aws

Classic Load Balancer

Elastic Load Balancing

Elastic Load Balancing: Classic Load Balancer

Table of Contents

Was ist ein Classic Load Balancer?

> **Note**
>
> Classic Load Balancers sind die vorherige Generation von Load Balancern von Elastic Load Balancing. Wir empfehlen Ihnen, zu einem Load Balancer der aktuellen Generation zu migrieren. Weitere Informationen finden Sie unter Migrieren Sie Ihren Classic Load Balancer.

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

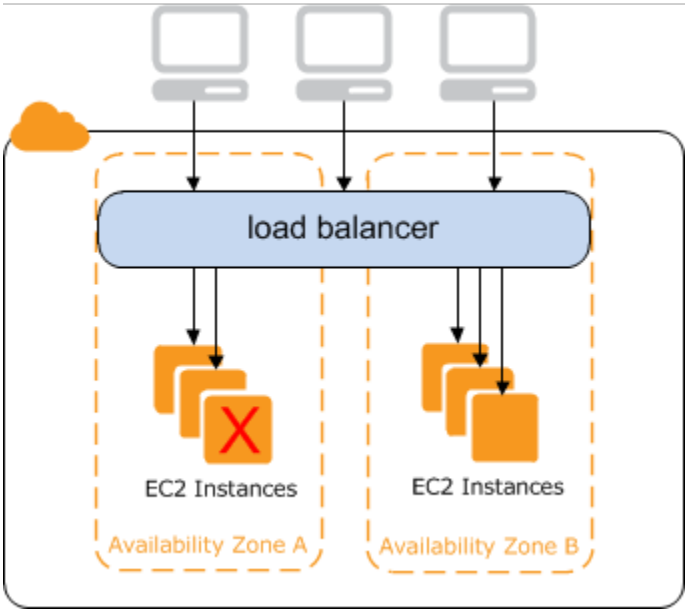
Classic Load Balancer – Übersicht

Ein Load Balancer verteilt den eingehenden Anwendungsdatenverkehr auf mehrere EC2 Instances in mehreren Availability Zones. Dies erhöht die Fehlertoleranz Ihrer Anwendungen. Elastic Load Balancing ermittelt fehlerhafte Instances und leitet den Datenverkehr nur an fehlerfreie Instances weiter.

Ihr Load Balancer dient als zentraler Kontaktpunkt für Clients. Dies erhöht die Verfügbarkeit Ihrer Anwendung. Sie können Instances zu Ihrem -Load Balancer hinzufügen und Instances entfernen, wenn sich Ihre Bedürfnisse ändern, ohne den allgemeinen Fluss von Anfragen an Ihre Anwendung zu unterbrechen. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der Datenverkehr zu Ihrer Anwendung im Laufe der Zeit ändert. Elastic Load Balancing kann für die meisten Workloads automatisch skaliert werden.

Ein Listener prüft Verbindungsanfragen von Clients mit dem von Ihnen konfigurierten Protokoll und Port und leitet Anfragen mit dem Protokoll und der Portnummer, das bzw. die Sie konfigurieren, an eine oder mehrere registrierte Instances weiter. Sie fügen Ihrem Load Balancer einen oder mehrere Listener hinzu.

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



Um sicherzustellen, dass Ihre registrierten Instances die Anfragelast in jeder Availability Zone verarbeiten können, ist es wichtig, dafür zu sorgen, dass etwa dieselbe Anzahl von Instances in jeder Availability Zones beim Load Balancer registriert ist. Beispiel: Wenn Sie zehn Instances in der Availability Zone us-west-2a und zwei Instances in us-west-2b haben, werden die Anfragen gleichmäßig auf die beiden Availability Zones verteilt. Dies hat zur Folge, dass die zwei Instances in der Region us-west-2b dieselbe Menge an Datenverkehr wie die zehn Instances in us-west-2a bewältigen. Stattdessen sollten Sie in jeder Availability Zone sechs Instances haben.

