Elastic Load Balancing

Gateway Load Balancer

Elastic Load Balancing: Gateway Load Balancer

Table of Contents

Was ist ein Gateway Load Balancer?

Verteilen Sie den eingehenden Datenverkehr automatisch mithilfe von Elastic Load Balancing auf mehrere Ziele in einer oder mehreren Availability Zones. Es überwacht den Zustand seiner registrierten Ziele und leitet den Verkehr nur zu den fehlerfreien Zielen weiter. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich Ihr eingehender Datenverkehr im Laufe der Zeit ändert. Die Mehrzahl der Workloads wird automatisch skaliert.

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

Gateway Load Balancer im Überblick

Gateway Load Balancers ermöglichen die Bereitstellung, Skalierung und Verwaltung virtueller Appliances, wie Firewalls, Intrusion Detection and Prevention Systeme und Deep Packet Inspection Systeme. Es kombiniert ein transparentes Netzwerkgateway (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. Es behält die Klebrigkeit der Flows zu einer bestimmten Ziel-Appliance mit 5-Tupel (für TCP/UDP-Flows) oder 3-Tupel (für Nicht-TCP/UDP-Flows) bei. Der Gateway Load Balancer und seine registrierten virtuellen Appliance-Instances tauschen Anwendungsdatenverkehr über das GENEVE-Protokoll auf Port 6081 aus.

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

Der Datenverkehr zu und von einem Gateway Load Balancer-Endpunkt wird mit Routing-Tabellen konfiguriert. Der Datenverkehr fließt von der Service Consumer-VPC über den Gateway Load Balancer-Endpunkt zum Gateway Load Balancer in der Service Provider-VPC und kehrt dann zur Service Consumer-VPC zurück. Sie müssen den Gateway Load Balancer-Endpunkt und die Anwendungsserver in verschiedenen Subnetzen erstellen. So können Sie den Gateway Load Balancer-Endpunkt als nächsten Hop in der Routing-Konfiguration für das Anwendungssubnetz konfigurieren.

Weitere Informationen finden SieAWS PrivateLink im AWS PrivateLinkHandbuch unter Zugriff auf virtuelle Appliances.

Appliance-Anbieter

Sie sind dafür verantwortlich, Software von Appliance-Anbietern auszuwählen und zu qualifizieren. Sie müssen der Appliance-Software vertrauen, um den Datenverkehr vom Load Balancer zu überprüfen oder

zu ändern. Die Appliance-Anbieter, die als Elastic Load Balancing Balancing-Partner aufgeführt sind, haben ihre Appliance-Software integriert und qualifiziertAWS. Sie können der Appliance-Software von Anbietern in dieser Liste ein höheres Maß an Vertrauen entgegenbringen. AWSGarantiert jedoch nicht die Sicherheit oder Zuverlässigkeit von Software dieser Anbieter.

Erste Schritte

So erstellen Sie einen Gateway Load Balancer mit derAWS Management ConsoleErste Schritte (p. 3)
So erstellen Sie einen Gateway Load Balancer mit derAWS Command Line InterfaceErste Schritte mit der Verwendung von der CLI (p. 10)

Preise

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 Balancern

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

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

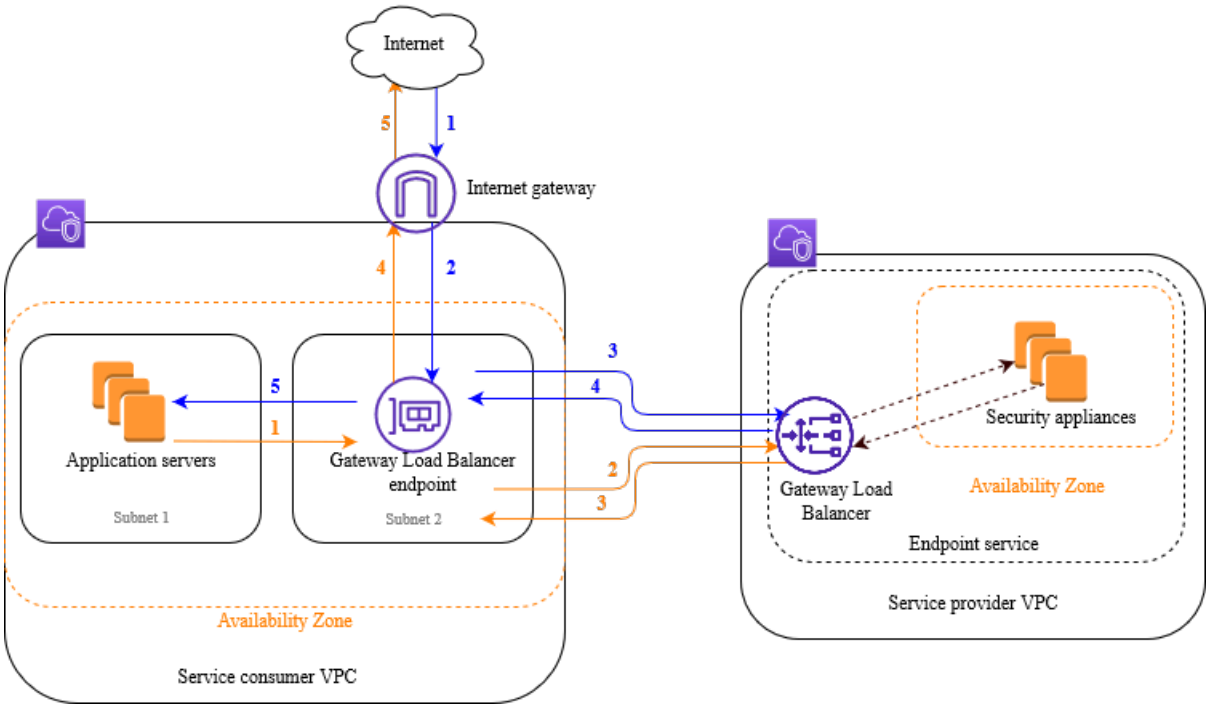
Inhalt

Übersicht

Ein Gateway Load Balancer-Endpunkt ist ein VPC-Endpunkt, der private Konnektivität zwischen virtuellen Appliances in der Serviceanbieter-VPC bereitstellt. Der Gateway Load Balancer wird in derselben VPC wie die virtuellen Appliances bereitgestellt. Diese Appliances sind als Zielgruppe für den Gateway Load Balancer registriert.

Die Anwendungsserver werden in einem Subnetz (Zielsubnetz) in der Service Consumer-VPC ausgeführt, während sich der Gateway Load Balancer-Endpunkt in einem anderen Subnetz derselben VPC befindet. Der gesamte Datenverkehr, der über das Internet-Gateway in die Service-Verbraucher-VPC gelangt, wird zunächst zur Überprüfung an den Gateway-Load-Balancer-Endpunkt weitergeleitet und dann an das Zielsubnetz.

Ebenso wird der gesamte Datenverkehr, der die Anwendungsserver (Zielsubnetz) verlässt, zur Überprüfung an den Gateway-Load-Balancer-Endpunkt geleitet, bevor er an das Internet zurückgeleitet wird. Das folgende Netzwerkdiagramm zeigt visuell, wie ein Gateway Load Balancer-Endpunkt für den Zugriff auf einen Endpunktdienst verwendet wird.



Die folgenden nummerierten Elemente markieren und erklären die im vorherigen Bild gezeigten Elemente.

Datenverkehr vom Internet zur Anwendung (blaue Pfeile):

1. Der Datenverkehr gelangt über das Internet-Gateway in die Service-Verbraucher-VPC.
2. Der Datenverkehr wird als Ergebnis des Ingress-Routings an den Gateway-Load-Balancer-Endpunkt gesendet.
3. Der Datenverkehr wird zur Überprüfung durch die Sicherheits-Appliance an den Gateway Load Balancer gesendet.
4. Der Datenverkehr wird nach der Überprüfung an den Gateway-Load-Balancer-Endpunkt zurückgesendet
5. Der Datenverkehr wird an die Anwendungsserver gesendet (Zielsubnetz).

Datenverkehr von der Anwendung ins Internet (orangefarbene Pfeile):

1. Der Datenverkehr wird als Ergebnis der im Anwendungsserversubnetz konfigurierten Standardroute an den Gateway-Load-Balancer-Endpunkt gesendet.
2. Der Datenverkehr wird zur Überprüfung durch die Sicherheits-Appliance an den Gateway Load Balancer gesendet.
3. Der Datenverkehr wird nach der Überprüfung an den Gateway-Load-Balancer-Endpunkt zurückgesendet
4. Der Datenverkehr wird basierend auf der Routingtabellenkonfiguration an das Internet-Gateway gesendet.
5. Der Datenverkehr wird zurück ins Internet geleitet.

Routing

Die Routing-Tabelle für das Internet-Gateway muss einen Eintrag enthalten, der Datenverkehr für die Anwendungsserver an den Gateway-Load-Balancer-Endpunkt leitet. Um den Gateway Load Balancer-Endpunkt anzugeben, verwenden Sie die ID des VPC-Endpunkts. Im folgenden Beispiel werden die Routen für eine Dualstackkonfiguration gezeigt.

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

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

Ziel	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 Datenverkehr, der von der Inspektion an sein endgültiges Ziel zurückfließt. Für Datenverkehr aus dem Internet stellt die lokale Route sicher, dass er die Anwendungsserver erreicht. Für Datenverkehr, der von den Anwendungsservern stammt, fügen Sie Einträge hinzu, die den gesamten Datenverkehr zum Internet-Gateway leitet.

Ziel	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 die Service Consumer-VPC mindestens zwei Subnetze für jede Availability Zone hat, die Anwendungsserver enthält. Ein Subnetz ist für den Gateway-Load-Balancer-Endpunkt und das andere für die Anwendungsserver vorgesehen.
- 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 Security Appliance-Instanz in jedem Security Appliance-Subnetz in der Service Provider-VPC. Die Sicherheitsgruppen für diese Instances müssen UDP-Datenverkehr auf Port 6081 zulassen.

