset-Pakete (RST), die von einem Ziel an einen Client gesendet werden. Diese Resets werden vom Ziel erzeugt und vom Load Balancer weitergeleitet.</p> <p>Berichtskriterien: Immer berichtet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer
UnHealthyHostCount	<p>Die Anzahl der als instabil betrachteten Ziele. Diese Metrik enthält keine Application Load Balancers, die als Ziele registriert sind.</p> <p>Berichtskriterien: Wird gemeldet, ob es registrierte Ziele gibt.</p> <p>Statistiken: Die nützlichsten Statistiken sind Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none">• LoadBalancer , TargetGroup• AvailabilityZone , LoadBalancer , TargetGroup
UnhealthyRoutingFlowCount	<p>Die Anzahl der Flows (oder Verbindungen), die mithilfe der Routing-Failover-Aktion (Fail-Open) weitergeleitet werden. Diese Metrik wird für TLS-Listener nicht unterstützt.</p> <p>Berichtskriterien: Ein Wert ungleich Null.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p>

Metrik	Description
ZonalHealthStatus	<p>Die Anzahl der Availability Zones, die der Load Balancer für fehlerfrei hält. Der Load Balancer gibt für jede fehlerfreie Availability Zone eine 1 und für jede fehlerhafte Availability Zone eine 0 aus.</p> <p>Berichtskriterien: Werden gemeldet, wenn Zustandsprüfungen aktiviert sind.</p> <p>Statistiken: Die nützlichsten Statistiken sind Maximum und Minimum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
QUIC_Unknown_Server_ID_Packet_Drop_Count	<p>Die Anzahl der gelöschten UDP-Datagramme, die eine Server-ID enthalten, die keinem Ziel im Network Load Balancer zugeordnet ist.</p> <p>Berichtskriterien: Nur für QUIC-Listener gemeldet.</p> <p>Statistiken: Die nützlichste Statistik ist Sum.</p> <p>Dimensionen</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik-Dimensionen für Network Load Balancers

Verwenden Sie die nachstehenden Dimensionen, um die Metriken für Ihren Load Balancer zu filtern.

Dimension	Description
AvailabilityZone	Filtert die Metrikdaten nach Availability Zone.

Dimension	Description
LoadBalancer	Filtert die Metrikdaten nach Load Balancer. Geben Sie den Load Balancer wie folgt an: net/ 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 Network-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/value Paar, das eine Metrik eindeutig identifiziert. Beispielsweise können Sie Statistiken für alle fehlerfreien EC2-Instances hinter einem Load Balancer, die in einer bestimmten Availability Zone gestartet wurden, anfordern.

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. Eine Erhöhung des Maximums von HealthyHostCount entspricht einer Reduzierung des Minimums von UnHealthyHostCount. Es wird empfohlen, den Maximalwert HealthyHostCount zu überwachen und einen Alarm auszulösen, wenn der Maximalwert HealthyHostCount unter das erforderliche Minimum fällt oder 0 beträgt. Auf diese Weise können Sie feststellen, wann Ihre Ziele fehlerhaft geworden sind. Es wird auch empfohlen, den Minimalwert UnHealthyHostCount zu überwachen und einen Alarm auszulösen, wenn der Mindestwert UnHealthyHostCount über 0 steigt. Auf diese Weise können Sie erkennen, wenn keine registrierten Ziele mehr vorhanden sind.

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.

CloudWatch Metriken für Ihren Load Balancer anzeigen

Sie können die CloudWatch Metriken für Ihre Load Balancer mithilfe der Amazon EC2 EC2-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 Amazon-EC2-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 aus und wählen Sie dann Monitoring.
 - 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 Monitoring.
 - 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 Konsole anzuzeigen CloudWatch

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 NetworkELB.
4. (Optional) Um eine Metrik für alle Dimensionen 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/NetworkELB
```

Um die Statistiken für eine Metrik abzurufen, verwenden Sie den AWS CLI

Verwenden Sie den folgenden [get-metric-statistics](#) Befehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. Beachten Sie, dass jede eindeutige Kombination von Dimensionen als separate Metrik CloudWatch behandelt wird. 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/NetworkELB \  
--metric-name UnHealthyHostCount --statistics Average --period 3600 \  
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \  
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \  
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

Das Folgende ist eine Beispielausgabe:

```
{  
  "Datapoints": [  
    {  
      "Timestamp": "2017-04-18T22:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    {  
      "Timestamp": "2017-04-18T04:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    ...  
  ],  
  "Label": "UnHealthyHostCount"  
}
```

Zugriffsprotokolle für Ihren Network Load Balancer

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen über die TLS-Verbindungen erfassen, die mit Ihrem Network Load Balancer hergestellt wurden. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembeseitigung verwenden.

Important

Während herkömmliche „ältere“ Zugriffsprotokolle (in diesem Abschnitt beschrieben) weiterhin verfügbar sind, bietet Network Load Balancer jetzt erweiterte Protokollierungsoptionen über CloudWatch Logs. CloudWatch Logs bieten flexiblere Lieferoptionen, unter anderem an Amazon CloudWatch Logs, Amazon Data Firehose und Amazon Simple Storage Service. Um diese verbesserten Protokollierungsoptionen zu konfigurieren, besuchen Sie den Tab Integrationen Ihres Load Balancers. Weitere Informationen zu CloudWatch Protokollen finden Sie unter [CloudWatch Logs für Ihren Network Load Balancer](#)

Important

Zugriffsprotokolle werden nur erstellt, wenn der Load Balancer über einen TLS-Listener verfügt, und die Protokolle enthalten nur Informationen zu TLS-Anfragen. In den Zugriffsprotokollen werden Anfragen nach bestem Wissen und Gewissen aufgezeichnet. Wir empfehlen, dass Sie die Zugriffsprotokolle verwenden, um die Art der Anforderungen zu verstehen, nicht als eine vollständige Buchführung aller Anforderungen.

Zugriffsprotokollierung ist ein optionales Feature von Elastic Load Balancing, das standardmäßig deaktiviert ist. Nachdem Sie die Zugriffsprotokollierung für Ihren Load Balancer aktiviert haben, erfasst Elastic Load Balancing die Protokolle als komprimierte Dateien und speichert sie in dem von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Zugriffsprotokollierung jederzeit deaktivieren.

Sie können serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) oder mit Key Management Service mit vom Kunden verwalteten Schlüsseln (SSE-KMS CMK) für Ihren S3-Bucket aktivieren. Jede Zugriffsprotokolldatei wird automatisch verschlüsselt, bevor sie im S3-Bucket gespeichert und beim Zugriff auf die Datei entschlüsselt wird. Sie müssen keine Maßnahmen ergreifen, weil zwischen dem Zugriff auf

verschlüsselte und unverschlüsselte Protokolldateien kein Unterschied besteht. Jede Protokolldatei ist mit einem eindeutigen Schlüssel verschlüsselt, der wiederum mit einem KMS-Schlüssel verschlüsselt wird, der regelmäßig gewechselt wird. Weitere Informationen finden Sie unter [Spezifizieren der Amazon S3 S3-Verschlüsselung \(SSE-S3\)](#) und [Spezifizieren der serverseitigen Verschlüsselung mit AWS KMS \(SSE-KMS\)](#) im Amazon S3 S3-Benutzerhandbuch.

Es fallen für die Zugriffsprotokolle keine zusätzlichen Gebühren an. 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](#)
- [Verarbeiten von Zugriffsprotokolldateien](#)
- [Zugriffsprotokolle für Ihren Network Load Balancer aktivieren](#)
- [Deaktivieren Sie die Zugriffsprotokolle für Ihren Network 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_net.load-balancer-id_end-time_random-string.log.gz
```

