Gateway Load Balancer

Elastic Load Balancing

Elastic Load Balancing: Gateway Load Balancer

Table of Contents

Was ist ein Gateway Load Balancer?

Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele in einer oder mehreren Availability Zones. Es überwacht den Zustand der registrierten Ziele und leitet den Datenverkehr nur an die fehlerfreie 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 Balancer, der Ihren Anforderungen am besten entspricht, auswählen. In diesem Handbuch werden Gateway Load Balancer beschrieben. Weitere Informationen zu den anderen Load Balancer finden Sie im Benutzerhandbuch für Application Load Balancer, im Benutzerhandbuch für Network Load Balancer und im Benutzerhandbuch für Classic Load Balancer.

Übersicht über Gateway Load Balancer

Gateway Load Balancer ermöglichen die Bereitstellung, Skalierung und Verwaltung virtueller Appliances, wie Firewalls, Eindringungserkennungs- und -präventionssysteme und Deep-Packet-Inspection-Systeme. Es kombiniert ein transparentes Netzwerk-Gateway (d. h. ein einziger Ein- und Ausstiegspunkt für den gesamten Datenverkehr) und verteilt den Datenverkehr, während Ihre virtuellen Appliances mit dem Bedarf skaliert werden.

Ein Gateway Load Balancer arbeitet auf der dritten Ebene des Open Systems Interconnection (OSI) -Modells, der Netzwerkschicht. Es überwacht alle IP-Pakete über alle Ports und leitet den Datenverkehr an die Zielgruppe weiter, die in der Listener-Regel angegeben ist. Mithilfe von 5-Tupel (Standard), 3-Tupel oder 2-Tupel bleibt der Datenfluss bei einer bestimmten Ziel-Appliance erhalten. Der Gateway Load Balancer und seine registrierten virtuellen Appliance-Instanzen tauschen Anwendungsdatenverkehr über das GENEVEProtokoll auf Port 6081 aus.

Gateway Load Balancer verwenden Gateway Load Balancer-Endpunkte, um Datenverkehr sicher über Grenzen hinweg auszutauschen. VPC Ein Gateway Load Balancer-Endpunkt ist ein VPC Endpunkt, der private Konnektivität zwischen virtuellen Appliances im Service Provider VPC und Anwendungsservern im Service Consumer VPC bereitstellt. Sie stellen den Gateway Load Balancer genauso VPC wie die virtuellen Appliances bereit. Sie registrieren die virtuellen Appliances bei einer Zielgruppe für den Gateway Load Balancer.

Der Verkehr zu und von einem Gateway Load Balancer-Endpunkt wird mithilfe von Routing-Tabellen konfiguriert. Der Datenverkehr fließt vom Service Consumer VPC über den Gateway Load Balancer-Endpunkt zum Gateway Load Balancer im Service Provider VPC und kehrt dann zum Service Consumer zurück. VPC Sie müssen den Gateway Load Balancer-Endpunkt und die Anwendungsserver in verschiedenen Subnetzen erstellen. Auf diese Weise können Sie den Gateway Load Balancer-Endpunkt als nächsten Hop in der Routing-Tabelle für das Anwendungssubnetz konfigurieren.

Weitere Informationen finden Sie unter Zugriff auf virtuelle Appliances über AWS PrivateLink im AWS PrivateLink Handbuch.

Appliance-Anbieter

Sie sind für die Auswahl und Qualifizierung der Software von Appliance-Anbietern verantwortlich. Sie müssen darauf vertrauen, dass die Appliance-Software den Datenverkehr vom Load Balancer überprüft oder verändert. Die Appliance-Anbieter, die als Elastic Load Balancing Partner aufgeführt sind, haben ihre Appliance-Software in integriert und qualifiziert AWS. Sie können der Appliance-Software von Anbietern aus dieser Liste ein höheres Maß an Vertrauen entgegenbringen. AWS garantiert jedoch nicht die Sicherheit oder Zuverlässigkeit der Software dieser Anbieter.

Erste Schritte

Informationen zum Erstellen eines Gateway Load Balancer mit dem finden Sie AWS Management Console unterErste Schritte. Informationen zum Erstellen eines Gateway Load Balancer mit dem finden Sie AWS Command Line Interface unterErste Schritte mit der CLI.

Preisgestaltung

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

Erste Schritte mit Gateway Load Balancer

Gateway Load Balancers erleichtern die Bereitstellung, Skalierung und Verwaltung virtueller Appliances von Drittanbietern, wie z. B. Sicherheits-Appliances.

In diesem Tutorial werden wir ein Inspektionssystem mit einem Gateway Load Balancer und einem Gateway Load Balancer-Endpunkt implementieren.

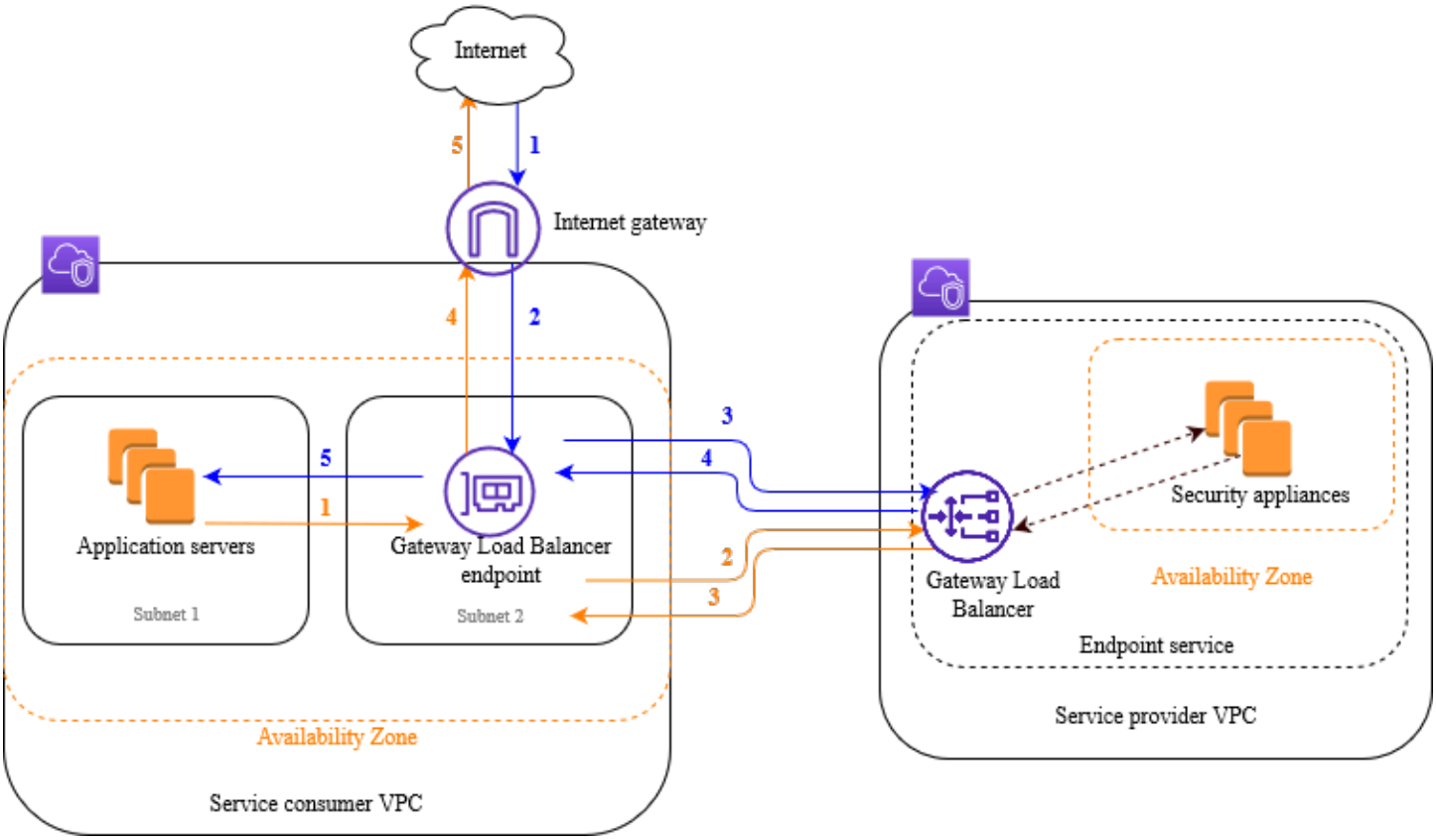
Inhalt

Übersicht

Ein Gateway Load Balancer-Endpunkt ist ein VPC Endpunkt, der private Konnektivität zwischen virtuellen Appliances im Service Provider VPC und Anwendungsservern im Service Consumer VPC bereitstellt. Der Gateway Load Balancer wird genauso eingesetzt VPC wie der der virtuellen Appliances. Diese Appliances werden als Zielgruppe des Gateway Load Balancers registriert.

Die Anwendungsserver werden in einem Subnetz (Zielsubnetz) im Service Consumer ausgeführtVPC, während sich der Gateway Load Balancer-Endpunkt in einem anderen Subnetz desselben Subnetzes befindet. VPC Der gesamte Datenverkehr, der VPC über das Internet-Gateway in den Service Consumer eingeht, wird zuerst an den Gateway Load Balancer-Endpunkt und dann an das Zielsubnetz weitergeleitet.

Ebenso wird der gesamte Datenverkehr, der die Anwendungsserver (Ziel-Subnetz) verlässt, an den Gateway Load Balancer-Endpunkt weitergeleitet, bevor er zurück ins Internet geleitet wird. Das folgende Netzwerkdiagramm veranschaulicht, wie ein Gateway Load Balancer-Endpunkt für den Zugriff auf einen Endpunktdienst verwendet wird.



Die folgenden nummerierten Punkte heben die in der vorangehenden Abbildung gezeigten Elemente hervor und erläutern sie.

Verkehr vom Internet zur Anwendung (blaue Pfeile):

1. Der Datenverkehr gelangt VPC über das Internet-Gateway zum Servicenutzer.
2. Der Verkehr wird als Ergebnis des Ingress-Routings an den Gateway Load Balancer-Endpunkt gesendet.
3. Der Datenverkehr wird an den Gateway Load Balancer gesendet, der den Datenverkehr an eine der Security Appliances weiterleitet.
4. Der Datenverkehr wird an den Gateway Load Balancer-Endpunkt zurückgesendet, nachdem er von der Security Appliance geprüft wurde.
5. Der Verkehr wird an die Anwendungsserver (Ziel-Subnetz) gesendet.

Verkehr von der Anwendung zum Internet (orangefarbene Pfeile):

1. Der Datenverkehr wird aufgrund der im Subnetz des Anwendungsservers konfigurierten Standardroute an den Gateway Load Balancer-Endpunkt gesendet.

2. Der Datenverkehr wird an den Gateway Load Balancer gesendet, der den Datenverkehr an eine der Security Appliances weiterleitet.
3. Der Datenverkehr wird an den Gateway Load Balancer-Endpunkt zurückgesendet, nachdem er von der Security Appliance geprüft wurde.
4. Der Datenverkehr wird basierend auf der Routing-Tabellenkonfiguration an das Internet-Gateway gesendet.
5. Der Datenverkehr wird zurück ins Internet geleitet.

Routing

Die Routing-Tabelle des Internet-Gateways muss einen Eintrag enthalten, der den für die Anwendungsserver bestimmten Datenverkehr an den Gateway Load Balancer-Endpunkt weiterleitet. Um den Gateway Load Balancer-Endpunkt anzugeben, verwenden Sie die ID des VPC Endpunkts. Das folgende Beispiel zeigt die Routen für eine Dualstack-Konfiguration.

Bestimmungsort	Ziel
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
Subnet 1 IPv4 CIDR	*vpc-endpoint-id*
Subnet 1 IPv6 CIDR	*vpc-endpoint-id*

Die Routing-Tabelle für das Subnetz mit den Anwendungsservern muss Einträge enthalten, die den gesamten Verkehr von den Anwendungsservern zum Gateway Load Balancer-Endpunkt leiten.