Schritt 1: Registrieren der Ziele und Erstellen eines Gateway-Load-Balancers

Gehen Sie wie folgt vor, um Ihre Zielgruppe zu erstellen, Ihre Security Appliance-Instanzen als Ziele zu registrieren und dann Ihren Load Balancer und Listener zu erstellen.

Erstellen einer Zielgruppe und Registrieren von Zielen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie Create target group (Zielgruppe erstellen) aus.
4. Wählen Sie unter Zieltyp auswählen die Option Instanzen aus, um Ziele anhand der Instanz-ID anzugeben, oder IP-Adressen, um Ziele anhand der IP-Adresse anzugeben.
5. Geben Sie unter Target group name einen Namen für Ihre Zielgruppe ein. Zum Beispiel **`my-targets`**.
6. Das Protokoll muss sein`GENEVE`, und der Port muss es sein`6081`. Es werden keine anderen Protokolle oder Ports unterstützt.
7. Wählen Sie für VPC eine Virtual Private Cloud (VPC) mit den Instances aus, die in die Zielgruppe aufgenommen werden sollen.
8. (Optional) Ändern Sie für Integritätsprüfungen die Einstellungen für die Integritätsprüfung nach Bedarf.
9. (Optional) Erweitern Sie Tags und fügen Sie Tags hinzu.
10. Wählen Sie Next (Weiter).
11. 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 unten „Als ausstehend einschließen“.
    - Wenn der Zieltyp IP-Adressen ist, wählen Sie das Netzwerk aus, geben Sie die IP-Adresse und die Ports ein und wählen Sie dann unten Als ausstehend einschließen aus.
12. Wählen Sie Create target group (Zielgruppe erstellen) aus.

So erstellen Sie einen Gateway Load Balancer

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Klicken Sie auf Create Load Balancer.
4. Wählen Sie unter Gateway Load Balancer die Option Erstellen aus.
5. Geben Sie im Feld Load balancer name (Name des Load Balancers) einen Namen für Ihren Load Balancer ein. Zum Beispiel **`my-glb`**.
6. Wählen Sie IPv4 aus, um nur IPv4-Adressen zu unterstützen, oder Dualstack, um IPv4- und IPv6-Adressen zu unterstützen.
7. Wählen Sie für VPC den Dienstanbieter VPC aus.
8. Wählen Sie für Mappings alle Availability Zones aus, in denen Sie Security Appliance-Instanzen gestartet haben, sowie die entsprechenden öffentlichen Subnetze.
9. Wählen Sie als Standardaktion eine Zielgruppe aus, an die der Traffic weitergeleitet werden soll. Wenn Sie nicht über eine Zielgruppe verfügen, erstellen Sie zuerst eine. Die Zielgruppe muss das GENEVE-Protokoll verwenden.

10. (Optional) Erweitern Sie Tags und fügen Sie Tags hinzu.
11. Überprüfen Sie Ihre Konfiguration und wählen Sie Create load balancer (Load Balancer erstellen) aus.

Schritt 2: Erstellen eines Gateway-Load-Balancer-Endpunkts

Verwenden Sie das folgende Verfahren, um einen Endpunkt-Service mit einem Gateway Load Balancer zu erstellen.

So erstellen Sie einen Gateway-Load-Balancer-End-Service

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Create endpoint service aus und gehen Sie folgendermaßen vor:
   a. Wählen Sie für Load balancer type (Load-Balancer-Typ) Gateway aus.
   b. Wählen Sie für Available load balancers (verfügbare Load Balancer) Ihren Gateway Load Balancer aus.
   c. Wählen Sie im Feld Require acceptance for endpoint aus, um Verbindungsanfragen für Ihren Service manuell zu akzeptieren. Andernfalls werden sie automatisch akzeptiert.
   d. Führen Sie für Supported IP address types (Unterstützte IP-Adresstyp) einen der folgenden Schritte aus:
      - Wählen Sie IPv4 – Aktivieren Sie den Endpunkt-Service, um IPv4-Anfragen anzunehmen.
      - Wählen Sie IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv6-Anfragen zu akzeptieren.
      - Wählen Sie IPv4 und IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv4- und IPv6-Anfragen zu akzeptieren.
   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 den Service-Namen. Sie benötigen ihn beim Erstellen des Endpunkts.
4. Wählen Sie den neuen Endpunktdienst aus und wählen Sie Actions, Allow Principals. Geben Sie die ARNs der Service-Verbraucher ein, die einen Endpunkt zu Ihrem Service erstellen dürfen. Ein Service-Verbraucher kann ein IAM-Benutzer, eine IAM-Rolle oder seinAWS-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. Gateway Load Balancer-Endpunkte sind zonal. Es wird empfohlen, einen Gateway Load Balancer-Endpunkt pro Zone zu erstellen. Weitere Informationen finden SieAWS PrivateLink im AWS PrivateLinkHandbuch unter Zugriff auf virtuelle Appliances.

So erstellen Sie einen Gateway-Load-Balancer-Endpunkt

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.

3. Wählen Sie Create endpoint (Endpunkt erstellen) aus und gehen Sie folgendermaßen vor:

   a. Wählen Sie für Service category (Servicekategorie) Other endpoint services (Andere Endpunkt-Services).
   b. Geben Sie als Dienstname den Dienstnamen ein, den Sie zuvor notiert haben, und wählen Sie dann Dienst überprüfen aus.
   c. Wählen Sie für VPC die Service-Consumer-VPC aus.
   d. Wählen Sie für Subnetze 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 über IPv4-Adressbereiche verfügen.
      - IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind.
      - Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche aufweisen.

   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 Create endpoint (Endpunkt erstellen). Der ursprüngliche Status ist `pending acceptance`.

Gehen Sie wie folgt vor, um die Schnittstellenendpunkt-Verbindungsanforderung zu akzeptieren.

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: Konfigurieren des Routings

Konfigurieren der Routingtabellen für die Service-Verbraucher-VPC wie folgt. Auf diese Weise können die Sicherheits-Appliances eine Sicherheitsüberprüfung für eingehenden Datenverkehr durchführen, der für die Anwendungsserver bestimmt ist.

So konfigurieren Sie das Routing

1. Öffnen Sie die Amazon VPC-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 Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
   b. Wählen Sie Add Route (Route hinzufügen) aus. Geben Sie als Ziel den IPv4-CIDR-Block für das Subnetz für die Anwendungsserver ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   c. Wenn Sie IPv6 unterstützen, wählen Sie Route hinzufügen. Geben Sie als Ziel den IPv6 CIDR-Block für das Subnetz für die Anwendungsserver ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.

   d. Wählen Sie Save Changes (Änderungen speichern).
4. Wählen Sie die Routing-Tabelle für das Subnetz mit den Anwendungsservern aus, und führen Sie folgende Schritte aus:
   a. Wählen Sie Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
   b. Wählen Sie Add Route (Route hinzufügen) aus. Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   c. Wenn Sie IPv6 unterstützen, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   d. Wählen Sie Save Changes (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 Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
   b. Wählen Sie Add Route (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 IPv6 unterstützen, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.
   d. Wählen Sie Save Changes.

Erste Schritte mit Gateway Load Balancern mit der Verwendung von Gateway Load BalancernAWS CLI

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

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

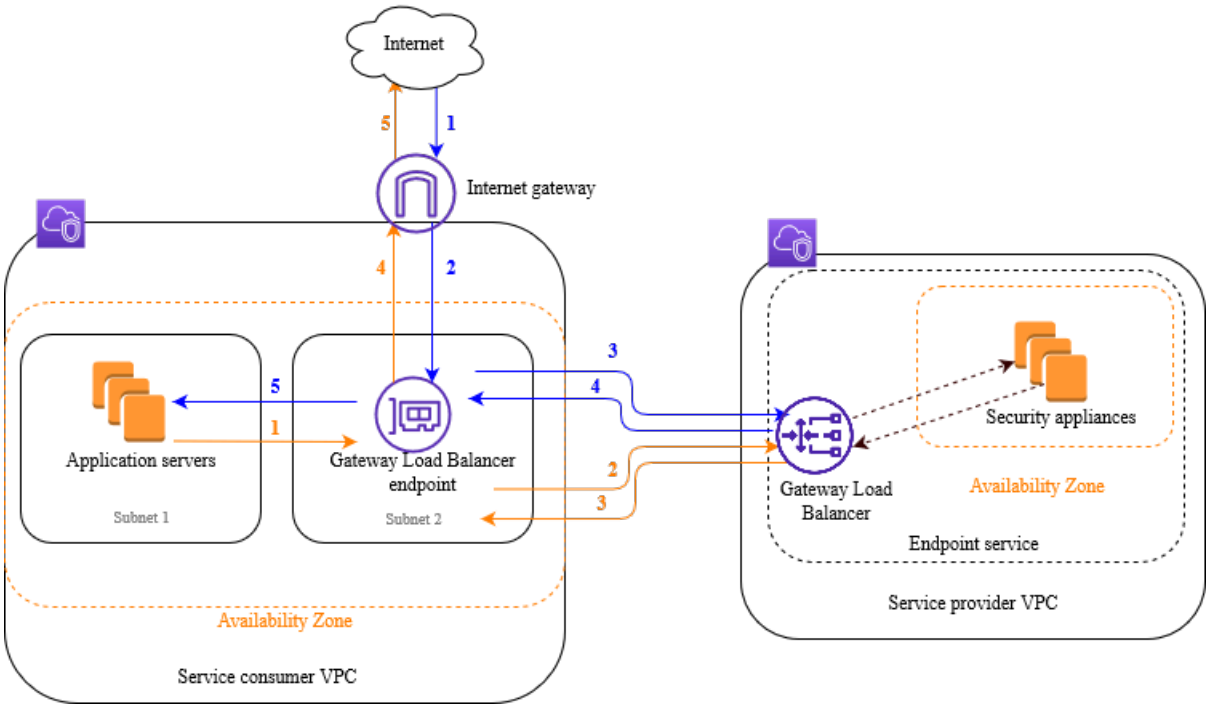
Inhalt

Übersicht

Ein Gateway Load Balancer-Endpunkt ist ein VPC-Endpunkt, der private Konnektivität zwischen virtuellen Appliances in der Serviceanbieter-VPC und Anwendungsservern in der Service-Consumer-VPC und Anwendungsservern in der Service-Consumer-VPC und Anwendungsservern in der Service-Consumer-VPC Der Gateway Load Balancer wird in derselben VPC wie die virtuellen Appliances bereitgestellt. Diese Appliances sind als Zielgruppe des Gateway-Load-Balancers registriert.