Der Load Balancer verteilt den Datenverkehr standardmäßig gleichmäßig auf die Availability Zones, die Sie für Ihren Load Balancer aktivieren. Um Datenverkehr gleichmäßig auf alle registrierten Instances in allen Availability Zones zu verteilen, aktivieren Sie in Ihrem Load Balancer zonenübergreifenden Lastausgleich. Für eine bessere Fehlertoleranz sollte allerdings dennoch etwa die gleiche Anzahl von Instances in jeder Availability Zone vorhanden sein.

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

Vorteile

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

- Unterstützung für TCP- und SSL-Listener
- Unterstützung für Sticky Sessions mit anwendungsgenerierten Cookies

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

Erste Schritte

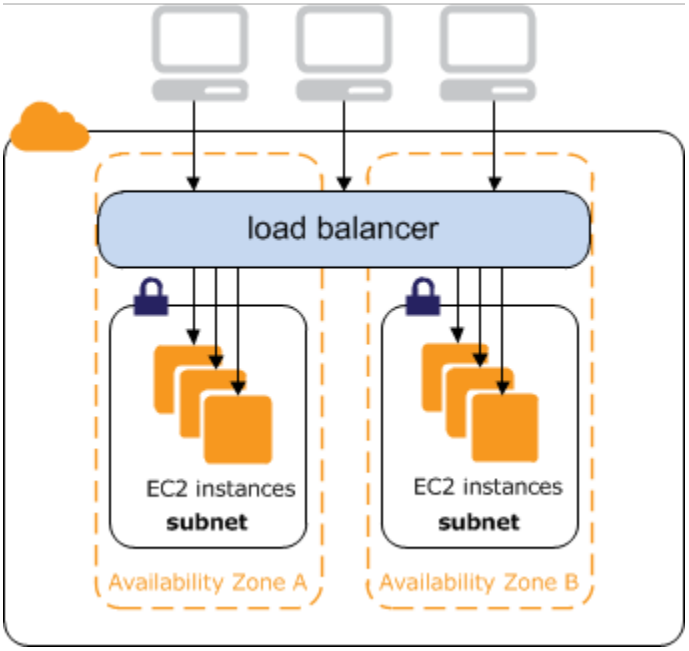
- Informationen dazu, wie Sie einen Classic Load Balancer erstellen und EC2 Instances damit registrieren, finden Sie unterEinen Classic Load Balancer mit Internetzugriff erstellen.
- Informationen dazu, wie Sie einen HTTPS-Load Balancer erstellen und EC2 Instances damit registrieren, finden Sie unter. Erstellen eines Classic Load Balancers mit einem HTTPS-Listener
- Informationen zur Verwendung der verschiedenen Funktionen, die von Classic Load Balancers unterstützt werden, finden Sie unter. Konfigurieren Ihres Classic Load Balancers

Preisgestaltung

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

Mit dem Internet verbundene Classic Load Balancer

Wenn Sie einen Classic Load Balancer erstellen, können Sie ihn zu einem internen Load Balancer oder einem mit dem Internet verbundenen Load Balancer machen. Ein mit dem Internet verbundener Load Balancer hat einen öffentlich auflösbaren DNS-Namen, sodass er Anfragen von Clients über das Internet an die Instances weiterleiten kann, die beim Load Balancer registriert sind. EC2



Der DNS-Name eines internen Load Balancers ist öffentlich zu den privaten IP-Adressen der Knoten auflösbar. Daher kann der interne Load Balancer nur Anforderungen von Clients mit Zugriff auf die VPC für den Load Balancer weiterleiten. Weitere Informationen finden Sie unter Interne Load Balancer.