Bestimmungsort	Ziel
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Die Routing-Tabelle für das Subnetz mit dem Gateway Load Balancer-Endpunkt muss den Verkehr, der von der Prüfung zurückkommt, an sein endgültiges Ziel leiten. Bei Datenverkehr, der aus dem Internet stammt, sorgt die lokale Route dafür, dass er die Anwendungsserver erreicht. Fügen Sie für den Datenverkehr, der von den Anwendungsservern stammt, Einträge hinzu, die den gesamten Datenverkehr an das Internet-Gateway weiterleiten.

Bestimmungsort	Ziel
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Voraussetzungen

- Stellen Sie sicher, dass der Service Consumer VPC über mindestens zwei Subnetze für jede Availability Zone verfügt, die Anwendungsserver enthält. Ein Subnetz ist für den Gateway Load Balancer-Endpunkt, das andere für die Anwendungsserver.
- Der Gateway Load Balancer und die Ziele können sich im selben Subnetz befinden.
- Sie können kein Subnetz verwenden, das von einem anderen Konto gemeinsam genutzt wird, um den Gateway Load Balancer bereitzustellen.
- Starten Sie mindestens eine Sicherheits-Appliance-Instanz in jedem Sicherheits-Appliance-Subnetz des Service Providers. VPC Die Sicherheitsgruppen für diese Instanzen müssen den UDP Verkehr auf Port 6081 zulassen.

Schritt 1: Erstellen eines Gateway Load Balancer

Gehen Sie wie folgt vor, um Ihren Load Balancer, Listener und Ihre Zielgruppe zu erstellen.

Um den Load Balancer, den Listener und die Zielgruppe mithilfe der Konsole zu erstellen

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 Load Balancer erstellen aus.
4. Wählen Sie unter Gateway Load Balancer die Option Erstellen aus.
5. Basiskonfiguration
   a. Geben Sie im Feld Name des Load Balancers einen Namen für Ihren Load Balancer ein.
   b. Wählen Sie für den IP-Adresstyp, ob IPv4nur IPv4 Adressen unterstützt werden sollen oder Dualstack, um beide IPv4 Adressen zu unterstützen. IPv6
6. Netzwerkzuordnung
   a. Wählen Sie für VPCden Dienstanbieter aus. VPC
   b. Wählen Sie unter Zuordnungen alle Verfügbarkeitszonen aus, in denen Sie Security Appliance Instances gestartet haben, und ein Subnetz pro Verfügbarkeitszone.
7. IP-Listener-Routing
   a. Wählen Sie unter Standardaktion eine bestehende Zielgruppe aus, die den Datenverkehr erhalten soll. Diese Zielgruppe muss das GENEVE Protokoll verwenden.

      Wenn Sie keine Zielgruppe haben, wählen Sie Zielgruppe erstellen. Dadurch wird ein neuer Tab in Ihrem Browser geöffnet. Wählen Sie einen Zieltyp, geben Sie einen Namen für die Zielgruppe ein und behalten Sie das GENEVE Protokoll bei. Wählen Sie die Instanzen VPC mit Ihrer Sicherheits-Appliance aus. Ändern Sie die Einstellungen für die Zustandsprüfung nach Bedarf und fügen Sie alle benötigten Tags hinzu. Wählen Sie Weiter. Sie können Ihre Security Appliance Instances jetzt oder nach Abschluss dieses Verfahrens bei der Zielgruppe registrieren. Wählen Sie Zielgruppe erstellen und kehren Sie dann zur vorherigen Browser-Registerkarte zurück.
   b. (Optional) Erweitern Sie die Listener-Tags und fügen Sie die benötigten Tags hinzu.
8. (Optional) Erweitern Sie die Load Balancer-Tags und fügen Sie die benötigten Tags hinzu.
9. Wählen Sie Load Balancer erstellen aus.

Schritt 2: Erstellen eines Gateway Load Balancer-Endpunktdienstes

Gehen Sie wie folgt vor, um einen Endpunktdienst mit Ihrem Gateway Load Balancer zu erstellen.

So erstellen Sie einen Gateway Load Balancer-Endpunktdienst

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

2. Wählen Sie im Navigationsbereich Endpunktservices aus.
3. Wählen Sie das folgende Verfahren aus, um das folgende Verfahren zu erstellen:
   a. Wählen Sie für Load-Balancer-Typ Gateway aus.
   b. Wählen Sie für Verfügbare Load Balancer Ihren Gateway-Load-Balancer aus.
   c. Wählen Sie unter Akzeptanz für Endpunkt erforderlich die Option Akzeptanz erforderlich, um Verbindungsanfragen zu Ihrem Dienst manuell zu akzeptieren. Andernfalls werden sie automatisch akzeptiert.
   d. Führen Sie für Unterstützte IP-Adresstyp einen der folgenden Schritte aus:
      - Wählen Sie IPv4— Aktivieren Sie den Endpunktservice für die Annahme von IPv4 Anfragen.
      - Wählen IPv6— Ermöglichen Sie dem Endpunktdienst die Annahme von IPv6 Anfragen.
      - Wählen Sie IPv4und IPv6— Aktivieren Sie den Endpunktdienst so, dass er IPv4 sowohl als auch IPv6 Anfragen akzeptiert.
   e. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Tag-Schlüssel und -Wert eingeben.
   f. Wählen Sie Create (Erstellen) aus. Notieren Sie sich den Namen des Dienstes; Sie benötigen ihn, wenn Sie den Endpunkt erstellen.
4. Wählen Sie den neuen Endpunktdienst aus und wählen Sie Aktionen, Prinzipale zulassen. Geben Sie ARNs die Servicekonsumenten ein, die einen Endpunkt für Ihren Service erstellen dürfen. Ein Servicekonsument kann ein Benutzer, eine IAM Rolle oder sein AWS-Konto. Wählen Sie auf Allow principals (Prinzipale erlauben) aus.

Schritt 3: Erstellen eines Gateway Load Balancer-Endpunkts

Gehen Sie wie folgt vor, um einen Gateway Load Balancer-Endpunkt zu erstellen, der eine Verbindung zu Ihrem Gateway Load Balancer-Endpunktdienst herstellt. Gateway Load Balancer Endpunkte sind zonal. Es wird empfohlen, einen Gateway Load Balancer-Endpunkt pro Zone zu erstellen. Weitere Informationen finden Sie unter Zugriff auf virtuelle Appliances über AWS PrivateLink im AWS PrivateLink Handbuch.

So erstellen Sie einen Gateway Load Balancer-Endpunkt

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

2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen und gehen Sie wie folgt vor:
   a. Wählen Sie für Servicekategorie Andere Endpunkt-Services.
   b. Geben Sie bei Dienstname den Namen des Dienstes ein, den Sie zuvor notiert haben, und wählen Sie dann Dienst überprüfen.
   c. Wählen Sie für VPCden Servicenutzer ausVPC.
   d. Wählen Sie unter Subnets ein Subnetz für den Gateway Load Balancer-Endpunkt aus.
   e. Wählen Sie für IP address type (IP-Adressentyp) eine der folgenden Optionen aus:
      - IPv4— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 Adressbereiche haben.
      - IPv6— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.
      - Dualstack — Weisen Sie Ihren IPv4 Endpunkt-Netzwerkschnittstellen sowohl IPv6 Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.
   f. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Tag-Schlüssel und -Wert eingeben.
   g. Wählen Sie Endpunkt erstellen aus. Der ursprüngliche Status ist `pending acceptance`.

Um die Endpunkt-Verbindungsanfrage zu akzeptieren, gehen Sie wie folgt vor.

1. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
2. Wählen Sie den Endpunktservice aus.
3. Wählen Sie die Endpunktverbindung auf der Registerkarte Endpoint connections (Endpunktverbindungen) aus.
4. Um die Verbindungsanforderung zu akzeptieren, wählen Sie Actions (Aktionen), Accept endpoint connection request (Endpunkt-Verbindungsanforderung akzeptieren). Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`accept`** ein und wählen Sie dann Accept (Akzeptieren).

Schritt 4: Routing konfigurieren

Konfigurieren Sie die Routing-Tabellen für den Service Consumer VPC wie folgt. Dadurch können die Security Appliances eine Sicherheitsüberprüfung des eingehenden Datenverkehrs durchführen, der für die Anwendungsserver bestimmt ist.

So konfigurieren Sie das Routing

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle für den Internet-Gateway aus, und führen Sie die folgenden Schritte aus:
   a. Wählen Sie Aktionen und dann Routen bearbeiten.
   b. Wählen Sie Route hinzufügen aus. Geben Sie als Ziel den IPv4 CIDR Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target den VPC Endpunkt aus.
   c. Wenn Sie dies unterstützenIPv6, wählen Sie Route hinzufügen. Geben Sie als Ziel den IPv6 CIDR Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target den VPC Endpunkt aus.
   d. Wählen Sie Änderungen speichern.
4. Wählen Sie die Routing-Tabelle für das Subnetz mit den Anwendungsservern aus, und führen Sie folgende Schritte aus:
   a. Wählen Sie Aktionen und dann Routen bearbeiten.
   b. Wählen Sie Route hinzufügen aus. Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target den VPC Endpunkt aus.
   c. Wenn Sie dies unterstützenIPv6, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target den VPC Endpunkt aus.
   d. Wählen Sie Änderungen speichern.
5. Wählen Sie die Routing-Tabelle für das Subnetz mit dem Gateway-Load-Balancer-Endpunkt aus und tun Sie Folgendes:
   a. Wählen Sie Aktionen und dann Routen bearbeiten.
   b. Wählen Sie Route hinzufügen aus. Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

c. Wenn Sie dies unterstützenIPv6, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

d. Wählen Sie Änderungen speichern.

Erste Schritte mit Gateway Load Balancers mithilfe der AWS CLI

Gateway Load Balancers erleichtern die Bereitstellung, Skalierung und Verwaltung virtueller Appliances von Drittanbietern, wie z. B. Sicherheits-Appliances.

In diesem Tutorial werden wir ein Inspektionssystem mit einem Gateway Load Balancer und einem Gateway Load Balancer-Endpunkt implementieren.