Die Anwendungsserver werden in einem Subnetz (Zielsubnetz) in der Service Consumer-VPC ausgeführt, während sich der Gateway Load Balancer-Endpunkt in einem anderen Subnetz derselben VPC befindet. Der gesamte Datenverkehr, der über das Internet-Gateway in die Service-Verbraucher-VPC gelangt, wird zunächst zur Überprüfung an den Gateway-Load-Balancer-Endpunkt weitergeleitet und dann an das Zielsubnetz.

Ebenso wird der gesamte Datenverkehr, der die Anwendungsserver (Zielsubnetz) verlässt, zur Überprüfung an den Gateway-Load-Balancer-Endpunkt geleitet, bevor er an das Internet zurückgeleitet wird. Das folgende Netzwerkdiagramm zeigt visuell, wie ein Gateway Load Balancer-Endpunkt für den Zugriff auf einen Endpunktdienst verwendet wird.



Die folgenden nummerierten Elemente markieren und erklären die im vorherigen Bild gezeigten Elemente.

Datenverkehr vom Internet zur Anwendung (blaue Pfeile):

1. Der Datenverkehr gelangt über das Internet-Gateway in die Service-Verbraucher-VPC.
2. Der Datenverkehr wird als Ergebnis des Ingress-Routings an den Gateway-Load-Balancer-Endpunkt gesendet.
3. Der Datenverkehr wird zur Überprüfung durch die Sicherheits-Appliance an den Gateway Load Balancer gesendet.
4. Der Datenverkehr wird nach der Überprüfung an den Gateway-Load-Balancer-Endpunkt zurückgesendet
5. Der Datenverkehr wird an die Anwendungsserver gesendet (Zielsubnetz).

Datenverkehr von der Anwendung ins Internet (orangefarbene Pfeile):

1. Der Datenverkehr wird als Ergebnis der im Anwendungsserversubnetz konfigurierten Standardroute an den Gateway-Load-Balancer-Endpunkt gesendet.
2. Der Datenverkehr wird zur Überprüfung durch die Sicherheits-Appliance an den Gateway Load Balancer gesendet.
3. Der Datenverkehr wird nach der Überprüfung an den Gateway-Load-Balancer-Endpunkt zurückgesendet
4. Der Datenverkehr wird basierend auf der Routingtabellenkonfiguration an das Internet-Gateway gesendet.
5. Der Datenverkehr wird zurück ins Internet geleitet.

Routing

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

Ziel	Ziel
VPC IPv4 CIDR-Datenverkehr	Local
VPC IPv6 CIDR-Datenverkehr	Local
Subnetz-1-IPv4-CIDR	*vpc-endpoint-id*
Subnetz 1 IPv6 CIDR	*vpc-endpoint-id*

Die Routing-Tabelle für das Subnetz mit den Anwendungsservern muss über Einträge verfügen, die den gesamten Datenverkehr von den Anwendungsservern an den Gateway-Load-Balancer-Endpunkt leiten.

Ziel	Ziel
VPC IPv4 CIDR-Datenverkehr	Local
VPC IPv6 CIDR-Datenverkehr	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 Datenverkehr, der von der Inspektion an ihr endgültiges Ziel zurückfließt. Für Datenverkehr aus dem Internet stellt die lokale Route sicher, dass er die Anwendungsserver erreicht. Für Datenverkehr, der von den Anwendungsservern stammt, fügen Sie Einträge hinzu, die den gesamten Datenverkehr an das Internet-Gateway leiten.

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

Voraussetzungen

- Installieren SieAWS CLI oder aktualisieren 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-Leitfaden.

- Stellen Sie sicher, dass die Service Consumer-VPC mindestens zwei Subnetze für jede Availability Zone hat, die Anwendungsserver enthält. Ein Subnetz ist für den Gateway-Load-Balancer-Endpunkt und das andere für die Anwendungsserver vorgesehen.
- Stellen Sie sicher, dass die Service Provider-VPC mindestens zwei Subnetze für jede Availability Zone hat, die Security Appliance-Instanzen enthält. Ein Subnetz ist für den Gateway Load Balancer und das andere für die Instances vorgesehen.
- Starten Sie mindestens eine Security Appliance-Instanz in jedem Security Appliance-Subnetz in der Service Provider-VPC. Die Sicherheitsgruppen für diese Instances müssen UDP-Datenverkehr auf Port 6081 zulassen.

Schritt 1: Erstellen eines Gateway-Load-Balancers und Registrierung von Zielen

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

So erstellen Sie einen Gateway Load Balancer und registrieren Sie Ziele

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

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

   Standardmäßig werden nur IPv4-Adressen unterstützt. Um IPv4- und IPv6-Adressen 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 die Service Provider-VPC anzugeben, in der Sie Ihre Instances gestartet haben.

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

   Die Ausgabe beinhaltet den 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 den ARN des Listeners im folgenden Format.

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

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

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

Schritt 2: Erstellen eines Gateway-Load-Balancer-Endpunkts

Verwenden Sie das folgende Verfahren, 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 überAWS PrivateLink.