bucket

Der Name des S3-Buckets.

prefix

Das Präfix (logische Hierarchie) im Bucket. Wenn Sie kein Präfix festlegen, werden die Protokolle auf der Bucket-Stammebene platziert.

aws-account-id

Die ID des Besitzers AWS-Konto .

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 20181220T2340Z enthält Einträge für Anfragen, die zwischen 23:35 und 23:40 durchgeführt wurden.

random-string

Eine vom System generierte zufällige Zeichenfolge.

Es folgt ein Beispiel für einen Protokolldateinamen:

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-loadbalancer.1234567890abcdef_20200501T0000Z_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 [Verwalten des Speicherlebenszyklus](#) im Amazon-S3-Benutzerhandbuch.

Zugriffsprotokolleinträge

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. Bei der Verarbeitung der Protokolldateien sollten Sie alle Felder am Ende des Protokolleintrags ignorieren, die Sie nicht erwartet haben.

Feld	Description
type	Der Listener Typ. Der unterstützte Wert ist <code>tls</code> .
version	Die Version des Protokolleintrags. Die aktuelle Version ist 2.0.
time	Die am Ende der TLS-Verbindung im ISO 8601-Format aufgezeichnete Zeit.
elb	Die Ressourcen-ID des Load Balancer.
Listener	Die Ressourcen-ID des TLS-Listeners für die Verbindung.
client_port	Die IP-Adresse und der Port des Clients.
Zielport	Die IP-Adresse und der Port des Ziels. Wenn der Client eine direkte Verbindung zum Load Balancer herstellt, ist das Ziel der Listener. Wenn der Client eine Verbindung über einen VPC-Endpunktdienst herstellt, ist das Ziel der VPC-Endpunkt.
connection_time	Die Gesamtzeit in Millisekunden, die für die Verbindungsdurchführung vom Anfang bis zum Abschluss benötigt wird.
tls_handshake_time	Die Gesamtzeit in Millisekunden für die Durchführung des TLS-Handshakes benötigt wird, nachdem die TCP-Verbindung hergestellt wurde und einschließlich der clientseitigen Verzögerungen. Diese Zeit ist im Feld <code>connection_time</code> enthalten. Wenn kein TLS-Handshake oder ein TLS-Handshake-Fehler vorliegt, wird dieser Wert auf <code>0</code> gesetzt. -
received_bytes	Die Anzahl der Bytes, die der Load Balancer nach der Entschlüsselung vom Client empfängt.
sent_bytes	Die Anzahl der Bytes, die der Load Balancer vor der Verschlüsselung an den Client sendet.
incoming_tls_alert	Der Ganzzahlwert der TLS-Warnungen, die der Load Balancer ggf. vom Client empfängt. Andernfalls ist dieser Wert auf <code>0</code> gesetzt. -

Feld	Description
chosen_cert_arn	Der ARN des Zertifikats, das auf dem Client gespeichert wird. Wenn keine gültige Client-Hello-Nachricht gesendet wird, wird dieser Wert auf gesetzt-.
chosen_cert_serial	Für die spätere Verwendung reserviert. Dieser Wert ist immer auf gesetzt-.
tls_cipher	Die mit dem Client ausgehandelte Verschlüsselungssammlung im OpenSSL-Format. Wenn die TLS-Aushandlung nicht abgeschlossen wird, wird dieser Wert auf gesetzt-.
tls_protocol_version	Das mit dem Client ausgehandelte TLS-Protokoll im Zeichenfolgenformat. Die möglichen Werte sind <code>tlsv10</code> , <code>tlsv11</code> , <code>tlsv12</code> und <code>tlsv13</code> . Wenn die TLS-Aushandlung nicht abgeschlossen wird, wird dieser Wert auf gesetzt-.
tls_keyexchange	Der Schlüsselaustausch, der bei Handshakes für TLS oder PQ-TLS verwendet wird. Wenn die TLS- oder PQ-TLS-Aushandlung nicht abgeschlossen wird, wird dieser Wert auf gesetzt. -
domain_name	Der Wert der <code>server_name</code> -Erweiterung in der Hello-Nachricht des Client. Dieser Wert ist URL-verschlüsselt. Wenn keine gültige Client-Hello-Nachricht gesendet wird oder die Erweiterung nicht vorhanden ist, wird dieser Wert auf gesetzt. -
alpn_fe_protocol	Das mit dem Client ausgehandelte Anwendungsprotokoll im Zeichenfolgenformat. Die möglichen Werte sind <code>h2</code> , <code>http/1.1</code> und <code>http/1.0</code> . Wenn im TLS-Listener keine ALPN-Richtlinie konfiguriert ist, kein passendes Protokoll gefunden wird oder keine gültige Protokollliste gesendet wird, wird dieser Wert auf gesetzt. -
alpn_be_protocol	Das mit dem Ziel ausgehandelte Anwendungsprotokoll im Zeichenfolgenformat. Die möglichen Werte sind <code>h2</code> , <code>http/1.1</code> und <code>http/1.0</code> . Wenn im TLS-Listener keine ALPN-Richtlinie konfiguriert ist, kein passendes Protokoll gefunden wird oder keine gültige Protokollliste gesendet wird, wird dieser Wert auf gesetzt. -