Inhalt

Öffentliche DNS-Namen für Ihren Load Balancer

Wenn der Load Balancer erstellt wird, erhält er einen öffentlichen DNS-Namen, den Clients zur Übermittlung von Anforderungen verwenden können. Die DNS-Server lösen den DNS-Namen Ihres Load Balancer in die öffentlichen IP-Adressen der Load Balancer-Knoten für Ihren Load Balancer auf. Jeder Load Balancer-Knoten ist über die private IP-Adresse mit den Backend-Instances verbunden.

In der Konsole wird ein öffentlicher DNS-Name im folgenden Format angezeigt:

```
name-1234567890.region.elb.amazonaws.com
```

Einen Classic Load Balancer mit Internetzugriff erstellen

Wenn Sie einen Load Balancer erstellen, konfigurieren Sie Listener, konfigurieren Integritätsprüfungen und registrieren Back-End-Instances. Sie konfigurieren einen Listener, indem Sie ein Protokoll und einen Port für Frontend-Verbindungen (Client zu Load Balancer) sowie ein Protokoll und einen Port für Backend-Verbindungen (Load Balancer zu Backend-Instances) konfigurieren. Sie können mehrere Listener für Ihren Load Balancer konfigurieren.

Dieses Tutorial bietet eine praktische Einführung in Classic Load Balancers über eine webbasierte Oberfläche. AWS Management Console Sie erstellen einen Load Balancer, der öffentlichen HTTP-Verkehr empfängt und an Ihre Instances sendet. EC2

Eine Anleitung zum Erstellen eines Load Balancer mit einem HTTPS-Listener finden Sie unter Erstellen eines Classic Load Balancers mit einem HTTPS-Listener.

Aufgaben

- Bevor Sie beginnen
- Erstellen Sie einen Classic Load Balancer mit dem AWS Management Console

Bevor Sie beginnen

- Erstellen einer Virtual Private Cloud (VPC). Weitere Informationen finden Sie unter Empfehlungen für Ihre VPC.
- Starten Sie die EC2 Instances, die Sie bei Ihrem Load Balancer registrieren möchten. Stellen Sie sicher, dass die Sicherheitsgruppen für diese Instances den HTTP-Zugriff auf Port 80 erlauben.
- Installieren Sie auf jeder Instance einen Webserver, z. B. Apache oder Internet Information Services (IIS), geben Sie den DNS-Namen in das Adressfeld eines mit dem Internet verbundenen Webbrowser ein und stellen Sie sicher, dass der Browser die Standardseite des Servers anzeigt.

Erstellen Sie einen Classic Load Balancer mit dem AWS Management Console

Gehen Sie wie folgt vor, um Ihren Classic Load Balancer zu erstellen. Geben Sie grundlegende Konfigurationsinformationen für Ihren Load Balancer an, z. B. einen Namen und ein Schema. Geben Sie anschließend Informationen über Ihr Netzwerk und den Listener an, der den Datenverkehr an Ihre Instances weiterleitet.

So erstellen Sie einen Classic Load Balancer mit der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste eine Region für Ihren Load Balancer aus. Achten Sie darauf, dieselbe Region auszuwählen, die Sie für Ihre EC2 Instances ausgewählt haben.
3. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
4. Wählen Sie Load Balancer erstellen aus.
5. Erweitern Sie den Abschnitt Classic Load Balancer und wählen Sie dann Create (Erstellen) aus.
6. Basiskonfiguration
   a. Geben Sie im Feld Load balancer name (Name des Load Balancers) einen Namen für Ihren Load Balancer ein.