So erstellen Sie einen Gateway-Load-Balancer-Endpunkt

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

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

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

Die Ausgabe enthält die Service-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 Service-Verbrauchern die Erstellung eines Endpunkts zu Ihrem Service zu ermöglichen. Ein Service-Verbraucher kann ein IAM-Benutzer, eine IAM-Rolle oder einAWS -Konto sein. Das folgende Beispiel fügt die Berechtigung für das angegebeneAWS Konto hinzu.

```
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 Dienst 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 IPv4- und IPv6-Adressen 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: Konfigurieren des Routings

Konfigurieren Sie die Routing-Tabellen für die Service-Verbraucher-VPC wie folgt. Auf diese Weise können die Sicherheits-Appliances eine Sicherheitsüberprüfung für eingehenden Datenverkehr durchführen, der für die Anwendungsserver bestimmt ist.

So konfigurieren Sie das Routing-Verfahren

1. Verwenden Sie den Befehl create-route, um der Routing-Tabelle für das Internet-Gateway, das Datenverkehr, der für die Anwendungsserver an den Gateway-Load-Balancer-Endpunkt geleitet wird.

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

   Wenn Sie IPv6 unterstützen, fügen Sie die folgende Route zu 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, das 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 IPv6 unterstützen, fügen Sie die folgende Route zu 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 Datenverkehr, der von den Anwendungsservern stammt, 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 IPv6 unterstützen, fügen Sie die folgende Route zu hinzu.

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

4. Wiederholen Sie den Vorgang für jede Anwendungssubnetz-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. Es überwacht alle IP-Pakete über alle Ports und leitet den Datenverkehr an die Zielgruppe weiter, die in der Listener-Regel angegeben ist.

Sie können Ziele zu Ihrem Load Balancer hinzufügen oder entfernen, wenn sich Ihre Bedürfnisse ändern, ohne den allgemeinen Fluss von 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 automatisch auf die überwiegende Mehrheit der Workloads skaliert werden.

Inhalt

Load Balancer-Status

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

`provisioning`

Der Gateway Load Balancer wird eingerichtet.

`active`

Der Gateway Load Balancer ist vollständig eingerichtet und bereit, den Verkehr weiterzuleiten.

`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 Balancer verwenden können. Im Folgenden werden die unterstützten IP-Adresstypen aufgeführt:

- `ipv4`— Nur IPv4 wird unterstützt.
- `dualstack`— Es werden IPv4 und IPv6 unterstützt.

Überlegungen zum Dualstack-Load Balancer

- Die Virtual Private Cloud (VPC) und die Subnetze, die Sie für den Load Balancer angeben, müssen IPv6-CIDR-Blöcken zugeordnet sein.
- Die Routing-Tabellen für die Subnetze in der Service Consumer-VPC müssen IPv6-Verkehr weiterleiten, und die Netzwerk-ACLs für diese Subnetze müssen IPv6-Verkehr zulassen.
- Ein Gateway Load Balancer kapselt sowohl IPv4- als auch IPv6-Client-Traffic mit einem IPv4-GENEVE-Header und sendet ihn an die Appliance. Die Appliance kapselt sowohl IPv4- als auch IPv6-Client-Traffic mit einem IPv4-GENEVE-Header und sendet ihn zurück an den Gateway Load Balancer.

Sie können den IP-Adresstyp festlegen, wenn Sie den Load Balancer erstellen. Sie können es auch jederzeit aktualisieren.

So aktualisieren Sie den IP-Adresstyp mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Load Balancer aus.
4. Klicken Sie auf Actions (Aktionen) und anschließend auf "Edit IP-address type (IP-Adressentyp bearbeiten).
5. Wählen Sie im Feld IP address type (IP-Adresstyp) die Option ipv4 aus, um nur IPv4-Adressen zu unterstützen, oder dualstack, um IPv4- und IPv6-Adressen zu unterstützen.
6. Wählen Sie Save (Speichern) aus.

So aktualisieren Sie den IP-Adresstyp mithilfe der AWS CLI

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

Load Balancer-Attribute

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

`deletion_protection.enabled`

Gibt an, ob der Löschschutz (p. 18) aktiviert ist. Der Standardwert ist `false`.

`load_balancing.cross_zone.enabled`

Gibt an, ob zonenübergreifendes Load Balancing (p. 19) aktiviert ist. Der Standardwert ist `false`.

Availability Zones

Wenn Sie einen Gateway Load Balancer erstellen, aktivieren Sie eine oder mehrere Availability Zones und geben das Subnetz an, das jeder Zone entspricht. Wenn Sie mehrere Availability Zones aktivieren, wird sichergestellt, dass der Load Balancer den Verkehr auch dann weiterleiten kann, wenn eine Availability Zone nicht mehr verfügbar ist. Die von Ihnen angegebenen Subnetze müssen jeweils mindestens 8

verfügbare IP-Adressen haben. Subnetze können nicht hinzugefügt oder entfernt werden, nachdem der Load Balancer erstellt wurde. Um ein Subnetz hinzuzufügen oder zu entfernen, müssen Sie einen neuen Load Balancer erstellen.

Netzwerk-MTU (Maximum Transmission Unit)

Die maximale Übertragungseinheit (MTU) ist die Größe des größten Datenpakets, das über das Netzwerk übertragen werden kann. Die Gateway Load Balancer-Schnittstelle MTU unterstützt Pakete bis zu 8.500 Byte.

Ein Gateway Load Balancer kapselt IP-Verkehr mit einem GENEVE-Header und leitet ihn an die Appliance weiter. Der GENEVE-Kapselungsprozess fügt dem Originalpaket 64 Byte hinzu. 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.

Deletion protection (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 Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer aus.
4. Wählen Sie Aktionen, Attribute bearbeiten.
5. Wählen Sie auf der Seite Edit load balancer attributes (Load Balancer-Attribute bearbeiten) Enable (Aktivieren) bei Delete Protection Schutz löschen) aus, und wählen Sie anschließend Save (Speichern).

So deaktivieren Sie mithilfe der Konsole den Löschschutz:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer aus.
4. Wählen Sie Aktionen, Attribute bearbeiten.
5. Löschen Sie auf der Seite Edit load balancer attributes (Load Balancer-Attribute bearbeiten) Enable (Aktivieren) bei Delete Protection (Schutz löschen), und wählen Sie anschließend Save (Speichern).

So aktivieren oder deaktivieren Sie den Löschschutz mit der 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 Availability Zone. Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Gateway Load Balancer-Knoten den Datenverkehr gleichmäßig auf die registrierten Ziele in allen aktivierten Availability Zones. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing im Elastic Load Balancing Balancing-Benutzerhandbuch.

Aktivieren des zonenübergreifenden Load Balancing mithilfe der Konsole

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

Aktivieren des zonenübergreifenden Load Balancing mit der AWS CLI

Verwenden Sie den modify-load-balancer-attributesBefehl mit demload_balancing.cross_zone.enabled Attribut.

Asymmetrische Flüsse

Gateway Load Balancer unterstützen asymmetrische Datenflüsse, wenn der Load Balancer das erste Flow-Paket verarbeitet und das Antwortflusspaket nicht durch den Load Balancer weitergeleitet wird. Gateway Load Balancer unterstützen keine asymmetrischen Datenflüsse, wenn der Load Balancer nicht das ursprüngliche Flow-Paket verarbeitet, sondern das Antwortflusspaket durch den Load Balancer weitergeleitet wird.

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-Instances.

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

Wie Sie einen Gateway Load Balancer mit der erstellenAWS CLI, finden Sie unterErste Schritte mit der Verwendung von der CLI (p. 10).

Um einen Gateway Load Balancer mit der zu erstellenAWS Management Console, führen Sie die folgenden Aufgaben aus.

Aufgaben

- Schritt 1: Konfiguriere deine Zielgruppe und registriere Ziele (p. 20)
- Schritt 2: Konfiguration des Load Balancers und des Listeners (p. 20)
- Wichtige nächste Schritte (p. 21)

Schritt 1: Konfiguriere deine Zielgruppe und registriere Ziele

Sie können Ziele, wie etwa EC2-Instances, bei einer Zielgruppe registrieren. Sie verwenden die Zielgruppe, die Sie in diesem Schritt konfiguriert haben, wenn Sie Ihren Load Balancer im nächsten Schritt konfigurieren. Weitere Informationen finden Sie unter Zielgruppen (p. 24).

So konfigurieren Sie Ihre Zielgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie Create target group (Zielgruppe erstellen) aus.
4. Grundkonfiguration
   a. Wählen Sie unter Zieltyp auswählen die Option Instanzen aus, um Ziele anhand der Instanz-ID anzugeben, oder wählen Sie IP-Adressen aus, um Ziele anhand der IP-Adresse anzugeben.
   b. Geben Sie im Feld Target Group name (Zielgruppenname) einen Namen für die Zielgruppe ein.
   c. Stellen Sie sicher, dass Protokoll`GENEVE` und Port sind`6081`. Es werden keine anderen Protokolle oder Ports unterstützt.
   d. Wählen Sie für VPC eine Virtual Private Cloud (VPC) mit den Instances aus, die Sie in Ihre Zielgruppe aufnehmen möchten.
5. (Optional) Ändern Sie Health Zustandsprüfungen die Einstellungen und die erweiterten Einstellungen nach Bedarf. Wenn die Integritätsprüfungen nacheinander den Schwellenwert für fehlerhafte Werte überschreiten, nimmt der Load Balancer das Ziel außer Betrieb. Wenn die Integritätsprüfungen nacheinander den Schwellenwert für fehlerfrei überschreiten, nimmt der Load Balancer das Ziel wieder in Betrieb. Weitere Informationen finden Sie unter Zustandsprüfungen für Ihre Zielgruppen (p. 30).
6. (Optional) Erweitern Sie Tags und fügen Sie Tags hinzu.
7. Wählen Sie Next (Weiter).
8. Fügen Sie für Registerziele 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 unten „Als ausstehend einschließen“.
   - Wenn der Zieltyp IP-Adressen ist, wählen Sie das Netzwerk aus, geben Sie die IP-Adresse und die Ports ein und wählen Sie dann unten Als ausstehend einschließen aus.
9. Wählen Sie Create target group (Zielgruppe erstellen) aus.

Schritt 2: Konfiguration des Load Balancers und des Listeners

Verwenden Sie das folgende Verfahren, 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 dann Informationen über Ihr Netzwerk und den IP-Listener an, der den Datenverkehr an Ihre Zielgruppen weiterleitet. Nur Zielgruppen mit GENEVE stehen für die Verwendung mit dem Gateway Load Balancer zur Verfügung.

So erstellen Sie einen Gateway Load Balancer

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Klicken Sie auf Create Load Balancer.
4. Wählen Sie unter Gateway Load Balancer die Option Erstellen aus.

5. Grundkonfiguration

   a. Geben Sie im Feld Load balancer name (Name des Load Balancers) einen Namen für Ihren Load Balancer ein. Zum Beispiel **`my-glb`**. Der Name Ihres Gateway Load Load Balancer muss innerhalb Ihrer Gruppe von Load Balancers für die Region eindeutig sein. Er darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen und Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.

   b. Wählen Sie im Feld IP address type type type type type type type type type type (IP-Adresstyp) die Option IP-Adresstyp die Option IP-Adresstyp (IP-Adresstyp) aus, um nur IPv4-Adressen zu unterstützen, oder dualstack, um IP-Adresstypen

6. Netzwerkzuordnung

   a. Wählen Sie für VPC den Dienstanbieter VPC aus.

   b. Wählen Sie für Mappings alle Availability Zones aus, in denen Sie Security Appliance-Instanzen gestartet haben, sowie die entsprechenden öffentlichen Subnetze.

7. IP-Listener-Routing

   - Wählen Sie als Standardaktion eine Zielgruppe aus, an die der Traffic weitergeleitet werden soll. Wenn Sie nicht über eine Zielgruppe verfügen, erstellen Sie zuerst eine. Die Zielgruppe muss das GENEVE-Protokoll verwenden.

8. (Optional) Erweitern Sie Tags und fügen Sie Tags hinzu.
9. Überprüfen Sie Ihre Konfiguration und wählen Sie dann Create load balancer (Load Balancer erstellen) aus.

Wichtige nächste Schritte

Stellen Sie nach der Erstellung Ihres Load Balancers sicher, dass Ihre EC2-Instances die erste Integritätsprüfung bestanden haben. Um Ihren Load Balancer-Endpunkt zu testen, müssen Sie einen Gateway-Load-Balancer-Endpunkt erstellen und Ihre Routingtabelle aktualisieren, damit der Gateway-Load-Balancer-Endpunkt der nächste Hop ist. Diese Konfigurationen werden in der Amazon VPC-Konsole festgelegt. Weitere Informationen finden Sie unterSchritt 3: Erstellen eines Gateway-Load-Balancer-Endpunkts (p. 7) undSchritt 4: Konfigurieren des Routings (p. 8) imErste Schritte mit Gateway Load Balancern (p. 3) Abschnitt.