Feld	Description
alpn_client_preference_list	Der Wert der Erweiterung application_layer_protocol_negotiation in der Client-Hello-Nachricht. Dieser Wert ist URL-verschlüsselt. Jedes Protokoll ist in doppelte Anführungszeichen eingeschlossen, und Protokolle werden durch ein Komma getrennt angegeben. Wenn im TLS-Listener keine ALPN-Richtlinie konfiguriert ist, keine gültige Client-Hello-Nachricht gesendet wird oder die Erweiterung nicht vorhanden ist, wird dieser Wert auf gesetzt. - Die Zeichenfolge wird abgeschnitten, wenn sie länger als 256 Byte ist.
tls_connection_creation_time	Die zu Beginne der TLS-Verbindung aufgezeichnete Zeit, im ISO 8601-Format.

Beispiel-Protokolleinträge

Es folgen beispielhafte Protokolleinträge. Beachten Sie, dass der Text nur aus Gründen der besseren Lesbarkeit auf mehrere Zeilen verteilt ist.

Im Folgenden finden Sie ein Beispiel für einen TLS-Listener ohne ALPN-Richtlinie.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

Im Folgenden finden Sie ein Beispiel für einen TLS-Listener mit ALPN-Richtlinie.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

Verarbeiten von Zugriffsprotokolldateien

Die Zugriffsprotokolldateien werden 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 line-by-line von 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 Network-Load-Balancer-Protokollen](#) im Benutzerhandbuch zu Amazon Athena.
- [Loggly](#)
- [Splunk](#)
- [Sumo Logic](#)

Zugriffsprotokolle für Ihren Network Load Balancer aktivieren

Wenn Sie die Zugriffsprotokollierung 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.

Important

Zugriffsprotokolle werden nur erstellt, wenn der Load Balancer über einen TLS-Listener verfügt, und die Protokolle enthalten nur Informationen zu TLS-Anfragen.

Bucket-Anforderungen

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.
- Das von Ihnen angegebene Präfix darf nicht AWSLogs enthalten. Wir fügen den Teil des Dateinamens hinzu, der mit AWSLogs nach dem von Ihnen angegebenen Bucket-Namen und dem Präfix beginnt.
- Der Bucket muss über eine Bucket-Richtlinie verfügen, die 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.

Beispiel einer Bucket-Richtlinie

Es folgt eine Beispielrichtlinie. Ersetzen Sie die Resource Elemente *amzn-s3-demo-destination-bucket* durch den Namen des S3-Buckets für Ihre Zugriffsprotokolle. Achten Sie darauf, das wegzulassen *Prefix/*, wenn Sie kein Bucket-Präfix verwenden. Geben Sie für `aws:SourceAccount` die ID des AWS Kontos beim Load Balancer an. Ersetzen Sie für `aws:SourceArn` *region* und jeweils *012345678912* durch die Region und die Konto-ID des Load Balancers.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryWrite",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "012345678912"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  },
  "ArnLike": {
    "aws:SourceArn": [
      "arn:aws:logs:us-east-1:012345678912:*"
    ]
  }
},
{
  "Sid": "AWSLogDeliveryWrite",
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-
bucket/Prefix/AWSLogs/account-ID/*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-acl": "bucket-owner-full-control",
      "aws:SourceAccount": [
        "012345678912"
      ]
    }
  },
  "ArnLike": {
    "aws:SourceArn": [
      "arn:aws:logs:us-east-1:012345678912:*"
    ]
  }
}
]
}

```

Verschlüsselung

Sie können die serverseitige Verschlüsselung für Ihren Amazon-S3-Zugriffsprotokoll-Bucket auf eine der folgenden Arten aktivieren:

- Von Amazon S3 verwaltete Schlüssel (SSE-S3)

- AWS KMS Schlüssel, die in AWS Key Management Service (SSE-KMS) † gespeichert sind

† Mit Network Load Balancer Balancer-Zugriffsprotokollen können Sie keine AWS verwalteten Schlüssel verwenden. Sie müssen vom Kunden verwaltete Schlüssel verwenden.

Weitere Informationen finden Sie unter [Spezifizieren der Amazon S3 S3-Verschlüsselung \(SSE-S3\)](#) und [Spezifizieren der serverseitigen Verschlüsselung mit AWS KMS \(SSE-KMS\)](#) im Amazon S3 S3-Benutzerhandbuch.

Die Schlüsselrichtlinie muss es dem Service ermöglichen, die Protokolle zu verschlüsseln und zu entschlüsseln. Es folgt eine Beispielrichtlinie .

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Konfigurieren Sie die Zugriffsprotokolle

Gehen Sie wie folgt vor, um Zugriffsprotokolle zu konfigurieren, um Anforderungsinformationen zu erfassen und Protokolldateien an Ihren S3-Bucket zu übermitteln.

Console

So aktivieren Sie Zugriffsprotokolle

1. Öffnen Sie die Amazon-EC2-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.

AWS CLI

So aktivieren Sie Zugriffsprotokolle

Verwenden Sie den [modify-load-balancer-attributes](#) Befehl mit den zugehörigen Attributen.

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes \  
    Key=access_logs.s3.enabled,Value=true \  
    Key=access_logs.s3.bucket,Value=amzn-s3-demo-logging-bucket \  
    Key=access_logs.s3.prefix,Value=logging-prefix
```

CloudFormation

So aktivieren Sie Zugriffsprotokolle

Aktualisieren Sie die [AWS::ElasticLoadBalancingV2::LoadBalancer](#) Ressource, sodass sie die zugehörigen Attribute enthält.

```
Resources:  
  myLoadBalancer:
```

```
Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'  
Properties:  
  Name: my-nlb  
  Type: network  
  Scheme: internal  
  Subnets:  
    - !Ref subnet-AZ1  
    - !Ref subnet-AZ2  
  SecurityGroups:  
    - !Ref mySecurityGroup  
  LoadBalancerAttributes:  
    - Key: "access_logs.s3.enabled"  
      Value: "true"  
    - Key: "access_logs.s3.bucket"  
      Value: "amzn-s3-demo-logging-bucket"  
    - Key: "access_logs.s3.prefix"  
      Value: "logging-prefix"
```

Deaktivieren Sie die Zugriffsprotokolle für Ihren Network Load Balancer

Sie können Zugriffsprotokollierung für Ihren Load Balancer jederzeit deaktivieren. Nachdem Sie Zugriffsprotokollierung 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.