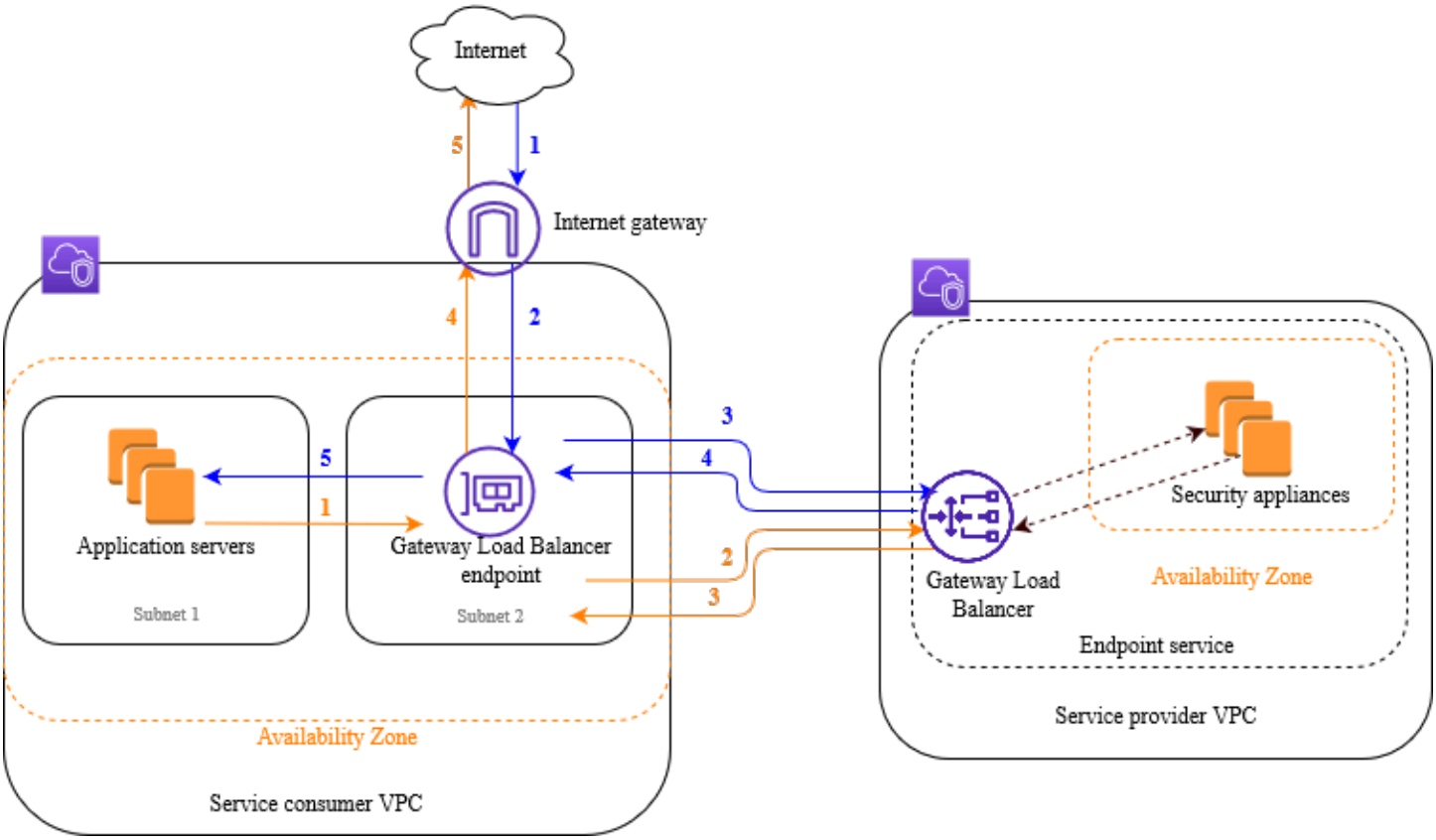
Inhalt

Übersicht

Ein Gateway Load Balancer-Endpunkt ist ein VPC Endpunkt, der private Konnektivität zwischen virtuellen Appliances im Service Provider VPC und Anwendungsservern im Service Consumer VPC bereitstellt. Der Gateway Load Balancer wird genauso eingesetzt VPC wie der der virtuellen Appliances. Diese Appliances werden als Zielgruppe des Gateway Load Balancers registriert.

Die Anwendungsserver werden in einem Subnetz (Zielsubnetz) im Service Consumer ausgeführtVPC, während sich der Gateway Load Balancer-Endpunkt in einem anderen Subnetz desselben Subnetzes befindet. VPC Der gesamte Datenverkehr, der VPC über das Internet-Gateway in den Service Consumer eingeht, wird zuerst an den Gateway Load Balancer-Endpunkt und dann an das Zielsubnetz weitergeleitet.

Ebenso wird der gesamte Datenverkehr, der die Anwendungsserver (Ziel-Subnetz) verlässt, an den Gateway Load Balancer-Endpunkt weitergeleitet, bevor er zurück ins Internet geleitet wird. Das folgende Netzwerkdiagramm veranschaulicht, wie ein Gateway Load Balancer-Endpunkt für den Zugriff auf einen Endpunktdienst verwendet wird.



Die folgenden nummerierten Punkte heben die in der vorangehenden Abbildung gezeigten Elemente hervor und erläutern sie.

Verkehr vom Internet zur Anwendung (blaue Pfeile):

1. Der Datenverkehr gelangt VPC über das Internet-Gateway zum Servicenutzer.
2. Der Verkehr wird als Ergebnis des Ingress-Routings an den Gateway Load Balancer-Endpunkt gesendet.
3. Der Datenverkehr wird an den Gateway Load Balancer gesendet, der den Datenverkehr an eine der Security Appliances weiterleitet.
4. Der Datenverkehr wird an den Gateway Load Balancer-Endpunkt zurückgesendet, nachdem er von der Security Appliance geprüft wurde.
5. Der Verkehr wird an die Anwendungsserver (Ziel-Subnetz) gesendet.

Verkehr von der Anwendung zum Internet (orangefarbene Pfeile):

1. Der Datenverkehr wird aufgrund der im Subnetz des Anwendungsservers konfigurierten Standardroute an den Gateway Load Balancer-Endpunkt gesendet.

2. Der Datenverkehr wird an den Gateway Load Balancer gesendet, der den Datenverkehr an eine der Security Appliances weiterleitet.
3. Der Datenverkehr wird an den Gateway Load Balancer-Endpunkt zurückgesendet, nachdem er von der Security Appliance geprüft wurde.
4. Der Datenverkehr wird basierend auf der Routing-Tabellenkonfiguration an das Internet-Gateway gesendet.
5. Der Datenverkehr wird zurück ins Internet geleitet.

Routing

Die Routing-Tabelle des Internet-Gateways muss einen Eintrag enthalten, der den für die Anwendungsserver bestimmten Datenverkehr an den Gateway Load Balancer-Endpunkt weiterleitet. Um den Gateway Load Balancer-Endpunkt anzugeben, verwenden Sie die ID des VPC Endpunkts. Das folgende Beispiel zeigt die Routen für eine Dualstack-Konfiguration.

Bestimmungsort	Ziel
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
Subnet 1 IPv4 CIDR	*vpc-endpoint-id*
Subnet 1 IPv6 CIDR	*vpc-endpoint-id*

Die Routing-Tabelle für das Subnetz mit den Anwendungsservern muss Einträge enthalten, die den gesamten Verkehr von den Anwendungsservern zum Gateway Load Balancer-Endpunkt leiten.

Bestimmungsort	Ziel
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Die Routing-Tabelle für das Subnetz mit dem Gateway Load Balancer-Endpunkt muss den Verkehr, der von der Prüfung zurückkommt, an sein endgültiges Ziel leiten. Bei Datenverkehr, der aus dem Internet stammt, sorgt die lokale Route dafür, dass er die Anwendungsserver erreicht. Fügen Sie für den Datenverkehr, der von den Anwendungsservern stammt, Einträge hinzu, die den gesamten Datenverkehr an das Internet-Gateway weiterleiten.

Bestimmungsort	Ziel
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Voraussetzungen

- Installieren Sie die AWS CLI oder aktualisieren Sie sie auf die aktuelle Version von, AWS CLI wenn Sie eine Version verwenden, die Gateway Load Balancers nicht unterstützt. Weitere Informationen finden Sie unter Installieren der AWS Command Line Interface im AWS Command Line Interface - Benutzerhandbuch.
- Stellen Sie sicher, dass der Service Consumer VPC über mindestens zwei Subnetze für jede Availability Zone verfügt, die Anwendungsserver enthält. Ein Subnetz ist für den Gateway Load Balancer-Endpunkt, das andere für die Anwendungsserver.
- Stellen Sie sicher, dass der Dienstanbieter VPC über mindestens zwei Subnetze für jede Availability Zone verfügt, die Sicherheits-Appliance-Instanzen enthält. Ein Subnetz ist für den Gateway Load Balancer, das andere für die Instances.
- Starten Sie mindestens eine Sicherheits-Appliance-Instanz in jedem Sicherheits-Appliance-Subnetz des Service Providers. VPC Die Sicherheitsgruppen für diese Instanzen müssen den UDP Verkehr auf Port 6081 zulassen.

Schritt 1: Erstellen Sie einen Gateway Load Balancer und registrieren Sie Ziele

Gehen Sie wie folgt vor, um Ihre Load Balancer-, Listener- und Zielgruppen zu erstellen und um Ihre Security Appliance Instances als Ziele zu registrieren.

So erstellen Sie einen Gateway Load Balancer und registrieren Ziele

1. Verwenden Sie den create-load-balancerBefehl, um einen Load Balancer des Typs zu erstellen. `gateway` Sie können für jede Verfügbarkeitszone, in der Sie Security Appliance Instances gestartet haben, ein Subnetz angeben.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer --type gateway --
   subnets provider-subnet-id
   ```

   Standardmäßig werden nur IPv4 Adressen unterstützt. Um IPv4 sowohl IPv6 Adressen als auch zu unterstützen, fügen Sie die `--ip-address-type dualstack` Option hinzu.

   Die Ausgabe enthält den Amazon-Ressourcennamen (ARN) des Load Balancers mit dem im folgenden Beispiel gezeigten Format.

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

2. Verwenden Sie den create-target-groupBefehl, um eine Zielgruppe zu erstellen, und geben Sie dabei den Dienstanbieter an, VPC bei dem Sie Ihre Instances gestartet haben.

   ```
   aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 --
   vpc-id provider-vpc-id
   ```

   Die Ausgabe umfasst die ARN der Zielgruppe mit dem folgenden Format.

   ```
   arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
   targets/0123456789012345
   ```

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

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

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

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --default-actions
 Type=forward,TargetGroupArn=targetgroup-arn
```

Die Ausgabe enthält die ARN des Zuhörers im folgenden Format.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/gwy/my-load-
balancer/1234567890123456/abc1234567890123
```

5. (Optional) Sie können den Zustand der registrierten Ziele für Ihre Zielgruppe mit dem folgenden describe-target-healthBefehl überprüfen.

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

Schritt 2: Erstellen eines Gateway Load Balancer-Endpunkts

Gehen Sie wie folgt vor, um einen Gateway Load Balancer-Endpunkt zu erstellen. Gateway Load Balancer Endpunkte sind zonal. Es wird empfohlen, einen Gateway Load Balancer-Endpunkt pro Zone zu erstellen. Weitere Informationen finden Sie unter Zugriff auf virtuelle Appliances über AWS PrivateLink.

So erstellen Sie einen Gateway Load Balancer-Endpunkt

1. Verwenden Sie den Befehl create-vpc-endpoint-service-configuration, um mit Ihrem Gateway Load Balancer eine Endpunktdienstkonfiguration zu erstellen.

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-
arns loadbalancer-arn --no-acceptance-required
```

Um sowohl IPv4 IPv6 Adressen als auch zu unterstützen, fügen Sie die `--supported-ip-address-types ipv4 ipv6` Option hinzu.

Die Ausgabe enthält die Dienst-ID (z. B. vpce-svc-12345678901234567) und den Dienstnamen (z. B. com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567).

2. Verwenden Sie den Befehl modify-vpc-endpoint-service-permissions, um es Servicekunden zu ermöglichen, einen Endpunkt für Ihren Service zu erstellen. Ein Dienstnutzer kann ein Benutzer, eine IAM Rolle oder AWS-Konto sein. Im folgenden Beispiel wird die Berechtigung für das angegebene Objekt hinzugefügt AWS-Konto.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-
svc-12345678901234567 --add-allowed-principals arn:aws:iam::123456789012:root
```

3. Verwenden Sie den create-vpc-endpointBefehl, um den Gateway Load Balancer-Endpunkt für Ihren Service zu erstellen.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --service-
name com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpc-
id --subnet-ids consumer-subnet-id
```

Um sowohl IPv4 IPv6 Adressen als auch zu unterstützen, fügen Sie die `--ip-address-type dualstack` Option hinzu.

Die Ausgabe enthält die ID des Gateway Load Balancer-Endpunkts (z. B. vpce-01234567890abcdef).

Schritt 3: Routing konfigurieren

Konfigurieren Sie die Routing-Tabellen für den Service Consumer VPC wie folgt. Dadurch können die Security Appliances eine Sicherheitsüberprüfung des eingehenden Datenverkehrs durchführen, der für die Anwendungsserver bestimmt ist.