Tags für Ihre Gateway Load Balancer

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. 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 ein Tag nicht mehr benötigen, können Sie es aus 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 darstellbar sind, sowie die folgenden Sonderzeichen: _:/@. Verwenden Sie keine führenden oder nachfolgenden Leerzeichen.

- Verwenden Sie in Tag-Namen oder -Werten nicht das Präfix `aws:`, da es für die AWS-Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

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

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Gateway Load Balancer aus.
4. Wählen Sie Tags, Add/Edit Tags, und führen Sie dann einen oder mehrere der folgenden Schritte aus:
   a. Um ein Tag zu aktualisieren, bearbeiten Sie die Werte für Key und Value.
   b. Um ein neues Tag hinzuzufügen, wählen Sie Create Tag. 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 Save (Speichern).

So aktualisieren Sie die Tags für einen Gateway Load Balancer mit derAWS 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 Nutzungsstunde oder Teilstunde, in der er ausgeführt wird. Wenn Sie den Gateway Load Balancer nicht mehr benötigen, können Sie ihn löschen. Sobald der Gateway Load Balancer gelöscht wurde, fallen keine Gebühren dafür mehr 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-Endpunktdienst zugeordnet ist, müssen Sie die Endpunktdienstkonfiguration löschen, bevor Sie den zugehörigen Gateway Load Balancer löschen können.

Durch das Löschen eines Gateway-Load-Balancers werden auch seine Listener gelöscht. Das Löschen eines Gateway Load Load Balancer hat keine Auswirkungen auf seine registrierten Ziele. Ihre EC2-Instances werden beispielsweise weiter ausgeführt und sind weiterhin bei ihren Zielgruppen registriert. Informationen zum Löschen Ihrer Zielgruppen finden Sie unter Löschen einer Zielgruppe (p. 39).

So löschen Sie einen Gateway Load Balancer mit der Konsole

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

So löschen Sie einen Gateway Load Balancer mit derAWS CLI

Verwenden Sie den delete-load-balancer-Befehl.

Listener für Ihre Gateway Load Balancer

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

Listener für Gateway Load Balancers überwachen alle IP-Pakete über alle Ports hinweg. Sie können kein Protokoll oder 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.

Aktualisieren Ihres Listeners unter Verwendung der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Load Balancer aus und wählen Sie anschließend Listeners aus.
4. WählenListener bearbeiten.
5. FürWeiterleitung an Zielgruppe, wählen Sie eine Zielgruppe aus
6. Wählen Sie Save (Speichern) aus.

Aktualisieren Ihres Listeners unter Verwendung der AWS CLI

Verwenden Sie den Befehl modify-listener.

Zielgruppen für Ihre Gatway Load Balancer

Die einzelnen Zielgruppen werden verwendet, um Anfragen an ein oder mehrere registrierte Ziele weiterzuleiten. Wenn Sie einen Listener erstellen, geben Sie eine Zielgruppe für die Standardaktion an. Der Datenverkehr wird an die Zielgruppe weitergeleitet, die in der Listener-Regel angegeben ist. Sie können unterschiedliche Zielgruppen für verschiedene Arten von Anfragen erstellen.

Sie definieren Zustandsprüfungseinstellungen für Ihren Gateway Load Balancer pro Zielgruppe. Jede Zielgruppe verwendet die standardmäßigen Zustandsprüfungseinstellungen, es sei denn, Sie überschreiben diese, wenn Sie die Zielgruppe erstellen, oder ändern sie später. Nachdem Sie in einer Regel für einen Listener eine Zielgruppe angegeben haben, überwacht der Gateway Load Balancer kontinuierlich den Zustand aller bei der Zielgruppe registrierten Ziele, die sich in einer Availability Zone befinden, die für den Gateway Load Balancer aktiviert ist. Der Gateway Load Balancer leitet Anfragen an die registrierten Ziele weiter, die fehlerfrei sind. Weitere Informationen finden Sie unter Zustandsprüfungen für Ihre Zielgruppen (p. 30).

Inhalt

Weiterleitungskonfiguration

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

- Protokoll: GENEVE
- Hafen: 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 `ip` ist, können Sie IP-Adressen von einem der folgenden CIDR-Blöcke angeben:

- Die Subnetze der VPC für die Zielgruppe
- 10.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

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

Registrierte Ziele

Ihr Gateway Load Balancer dient als zentrale Anlaufstelle für Kunden und verteilt eingehenden Datenverkehr auf seine fehlerfreien registrierten Ziele. Jede Zielgruppe muss mindestens ein registriertes Ziel in jeder Availability Zone haben, das für den Gateway Load Balancer aktiviert ist. Sie können jedes Ziel bei einer oder mehreren Zielgruppen registrieren.

Steigt die Nachfrage, können Sie zusätzliche Ziele bei einer oder mehreren Zielgruppen registrieren, um die Nachfrage zu bewältigen. Der Gateway Load Balancer beginnt, den Datenverkehr an ein neu registriertes Ziel weiterzuleiten, sobald der Registrierungsprozess abgeschlossen ist.

Wenn die Nachfrage sinkt oder Sie Ihre Ziele bedienen müssen, können Sie Ziele von 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 die Weiterleitung des Datenverkehrs an ein Ziel, sobald es abgemeldet ist. 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 für Zielgruppen verwenden:

`deregistration_delay.timeout_seconds`

Die Zeitspanne, wie lange Elastic Load Balancing wartet, bevor der Status eines deregistrierten Ziels von`draining` in geändert wird`unused`. 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 gesetzt ist`false`, wird 5_tuple verwendet.

`stickiness.type`

Gibt den Typ der Klebrigkeit des Ablaufs an. Die möglichen Werte für Zielgruppen, die Gateway Load Balancers zugeordnet sind, sind:

- `source_ip_dest_ip`
- `source_ip_dest_ip_proto`

`target_failover.on_deregistration`

Gibt an, wie der Gateway Load Balancer mit vorhandenen Flows umgeht, 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 mit vorhandenen Flows umgeht, 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.

Verzögerung der Registrierungsaufhebung

Wenn Sie ein Ziel abmelden, verwaltet der Gateway Load Balancer Flows zu diesem Ziel auf folgende Weise:

Neue Flüsse:

Der Gateway Load Balancer sendet keine neuen Flows mehr an ein deregistriertes Ziel.

Bestehende Abläufe:

Der Gateway Load Balancer verarbeitet bestehende Flows protokollbasiert.

- TCP-Protokolle: Bestehende Datenflüsse für TCP-Protokolle werden geschlossen, wenn sie länger als 350 Sekunden inaktiv sind.
- Nicht-TCP-Protokolle: Bestehende Datenflüsse für alle Nicht-TCP-Protokolle werden geschlossen, wenn sie länger als 120 Sekunden inaktiv sind.

Um bestehende Flows zu entlasten, empfehlen wir, den gesamten Datenverkehr nicht mehr an den Load Balancer zu senden. Dadurch kann das durch die Deregistrierung verursachte Leerlauf-Timeout wirksam werden. Ein deregistriertes Ziel zeigt an, dass es so`draining` lange dauert, bis das Timeout abläuft. Nach Ablauf des Zeitlimits für die Deregistrierungsverzögerung geht das Ziel in einen`unused` Zustand über.

So aktualisieren Sie den Wert für die Deregistrierungsverzögerung mithilfe der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die 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 Deregistrationsverzögerung nach Bedarf.
6. Wählen Sie Save Changes (Änderungen speichern).

So aktualisieren Sie den Wert für die Verzögerung der Registrierungsaufhebung mithilfe der AWS CLI

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

Ziel-Failover

Mit Target Failover geben Sie an, wie der Gateway Load Balancer mit vorhandenen Datenverkehrsströmen umgeht, wenn ein Ziel fehlerhaft wird oder wenn das Ziel abgemeldet wird. Standardmäßig sendet der Gateway Load Balancer weiterhin bestehende Flows an dasselbe Ziel, auch wenn das Ziel ausgefallen ist oder deregistriert wurde. Sie können diese Flows verwalten, indem Sie sie entweder erneut aufwärmen (`rebalance`) oder sie im Standardzustand belassen (`no_rebalance`).

Keine Neugewichtung:

Der Gateway Load Balancer sendet weiterhin bestehende Flows an ausgefallene oder ausgelastete Ziele. Neue Ströme werden jedoch zu gesunden Zielen geschickt. Dies ist das Standardverhalten.

Neuausrichtung:

Der Gateway Load Balancer berechnet vorhandene Flows erneut und sendet sie nach dem Timeout der Deregistrierungsverzögerung an fehlerfreie Ziele.

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

Bei Zielen mit fehlerhaften Zielen hängt die Mindestzeit bis zum Failover von der Konfiguration der Zielgruppen-Integritätsprüfung ab (Intervall mal Schwellenwert). Dies ist die Mindestzeit, vor der ein Ziel als ungesund gekennzeichnet wird. Nach Ablauf dieser Zeit kann der Gateway Load Balancer aufgrund der zusätzlichen Übertragungszeit und des Backoffs der TCP-Neuübertragung mehrere Minuten in Anspruch nehmen, bevor er neue Flows an fehlerfreie Ziele umleitet.

So aktualisieren Sie den Ziel-Failover-Wert mithilfe der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die 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 Target-Failover nach Bedarf.
6. Wählen Sie Save Changes (Änderungen speichern).

Um den Ziel-Failover-Wert mit dem zu aktualisierenAWS CLI

Verwenden Sie den modify-target-group-attributesBefehl mit den folgenden Schlüsselwertpaaren:

- 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.

Klebrigkeit

Standardmäßig behält der Gateway Load Balancer mit 5-Tupel (für TCP/UDP-Flows) die Klebrigkeit der Flows zu einer bestimmten Ziel-Appliance mit. 5-Tupel umfasst Quell-IP, Quell-Port, Ziel-Port, Ziel-Port und Transportprotokoll. Sie können das Attribut stickiness type verwenden, um die Standardeinstellung (5-Tupel) zu ändern und entweder 3-Tupel (Quell-IP, Ziel-IP und Transportprotokoll) oder 2-Tupel (Quell-IP und Ziel-IP) wählen.

Überlegungen zur Klebrigkeit

- Flow Stickiness wird auf Zielgruppenebene konfiguriert und angewendet, und sie gilt für den gesamten Traffic, der an die Zielgruppe geht.
- Flow Stickiness funktioniert nicht, wenn der Gateway Load Balancer integriert ist,AWS Transit Gateway wenn der Appliance-Modus aktiviert ist.
- Ein klebriger Fluss kann zu einer ungleichmäßigen Verteilung von Verbindungen und Strömen führen, was sich auf die Verfügbarkeit des Ziels auswirken kann. Es wird empfohlen, alle vorhandenen Flows zu beenden oder zu löschen, bevor Sie den Stickiness-Typ der Zielgruppe ändern.

So aktualisieren Sie die Klebrigkeit mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Target Groups (Zielgruppen) aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die 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 Flow Stickiness nach Bedarf.
6. Wählen Sie Save Changes (Änderungen speichern).

Um die Flow-Stickiness zu aktivieren oder zu ändern, verwenden Sie denAWS CLI

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

Erstellen einer Zielgruppe für Ihren Gateway Load Balancer

Sie registrieren Ziele für Ihren Gateway Load Balancer anhand 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 (p. 23).

Sie können jederzeit Ziele zu Ihrer Zielgruppe hinzufügen oder aus dieser entfernen. Weitere Informationen finden Sie unter Ziele registrieren (p. 35). Sie können auch die Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern. Weitere Informationen finden Sie unter Ändern der Zustandsprüfung (p. 34).

New console

Erstellen einer Zielgruppe mit der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie Create target group (Zielgruppe erstellen) aus.
4. Wählen Sie unter Zieltyp auswählen die Option Instanzen aus, um Ziele anhand der Instanz-ID zu registrieren, oder IP-Adressen, um Ziele nach IP-Adresse zu registrieren.
5. Geben Sie im Feld Target Group name (Zielgruppenname) einen Namen für die Zielgruppe ein. Dieser Name muss für jede Region und jedes Konto eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen oder Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen.
6. Verwenden Sie für Protokoll GENEVE. Beim GENEVE-Protokoll muss der Port 6081 sein.