Console

Um Zugriffsprotokolle zu deaktivieren

1. Öffnen Sie die Amazon-EC2-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.

AWS CLI

Um Zugriffsprotokolle zu deaktivieren

Verwenden Sie den Befehl [modify-load-balancer-attributes](#).

```
aws elbv2 modify-load-balancer-attributes \  
  --load-balancer-arn load-balancer-arn \  
  --attributes Key=access_logs.s3.enabled,Value=false
```

Beheben von Problemen mit Ihrem Network Load Balancer

Die folgenden Informationen können Ihnen helfen, Probleme bei Ihren Network Load Balancern zu beheben.

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 [Zustandsprüfungen für Zielgruppen von Network Load Balancer](#).

Überprüfen Sie, ob Ihre Instance Zustandsprüfungen nicht besteht und prüfen Sie dann Folgendes:

Eine Sicherheitsgruppe erlaubt keinen Datenverkehr

Die mit einer Instance verbundenen Sicherheitsgruppen müssen Datenverkehr vom Load Balancer über den Zustandsprüfungsport und das Zustandsprüfungsprotokoll zulassen. Weitere Informationen finden Sie unter [Zielsicherheitsgruppen](#). Außerdem muss die Sicherheitsgruppe für Ihren Load Balancer Datenverkehr zu den Instances zulassen. Weitere Informationen finden Sie unter [Aktualisieren Sie die Sicherheitsgruppen für Ihren Network Load Balancer](#).

Eine Netzwerk-Zugriffskontrollliste (ACL) erlaubt keinen Datenverkehr

Die Netzwerk-ACL, die den Subnetzen für Ihre Instances und den Subnetzen für Ihren Load Balancer zugeordnet ist, muss Datenverkehr und Zustandsprüfungen durch den Load Balancer zulassen. Weitere Informationen finden Sie unter [Netzwerk ACLs](#).

Anfragen werden nicht an Ziele weitergeleitet.

Überprüfen Sie Folgendes:

Eine Sicherheitsgruppe erlaubt keinen Datenverkehr

Die den Instances zugeordneten Sicherheitsgruppen müssen den Datenverkehr auf dem Listener-Port von Client-IP-Adressen (falls Ziele nach Instance-ID angegeben sind) oder Load Balancer-Knoten (falls Ziele nach IP-Adresse angegeben sind) erlauben. Weitere Informationen finden Sie unter [Zielsicherheitsgruppen](#). Außerdem muss die Sicherheitsgruppe für Ihren Load Balancer

Datenverkehr zu den Instances zulassen. Weitere Informationen finden Sie unter [Aktualisieren Sie die Sicherheitsgruppen für Ihren Network Load Balancer](#).

Eine Netzwerk-Zugriffskontrollliste (ACL) erlaubt keinen Datenverkehr

Das mit den Subnetzen für Ihre VPC ACLs verknüpfte Netzwerk muss es dem Load Balancer und den Zielen ermöglichen, auf dem Listener-Port in beide Richtungen zu kommunizieren. Weitere Informationen finden Sie unter [Netzwerk ACLs](#).

Die Ziele befinden sich in einer Availability Zone, die nicht aktiviert ist.

Wenn Sie Ziele in einer Availability Zone registrieren, aber die Availability Zone nicht aktivieren, erhalten diese registrierten Ziele keinen Datenverkehr vom Load Balancer.

Die Instance befindet sich in einer per Peering verbundenen VPC.

Wenn sich Instances in einer VPC befinden, die mit der Load Balancer-VPC per Peering verbunden ist, müssen Sie sie nach IP-Adresse und nicht nach Instance-ID bei Ihrem Load Balancer registrieren.

Die konfigurierte Server-ID stimmt nicht mit der auf dem Ziel konfigurierten ID überein

Wenn Sie QUIC-Listener verwenden, stellen Sie sicher, dass die auf dem Ziel konfigurierte ID mit der ID übereinstimmt, die für die Network Load Balancer Balancer-Zielgruppe konfiguriert ist.

Ziele erhalten mehr Zustandsprüfungsanfragen als erwartet.

Zustandsprüfungen für Network Load Balancers sind verteilt und verwenden einen Konsensmechanismus, um den Zustand des Ziels zu bestimmen. Daher erhalten Ziele mehr als die Anzahl der Zustandsprüfungen, die über die Einstellung `HealthCheckIntervalSeconds` konfiguriert wurden.

Ziele erhalten weniger Zustandsprüfungsanfragen als erwartet.

Überprüfen Sie, ob `net.ipv4.tcp_tw_recycle` aktiviert ist. Es ist bekannt, dass diese Einstellung Probleme mit Load Balancern verursachen kann. Die `net.ipv4.tcp_tw_reuse`-Einstellung wird als eine sicherere Alternative betrachtet.

Fehlerhafte Ziele erhalten Anfragen vom Load Balancer.

Dies tritt auf, wenn alle registrierten Ziele fehlerhaft sind. Wenn mindestens ein fehlerfreies registriertes Ziel vorhanden ist, leitet Ihr Network Load Balancer Anforderungen nur seine fehlerfreien registrierten Ziele weiter.

Wenn nur fehlerhafte registrierte Ziele vorhanden sind, leitet der Ihr Network Load Balancer Anforderungen an alle registrierten Ziele weiter, bekannt als Fail-open-Modus. Der Network Load Balancer tut dies, anstatt alle IP-Adressen aus dem DNS zu entfernen, wenn alle Ziele fehlerhaft sind und die jeweiligen Availability Zones kein fehlerfreies Ziel haben, an das Anforderungen gesendet werden können.