So konfigurieren Sie das Routing

1. Verwenden Sie den Befehl create-route, um der Routing-Tabelle für das Internet-Gateway Einträge hinzuzufügen, die den für die Anwendungsserver bestimmten Verkehr an den Gateway Load Balancer-Endpunkt weiterleiten.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1
 IPv4 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

Wenn Sie dies unterstützenIPv6, fügen Sie die folgende Route hinzu.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1
 IPv6 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

2. Verwenden Sie den Befehl create-route, um der Routing-Tabelle für das Subnetz mit den Anwendungsservern einen Eintrag hinzuzufügen, der den gesamten Datenverkehr von den Anwendungsservern an den Gateway Load Balancer-Endpunkt leitet.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block
 0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef
```

Wenn Sie dies unterstützenIPv6, fügen Sie die folgende Route hinzu.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block ::/0
 --vpc-endpoint-id vpce-01234567890abcdef
```

3. Verwenden Sie den Befehl create-route, um der Routing-Tabelle für das Subnetz mit dem Gateway Load Balancer-Endpunkt einen Eintrag hinzuzufügen, der den gesamten von den Anwendungsservern stammenden Datenverkehr an das Internet-Gateway weiterleitet.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-01234567890abcdef
```

Wenn Sie dies unterstützenIPv6, fügen Sie die folgende Route hinzu.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block ::/0 --
gateway-id igw-01234567890abcdef
```

4. Wiederholen Sie diesen Vorgang für jede Anwendungsteilnetz-Routing-Tabelle in jeder Zone.

Gateway Load Balancer

Verwenden Sie einen Gateway Load Balancer, um eine Flotte virtueller Appliances bereitzustellen und zu verwalten, die das GENEVE Protokoll unterstützen.

Ein Gateway Load Balancer arbeitet auf der dritten Ebene des Open Systems Interconnection (OSI) -Modells. Er überwacht alle IP-Pakete an allen Ports und leitet den Datenverkehr mithilfe des Protokolls auf Port 6081 an die in der Listener-Regel angegebene Zielgruppe weiter. GENEVE

Sie können Ziele zu Ihrem Load Balancer hinzufügen oder entfernen, wenn sich Ihre Anforderungen ändern, ohne den Gesamtfluss der Anfragen 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 Arbeitslasten automatisch skaliert werden.

Inhalt

Load Balancer-Status

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

`provisioning`

Der Gateway Load Balancer wird gerade eingerichtet.

`active`

Der Gateway Load Balancer ist vollständig eingerichtet und bereit, den Datenverkehr zu routen.

`failed`

Der Gateway Load Balancer konnte nicht eingerichtet werden.

IP-Adresstyp

Sie können die Arten von IP-Adressen festlegen, die die Anwendungsserver für den Zugriff auf Ihre Gateway Load Balancers verwenden können.

Gateway Load Balancer unterstützen die folgenden IP-Adresstypen:

`ipv4`

Nur IPv4 wird unterstützt.

`dualstack`

Sowohl als IPv4 auch IPv6 werden unterstützt.

Überlegungen

- Der virtuellen privaten Cloud (VPC) und den Subnetzen, die Sie für den Load Balancer angeben, müssen Blöcke zugeordnet IPv6 CIDR sein.
- Die Routing-Tabellen für die Subnetze im Service Consumer VPC müssen den IPv6 Verkehr weiterleiten, und das Netzwerk ACLs für diese Subnetze muss Datenverkehr zulassen. IPv6
- Ein Gateway Load Balancer kapselt sowohl IPv4 den Client-Verkehr als auch den IPv6 Client-Verkehr mit einem IPv4 GENEVE Header und sendet ihn an die Appliance. Die Appliance kapselt sowohl IPv4 den Client-Verkehr als auch den IPv6 Client-Verkehr mit einem IPv4 GENEVE Header und sendet ihn zurück an den Gateway Load Balancer.

Weitere Hinweise zu IP-Adresstypen finden Sie unter. Aktualisieren Sie die IP-Adresstypen für Ihren Gateway Load Balancer

Verfügbarkeitszonen

Wenn Sie einen Gateway Load Balancer erstellen, aktivieren Sie eine oder mehrere Verfügbarkeitszonen und geben das Subnetz an, das jeder Zone entspricht. Wenn Sie mehrere Verfügbarkeitszonen aktivieren, wird sichergestellt, dass der Load Balancer den Datenverkehr auch dann weiterleiten kann, wenn eine Verfügbarkeitszone nicht mehr verfügbar ist. Die von Ihnen angegebenen Teilnetze müssen jeweils über mindestens 8 verfügbare IP-Adressen verfügen. Subnetze können nicht entfernt werden, nachdem der Load Balancer erstellt wurde. Um ein Subnetz zu entfernen, müssen Sie einen neuen Load Balancer erstellen.

Timeout bei Leerlauf

Für jede TCP Anfrage, die über einen Gateway 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. Nach Ablauf des Timeouts im Leerlauf betrachtet der Load Balancer den nächsten Flow TCP SYN als neuen Flow und leitet ihn an ein neues Ziel weiter. Datenpakete, die nach Ablauf des Timeouts im Leerlauf gesendet werden, werden jedoch verworfen.

Der Standardwert für das Leerlauf-Timeout für TCP Flows 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 zurückzusetzen.

Der Load Balancer UDP ist zwar verbindungslos, behält aber den UDP Flussstatus auf der Grundlage der Quell- und Ziel-IP-Adressen und -Ports bei. Dadurch wird sichergestellt, dass Pakete, die zu demselben Flow gehören, konsistent an dasselbe Ziel gesendet werden. Nach Ablauf des Timeouts im Leerlauf betrachtet der Load Balancer das eingehende UDP Paket als neuen Datenfluss 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.

EC2Instances 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

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

`deletion_protection.enabled`

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

`load_balancing.cross_zone.enabled`

Gibt an, ob zonenübergreifendes Load Balancing aktiviert ist. Der Standardwert ist `false`.

Weitere Informationen finden Sie unter Bearbeiten Sie die Load Balancer-Attribute.

Netzwerk ACLs

Wenn sich die Anwendungsserver und der Gateway Load Balancer-Endpunkt im selben Subnetz befinden, werden die NACL Regeln für den Datenverkehr von den Anwendungsservern zum Gateway Load Balancer-Endpunkt ausgewertet.

Asymmetrische Strömungen

Gateway Load Balancer unterstützen asymmetrische Datenflüsse, wenn der Load Balancer das anfängliche Flow-Paket verarbeitet und das Antwort-Flow-Paket nicht durch den Load Balancer geleitet wird. Asymmetrisches Routing wird nicht empfohlen, da es zu einer verringerten Netzwerkleistung führen kann. Gateway Load Balancers unterstützen keine asymmetrischen Flüsse, wenn der Load Balancer das erste Flusspaket nicht verarbeitet, sondern das Antwort-Flow-Paket durch den Load Balancer geleitet wird.

Maximale Übertragungseinheit des Netzwerks () MTU

Die maximale Übertragungseinheit (MTU) entspricht der Größe des größten Datenpakets, das über das Netzwerk übertragen werden kann. Die Gateway Load Balancer-Schnittstelle MTU unterstützt Pakete mit bis zu 8.500 Byte. Pakete mit einer Größe von mehr als 8 500 Byte, die an der Gateway Load Balancer-Schnittstelle ankommen, werden verworfen.

Ein Gateway Load Balancer kapselt IP-Verkehr mit einem GENEVE Header und leitet ihn an die Appliance weiter. Durch den GENEVE Kapselungsprozess werden dem Originalpaket 64 Byte hinzugefügt. Um Pakete mit bis zu 8.500 Byte zu unterstützen, stellen Sie daher sicher, dass die MTU Einstellung Ihrer Appliance Pakete mit mindestens 8.564 Byte unterstützt.

Gateway Load Balancer unterstützen keine IP-Fragmentierung. Darüber hinaus generieren Gateway Load Balancer keine ICMP Meldung „Ziel nicht erreichbar: Fragmentierung erforderlich und DF gesetzt“. Aus diesem Grund wird Path MTU Discovery (PMTUD) nicht unterstützt.

Erstellen eines Gateway-Load-Balancers

Ein Gateway Load Balancer nimmt Anfragen von Clients entgegen und verteilt sie auf Ziele in einer Zielgruppe, z. B. EC2 auf Instanzen.

Führen Sie die folgenden Aufgaben aus AWS Management Console, um einen Gateway Load Balancer mit dem zu erstellen. Informationen zum Erstellen eines Gateway Load Balancer mit dem finden Sie AWS CLI alternativ unterErste Schritte mit der CLI.

Aufgaben

- Voraussetzungen
- Erstellen Sie den Load Balancer
- Wichtige nächste Schritte

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass die virtuelle private Cloud (VPC) für Ihren Gateway Load Balancer mindestens ein Subnetz in jeder Availability Zone hat, in der Sie Ziele haben.

Erstellen Sie den Load Balancer

Gehen Sie wie folgt vor, um Ihren Gateway Load Balancer zu erstellen. Geben Sie grundlegende Konfigurationsinformationen für Ihren Load Balancer an, z. B. einen Namen und einen IP-Adresstyp. Geben Sie anschließend Informationen über Ihr Netzwerk und den Listener an, der den Datenverkehr an Ihre Zielgruppen weiterleitet. Gateway Load Balancer benötigen Zielgruppen, die das Protokoll verwenden. GENEVE

Um den Load Balancer und den Listener mithilfe der Konsole zu erstellen

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 Load Balancer erstellen aus.
4. Wählen Sie unter Gateway Load Balancer die Option Erstellen aus.

5. Basiskonfiguration
    a. Geben Sie im Feld Name des Load Balancers einen Namen für Ihren Load Balancer ein. Beispiel, **`my-glb`**. Der Name Ihres Gateway Load Balancer muss innerhalb Ihrer Gruppe von Load Balancers für die Region eindeutig sein. Er darf maximal 32 Zeichen lang sein, nur alphanumerische Zeichen und Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.
    b. Wählen Sie für den IP-Adresstyp, ob IPv4nur IPv4 Adressen unterstützt werden sollen oder Dualstack, um beide IPv4 Adressen zu unterstützen. IPv6
6. Netzwerkzuordnung
    a. Wählen Sie für VPCden Dienstanbieter aus. VPC
    b. Wählen Sie unter Zuordnungen alle Verfügbarkeitszonen aus, in denen Sie Security Appliance Instances gestartet haben, sowie die entsprechenden öffentlichen Subnetze.
7. IP-Listener-Routing
    a. Wählen Sie unter Standardaktion die Zielgruppe aus, die den Datenverkehr erhalten soll. Wenn Sie keine Zielgruppe haben, wählen Sie Zielgruppe erstellen. Weitere Informationen finden Sie unter Erstellen einer Zielgruppe.
    b. (Optional) Erweitern Sie die Listener-Tags und fügen Sie die benötigten Tags hinzu.
8. (Optional) Erweitern Sie die Load Balancer-Tags und fügen Sie die benötigten Tags hinzu.
9. Überprüfen Sie Ihre Konfiguration, und wählen Sie dann Load Balancer erstellen.

Wichtige nächste Schritte

Nachdem Sie Ihren Load Balancer erstellt haben, stellen Sie sicher, dass Ihre EC2 Instances die erste Zustandsprüfung bestanden haben. Um Ihren Load Balancer zu testen, müssen Sie einen Gateway Load Balancer-Endpunkt erstellen und Ihre Routing-Tabelle aktualisieren, damit der Gateway Load Balancer-Endpunkt der nächste Hop ist. Diese Konfigurationen werden in der VPC Amazon-Konsole festgelegt. Weitere Informationen finden Sie im Tutorial Erste Schritte.

Aktualisieren Sie die IP-Adresstypen für Ihren Gateway Load Balancer

Sie können Ihren Gateway Load Balancer so konfigurieren, dass Anwendungsserver nur über Adressen oder über beide IPv4 IPv4 Adressen auf Ihren Load Balancer zugreifen können

(IPv6Dualstack). Der Load Balancer kommuniziert mit Zielen auf der Grundlage des IP-Adresstyps der Zielgruppe. Weitere Informationen finden Sie unter IP-Adresstyp.