7. Wählen Sie im Feld VPC eine Virtual Private Cloud (VPC) aus.
8. Ändern Sie im Abschnitt Health Checks (optional) die Standardeinstellungen nach Bedarf.
9. Erweitern Sie den Abschnitt „Tags“ (optional) und fügen Sie ein oder mehrere Tags hinzu. Um ein Tag hinzuzufügen, wählen Sie Add Tags (Markierung) hinzufügen) und geben Sie den Markierungsschlüssel und -Wert ein.
10. Wählen Sie Next (Weiter).
11. 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 unten „Als ausstehend einschließen“.
    - Wenn der Zieltyp IP-Adressen ist, wählen Sie das Netzwerk aus, geben Sie die IP-Adresse und die Ports ein und wählen Sie dann unten Als ausstehend einschließen aus.
12. Wählen Sie Create target group (Zielgruppe erstellen) aus.

Old console

Erstellen einer Zielgruppe mit der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie Create target group (Zielgruppe erstellen) aus.
4. Geben Sie im Feld Target Group name (Zielgruppenname) einen Namen für die Zielgruppe ein. Dieser Name muss für jede Region und jedes Konto eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen oder Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen.
5. Verwenden Sie für Protokoll GENEVE. Beim GENEVE-Protokoll muss der Port 6081 sein.
6. Wählen Sie für Target type `instance` aus, um Ziele nach Instance-ID anzugeben, oder `ip`, um Ziele nach IP-Adresse anzugeben.
7. Wählen Sie im Feld VPC eine Virtual Private Cloud (VPC) aus.
8. (Optional) Ändern Sie in den Feldern Health check settings und Advanced health check settings die Standardeinstellungen nach Bedarf. Wählen Sie Create (Erstellen) aus.
9. (Optional) Fügen Sie einen oder mehrere Tags wie folgt hinzu:

    a. Wählen Sie die neu erstellte Zielgruppe aus.

b. Wählen Sie Tags, Add/Edit Tags.

c. Klicken Sie auf der Seite Add/Edit Tags für jedes Tag, das Sie hinzufügen auf Create Tag, und geben Sie den Tag-Schlüssel und -Wert an. Wenn Sie fertig mit dem Hinzufügen der Tags sind, klicken Sie auf Save (Speichern).

10. (Optional) Informationen dazu, wie Sie Ziele einer Zielgruppe hinzufügen, finden Sie unter Registrieren von Zielen für Ihre Zielgruppe (p. 35).

Erstellen einer Zielgruppe mit der 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.

Zustandsprüfungen für Ihre Zielgruppen

Sie können Ihre Ziele bei einer oder mehreren Zielgruppen registrieren. Ihr Gateway Load Balancer beginnt mit der Weiterleitung von Anfragen an ein neu registriertes Ziel, sobald der Registrierungsprozess abgeschlossen ist. Es kann einige Minuten dauern, bis der Registrierungsprozess abgeschlossen ist und die Zustandsprüfungen beginnen.

Der Gateway Load Balancer sendet regelmäßig eine Anfrage an jedes registrierte Ziel, um seinen Status zu überprüfen. Nachdem jede Integritätsprüfung abgeschlossen ist, schließt der Gateway Load Balancer die Verbindung, die für die Integritätsprüfung eingerichtet wurde.

Zustandsprüfungseinstellungen

Sie konfigurieren aktive Integritätsprüfungen für die Ziele in einer Zielgruppe mithilfe der folgenden Einstellungen. Wenn die Integritätsprüfungen die angegebene Anzahl von überschreitenUnhealthyThresholdCountBei aufeinanderfolgenden Ausfällen nimmt der Gateway Load Balancer das Ziel außer Betrieb. Wenn die Integritätsprüfungen die angegebene Anzahl von überschreitenHealthyThresholdCountIn Folge erfolgreich, setzt der Gateway Load Balancer das Ziel wieder in Betrieb.

Einstellung	Beschreibung
HealthCheckProtocol	Das Protokoll, das der Load Balancer für die Zustandsprüfungen der Ziele verwendet. Möglichen Protokolle sind HTTP, HTTPS und TCP. Die Standardeinstellung ist „TCP“.
HealthCheckPort	Der Port, den Gateway Load Balancer für die Zustandsprüfungen der Ziele verwendet. Der Bereich liegt zwischen 0 und 65535. Die Standardeinstellung ist 80.
HealthCheckPath	[HTTP/HTTPS-Zustandsprüfungen] Die Ping-Pfad, der als Zielpfad für die Ziele der Zustandsprüfungen gilt. Der Standardwert ist /.
HealthCheckTimeoutSeconds	Die Anzahl der Sekunden, in denen keine Antwort von einem Ziel bedeutet, dass die Zustandsprüfung fehlgeschlagen ist. Der Bereich liegt zwischen 2 und 120. Der Standardwert für ist 5.

Einstellung	Beschreibung
HealthCheckIntervalSeconds	Der etwaige Zeitraum in Sekunden zwischen den Zustandsprüfungen der einzelnen Ziele. Der Bereich liegt zwischen 5 und 300. Standardmäßig ist ein Zeitraum von 10 Sekunden festgelegt. Dieser Wert muss größer oder gleich seinHealthCheckTimeoutSeconds. **Important** Integritätsprüfungen für Gateway Load Balancer werden verteilt und verwenden einen Konsensmechanismus, um die Zielintegrität zu bestimmen. Daher sollten Sie erwarten, dass Ziel-Appliances innerhalb des konfigurierten Zeitintervalls mehrere Integritätsprüfungen erhalten.
HealthyThresholdCount	Die Anzahl der aufeinanderfolgenden erfolgreichen Zustandsprüfungen, die erforderlich ist, damit ein fehlerhaftes Ziel als stabil eingestuft wird. Der Bereich liegt zwischen 2 und 10. Die Voreinstellung ist 3.
UnhealthyThresholdCount	Die Anzahl fortlaufender fehlgeschlagener Zustandsprüfungen, die erforderlich ist, damit ein Ziel als nicht betriebsbereit eingestuft wird. Der Bereich liegt zwischen 2 und 10. Die Voreinstellung ist 3.
Matcher	[HTTP/HTTPS-Zustandsprüfungen] Die HTTP-Codes, die verwendet werden, um ein Ziel auf eine erfolgreiche Antwort zu überprüfen. Der Wert muss 200 bis 399 betragen.

Zustandsstatus des Ziels

Bevor der Gateway Load Balancer eine Anforderung zur Integritätsprüfung an ein Ziel sendet, müssen Sie es bei einer Zielgruppe registrieren, seine Zielgruppe in einer Listener-Regel angeben und sicherstellen, dass die Availability Zone 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 registriert gerade das Ziel oder führt die ersten Integritätsprüfungen des Ziels durch. Zugehörige Ursachencodes: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	Das Ziel ist fehlerfrei. Verwandte Ursachencodes: Keine

Wert	Beschreibung
`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 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 ein anderer Wert ist als`Healthy`gibt die API einen Ursachencode und eine Beschreibung des Problems zurück, und die Konsole zeigt dieselbe Beschreibung an. Ursachencodes, die beginnen mit`Elb`stammen von der Gateway Load Balancer-Seite und Ursachencodes, die mit beginnen`Target`entstehen auf der Zielseite.

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

Ursachencode	Beschreibung
`Target.NotInUse`	Die Zielgruppe ist nicht für den Empfang von Datenverkehr vom Gateway Load Balancer konfiguriert Ziel befindet sich in einer Availability Zone, die nicht für den Gateway Load Balancer aktiviert ist
`Target.NotRegistered`	Ziel ist nicht in der Zielgruppe registriert

Gateway Load Balancer Balancer-Zielszenarien

Bestehende Flows: Bestehende Flows gehen immer auf dasselbe Ziel über, es sei denn, die Flows laufen ab oder werden zurückgesetzt, unabhängig vom Integritätsstatus des Ziels. Dieser Ansatz erleichtert das Entleeren der Verbindung und berücksichtigt Firewalls von Drittanbietern, die aufgrund der hohen CPU-Auslastung manchmal nicht in der Lage sind, auf Zustandsprüfungen zu reagieren.

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, auch wenn das Ziel fehlerhaft wird oder andere Ziele fehlerhaft werden.

Wenn alle Ziele fehlerhaft sind, wählt der Gateway Load Balancer ein Ziel nach dem Zufallsprinzip aus und leitet den Datenverkehr für die Dauer des Flows an dieses weiter, bis es entweder zurückgesetzt wird oder ein Timeout aufgetreten ist. Da der Datenverkehr an ein fehlerhaftes Ziel weitergeleitet wird, wird der Datenverkehr verworfen, bis dieses Ziel wieder fehlerfrei ist.

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

Zonenübergreifendes Load Balancing: Standardmäßig ist der Lastenausgleich über Availability Zones hinweg deaktiviert. Wenn Load Balancing über Zonen hinweg aktiviert ist, kann jeder Gateway Load Balancer alle Ziele in allen Availability Zones sehen und sie werden unabhängig von ihrer Zone gleich behandelt.

Entscheidungen über Lastenausgleich und Integritätsprüfungen sind zwischen den Zonen immer unabhängig. Selbst wenn der Lastausgleich über Zonen hinweg aktiviert ist, ist das Verhalten für vorhandene und neue Flows dasselbe wie oben beschrieben. Weitere Informationen finden Sie unterZonenübergreifendes Load Balancingin derElastic Load Balancing Benutzerhandbuch.

Zustand der Ziele prüfen

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

New console

So überprüfen Sie den Zustand Ihrer Ziele mit der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie den Namen einer Zielgruppe aus, um die Detailseite zu öffnen.
4. In der Registerkarte Targets (Ziele) gibt die Spalte Status den Status der einzelnen Ziele wider.
5. Wenn der Zielstatus ein anderer Wert ist als`Healthy`, dasEinzelheiten zum Statusenthält weitere Informationen.

Old console

So überprüfen Sie den Zustand Ihrer Ziele mit der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie die Zielgruppe aus.
4. Wählen Sie Targets und überprüfen Sie den Status jedes Ziels in der Spalte Status. Wenn der Status ein anderer Wert ist als`Healthy`zeigt die Konsole weitere Informationen an.

Überprüfen des Zustands Ihrer Ziele mit der AWS CLI

Verwenden Sie den describe-target-health-Befehl. 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 von CloudWatch Alarme, um eine Lambda-Funktion auszulösen, um Details über ungesunde Ziele zu senden. Für step-by-step Anweisungen finden Sie im folgenden Blogbeitrag: Identifizieren von fehlerhaften Zielen Ihres Load Balancers.

Ändern der Zustandsprüfung

Sie können einige Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern.

New console

So ändern Sie die Einstellungen für die Integritätsprüfung einer Zielgruppe mithilfe der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie den Namen einer Zielgruppe aus, um die Detailseite zu öffnen.
4. Auf derAngaben zur GruppeRegisterkarte, in derZustandsprüfungseinstellungenAbschnitt, wählen SieBearbeiten.
5. Auf derBearbeiten der Zustandsprüfungändern Sie die Einstellungen nach Bedarf und wählen Sie dannSpeichern Sie die Änderungen.

Old console

So ändern Sie die Einstellungen für die Integritätsprüfung einer Zielgruppe mithilfe der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie die Zielgruppe aus.
4. Wählen Sie Health checks, Edit.
5. Passen Sie die Einstellungen auf der Seite Edit target group (Zielgruppe bearbeiten) nach Bedarf an und wählen Sie dann Save (Speichern) aus.

Ändern von Zustandsprüfungseinstellungen für eine Zielgruppe mithilfe der AWS CLI

Verwenden Sie den modify-target-group-Befehl.

Registrieren von Zielen für Ihre Zielgruppe

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, Anfragen an das Ziel weiterzuleiten, sobald der Registrierungsprozess abgeschlossen ist und das Ziel die ersten Integritätsprüfungen bestanden hat. Es kann einige Minuten dauern, bis der Registrierungsvorgang abgeschlossen ist und die Zustandsprüfungen gestartet werden. Weitere Informationen finden Sie unter Zustandsprüfungen für Ihre Zielgruppen (p. 30).

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 die Weiterleitung von Anfragen an das Ziel beendet. Wenn der Bedarf nachträglich steigt, können Sie Ziele, die Sie bei der Zielgruppe abgemeldet haben, erneut registrieren. Muss ein Ziel gewartet werden, können Sie es abmelden und dann erneut registrieren, wenn die Wartung abgeschlossen ist.

Wenn Sie ein Ziel abmelden, wartet Elastic Load Balancing, bis die Anfragen während des Fluges abgeschlossen sind. Dies wird als Verbindungsausgleich bezeichnet. Der Status eines Ziels ist `draining`, während ein Verbindungsausgleich erfolgt. Nach Aufheben der Registrierung ändert sich der Status des Ziels in `unused`. Weitere Informationen finden Sie unter Verzögerung der Registrierungsaufhebung (p. 26).

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 Balancers 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 Network Access Control Lists (ACL) für die Subnetze Ihrer Instances Datenverkehr auf Port 6081 zulassen. Die Standard-Netzwerk-ACL für eine VPC lässt den gesamten ein- und ausgehenden Datenverkehr zu. Wenn Sie benutzerdefinierte Netzwerk-ACLs erstellen, stellen Sie sicher, dass sie den entsprechenden Datenverkehr zulassen.

Registrieren oder Aufheben der Registrierung von Zielen