Am Ziel schlagen HTTP- oder HTTPS-Zustandsprüfungen aufgrund nicht übereinstimmender Host-Header fehl

Der HTTP-Host-Header in der Zustandsprüfungsanforderung enthält die IP-Adresse des Load Balancer-Knotens und des Listener-Ports anstelle der IP-Adresse des Ziels und des Zustandsprüfungs-Ports. Wenn Sie eingehende Anforderungen nach Host-Header zuweisen, müssen Sie sicherstellen, dass Zustandsprüfungen mit den HTTP-Host-Header übereinstimmen. Eine weitere Möglichkeit besteht darin, an einem anderen Port einen separaten HTTP-Dienst hinzuzufügen und die Zielgruppe so zu konfigurieren, dass sie stattdessen diesen Port für Zustandsprüfungen verwendet. Alternativ können Sie TCP-Zustandsprüfungen verwenden.

Einem Load Balancer konnte keine Sicherheitsgruppe zugeordnet werden

Wenn der Network Load Balancer ohne Sicherheitsgruppen erstellt wurde, kann er nach der Erstellung keine Sicherheitsgruppen unterstützen. Sie können eine Sicherheitsgruppe nur während der Erstellung einem Load Balancer oder einem vorhandenen Load Balancer zuordnen, der ursprünglich mit Sicherheitsgruppen erstellt wurde.

Es konnten nicht alle Sicherheitsgruppen entfernt werden

Wenn der Network Load Balancer mit Sicherheitsgruppen erstellt wurde, muss ihm jederzeit mindestens eine Sicherheitsgruppe zugeordnet sein. Sie können nicht alle Sicherheitsgruppen gleichzeitig aus dem Load Balancer entfernen.

Erhöhung der TCP_ELB_Reset_Count-Metrik

Für jede TCP-Anforderung, die ein Client über einen Network Load Balancer sendet, wird der Zustand dieser Verbindung nachverfolgt. Werden länger als die vorgegebene Leerlaufzeit weder vom Client noch vom Ziel Daten über die Verbindung gesendet, wird die Verbindung beendet. Wenn bis zum Ablauf des Leerlaufzeitlimits keine Daten von einem Client oder Ziel gesendet wurden, empfängt er ein TCP-RST-Paket, um anzugeben, dass die Verbindung nicht mehr gültig ist. Wenn ein Ziel fehlerhaft wird, sendet der Load Balancer außerdem ein TCP RST für Pakete, die auf den mit dem Ziel verknüpften Client-Verbindungen empfangen werden, es sei denn, das fehlerhafte Ziel veranlasst den Load Balancer zum Fail-Open.

Wenn Sie kurz vor oder kurz vor dem Anstieg der TCP_ELB_Reset_Count-Metrik einen Anstieg der UnhealthyHostCount-Metrik feststellen, wurden die TCP-RST-Pakete wahrscheinlich gesendet, weil das Ziel mit dem Fail begann, aber nicht als fehlerhaft markiert wurde. Wenn Sie einen dauerhaften Anstieg von TCP_ELB_Reset_Count feststellen, ohne dass Ziele als fehlerhaft markiert wurden, können Sie die VPC-Flow-Protokolle für Clients überprüfen, die Daten zu abgelaufenen Flows senden.

Verbindungen überschreiten bei Anfragen von einem Ziel an dessen Load Balancer das Zeitlimit.

Prüfen Sie, ob die IP-Erhaltung des Clients für Ihre Zielgruppe aktiviert ist. NAT-Loopback, auch bekannt als Hairpinning, wird nicht unterstützt, wenn die Client-IP-Erhaltung aktiviert ist.

Wenn es sich bei einer Instance um einen Client eines Load Balancers handelt, bei dem sie registriert ist und für die Client-IP-Erhaltung aktiviert ist, ist die Verbindung nur erfolgreich, wenn die Anfrage an eine andere Instanz weitergeleitet wird. Wenn die Anfrage an dieselbe Instance weitergeleitet wird, von der sie gesendet wurde, tritt bei der Verbindung ein Timeout auf, da die Quell- und Ziel-IP-Adressen identisch sind. Beachten Sie, dass dies für Amazon EKS-Pods gilt, die in derselben EC2-Worker-Node-Instance ausgeführt werden, obwohl sie unterschiedliche IP-Adressen haben.

Wenn eine Instance Anfragen an einen Load Balancer senden muss, mit dem sie registriert ist, führen Sie einen der folgenden Schritte aus:

- Deaktivieren Sie die Erhaltung der Client-IP. Verwenden Sie stattdessen das Proxy Protocol v2, um die Client-IP-Adresse abzurufen.
- Stellen Sie sicher, dass sich Container, die kommunizieren müssen, auf unterschiedlichen Container-Instances befinden.

Die Leistung nimmt beim Verschieben von Zielen an einen Network Load Balancer ab.

Sowohl Classic Load Balancers als auch Application Load Balancers verwenden Verbindungsmultiplexing, Network Load Balancers jedoch nicht. Aus diesem Grund können Ihre Ziele mehr TCP-Verbindungen hinter einem Network Load Balancer erhalten. Stellen Sie sicher, dass Ihre Ziele bereit sind, die Menge der Verbindungsanforderungen zu verarbeiten, die sie erhalten könnten.

Fehler bei der Portzuweisung für Back-End-Flows

Bei PrivateLink Datenverkehr oder wenn die [Client-IP-Erhaltung](#) deaktiviert ist, unterstützt ein Network Load Balancer 55.000 gleichzeitige Verbindungen oder etwa 55.000 Verbindungen pro Minute zu jedem eindeutigen Ziel (IP-Adresse und Port). Wenn Sie diese Grenzwerte überschreiten, steigt die Wahrscheinlichkeit von Fehlern bei der Portzuweisung. Mithilfe der `PortAllocationErrorCount` Metrik können Sie Fehler bei der Portzuweisung verfolgen. Sie können aktive Verbindungen mithilfe der `ActiveFlowCount` Metrik verfolgen. Weitere Informationen finden Sie unter [CloudWatch Metriken für Ihren Network Load Balancer](#).

Um Fehler bei der Portzuweisung zu beheben, empfehlen wir, der Zielgruppe Ziele hinzuzufügen.

Wenn Sie der Zielgruppe keine Ziele hinzufügen können, können Sie alternativ bis zu 7 [sekundäre IP-Adressen](#) zu den Netzwerkschnittstellen des Load Balancers hinzufügen. Die sekundären IP-Adressen werden automatisch aus den IPv4 CIDR-Blöcken der entsprechenden Subnetze zugewiesen. Jede sekundäre IP-Adresse verbraucht 6 Netzwerkadressierungseinheiten. Beachten Sie, dass Sie eine sekundäre IP-Adresse nach dem Hinzufügen nicht mehr entfernen können. Die einzige Möglichkeit, die sekundären IP-Adressen freizugeben, besteht darin, den Load Balancer zu löschen.