So aktualisieren Sie den IP-Adresstyp mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf Aktionen und anschließend auf IP-Adressentyp bearbeiten.
5. Wählen Sie als IP-Adresstyp IPv4, um nur IPv4 Adressen zu unterstützen, oder Dualstack, um beide IPv4 Adressen zu unterstützen. IPv6
6. Wählen Sie Save (Speichern) aus.

Um den IP-Adresstyp mit dem zu aktualisieren AWS CLI

Verwenden Sie den set-ip-address-typeBefehl.

Attribute für Ihren Gateway Load Balancer bearbeiten

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

Load Balancer-Attribute

- Löschschutz
- Zonenübergreifendes Load Balancing

Löschschutz

Um zu verhindern, dass Ihr Gateway Load Balancer versehentlich gelöscht wird, können Sie den Löschschutz aktivieren. Der Löschschutz ist standardmäßig deaktiviert.

Wenn Sie den Löschschutz für Ihren Gateway Load Balancer aktiviert haben, müssen Sie ihn deaktivieren, bevor Sie den Gateway Load Balancer löschen können.

So aktivieren Sie mithilfe der Konsole den Löschschutz:

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

2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer.
4. Wählen Sie Aktionen, Attribute bearbeiten.
5. Wählen Sie auf der Seite Load Balancer-Attribute bearbeiten die Option Aktivieren für Löschschutz und wählen Sie dann Speichern.

So deaktivieren Sie mithilfe der Konsole den Löschschutz:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer.
4. Wählen Sie Aktionen, Attribute bearbeiten.
5. Löschen Sie auf der Seite Load Balancer-Attribute bearbeiten die Option Aktivieren für Löschschutz und wählen Sie dann Speichern.

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

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

Zonenübergreifendes Load Balancing

Standardmäßig verteilt jeder Load Balancer-Knoten Datenverkehr nur auf die registrierten Ziele in seiner Verfügbarkeitszone. Wenn Sie den zonenübergreifenden Load Balancing aktivieren, verteilt jeder Gateway Load Balancer-Knoten den Datenverkehr auf die registrierten Ziele in allen aktivierten Verfügbarkeitszonen. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing im Benutzerhandbuch für Elastic Load Balancing.

Aktivieren des zonenübergreifenden Load Balancing mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer.
4. Wählen Sie Aktionen, Attribute bearbeiten.
5. Wählen Sie auf der Seite Load Balancer-Attribute bearbeiten die Option Aktivieren für zonenübergreifendes Load Balancing und wählen Sie dann Speichern.

Um den zonenübergreifenden Lastenausgleich mit dem zu aktivieren AWS CLI

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

Einen Gateway Load Balancer taggen

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

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

Wenn Sie mit einem Tag fertig sind, können Sie es von Ihrem Gateway 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. Zulässige Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF -8 dargestellt werden können, 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 AWS die Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

So aktualisieren Sie die Tags für einen Gateway Load Balancer über die Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer.
4. Wählen Sie Tags, Tags hinzufügen/bearbeiten, und führen Sie dann einen oder mehrere der folgenden Schritte aus:

   a. Um ein Tag zu aktualisieren, bearbeiten Sie die Werte von Schlüssel und Wert.

   b. Um ein neues Tag hinzuzufügen, wählen Sie Tag erstellen. Geben Sie für Schlüssel und Wert Werte ein.
   c. Um ein Tag zu löschen, wählen Sie das Symbol „Löschen“ (X) neben dem Tag.
5. Wenn Sie mit dem Aktualisieren der Tags fertig sind, klicken Sie auf Speichern.

Um die Tags für einen Gateway Load Balancer mit dem AWS CLI

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

Löschen eines Gateway-Load-Balancers

Sobald Ihr Gateway Load Balancer verfügbar ist, wird Ihnen jede angefangene Stunde, die Sie ihn in Betrieb halten, in Rechnung gestellt. Wenn Sie den Gateway Load Balancer nicht mehr benötigen, können Sie ihn löschen. Sobald der Gateway Load Balancer gelöscht wird, fallen keine Gebühren mehr für ihn an.

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

Das Löschen eines Gateway Load Balancers löscht auch dessen Listener. Das Löschen eines Gateway Load Balancers hat keine Auswirkungen auf seine registrierten Ziele. Beispielsweise laufen Ihre EC2 Instanzen weiter und sind weiterhin für ihre Zielgruppen registriert. Informationen zum Löschen Ihrer Zielgruppen finden Sie unter Löschen Sie eine Zielgruppe für Ihren Gateway Load Balancer.

So löschen Sie einen Gateway Load Balancer mithilfe der Konsole

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

Um einen Gateway Load Balancer mit dem AWS CLI

Verwenden Sie den delete-load-balancerBefehl.

Listener für Ihre Gateway Load Balancer

Wenn Sie Ihren Gateway Load Balancer erstellen, fügen Sie einen Listener hinzu. Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft.

Listener für Gateway Load Balancer überwachen alle IP-Pakete an allen Ports. Sie können kein Protokoll oder keinen Port angeben, wenn Sie einen Listener für einen Gateway Load Balancer erstellen.

Wenn Sie einen Listener erstellen, geben Sie eine Regel für Routing-Anforderungen an. Diese Regel leitet Anfragen an die angegebene Zielgruppe weiter. Sie können die Listener-Regel aktualisieren, um Anfragen an eine andere Zielgruppe weiterzuleiten.

Listener-Attribute

Im Folgenden sind die Listener-Attribute für Gateway 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.

Aktualisieren Sie die Zielgruppe für Ihren Gateway Load Balancer-Listener

Wenn Sie einen Listener erstellen, geben Sie eine Regel für Routing-Anforderungen an. Diese Regel leitet Anfragen an die angegebene Zielgruppe weiter. Sie können die Listener-Regel aktualisieren, um Anfragen an eine andere Zielgruppe weiterzuleiten.

Aktualisieren Ihres Listeners unter Verwendung der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Load Balancer aus und wählen Sie anschließend Listeners aus.

4. Wählen Sie Listener bearbeiten.
5. Wählen Sie für Weiterleitung an Zielgruppe eine Zielgruppe aus.
6. Wählen Sie Save (Speichern) aus.

Um Ihren Listener mit dem zu aktualisieren AWS CLI

Verwenden Sie den Befehl modify-listener.

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

Für jede TCP Anfrage, die über einen Gateway 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. Der Standardwert für das Leerlauf-Timeout für TCP Flows beträgt 350 Sekunden, kann aber auf einen beliebigen Wert zwischen 60 und 6000 Sekunden aktualisiert werden.

Um das TCP Leerlauf-Timeout mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer.
4. Wählen Sie auf der Registerkarte „Listener“ die Optionen „Aktionen“, „Listener-Details anzeigen“ aus.
5. Wählen Sie auf der Listener-Detailseite auf der Registerkarte Attribute die Option Bearbeiten aus.
6. Geben Sie auf der Seite Listener-Attribute bearbeiten im Abschnitt Listener-Attribute einen Wert für TCP das Leerlauf-Timeout ein.
7. Wählen Sie Save Changes (Änderungen speichern)

Um das TCP Leerlauf-Timeout zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den modify-listener-attributesBefehl mit dem `tcp.idle_timeout.seconds` Attribut.

Zielgruppen für Ihre Gateway Load Balancer

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 Verkehr wird an die in der Listener-Regel angegebene Zielgruppe weitergeleitet. Sie können unterschiedliche Zielgruppen für verschiedene Arten von Anfragen erstellen.

Sie definieren die Einstellungen für die Zustandsprüfung Ihres Gateway Load Balancer auf der Basis der einzelnen Zielgruppen. 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 Gateway Load Balancer kontinuierlich den Zustand aller mit der Zielgruppe registrierten Ziele, die sich in einer für den Gateway Load Balancer aktivierten Availability Zone befinden. Der Gateway Load Balancer leitet Anfragen an die registrierten Ziele weiter, die in Ordnung sind. Weitere Informationen finden Sie unter Gesundheitschecks für Gateway Load Balancer Balancer-Zielgruppen.

Inhalt

Weiterleitungskonfiguration

Zielgruppen für Gateway Load Balancer unterstützen das folgende Protokoll und den folgenden Port:

- Protokoll: GENEVE

- Port: 6081

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.

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

- Die Subnetze der VPC für die Zielgruppe
- 10.0.0.0/8 (1918) RFC
- 100,64,0,0/10 (6598) RFC
- 172,16,0,0/12 RFC (1918)
- 192.168,0,0/16 (RFC1918)

> **Important**
>
> Sie können keine öffentlich weiterleitungsfähigen IP-Adressen angeben.

Registrierte Ziele

Ihr Gateway Load Balancer dient als zentraler Kontaktpunkt für Clients und verteilt den eingehenden Datenverkehr an die fehlerfreien registrierten Ziele. Jede Zielgruppe muss mindestens ein registriertes Ziel in jeder Availability Zone haben, die für den Gateway Load Balancer aktiviert ist. Sie können jedes Ziel bei einer oder mehreren Zielgruppen registrieren.

Wenn die Nachfrage steigt, können Sie zusätzliche Ziele mit einer oder mehreren Zielgruppen registrieren, um die Nachfrage zu bewältigen. Der Gateway Load Balancer beginnt mit dem Routing des Datenverkehrs zu einem neu registrierten Ziel, sobald der Registrierungsprozess abgeschlossen ist.

Wenn die Nachfrage zurückgeht oder Sie Ihre Ziele warten müssen, können Sie Ziele aus Ihren Zielgruppen abmelden. Bei der Aufhebung der Registrierung eines Ziels wird es aus Ihrer Zielgruppe entfernt. Ansonsten hat dies keine Auswirkungen auf das Ziel. Der Gateway Load Balancer beendet das Routing des Datenverkehrs zu einem Ziel, sobald es abgemeldet 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.

Zielgruppenattribute

Sie können die folgenden Attribute mit Zielgruppen verwenden:

`deregistration_delay.timeout_seconds`

Die Zeitspanne, die Elastic Load Balancing warten soll, bevor es den Status eines abgemeldeten Ziels von `draining` auf `unused` ändert. Der Bereich liegt zwischen 0 und 3 600 Sekunden. Der Standardwert beträgt 300 Sekunden.

`stickiness.enabled`

Gibt an, ob die konfigurierbare Flow-Stickiness für die Zielgruppe aktiviert ist. Die möglichen Werte sind `true` oder `false`. Der Standardwert lautet „false“. Wenn das Attribut auf `false` gesetzt ist, wird 5_tuple verwendet.

`stickiness.type`

Gibt die Art der Flow-Stickiness an. Die möglichen Werte für Zielgruppen, die Gateway Load Balancern zugeordnet sind, sind:

- `source_ip_dest_ip`
- `source_ip_dest_ip_proto`

`target_failover.on_deregistration`

Gibt an, wie der Gateway Load Balancer bestehende Flows behandelt, wenn ein Ziel abgemeldet wird. Die möglichen Werte sind `rebalance` und `no_rebalance`. Der Standardwert ist `no_rebalance`. Die beiden Attribute (`target_failover.on_deregistration` und

`target_failover.on_unhealthy`) können nicht unabhängig voneinander festgelegt werden. Der Wert, den Sie für beide Attribute festlegen, muss identisch sein.

`target_failover.on_unhealthy`

Gibt an, wie der Gateway Load Balancer bestehende Flows behandelt, wenn ein Ziel fehlerhaft ist. Die möglichen Werte sind `rebalance` und `no_rebalance`. Der Standardwert ist `no_rebalance`. Die beiden Attribute (`target_failover.on_deregistration` und `target_failover.on_unhealthy`) können nicht unabhängig voneinander festgelegt werden. Der Wert, den Sie für beide Attribute festlegen, muss identisch sein.

Weitere Informationen finden Sie unter Zielgruppenattribute bearbeiten.

Erstellen Sie eine Zielgruppe für Ihren Gateway Load Balancer

Sie registrieren Ziele für Ihren Gateway Load Balancer mit Hilfe einer Zielgruppe.

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 Listener.