Jede Zielgruppe muss mindestens ein registriertes Ziel in jeder Availability Zone haben, das 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 (p. 24).

Voraussetzungen

- Sie können Instances nicht anhand der Instanz-ID registrieren, wenn sie sich in einer VPC befinden, die Peering zur Load Balancer-VPC durchführt (gleiche Region oder andere Region). Sie können diese Instances nach IP-Adresse registrieren.

Inhalt

Ziele nach Instance-ID registrieren oder die Registrierung aufheben

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

New console

So registrieren Sie Ziele mithilfe der neuen Konsole anhand der Instanz-ID oder deregistrieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Targets (Ziele).
5. Um Instanzen zu registrieren, wählen Sie Ziele registrieren. Wählen Sie eine oder mehrere Instances aus. Wählen Sie dann im Folgenden die Option Als ausstehend einschließen). Wenn Sie mit dem Hinzufügen der Instances mit dem Hinzufügen der Instances (Markierungen) fertig sind, wählen Sie Registering
6. Um Instanzen abzumelden, wählen Sie die Instance aus und wählen Sie dann Deregister.

Old console

So registrieren oder deregistrieren Sie Ziele anhand der Instanz-ID mithilfe der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie die Zielgruppe aus.
4. Wählen Sie Targets, Edit.
5. (Optional) Wählen Sie im Feld Registered instances alle Instances aus, deren Registrierung aufgehoben werden soll, und wählen Sie Remove (Entfernen) aus.
6. (Optional) Wählen Sie für Instances alle laufenden Instances aus, die registriert werden sollen, und wählen Sie dann Zu registrierten Instanzen hinzufügen.
7. Wählen Sie Save (Speichern) aus.

Ziele nach IP-Adresse registrieren oder die Registrierung aufheben

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 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

New console

So registrieren oder deregistrieren Sie Ziele anhand der IP-Adresse mithilfe der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Targets (Ziele).
5. Um IP-Adressen zu registrieren, wählen Sie Ziele registrieren. Wählen Sie für jede IP-Adresse das Netzwerk, die Availability Zone, die IP-Adresse und den Port aus und wählen Sie dann unten Als ausstehend einschließen aus. Wählen Sie aus, wenn Sie alle gewünschten Adressen angegeben haben, wählen Sie Registered Tags (ausstehende Ziele registrieren).
6. Um IP-Adressen abzumelden, wählen Sie die IP-Adressen aus und wählen Sie dann Deregister. Wenn Sie viele registrierte IP-Adressen haben, können Sie einen Filter hinzufügen oder die Sortierreihenfolge ändern.

Old console

So registrieren oder deregistrieren Sie Ziele anhand der IP-Adresse mithilfe der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie die Zielgruppe aus und wählen Sie Targets, Edit.
4. Um IP-Adressen zu registrieren, wählen Sie das Symbol Register targets (das Pluszeichen) in der Menüleiste. Für jede IP-Adresse geben Sie das Netzwerk, Availability Zone, IP-Adresse und Port an, und wählen dann Add to list. Wenn Sie mit der Angabe der Adressen fertig sind, wählen Sie Register.
5. Um die Registrierung von IP-Adressen aufzuheben, wählen Sie das Symbol Deregister targets (das Minuszeichen) in der Menüleiste. Wenn Sie viele registrierte IP-Adressen haben, können Sie einen Filter hinzufügen oder die Sortierreihenfolge ändern. Wählen Sie die IP-Adressen aus und wählen Sie dann Deregister.
6. Wählen Sie in der Menüleiste Back to target group (die Zurück-Schaltfläche) aus, um diesen Bildschirm zu verlassen.

Registrieren oder Aufheben der Registrierung von Zielen mithilfe der AWS CLI

Verwenden Sie den Befehl register-targets zum Hinzufügen von Zielen und den Befehl deregister-targets zum Entfernen von Zielen.

Tags für Ihre Zielgruppe

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

Sie können mehrere Tags für jede Zielgruppe hinzufügen. Tag-Schlüssel müssen für jede Zielgruppe eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der der Zielgruppe bereits zugeordnet ist, ändert sich der Wert dieses Tags.

Wenn Sie ein Tag nicht mehr benötigen, können Sie es entfernen.

Einschränkungen

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

New console

So aktualisieren Sie die Tags für eine Zielgruppe mit der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen der Zielgruppe aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte „Tags“ die Option „Tags verwalten“ und führen Sie eine oder mehrere der folgenden Aktionen 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 Remove (Entfernen) neben dem zu löschenden Tag.
5. Wenn Sie mit der Aktualisierung der Tags fertig sind, wählen Sie Änderungen speichern.

Old console

So aktualisieren Sie die Tags für eine Zielgruppe mit der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie die Zielgruppe aus.
4. Klicken Sie in der Registerkarte Tags auf Add/Edit 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 für Key und Value.
   b. Um ein neues Tag hinzuzufügen, wählen Sie Tag erstellen und geben Sie dann Werte für Schlüssel und Wert 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 Save (Speichern).

So aktualisieren Sie die Tags für eine Zielgruppe mithilfe der AWS CLI

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

Löschen einer Zielgruppe

Sie können eine Zielgruppe löschen, wenn sie nicht durch die Weiterleitungsaktionen einer Listener-Regel referenziert wird. Das Löschen einer Zielgruppe hat keine Auswirkungen auf die Ziele hat, die bei der Zielgruppe registriert sind. Wenn Sie die registrierte EC2-Instance nicht mehr benötigen, können Sie sie anhalten oder beenden.

New console

Löschen einer Zielgruppe mit der neuen Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie Ihre Zielgruppe aus und wählen Sie dann Actions, Delete.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Yes, Delete (Ja, löschen).

Old console

Löschen einer Zielgruppe mit der alten Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING (LASTVERTEILUNG) die Option Load Balancers(Lastverteiler) aus.
3. Wählen Sie Ihre Zielgruppe aus und wählen Sie dann Actions, Delete.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Yes (Ja) aus.

Löschen einer Zielgruppe mithilfe der AWS CLI

Verwenden Sie den delete-target-group-Befehl.

Überwachen Sie Ihre Gateway Load Balancer

Mit den folgenden Funktionen können Sie Ihre Gateway Load Balancer überwachen, Datenverkehrsmuster analysieren und Probleme beheben. Der Gateway Load Balancer generiert jedoch keine Zugriffsprotokolle, da es sich um einen transparenten Layer-3-Load-Balancer handelt, der Flows nicht beendet. Um Zugriffsprotokolle zu erhalten, müssen Sie die Zugriffsprotokollierung auf Gateway Load Balancer Balancer-Ziel-Appliances wie Firewalls, IDS/IPS und Sicherheitsappliances aktivieren. Darüber hinaus können Sie auch VPC-Flow-Protokolle auf Gateway Load Balancers aktivieren.

CloudWatch-Metriken

Sie können mit Amazon CloudWatch Statistiken zu Datenpunkten für Ihre Gateway Load Balancer und Ziele als eine geordnete Reihe von Zeitreihendaten, auch bekannt alsMetrikenaus. 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 (p. 40).

VPC-Flow-Protokolle

Sie können mit VPC Flow Logs detaillierte Informationen über den Datenverkehr zu und von Ihrem Gateway Load Balancer erfassen. Weitere Informationen finden Sie unterVPC Flow LogsimAmazon VPC User Guideaus.

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

Es gibt zwei Einträge für jede Verbindung über Ihren Gateway Load Balancer, eine für die Frontend-Verbindung zwischen dem Client und dem Gateway Load Balancer und die andere 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 Instance keine Verbindungen vom Client zulässt, aber die Netzwerk-ACLs für das Subnetz sie zulassen, zeigen die Protokolle für die Netzwerkschnittstelle für den Gateway Load Balancer „ACCEPT OK“ für die Frontend- und Backend-Verbindungen an, während die Protokolle für die Netzwerkschnittstelle für die Instance zeigen „REJECT OK“ für die Verbindung.

CloudTrail-Protokolle

Sie könnenAWS CloudTrailum detaillierte Informationen zu den Aufrufen der Elastic Load Balancing Balancing-API zu erfassen, und sie als Protokolldateien in Amazon S3 speichern. Sie können diese CloudTrail-Protokolle verwenden, um die durchgeführten Aufrufe, die Quell-IP-Adresse, von welcher der Aufruf stammte, den Aufrufer, den Zeitpunkt des Aufrufs usw. zu ermitteln. Weitere Informationen finden Sie unter Protokollieren von API-Aufrufen für Ihren Gateway Load Balancer mitAWS CloudTrail (p. 44).

CloudWatch-Metriken für Ihren Gateway Load Balancer

Elastic Load Balancing veröffentlicht Datenpunkte für Ihre Gateway Load Balancers und Ihre Ziele auf Amazon CloudWatch. CloudWatch ermöglicht Ihnen, Statistiken zu diesen Datenpunkten als geordneten

Satz von Zeitreihendaten, bekannt alsMetrikenaus. 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 z. B. einen CloudWatch-Alarm erstellen, um eine bestimmte Metrik zu überwachen, und eine Aktion einleiten (z. B. Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb eines für Sie akzeptablen Bereichs liegt.

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

Weitere Informationen finden Sie im Amazon-CloudWatch-Benutzerhandbuch.

Inhalt

Gateway Load Balancer Balancer-Metriken

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

Metrik	Description
`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`aus. Dimensionen • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ConsumedLCUs`	Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden. Sie zahlen nur für die pro Stunde genutzte Anzahl der LCU. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing. Berichtkriterien: Immer gemeldet Statistiken: Alle Dimensionen • `LoadBalancer`
`HealthyHostCount`	Anzahl der als stabil betrachteten Ziele.

Metrik	Description
	Berichtkriterien: Wird gemeldet, wenn Zustandsprüfungen aktiviert sind Statistiken: Die nützlichsten Statistiken sind`Maximum`und`Minimum`aus. 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`aus. Dimensionen • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ProcessedBytes`	Die Gesamtzahl der vom Load Balancer verarbeiteten Byte. Diese Anzahl umfasst Datenverkehr zu und von Zielen, nicht jedoch Datenverkehr für Zustandsprüfungen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist`Sum`aus. 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`aus. Dimensionen • `LoadBalancer`, `TargetGroup` • `AvailabilityZone`, `LoadBalancer`, `TargetGroup`

Metrikdimensionen für Gateway Load Balancer

Verwenden Sie die nachstehenden Dimensionen, um die Metriken für Ihren Gateway Load Balancer zu filtern.

Dimension	Description
`AvailabilityZone`	Filtert die Metrikdaten nach Availability Zone.

Dimension	Description
`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 des ARN).
`TargetGroup`	Filtert die Metrikdaten nach der Zielgruppe. Geben Sie die Zielgruppe wie folgt an: app/Name der Zielgruppe/1234567890123456 (der letzte Teil des Zielgruppen-ARNs).

Anzeigen von CloudWatch-Metriken für Ihren Gateway Load Balancer

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

Alternativ können Sie Metriken für Ihren Gateway Load Balancer mit der CloudWatch-Konsole anzeigen.

Zeigen Sie Metriken mithilfe der Amazon EC2-Konsole wie folgt an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um nach Zielgruppe gefilterte Metriken anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Navigationsbereich Target Groups aus.
   b. Wählen Sie Ihre Zielgruppe aus und wählen Sie dann Monitoring.
   c. (Optional) Wählen Sie in Showing data for einen Zeitbereich aus., um die Ergebnisse nach Zeit zu filtern.
   d. Wenn Sie eine größere Ansicht einer Metrik aufrufen möchten, wählen Sie ihr Diagramm aus.
3. Um nach 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 aus und wählen SieÜberwachungaus.
   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.

So zeigen Sie Metriken mit der CloudWatch-Konsole an:

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metrics (Metriken) aus.
3. Wählen Sie dasGatewayeLBNamespace.
4. (Optional) Um eine Metrik für alle Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.

So zeigen Sie Metriken mit der a AWS CLI

Verwenden Sie den folgenden list-metrics-Befehl, um die verfügbaren Metriken aufzuführen:

```
aws cloudwatch list-metrics --namespace AWS/GatewayELB
```

So rufen Sie die Statistiken für eine Metrik mithilfe der AWS CLI ab

Verwenden Sie den folgenden get-metric-statistics-Befehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. Beachten Sie, dass CloudWatch jede eindeutige Kombination von Dimensionen als separate Metrik behandelt. 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"
}
```

Protokollieren von API-Aufrufen für Ihren Gateway Load Balancer mitAWS CloudTrail

Elastic Load Balancing ist integriert mitAWS CloudTrail, ein Service, der die Aktionen eines Benutzers, einer Rolle oder einesAWS-Dienst in Elastic Load Balancing. CloudTrail erfasst alle API-Aufrufe für Elastic Load Balancing als Ereignisse. Die erfassten Aufrufe umfassen Aufrufe von derAWS Management Consoleund Code-Aufrufe der Elastic Load Balancing -API-Operationen. Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignissen für Elastic Load Balancing. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Anhand der von CloudTrail erfassten Informationen können Sie die an Elastic Load Balancing gestellte Anfrage, die IP-Adresse, von der die Anforderung gestellt wurde, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Informationen zu Elastic Load Balancing in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in Elastic Load Balancing auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen aufgezeichnetAWSServiceereignisse inEreignisverlauf deraus. Sie können die neusten Ereignisse in Ihr

AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-API-Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in IhremAWSErstellen Sie einen Trail, einschließlich Ereignissen für Elastic Load Balancing, einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Elastic Load Balancing Balancing-Aktionen für Gateway Load Balancers werden von CloudTrail protokolliert und sind imElastic Load Balancing API Referenzversion 2015-12-01aus. Zum Beispiel werden durch Aufrufe`CreateLoadBalancer`und`DeleteLoadBalancer`Aktionen generieren Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde.
- Whether the request was made by another AWS service.

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Grundlegendes zu Elastic Load Balancing Balancing-Einträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket übermittelt werden. CloudTrail log files contain one or more log entries. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Die Protokolldateien enthalten Ereignisse für alleAWSAPI-Aufrufe für IhrenAWSKonto, nicht nur Elastic Load Balancing API-Aufrufe. Sie können Aufrufe der Elastic Load Balancing API finden, indem Sie nach`eventSource`elemente mit dem Wert`elasticloadbalancing.amazonaws.com`aus. Um einen Datensatz für eine bestimmte Aktion anzuzeigen, z. B. `CreateLoadBalancer`, suchen Sie nach `eventName`-Elementen mit dem Aktionsnamen.

Das folgende Beispiel zeigt -CloudTrail-Protokolleinträge für Elastic Load Balancing für einen Benutzer, der einen Gateway Load Balancer erstellt und dann mit der gelöscht hat.AWS CLIaus. Sie können die CLI mithilfe der `userAgent`-Elemente identifizieren. Sie können die angeforderten API-Aufrufe mithilfe der `eventName`-Elemente identifizieren. Informationen zum Benutzer (`Alice`) finden Sie im `userIdentity`-Element.

Example Beispiel: CreateLoadBalancer


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2020-12-11T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "name": "my-load-balancer",
        "type": "gateway"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "gateway",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "createdTime": "Dec 11, 2020 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0",
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```


Example Beispiel: DeleteLoadBalancer


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2020-12-12T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
```

```
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Kontingente für Ihre Gateway Load Balancer

Das AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden AWS-Service. 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 Kontingenterhöhung anzufordern, können Sie das Formular zur Erhöhung des Limits verwenden

Load Balancer

IhrAWS -Konto umfasst die folgenden Kontingente für Gateway Load Balancer.

Name	Standard	Anpassbar
Gateway Load Balancer pro Region	100	Ja
Gateway Load Balancer pro VPC	100	Ja
Gateway Load Balancer ENIs pro VPC	300 *	Ja
Listenancer 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
GENEVE-Zielgruppen pro Region	100	Ja
Ziele pro Zielgruppe	1.000	Ja
Ziele pro Availability Zone und GENEVE-Zielgruppe	300	Nein
Ziele pro Availability Zone und Gateway Load Balancer	300	Nein
Ziele pro Gateway Load Balancer	300	Nein

Bandbreite

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

Dokumentenverlauf für Gateway Load Balancers

In der folgenden Tabelle werden die Veröffentlichungen für Gateway Load Balancers beschrieben.

Änderung	Beschreibung	Datum
IPv6-Support (p. 49)	Sie können Ihren Gateway Load Balancer so konfigurieren, dass IPv4- und IPv6-Adressen unterstützt.	12. Dezember 2022
Konfigurierbare Fließklebrigkeit	Sie können das Hashing so konfigurieren, dass die Datenflüsse an eine bestimmte Ziel-Appliance gebunden bleiben.	25. August 2022
Erstversion (p. 49)	In dieser Version von Elastic Load Balancing werden Gateway Load Balancers 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.