Zeitweise fehlgeschlagener TCP-Verbindungsaufbau oder Verzögerungen beim TCP-Verbindungsaufbau

Wenn die Beibehaltung der Client-IP-Adresse aktiviert ist, kann ein Client über denselben kurzlebigen Quellport eine Verbindung zu einer anderen Ziel-IP-Adresse herstellen. Diese Ziel-IP-Adressen können von demselben Load Balancer (in verschiedenen Availability Zones) stammen, wenn zonenübergreifender Load Balancing aktiviert ist, oder von verschiedenen Network Load Balancern, die dieselbe Ziel-IP-Adresse und denselben Port verwenden, registriert sind. Wenn diese

Verbindungen in diesem Fall an dieselbe Ziel-IP-Adresse und denselben Zielport weitergeleitet werden, sieht das Ziel eine doppelte Verbindung, da sie von derselben Client-IP-Adresse und demselben Port stammen. Dies führt zu Verbindungsfehlern und Verzögerungen beim Aufbau einer dieser Verbindungen. Dies tritt häufig auf, wenn sich ein NAT-Gerät vor dem Client befindet und dieselbe Quell-IP-Adresse und derselben Quellport zugewiesen werden, wenn eine Verbindung zu mehreren Network Load Balancer Balancer-IP-Adressen gleichzeitig hergestellt wird.

Sie können diese Art von Verbindungsfehlern reduzieren, indem Sie die Anzahl der vom Client oder NAT-Gerät zugewiesenen temporären Quellports oder die Anzahl der Ziele für den Load Balancer erhöhen. Wir empfehlen Clients, den Quellport zu ändern, der bei der Wiederverbindung nach diesen Verbindungsfehlern verwendet wird. Um diese Art von Verbindungsfehlern zu vermeiden, können Sie, wenn Sie einen einzelnen Network Load Balancer verwenden, in Betracht ziehen, den zonenübergreifenden Load Balancer zu deaktivieren. Wenn Sie mehrere Network Load Balancer verwenden, können Sie erwägen, nicht dieselbe Ziel-IP-Adresse und denselben Port zu verwenden, die in mehreren Zielgruppen registriert sind. Alternativ können Sie erwägen, die Client-IP-Erhaltung zu deaktivieren. Wenn Sie die Client-IP benötigen, können Sie sie mithilfe des Proxyprotokolls v2 abrufen. Weitere Informationen über das Proxyprotokoll v2 finden Sie unter [Proxy-Protokoll](#).

Möglicher Fehler bei der Bereitstellung des Load Balancers

Einer der Gründe, warum ein Network Load Balancer bei der Bereitstellung ausfallen könnte, ist, wenn Sie eine IP-Adresse verwenden, die bereits an anderer Stelle zugewiesen wurde (z. B. als sekundäre IP-Adresse für eine EC2-Instance zugewiesen). Diese IP-Adresse verhindert, dass der Load Balancer eingerichtet wird, und sein Zustand ist `failed`. Sie können dieses Problem lösen, indem Sie die Zuordnung der zugehörigen IP-Adresse aufheben und den Erstellungsvorgang erneut versuchen.

Der Verkehr ist ungleichmäßig auf die Ziele verteilt

TCP- und TLS-Listener leiten TCP-Verbindungen und UDP-Listener leiten UDP-Streams weiter. Der Load Balancer wählt Ziele mithilfe eines Flow-Hash-Algorithmus aus. Eine einzelne Verbindung von einem Client ist von Natur aus stickig.

Wenn Sie feststellen, dass einige Ziele offenbar mehr Traffic erhalten als andere, empfehlen wir Ihnen, die VPC-Flow-Logs zu überprüfen. Vergleichen Sie die Anzahl der eindeutigen Verbindungen für jede Ziel-IP-Adresse. Halten Sie das Zeitfenster so kurz wie möglich, da sich Zielregistrierung, -abmeldung und fehlerhafte Ziele auf diese Verbindungsnummern auswirken.

Im Folgenden sind mögliche Szenarien aufgeführt, in denen Verbindungen ungleichmäßig verteilt sein können:

- Wenn Sie mit einer kleinen Anzahl von Zielen beginnen und später weitere Ziele registrieren, haben die ursprünglichen Ziele immer noch Verbindungen zu Clients. Bei einem HTTP-Workload stellen Keepalives sicher, dass Clients Verbindungen wiederverwenden. Wenn Sie die maximale Anzahl an Keepalives in Ihrer Webanwendung verringern, würden Clients häufiger neue Verbindungen öffnen.
- Wenn die Zielgruppenbindung aktiviert ist, es nur eine geringe Anzahl von Clients gibt und die Clients über ein NAT-Gerät mit einer einzigen Quell-IP-Adresse kommunizieren, werden Verbindungen von diesen Clients an dasselbe Ziel weitergeleitet.
- Wenn der zonenübergreifende Lastenausgleich deaktiviert ist und die Clients die IP-Adresse des Load Balancers aus einer der Load Balancer-Zonen bevorzugen, würden die Verbindungen ungleichmäßig zwischen den Load Balancer-Zonen verteilt.

Die DNS-Namensauflösung enthält weniger IP-Adressen als aktivierte Availability Zones

Idealerweise stellt Ihr Network Load Balancer eine IP-Adresse pro aktivierter Availability Zone bereit, wenn mindestens ein fehlerfreier Host in der Availability Zone vorhanden ist. Wenn es in einer bestimmten Availability Zone keinen fehlerfreien Host gibt und das zonenübergreifende Load Balancing deaktiviert ist, wird die IP-Adresse des Network Load Balancer für diese AZ aus dem DNS entfernt.

Nehmen wir zum Beispiel an, Ihr Network Load Balancer hat drei Availability Zones aktiviert, die alle mindestens eine fehlerfreie registrierte Ziel-Instance haben.