Sie können jederzeit Ziele zu Ihrer Zielgruppe hinzufügen oder aus dieser entfernen. Weitere Informationen finden Sie unter Ziele registrieren. Sie können auch die Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern. Weitere Informationen finden Sie unter Einstellungen für die Zustandsprüfung ändern.

Erstellen einer Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Basiskonfiguration
   a. Wählen Sie unter Zieltyp wählen die Option Instancen, um Ziele nach Instance-ID anzugeben, oder wählen Sie IP-Adressen, um Ziele nach IP-Adresse anzugeben.
   b. Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein. Dieser Name muss pro Region und Konto eindeutig sein, darf maximal 32 Zeichen lang sein, nur

alphanumerische Zeichen oder Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.

c. Stellen Sie sicher, dass Protokoll `GENEVE` und Port sind`6081`. Andere Protokolle oder Ports werden nicht unterstützt.

d. Wählen Sie für VPCdie virtuelle private Cloud (VPC) mit den Security Appliance-Instances aus, die Sie in Ihre Zielgruppe aufnehmen möchten.

5. (Optional) Ändern Sie die Einstellungen für die Zustandsprüfungen und die erweiterten Einstellungen nach Bedarf. Überschreitet die Anzahl der Zustandsprüfung nacheinander den Schwellenwert für fehlerhaften Zustand, nimmt der Load Balancer das Ziel aus dem Verkehr. Überschreitet die Anzahl der Zustandsprüfungen nacheinander den Schwellenwert für fehlerfreien Zustand, nimmt der Load Balancer das Ziel wieder in Betrieb. Weitere Informationen finden Sie unter Gesundheitschecks für Gateway Load Balancer Balancer-Zielgruppen.
6. (Optional) Erweitern Sie Tags und fügen Sie die benötigten Tags hinzu.
7. Wählen Sie Weiter.
8. Unter Ziele registrieren fügen Sie ein oder mehrere Ziele wie folgt hinzu:
   - Wenn der Zieltyp Instances ist, wählen Sie eine oder mehrere Instances aus, geben Sie einen oder mehrere Ports ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus.
   - Wenn der Zieltyp IP-Adressen ist, wählen Sie das Netzwerk aus, geben Sie die IP-Adresse und die Ports ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus.
9. Wählen Sie Zielgruppe erstellen aus.

Um eine Zielgruppe mit dem zu erstellen AWS CLI

Verwenden Sie den create-target-groupBefehl, um die Zielgruppe zu erstellen, den Befehl add-tags, um Ihre Zielgruppe zu taggen, und den Befehl register-targets, um Ziele hinzuzufügen.

Gesundheitschecks für Gateway Load Balancer Balancer-Zielgruppen

Sie können Ihre Ziele bei einer oder mehreren Zielgruppen registrieren. Ihr Gateway Load Balancer beginnt mit dem Routing von Anfragen an ein neu registriertes Ziel, sobald der Registrierungsprozess

abgeschlossen ist. Es kann einige Minuten dauern, bis der Registrierungsvorgang abgeschlossen ist und die Zustandsprüfungen beginnen.

Der Gateway Load Balancer sendet in regelmäßigen Abständen eine Anfrage an jedes registrierte Ziel, um dessen Status zu überprüfen. Nach Abschluss jeder Zustandsprüfung schließt der Gateway Load Balancer die Verbindung, die für die Zustandsprüfung hergestellt wurde.

Zustandsprüfungseinstellungen

Sie konfigurieren aktive Zustandsprüfungen für die Ziele in einer Zielgruppe, indem Sie die folgenden Einstellungen verwenden. Wenn die Integritätsprüfungen die angegebene Anzahl UnhealthyThresholdCountaufeinanderfolgender Fehler überschreiten, nimmt der Gateway Load Balancer das Ziel außer Betrieb. Wenn die Zustandsprüfungen die angegebene Anzahl von HealthyThresholdCountaufeinanderfolgenden Erfolgen überschreiten, nimmt der Gateway Load Balancer das Ziel wieder in Betrieb.

Einstellung	Beschreibung
HealthCheckProtocol	Das Protokoll, das der Load Balancer bei der Durchführung von Zustandsprüfungen für Ziele verwendet. Die möglichen Protokolle sind HTTPHTTPS, undTCP. Die Standardeinstellun g istTCP.
HealthCheckPort	Der Port, den Gateway Load Balancer bei der Durchführung von Zustandsprüfungen für Ziele verwendet. Der Bereich reicht von 1 bis 65 535. Der Standardwert ist 80.
HealthCheckPath	[HTTP/HTTPShealth checks] 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

Einstellung	Beschreibung
	Bereich reicht von 2 bis 120. Der Standardwert ist 5.
HealthCheckIntervalSeconds	Der etwaige Zeitraum in Sekunden zwischen den Zustandsprüfungen der einzelnen Ziele. Der Bereich reicht von 5 bis 300. Standardm äßig ist ein Zeitraum von 10 Sekunden festgelegt. Dieser Wert muss größer oder gleich sein HealthCheckTimeoutSeconds. **Important** Zustandsprüfungen für Gateway Load Balancers sind verteilt und verwenden einen Konsensmechanismus, um den Zustand des Ziels zu bestimmen. Daher sollten Sie damit rechnen, dass die Ziel-Appliances innerhalb des konfiguri erten Zeitintervalls mehrere Zustandsp rüfungen erhalten.
HealthyThresholdCount	Die Anzahl der aufeinanderfolgenden erfolgrei chen Zustandsprüfungen, die erforderlich ist, damit ein fehlerhaftes Ziel als stabil eingestuft wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 5.
UnhealthyThresholdCount	Die Anzahl fortlaufender fehlgeschlagener Zustandsprüfungen, die erforderlich ist, damit ein Ziel als nicht betriebsbereit eingestuft wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 2.

Einstellung	Beschreibung
Matcher	[HTTP/HTTPSHealth Checks] Die HTTP Codes, die verwendet werden sollen, wenn geprüft wird, ob ein Ziel erfolgreich reagiert hat. Dieser Wert muss 200–399 betragen.

Zustandsstatus des Ziels

Bevor der Gateway Load Balancer eine Zustandsprüfungsanfrage an ein Ziel sendet, müssen Sie es in einer Zielgruppe registrieren, seine Zielgruppe in einer Listener-Regel angeben und sicherstellen, dass die Verfügbarkeitszone des Ziels für den Gateway Load Balancer aktiviert ist.

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

Wert	Beschreibung
`initial`	Der Gateway Load Balancer ist gerade dabei, das Ziel zu registrieren oder die ersten Zustandsprüfungen des Ziels durchzuführen. Zugehörige Ursachencodes: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	Das Ziel ist fehlerfrei. Zugehörige Ursachencodes: Keine
`unhealthy`	Das Ziel hat nicht auf eine Zustandsprüfung geantwortet oder die Zustandsprüfung ist fehlgeschlagen. Zugehöriger Ursachencode: `Target.FailedHealthChecks`
`unused`	Das Ziel wurde nicht für eine Zielgruppe registriert, die Zielgruppe wird nicht in einer Listener-Regel verwendet oder das Ziel befindet sich in einer Availability Zone, die

Wert	Beschreibung
	nicht aktiviert ist, oder das Ziel sich im Status „Angehalten“ oder „Beendet“. Zugehörige Ursachencodes: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`
`draining`	Die Registrierung für das Ziel wird aufgehoben, und Connection Draining wird durchgeführt. Zugehöriger Ursachencode: `Target.DeregistrationInProgress`
`unavailable`	Die Zielintegrität ist nicht verfügbar. Zugehöriger Ursachencode: `Elb.InternalError`

Ursachencodes für Zustandsprüfungen

Wenn der Status eines Ziels einen anderen Wert als hat`Healthy`, werden ein Ursachencode und eine Beschreibung des Problems API zurückgegeben, und die Konsole zeigt dieselbe Beschreibung an. Ursachencodes, die mit `Elb` beginnen, haben ihren Ursprung auf dem Gateway Load Balancer, und Ursachencodes, die mit `Target` beginnen, haben ihren Ursprung auf der Seite des Ziels.

Ursachencode	Beschreibung
`Elb.InitialHealthChecking`	Anfängliche Zustandsprüfungen in Bearbeitung
`Elb.InternalError`	Zustandsprüfungen aufgrund eines internen Fehles fehlgeschlagen
`Elb.RegistrationInProgress`	Zielregistrierung wird durchgeführt
`Target.DeregistrationInProgress`	Zielregistrierung wird aufgehoben

Ursachencode	Beschreibung
`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 Gateway Load Balancer zu erhalten Ziel ist in einer Verfügbarkeitszone, die nicht für den Gateway Load Balancer aktiviert ist
`Target.NotRegistered`	Ziel ist nicht in der Zielgruppe registriert

Gateway Load Balancer Ziel-Ausfall-Szenarien

Bestehende Flows: Standardmäßig werden bestehende Flows an dasselbe Ziel weitergeleitet, es sei denn, der Flow läuft ab oder wird zurückgesetzt, unabhängig vom Status und dem Registrierungsstatus des Ziels. Dieser Ansatz erleichtert den Verbindungsverlust und eignet sich auch für Firewalls von Drittanbietern, die aufgrund der hohen Auslastung manchmal nicht in der Lage sind, auf Integritätsprüfungen zu reagieren. CPU Weitere Informationen finden Sie unter Target-Failover.

Neue Flows: Neue Flows werden an ein gesundes Ziel gesendet. Wenn eine Lastausgleichsentscheidung für einen Flow getroffen wurde, sendet der Gateway Load Balancer den Flow an dasselbe Ziel, selbst wenn dieses Ziel fehlerhaft wird oder andere Ziele fehlerfrei werden.

Wenn alle Ziele fehlerhaft sind, wählt der Gateway Load Balancer ein zufälliges Ziel aus und leitet den Datenverkehr für die Dauer des Datenflusses an dieses Ziel weiter, bis es entweder

zurückgesetzt wird oder die Zeit abgelaufen ist. Da der Datenverkehr an ein fehlerhaftes Ziel weitergeleitet wird, wird der Datenverkehr unterbrochen, bis das Ziel wieder fehlerfrei ist.

TLS1.3: Wenn eine Zielgruppe mit HTTPS Integritätsprüfungen konfiguriert ist, bestehen ihre registrierten Ziele die Integritätsprüfungen nicht, wenn sie nur TLS 1.3 unterstützen. Diese Ziele müssen eine frühere Version von unterstützenTLS, z. B. TLS 1.2.

Zonenübergreifender Load Balancer: Standardmäßig ist der Load Balancer zwischen Verfügbarkeitszonen deaktiviert. Wenn der zonenübergreifende Load Balancer aktiviert ist, kann jeder Gateway Load Balancer alle Ziele in allen Verfügbarkeitszonen sehen, und sie werden alle gleich behandelt, unabhängig von ihrer Zone.

Entscheidungen über Load Balancing und Zustandsprüfung sind zwischen den Zonen stets unabhängig. Selbst wenn der zonenübergreifende Load Balancer aktiviert ist, ist das Verhalten für bestehende und neue Flows dasselbe wie oben beschrieben. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing im Benutzerhandbuch für Elastic Load Balancing.

Zustand der Ziele prüfen

Sie können den Zustand der Ziele, die in Ihren Zielgruppen registriert sind, überprüfen.

Überprüfen des Zustands Ihrer Ziele mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancer aus.
3. Wählen Sie den Namen der Zielgruppe, um deren Detailseite zu öffnen.
4. In der Registerkarte Targets (Ziele) gibt die Spalte Status den Status der einzelnen Ziele wider.
5. Wenn der Zielstatus einen anderen Wert als `Healthy` hat, enthält die Spalte Statusdetails weitere Informationen.

Um den Zustand Ihrer Ziele mit dem zu überprüfen AWS CLI

Verwenden Sie den describe-target-healthBefehl. Die Ausgabe dieses Befehls enthält den Zustand des Ziels. Sie enthält auch einen Ursachencode, wenn der Status einen anderen Wert als `Healthy` aufweist.

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.