- Wenn die registrierten Ziel-Instances in Availability Zone A fehlerhaft werden, wird die entsprechende IP-Adresse der Availability Zone A für den Network Load Balancer aus dem DNS entfernt.
- Wenn zwei der aktivierten Availability Zones keine fehlerfreien registrierten Ziel-Instances haben, werden die jeweiligen beiden IP-Adressen des Network Load Balancer aus dem DNS entfernt.
- Wenn in allen aktivierten Availability Zones keine fehlerfreien registrierten Zielinstanzen vorhanden sind, ist der Fail-Open-Modus aktiviert und DNS stellt alle IP-Adressen der drei im Ergebnis aktivierten IP-Adressen bereit. AZs

IP-fragmentierte Pakete werden nicht an Ziele weitergeleitet

Network Load Balancer unterstützen keine fragmentierten IP-Pakete für Nicht-UDP-Verkehr.

Beheben Sie Fehler bei fehlerhaften Zielen mithilfe der Ressourcenübersicht

Wenn Ihre Network 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 Network Load Balancer Balancer-Ressourcenübersicht an](#).

Die Ressourcenübersicht bietet zwei Ansichten: Übersicht und Karte mit fehlerhaften Zielen. 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 Network Load Balancer zugeordnet ist.

Note

Die Option „Ressourcendetails anzeigen“ muss aktiviert sein, damit die Zusammenfassung der Integritätsprüfung und die Fehlermeldungen für alle entsprechenden Ressourcen in der Ressourcenübersicht angezeigt werden können. 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 Gesundheitschecks nicht bestehen, überprüfen Sie die Einstellungen für die Gesundheitsprüfung 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. 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 Network 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: Das Zeitlimit für die Anfrage wurde überschritten
 - Stellen Sie sicher, dass die Sicherheitsgruppen und Network Access Control Lists (ACL), die Ihren Zielen und dem Network Load Balancer zugeordnet sind, die Konnektivität nicht blockieren.
 - Stellen Sie sicher, dass das Ziel über ausreichend Kapazität verfügt, um Verbindungen vom Network Load Balancer anzunehmen.
 - Die Antworten des Network Load Balancers auf die Systemdiagnose können in den Anwendungsprotokollen der einzelnen Ziele eingesehen werden. Weitere Informationen finden Sie unter [Ursachencodes für Gesundheitschecks](#).
- Ungesund: FailedHealthChecks
 - Stellen Sie sicher, dass das Ziel auf dem Health Check-Port auf Datenverkehr wartet.

Bei Verwendung eines TLS-Listeners

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 einer Ihrer Zuhörer:

- FIPS-Post-Quantum-TLS-Richtlinie — Verwendung von Backend-Verbindungen
ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09
- FIPS-Richtlinie — Verwendung von Backend-Verbindungen
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04
- Post-Quantum-TLS-Richtlinie — Nutzung von Backend-Verbindungen
ELBSecurityPolicy-TLS13-1-0-PQ-2025-09
- TLS 1.3-Richtlinie — Verwendung von Backend-Verbindungen
ELBSecurityPolicy-TLS13-1-0-2021-06
- Alle anderen TLS-Richtlinien, die Backend-Verbindungen verwenden
ELBSecurityPolicy-2016-08

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 Network Load Balancer bereitgestelltes Protokoll zur Einrichtung von TLS-Handshakes unterstützt.

Kontingente für Ihre Network Load Balancers

Ihr AWS-Konto hat Standardkontingente, früher als Limits bezeichnet, für jeden AWS Dienst. Sofern 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 Quoten für Ihre Network Load Balancers anzuzeigen, öffnen Sie die Konsole [Service Quotas](#). Wählen Sie im Navigationsbereich AWS-Services und wählen Sie Elastic Load Balancing. 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 Balancer](#)
- [Zielgruppen](#)
- [Load Balancer Balancer-Kapazitätseinheiten](#)

Load Balancer

Ihr AWS-Konto hat die folgenden Kontingente für Network Load Balancers.

Name	Standard	Anpassbar
Zertifikate pro Network Load Balancer	25	Ja
Listener pro Network Load Balancer	50	Nein
Network Load Balancer ENIs pro VPC	1 200 ¹	Ja
Network Load Balancers pro Region	50	Ja
Ziele pro Availability Zone und Network Load Balancer	500 ^{2, 3}	Ja
Ziele pro Network Load Balancer	3 000 ³	Ja

¹ Jeder Network Load Balancer verwendet eine Netzwerkschnittstelle pro Zone. Das Kontingent wird auf VPC-Ebene festgelegt. Bei der gemeinsamen Nutzung von Subnetzen oder VPCs wird die Nutzung für alle Mandanten berechnet.

² Wenn ein Ziel mit N Zielgruppen registriert ist, wird es als N Ziele für dieses Limit angerechnet. Jeder Application Load Balancer, der ein Ziel des Network Load Balancers ist, zählt als 50 Ziele, wenn zonenübergreifendes Load Balancing deaktiviert ist, oder als 100 Ziele, wenn zonenübergreifendes Load Balancing aktiviert ist.

³ Wenn zonenübergreifendes Load Balancing aktiviert ist, liegt das Maximum bei 500 Zielen pro Load Balancer, unabhängig von der Anzahl der Availability Zones.

Zielgruppen

Die folgenden Kontingente gelten für Zielgruppen.

Name	Standard	Anpassbar
Zielgruppen pro Region	3 000 ¹	Ja
Ziele pro Zielgruppe pro Region (Instances oder IP-Adressen)	1.000	Ja
Ziele pro Zielgruppe pro Region (Application Load Balancers)	1	Nein

¹ Dieses Kontingent wird von Application Load Balancers und Network Load Balancers geteilt.

Load Balancer Balancer-Kapazitätseinheiten

Die folgenden Kontingente gelten für Load Balancer-Kapazitätseinheiten (LCUs).

Name	Standard	Anpassbar
Reservierte Network Load Balancer-Kapazitätseinheiten (LCUs) pro Network Load Balancer, pro Availability Zone	45000	Ja

Name	Standard	Anpassbar
Reservierte Network Load Balancer Balancer-Kapazitätseinheiten (LCU) pro Region	0	Ja

Dokumentverlauf für Network Load Balancers

In der folgenden Tabelle werden die Versionen für Network Load Balancers beschrieben.

Änderung	Beschreibung	Datum
<u>Gewichtete Zielgruppen</u>	Diese Version bietet Unterstützung für Standardaktionen mit gewichteten Zielgruppen.	19. November 2025
<u>Support für QUIC- und TCP_QUIC-Protokolle</u>	Diese Version bietet Unterstützung für die Protokolle QUIC und TCP_QUIC.	13. November 2025
<u>Sekundäre IPv4 Adressen</u>	Diese Version bietet Unterstützung für das Hinzufügen von sekundären IPv4 Adressen zu den Netzwerkschnittstellen des Load Balancers.	29. Juli 2025
<u>Deaktivieren Sie Availability Zones</u>	Diese Version bietet Unterstützung für die Deaktivierung einer Availability Zone für einen vorhandenen Load Balancer.	13. Februar 2025
<u>Reservierung von Kapazitätseinheiten</u>	Diese Version bietet Unterstützung für die Festlegung einer Mindestkapazität für Ihren Load Balancer.	20. November 2024
<u>UDP-Unterstützung IPv6 für Dual-Stack-Loadbalancer</u>	Diese Version ermöglicht Clients den Zugriff auf UDP-basierte Anwendungen über IPv6	31. Oktober 2024
<u>RSA 3072-Bit- und ECDSA 256/384/521-Bit-Zertifikate</u>	Diese Version bietet Unterstützung für RSA 3072-Bit-	19. Januar 2024

	Zertifikate und 256-, 384- und 521-Bit-Zertifikate über (ACM) für den Elliptic Curve Digital Signature Algorithm (ECDSA). AWS Certificate Manager	
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
Zonale DNS-Affinität	Diese Version bietet Unterstützung für Clients, die den Load Balancer-DNS so auflösen, dass sie eine IP-Adresse in derselben Availability Zone (AZ) erhalten, in der sie sich befinden.	12. Oktober 2023
Deaktivieren Sie die Beendigung einer fehlerhaften Zielverbindung	Diese Version bietet Unterstützung für die Aufrechterhaltung aktiver Verbindungen zu Zielen, bei denen die Integritätsprüfungen nicht bestanden haben.	12. Oktober 2023
Standardmäßige Beendigung der UDP-Verbindung	Diese Version bietet standardmäßig Unterstützung für das Beenden von UDP-Verbindungen am Ende des Abmelde-Timeouts.	12. Oktober 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

Sicherheitsgruppen für Ihren Network Load Balancer	Diese Version bietet Unterstützung bei der Zuordnung von Sicherheitsgruppen zu Ihren Network Load Balancern bei der Erstellung.	10. August 2023
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.	17. November 2022
Zustandsprüfungskonfiguration	Diese Version bietet Verbesserungen an der Konfiguration von Zustandsprüfungen.	17. November 2022
Zonenübergreifendes Load Balancing	Diese Version bietet Unterstützung für die Konfiguration von zonenübergreifendem Load Balancing auf Zielgruppenebene.	17. November 2022
IPv6 Zielgruppen	Diese Version bietet Unterstützung für die Konfiguration von IPv6 Zielgruppen für Network Load Balancer.	23. November 2021
IPv6 interne Load Balancer	Diese Version bietet Unterstützung für die Konfiguration von IPv6 Zielgruppen für Network Load Balancer.	23. November 2021

TLS 1.3	Mit dieser Version werden Sicherheitsrichtlinien hinzugefügt, die TLS-Version 1.3 unterstützen.	14. Oktober 2021
Application Load Balancers als Ziele	Mit dieser Version wird die Unterstützung für die Konfiguration eines Application Load Balancer als Ziel eines Network Load Balancers hinzugefügt.	27. September 2021
Client-IP-Erhaltung	Mit dieser Version wird die Unterstützung für die Client-IP-Erhaltung hinzugefügt.	4. 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
Dual-Stack-Modus	Diese Version bietet Unterstützung für den Dual-Stack-Modus, der es Clients ermöglicht, sowohl über Adressen als auch über IPv4 Adressen eine Verbindung zum Load Balancer herzustellen. IPv6	13. November 2020
Verbindungsabbruch bei Abmeldung	Mit diesem Release wird die Unterstützung für das Schließen von Verbindungen zu abgemeldeten Zielen nach dem Timeout der Abmeldung hinzugefügt.	13. November 2020

ALPN-Richtlinien	In dieser Version wird Unterstützung für Application Layer Protocol Negotiation (ALPN)-Einstellungslisten hinzugefügt.	27. Mai 2020
Sticky Sessions	Diese Version unterstützt Sticky Sessions basierend auf Quell-IP-Adresse und -protokoll.	28. Februar 2020
Gemeinsam genutzte Subnetze	Diese Version bietet Unterstützung für die Angabe von Subnetzen, die von einem anderen AWS-Konto für Sie freigegeben wurden.	26. November 2019
Private IP-Adressen	In dieser Version können Sie eine private IP-Adresse aus dem IPv4 Adressbereich des Subnetzes angeben, das Sie angeben, wenn Sie eine Availability Zone für einen internen Load Balancer aktivieren.	25. November 2019
Subnetze hinzufügen	Diese Version bietet Unterstützung für die Aktivierung zusätzlicher Availability Zones, nachdem Sie Ihren Load Balancer erstellt haben.	25. November 2019
Sicherheitsrichtlinien für FS	Diese Version bietet Unterstützung für drei weitere vordefinierte Forward Secrecy-Sicherheitsrichtlinien.	8. Oktober 2019

<u>SNI-Unterstützung</u>	In dieser Version wurde SNI-Unterstützung (Server Name Indication) hinzugefügt.	12. September 2019
<u>UDP-Protokoll</u>	Diese Version bietet Unterstützung für das UDP-Protokoll.	24. Juni 2019
<u>In einer neuen Region verfügbar</u>	Diese Version bietet Unterstützung für Network Load Balancer in der Region Asien-Pazifik (Osaka).	12. Juni 2019
<u>TLS-Protokoll</u>	Diese Version bietet Unterstützung für das TLS-Protokoll.	24. Januar 2019
<u>Zonenübergreifendes Load Balancing</u>	In dieser Version wurde Support für die Aktivierung von zonenübergreifendem Load Balancing hinzugefügt.	22. Februar 2018
<u>Proxy-Protokoll</u>	Diese Version fügt Support für die Aktivierung des Proxy-Protokolls hinzu.	17. November 2017
<u>IP-Adressen als Ziele</u>	Diese Version bietet Unterstützung für die Registrierung von IP-Adressen als Ziele.	21. September 2017
<u>Neuer Typ von Load Balancern</u>	Mit dieser Version von Elastic Load Balancing werden Network Load Balancers eingeführt.	7. September 2017

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.