Einstellungen für die Zustandsprüfung ändern

Sie können einige Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern.

Ändern von Zustandsprüfungseinstellungen für eine Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancer aus.
3. Wählen Sie den Namen der Zielgruppe, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Gruppendetails im Abschnitt Einstellungen für die Zustandsprüfung die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Einstellungen für die Zustandsprüfung bearbeiten die Einstellungen nach Bedarf und wählen Sie dann Änderungen speichern.

Um die Einstellungen für den Gesundheitscheck für eine Zielgruppe zu ändern, verwenden Sie den AWS CLI

Verwenden Sie den modify-target-groupBefehl.

Zielgruppenattribute für Ihren Gateway Load Balancer bearbeiten

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

Zielgruppenattribute

- Ziel-Failover
- Verzögerung der Registrierungsaufhebung
- Flow-Stickiness

Ziel-Failover

Mit Ziel-Failover legen Sie fest, wie der Gateway Load Balancer bestehende Verkehrsflüsse behandelt, wenn ein Ziel nicht mehr funktionsfähig ist oder wenn das Ziel abgemeldet wird.

Standardmäßig sendet der Gateway Load Balancer vorhandene Flows weiterhin an dasselbe Ziel, selbst wenn das Ziel ausgefallen oder abgemeldet ist. Sie können diese Flows verwalten, indem Sie sie entweder erneut verarbeiten (`rebalance`) oder sie im Standardstatus belassen (`no_rebalance`).

Keine Neugewichtung:

Der Gateway Load Balancer sendet weiterhin bestehende Flows an ausgefallene oder leere Ziele. Wenn der Gateway Load Balancer das Ziel nicht erreichen kann, wird der Verkehr unterbrochen.

Neue Flows werden jedoch an fehlerfreie Ziele gesendet. Dies ist das Standardverhalten.

Neugewichtung:

Der Gateway Load Balancer bereitet die vorhandenen Flows neu auf und sendet sie nach Ablauf der Verzögerungszeit für die Deregistrierung an fehlerfreie Ziele.

Bei abgemeldeten Zielen hängt die Mindestzeit bis zum Failover von der Verzögerung bei der Abmeldung ab. Das Ziel wird erst als abgemeldet markiert, wenn die Verzögerung bei der Abmeldung abgeschlossen ist.

Bei fehlerhaften Zielen hängt die Mindestzeit bis zum Failover von der Konfiguration der Zielgruppen-Zustandsprüfung ab (Intervall mal Schwellenwert). Dies ist die Mindestzeit, vor der ein Ziel als fehlerhaft gekennzeichnet wird. Nach Ablauf dieser Zeit kann es aufgrund der zusätzlichen Übertragungszeit und des Backoffs für die TCP erneute Übertragung mehrere Minuten dauern, bis der Gateway Load Balancer neue Datenflüsse an fehlerfreie Ziele umleitet.

Um das Ziel-Failover-Attribut mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Seite mit den Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Attribute bearbeiten den Wert von Ziel-Failover nach Bedarf.
6. Wählen Sie Änderungen speichern.

Um das Ziel-Failover-Attribut mit dem zu aktualisieren AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit den folgenden Schlüssel-Wert-Paaren:

- Key=`target_failover.on_deregistration` und Value= `no_rebalance` (Standard) oder `rebalance`
- Key= `target_failover.on_unhealthy` und Value= `no_rebalance` (Standard) oder `rebalance`

> **Note**
>
> Beide Attribute (`target_failover.on_deregistration` und `target_failover.on_unhealthy`) müssen denselben Wert haben.

Verzögerung der Registrierungsaufhebung

Wenn Sie ein Ziel deregistrieren, verwaltet der Gateway Load Balancer die Datenströme zu diesem Ziel wie folgt:

Neue Flows

Der Gateway Load Balancer sendet keine neuen Flows mehr.

Bestehende Flows

Der Gateway Load Balancer verarbeitet die vorhandenen Flows auf der Grundlage des Protokolls:

- TCP: Bestehende Flows werden geschlossen, wenn sie länger als 350 Sekunden inaktiv waren.
- Andere Protokolle: Bestehende Flows werden geschlossen, wenn sie länger als 120 Sekunden inaktiv waren.

Um das Leeren bestehender Flows zu erleichtern, können Sie das Flow-Rebalancing für Ihre Zielgruppe aktivieren. Weitere Informationen finden Sie unter the section called “Ziel-Failover”.

Bei einem abgemeldeten Ziel wird angezeigt, dass es `draining` ist, bis der Timeout abläuft. Nach Ablauf des Timeouts für die Verzögerung bei der Abmeldung wechselt das Ziel in einen Status `unused`.

Um das Delay-Attribut für die Abmeldung mithilfe der Konsole zu aktualisieren

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

2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Seite mit den Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Attribute bearbeiten den Wert für Abmeldeverzögerung nach Bedarf.
6. Wählen Sie Änderungen speichern.

Um das Attribut für die Verzögerung bei der Abmeldung zu aktualisieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl modify-target-group-attributes.

Flow-Stickiness

Standardmäßig hält der Gateway Load Balancer mithilfe von 5-Tupel (für TCP /-Flows) die Bindung von UDP Datenströmen an eine bestimmte Ziel-Appliance aufrecht. Das 5-Tupel umfasst Quell-IP, Quellport, Ziel-IP, Zielport und Transportprotokoll. Sie können das Attribut Beibehaltungs-Typ verwenden, um die Vorgabe (5-Tupel) zu ändern und entweder 3-Tupel (Quell-IP, Ziel-IP und Transportprotokoll) oder 2-Tupel (Quell-IP und Ziel-IP) zu wählen.

Erwägungen zur Flow-Stickiness

- Flow-Stickiness wird auf Zielgruppenebene konfiguriert und angewendet und gilt für den gesamten Verkehr, der an die Zielgruppe geht.
- Flow-Stickiness mit 2- und 3-Tupeln werden nicht unterstützt, wenn AWS Transit Gateway der Appliance-Modus aktiviert ist. Um den Appliance-Modus auf Ihrem zu verwenden AWS Transit Gateway, verwenden Sie 5-Tuple Flow Stickiness auf Ihrem Gateway Load Balancer
- Flow-Stickiness kann zu einer ungleichmäßigen Verteilung von Verbindungen und Flüssen führen, was die Verfügbarkeit des Ziels beeinträchtigen kann. Es wird empfohlen, alle bestehenden Flows zu beenden oder abfließen zu lassen, bevor Sie den Beibehaltungs-Typ der Zielgruppe ändern.

Um das Flow Stickiness-Attribut mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.

3. Wählen Sie den Namen der Zielgruppe, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Seite mit den Gruppendetails im Abschnitt Attribute die Option Bearbeiten aus.
5. Ändern Sie auf der Seite Attribute bearbeiten den Wert für Flow Stickiness nach Bedarf.
6. Wählen Sie Änderungen speichern.

Um das Flow Stickiness-Attribut mit dem zu aktualisieren AWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit den Attributen `stickiness.enabled` und `stickiness.type` Zielgruppenattributen.

Registrieren Sie Ziele für Ihren Gateway Load Balancer

Wenn Ihr Ziel dazu bereit ist, Anforderungen zu bearbeiten, registrieren Sie es bei mindestens einer Zielgruppe. Sie können sich Ziele nach Instance-ID oder IP-Adresse registrieren. Der Gateway Load Balancer beginnt mit der Weiterleitung von Anfragen an das Ziel, sobald der Registrierungsvorgang abgeschlossen ist und das Ziel die anfänglichen Zustandsprüfungen bestanden hat. Es kann einige Minuten dauern, bis der Registrierungsvorgang abgeschlossen ist und die Zustandsprüfungen gestartet werden. Weitere Informationen finden Sie unter Gesundheitschecks für Gateway Load Balancer Balancer-Zielgruppen.

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 Gateway Load Balancer keine Anfragen mehr an das Ziel weiterleitet. 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.

Inhalt

- Ziele deregistrieren

Überlegungen

- Jede Zielgruppe muss mindestens ein registriertes Ziel in jeder Availability Zone haben, die für den Gateway Load Balancer aktiviert ist.
- Der Zieltyp der Zielgruppe legt fest, wie Sie Ziele bei dieser Zielgruppe registrieren. Weitere Informationen finden Sie unter Zieltyp.
- Sie können keine Ziele für ein VPC regionsübergreifendes Peering registrieren.
- Sie können Instances bei einem regionsinternen VPC Peering nicht anhand der Instanz-ID registrieren, aber Sie können sie anhand der IP-Adresse registrieren.

Zielsicherheitsgruppen

Wenn Sie EC2 Instances als Ziele registrieren, müssen Sie sicherstellen, dass die Sicherheitsgruppen für diese Instances eingehenden und ausgehenden Datenverkehr auf Port 6081 zulassen.

Gateway Load Balancer haben keine zugehörigen Sicherheitsgruppen. Aus diesem Grund müssen bei den Sicherheitsgruppen für Ihre Ziele IP-Adressen verwendet werden, um Datenverkehr vom Load Balancer zu erlauben.

Netzwerk ACLs

Wenn Sie EC2 Instances als Ziele registrieren, müssen Sie sicherstellen, dass die Netzwerkzugriffskontrolllisten (ACL) für die Subnetze Ihrer Instances Datenverkehr auf Port 6081 zulassen. Das Standardnetzwerk ACL für a VPC lässt den gesamten eingehenden und ausgehenden Datenverkehr zu. Wenn Sie ein benutzerdefiniertes Netzwerk erstellenACLs, stellen Sie sicher, dass es den entsprechenden Datenverkehr zulässt.

Registrieren Sie Ziele anhand der Instanz-ID

Die Instance muss sich bei der Registrierung im Status „`running`“ befinden.

Um Ziele mithilfe der Konsole anhand der Instanz-ID zu registrieren

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

2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Ziele die Option Ziele registrieren aus.
5. Wählen Sie die Instances aus und klicken Sie anschließend unten auf Als ausstehend einbeziehen.
6. Wenn Sie mit dem Hinzufügen der Instances fertig sind, wählen Sie Ausstehende Ziele registrieren aus.

Um Ziele anhand der Instanz-ID zu registrieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl register-targets mit den IDs Instanzen.

Registrieren Sie Ziele nach IP-Adresse

Eine IP-Adresse, die Sie registrieren, muss aus einem der folgenden CIDR Blöcke stammen:

- Die Subnetze der VPC für die Zielgruppe
- 10.0.0.0/8 (1918) RFC
- 100,64,0,0/10 (6598) RFC
- 172,16,0,0/12 RFC (1918)
- 192.168,0,0/16 (RFC1918)

Um Ziele anhand der IP-Adresse mithilfe der Konsole zu registrieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Ziele die Option Ziele registrieren aus.
5. Wählen Sie das Netzwerk, die IP-Adressen und die Ports aus und klicken Sie anschließend unten auf Als ausstehend einbeziehen.
6. Wenn Sie die Eingabe der Adressen abgeschlossen haben, wählen Sie Ausstehende Ziele registrieren.

Um Ziele anhand der IP-Adresse zu registrieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl register-targets mit den IP-Adressen der Ziele.

Ziele deregistrieren

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.

Um Ziele mit der Konsole abzumelden

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Ziele.
5. Wählen Sie die Ziele aus und klicken Sie dann auf Abmelden.

Um Ziele abzumelden, verwenden Sie den AWS CLI

Verwenden Sie den Befehl deregister-targets, um Ziele zu entfernen.

Markieren Sie eine Zielgruppe für Ihren Gateway 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. Zulässige Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF -8 dargestellt werden können, 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 AWS die Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

So aktualisieren Sie die Tags für eine Zielgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Tags die Option Tags verwalten und führen Sie einen oder mehrere der folgenden Schritte aus:
   a. Um ein Tag zu aktualisieren, geben Sie neue Werte für Schlüssel und Wert ein.
   b. Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen und geben Sie Werte für Schlüssel und Wert ein.
   c. Um ein Tag zu löschen, wählen Sie Entfernen neben dem Tag.
5. Wenn Sie die Aktualisierung der Tags abgeschlossen haben, wählen Sie Änderungen speichern.

Um die Tags für eine Zielgruppe mit dem zu aktualisieren AWS CLI

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

Löschen Sie eine Zielgruppe für Ihren Gateway 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 hat, die bei der Zielgruppe registriert sind. Wenn Sie eine registrierte EC2 Instance nicht mehr benötigen, können Sie sie beenden oder beenden.

Löschen einer Zielgruppe mithilfe der Konsole

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

Um eine Zielgruppe mit dem zu löschen AWS CLI

Verwenden Sie den delete-target-groupBefehl.

Überwachen Sie Ihre Gateway Load Balancer

Mit den folgenden Funktionen können Sie Ihre Gateway Load Balancer überwachen, um Verkehrsmuster zu analysieren und Probleme zu beheben. Der Gateway Load Balancer generiert jedoch keine Zugriffsprotokolle, da es sich um einen transparenten Layer-3-Load Balancer handelt, der Datenflüsse nicht beendet. Um Zugriffsprotokolle zu erhalten, müssen Sie die Zugriffsprotokollierung auf Gateway Load Balancer-Zielgeräten wie FirewallsIPS,IDS/und Sicherheitsgeräten aktivieren. Darüber hinaus können Sie sich auch dafür entscheiden, VPC Flow-Logs auf Gateway Load Balancers zu aktivieren.

CloudWatch Metriken

Sie können Amazon verwenden CloudWatch , um Statistiken über Datenpunkte für Ihre Gateway Load Balancer und Ziele als einen geordneten Satz 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 Gateway Load Balancer.

VPC-Flow-Protokolle

Sie können VPC Flow Logs verwenden, um detaillierte Informationen über den Datenverkehr zu und von Ihrem Gateway Load Balancer zu erfassen. Weitere Informationen finden Sie unter VPCFlow Logs im VPCAmazon-Benutzerhandbuch.

Erstellen Sie ein Ablaufprotokoll für jede Netzwerkschnittstelle Ihres Gateway Load Balancers. Pro Subnetz gibt es eine Netzwerkschnittstelle. Um die Netzwerkschnittstellen für einen Gateway Load Balancer zu identifizieren, suchen Sie im Beschreibungsfeld der Netzwerkschnittstelle nach dem Namen des Gateway Load Balancers.

Es gibt zwei Einträge für jede Verbindung durch Ihren Gateway Load Balancer, einen für die Frontend-Verbindung zwischen dem Client und dem Gateway Load Balancer und den anderen für die Backend-Verbindung zwischen dem Gateway Load Balancer und dem Ziel. Wenn das Ziel nach Instance-ID registriert ist, stellt sich die Verbindung gegenüber der Instance als eine vom Client kommende Verbindung dar. Wenn die Sicherheitsgruppe der Instanz keine Verbindungen vom Client zulässt, das Netzwerk ACLs für das Subnetz sie jedoch zulässt, zeigen die Protokolle für die Netzwerkschnittstelle für den Gateway Load Balancer "ACCEPTOK“ für die Frontend- und Backend-Verbindungen an, während die Protokolle für die Netzwerkschnittstelle für die Instanz "REJECTOK“ für die Verbindung anzeigen.

CloudTrail protokolliert

Sie können AWS CloudTrail damit detaillierte Informationen zu den Aufrufen von Elastic Load Balancing API erfassen und sie als Protokolldateien in Amazon S3 speichern. Sie können diese CloudTrail Protokolle verwenden, um festzustellen, welche Anrufe 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 APILog-Aufrufe für Elastic Load Balancing mit CloudTrail.

CloudWatch Metriken für Ihren Gateway Load Balancer

Elastic Load Balancing veröffentlicht Datenpunkte CloudWatch für Ihre Gateway Load Balancer und Ihre Ziele auf Amazon. CloudWatch ermöglicht 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 Gateway 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 eines für Sie akzeptablen Bereichs liegt.

Elastic Load Balancing meldet Metriken CloudWatch nur dann, wenn Anfragen über den Gateway Load Balancer fließen. Wenn es Anfragen gibt, misst und sendet Elastic Load Balancing seine Metriken in 60-Sekunden-Intervallen. Wenn keine Anfragen eingehen oder keine Daten für eine Kennzahl vorliegen, wird die Kennzahl nicht gemeldet.

Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Inhalt

Gateway-Load-Balancer-Metriken

Der `AWS/GatewayELB`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung
`ActiveFlowCount`	Die Gesamtzahl der gleichzeitigen Datenflüsse (oder Verbindungen) von Clients zu Zielen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichsten Statistiken sind `Average`, `Maximum` und `Minimum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ConsumedLCUs`	Die Anzahl der Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden. Sie zahlen für die AnzahlLCUs, die Sie pro Stunde nutzen. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing. Berichtkriterien: Always reported Statistiken: Alle Dimensionen • `LoadBalancer`
`HealthyHostCount`	Anzahl der als stabil betrachteten Ziele. Berichtkriterien: Wird gemeldet, wenn Zustandsprüfungen aktiviert sind Statistiken: Die nützlichsten Statistiken sind `Maximum` und `Minimum`.

Metrik	Beschreibung
	Dimensionen • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`NewFlowCount`	Die Gesamtanzahl neuer Datenflüsse (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes`	Die Gesamtzahl der vom Load Balancer verarbeiteten Bytes. Diese Zählung umfasst den Verkehr zu und von den Zielorten, nicht aber den Verkehr im Rahmen der Zustandsprüfung. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Beschreibung
`RejectedFlowCount`	Die Gesamtzahl der vom Load Balancer zurückgewiesenen Datenflüsse (oder Verbindungen). Berichtkriterien: Immer berichtet. Statistiken: Die nützlichsten Statistiken sind `Average`, `Maximum` und `Minimum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedFlowCount_TCP`	Die Anzahl der vom Load Balancer zurückgewiesenen TCP Flows (oder Verbindungen). Berichtkriterien: Ein Wert ungleich Null. Statistiken: Die nützlichste Statistik ist `Sum`. Dimensionen • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`UnHealthyHostCount`	Die Anzahl der als instabil betrachteten Ziele. Berichtkriterien: Wird gemeldet, wenn Zustandsprüfungen aktiviert sind Statistiken: Die nützlichsten Statistiken sind `Maximum` und `Minimum`. Dimensionen • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Metrische Abmessungen für Gateway Load Balancer

Um die Metriken für Ihren Gateway Load Balancer zu filtern, verwenden Sie die folgenden Dimensionen.

Dimension	Beschreibung
`AvailabilityZone`	Filtert die Metrikdaten nach Availability Zone.
`LoadBalancer`	Filtert die Metrikdaten nach Gateway Load Balancer. Geben Sie den Gateway Load Balancer wie folgt an: gateway/ load-balancer-name /1234567890123456 (der letzte Teil von). ARN
`TargetGroup`	Filtert die Metrikdaten nach der Zielgruppe. Geben Sie die Zielgruppe wie folgt an: targetgroup/ target-group-name/1234567890123456 (der letzte Teil der Zielgruppe). ARN

CloudWatch Metriken für Ihren Gateway Load Balancer anzeigen

Sie können die CloudWatch Metriken für Ihre Gateway Load Balancer mithilfe der EC2 Amazon-Konsole anzeigen. Diese Metriken werden in Überwachungsdiagrammen dargestellt. Die Überwachungsgrafiken zeigen Datenpunkte an, wenn der Gateway Load Balancer aktiv ist und Anfragen empfängt.

Alternativ können Sie Metriken für Ihren Gateway Load Balancer über die CloudWatch Konsole anzeigen.

So zeigen Sie Metriken mithilfe der -Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um nach Zielgruppe gefilterte Metriken anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Navigationsbereich Target Groups aus.
   b. Wählen Sie Ihre Zielgruppe 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 Gateway Load Balancer gefilterte Metriken anzuzeigen, gehen Sie wie folgt vor:

   a. Klicken Sie im Navigationsbereich auf Load Balancers.
   b. Wählen Sie Ihren Gateway Load Balancer und wählen Sie Überwachung.
   c. (Optional) Wählen Sie in Showing data for einen Zeitbereich aus., um die Ergebnisse nach Zeit zu filtern.
   d. Wenn Sie eine größere Ansicht einer Metrik aufrufen möchten, wählen Sie ihr Diagramm aus.

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den ELBGateway-Namespace aus.
4. (Optional) Um eine Metrik in allen 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/GatewayELB
```

Um die Statistiken für eine Metrik abzurufen, verwenden Sie AWS CLI

Verwenden Sie den folgenden get-metric-statisticsBefehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. 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/GatewayELB \
--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
```

Es folgt eine Beispielausgabe.

```
{
    "Datapoints": [
        {
            "Timestamp": "2020-12-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2020-12-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Kontingente für Ihre Gateway Load Balancer

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um eine Kontigenterhöhung zu beantragen, verwenden Sie das Formular für die Erhöhung des Limits

Load Balancers

Ihr AWS Konto hat die folgenden Kontingente für Gateway Load Balancers.

Name	Standard	Anpassbar
Gateway Load Balancer pro Region	100	Ja
Gateway Load Balancer pro VPC	100	Ja
Gateway Load Balancer ENIs für VPC	300 *	Ja
Listener pro Gateway Load Balancer	1	Nein

* Jeder Gateway Load Balancer verwendet eine Netzwerkschnittstelle pro Zone.

Zielgruppen

Die folgenden Kontingente gelten für Zielgruppen.

Name	Standard	Anpassbar
GENEVEZielgruppen pro Region	100	Ja
Ziele pro Zielgruppe	1.000	Ja
Ziele pro Availability Zone pro GENEVE Zielgruppe	300	Nein
Ziele pro Verfügbarkeitszone pro Gateway Load Balancer	300	Nein

Name	Standard	Anpassbar
Ziele pro Gateway Load Balancer	300	Nein

Bandbreite

Standardmäßig unterstützt jeder VPC Endpunkt eine Bandbreite von bis zu 10 Gbit/s pro Availability Zone und skaliert automatisch auf bis zu 100 Gbit/s. Wenn Ihre Anwendung einen höheren Durchsatz benötigt, wenden Sie sich an AWS den Support.

Dokumentverlauf für Gateway Load Balancer

In der folgenden Tabelle werden die Versionen für Gateway Load Balancer beschrieben.

Änderung	Beschreibung	Datum
IPv6Unterstützung	Sie können Ihren Gateway Load Balancer so konfiguri eren, dass er IPv4 sowohl IPv6 Adressen als auch unterstützt.	12. Dezember 2022
Neuausrichtung des Datenflus ses	Diese Version bietet Unterstüt zung für die Definition des Flow-Handling-Verhaltens für Gateway Load Balancer, wenn Ziele ausfallen oder deren Registrierung aufgehoben wird.	13. Oktober 2022
Konfigurierbare Flow-Stic kiness	Sie können das Hashing so konfigurieren, dass das Stickiness von Flows an eine bestimmte Ziel-Appliance aufrechterhalten wird.	25. August 2022
In neuen Regionen verfügbar	Diese Version bietet Unterstüt zung für Gateway Load Balancer in den AWS GovCloud (US) Regionen.	17. Juni 2021
In neuen Regionen verfügbar	Diese Version bietet Unterstüt zung für Gateway Load Balancers in den Regionen Kanada (Zentral), Asien-Paz ifik (Seoul) und Asien-Pazifik (Osaka).	31. März 2021

In neuen Regionen verfügbar	Diese Version bietet Unterstützung für Gateway Load Balancers in den Regionen USA West (Nordkalifornien), Europa (London), Europa (Paris), Europa (Mailand), Afrika (Kapstadt), Naher Osten (Bahrain), Asien-Pazifik (Hongkong), Asien-Pazifik (Singapur) und Asien-Pazifik (Mumbai).	19. März 2021
Erstversion	Mit dieser Version von Elastic Load Balancing werden Gateway Load Balancer eingeführt.	10. November 2020

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.