      Der Name des Classic Load Balancers muss innerhalb Ihrer Gruppe mit Classic Load Balancern für die Region eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen sowie Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.
   b. Wählen Sie für Scheme (Schema) die Option Internet-facing (Internet verbunden) aus.
7. Netzwerkzuordnung
   a. Wählen Sie im Feld VPC die VPC aus, die Sie für Ihre Instances verwendet haben.
   b. Wählen Sie für Mappings (Zuordnungen) zunächst eine Availability Zone und dann ein öffentliches Subnetz aus den verfügbaren Subnetzen aus. Sie können nur ein Subnetz pro Availability Zone auswählen. Zur Verbesserung der Verfügbarkeit Ihrer Load Balancer wählen Sie mehr als eine Availability Zone und ein Subnetz aus.
8. Sicherheitsgruppen

- Wählen Sie für Security groups (Sicherheitsgruppen) eine vorhandene Sicherheitsgruppe aus, die so konfiguriert ist, dass sie den erforderlichen HTTP-Verkehr auf Port 80 zulässt.

9. Listener und Routing

   a. Stellen Sie für Listener sicher, dass das Protokoll `HTTP` und der Port `80` ist.

   b. Stellen Sie für Instance sicher, dass das Protokoll `HTTP` und der Port `80` ist.

10. Health checks (Zustandsprüfungen)

    a. Stellen Sie für Ping Protocol (Ping-Protokoll) sicher, dass das Protokoll `HTTP` ist.

    b. Stellen Sie für Ping Port sicher, dass der Port `80` ist.

    c. Stellen Sie für Ping Path (Ping-Pfad) sicher, dass der Pfad `/` ist.

    d. Verwenden Sie für die Advanced health check settings (Einstellungen für erweiterte Zustandsprüfungen) die Standardwerte.

11. Instances

    a. Wählen Sie Add instances (Instances hinzufügen) aus, um den Bildschirm zur Instance-Auswahl aufzurufen.

    b. Unter Available instances (Verfügbare Instances) können Sie basierend auf den aktuellen Netzwerkeinstellungen aus den aktuellen Instances auswählen, die für den Load Balancer verfügbar sind.

    c. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Confirm (Bestätigen) aus, um die zu registrierenden Instances zum Load Balancer hinzuzufügen.

12. Attribute

    - Behalten Sie für Enable cross-zone load balancing (Zonenübergreifendes Load Balancing aktivieren), Enable connection draining (Connection Draining aktivieren) und Timeout (draining interval) (Timeout (Draining-Intervall)) die Standardwerte bei.

13. Load balancer tags (optional) (Load-Balancer-Tags (optional))

    a. Das Feld Key (Schlüssel) ist ein Pflichtfeld.

    b. Das Feld Value (Wert) ist optional.

    c. Um ein weiteres Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) aus und geben Sie dann Ihre Werte in das Feld Key (Schlüssel) und optional in das Feld Value (Wert) ein.

d. Um ein vorhandenes Tag zu entfernen, wählen Sie neben dem zu entfernenden Tag die Option Remove (Entfernen).

14. Summary and creation (Zusammenfassung und Erstellung)

    a. Wenn Sie Einstellungen ändern müssen, wählen Sie neben der Einstellung, die geändert werden muss, Edit (Bearbeiten) aus.

    b. Wenn Sie mit allen in der Zusammenfassung angezeigten Einstellungen zufrieden sind, wählen Sie Create load balancer (Load Balancer erstellen) aus, um mit der Erstellung Ihres Load Balancers zu beginnen.

    c. Wählen Sie auf der letzten Erstellungsseite Load Balancer anzeigen aus, um Ihren Load Balancer in der EC2 Amazon-Konsole anzuzeigen.

15. Verify

    a. Wählen Sie den neuen Load Balancer aus.

    b. Überprüfen Sie auf der Registerkarte Target instances (Ziel-Instances) die Spalte Health status (Zustandsstatus). Sobald mindestens eine Ihrer EC2 Instances in Betrieb ist, können Sie Ihren Load Balancer testen.

    c. Kopieren Sie im Abschnitt Details den DNS name (DNS-Namen) des Load Balancers, der etwa wie `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com` aussehen würde.

    d. Fügen Sie den DNS name (DNS-Namen) Ihres Load Balancers in das Adressfeld eines öffentlichen Webbrowsers mit Internetanschluss ein. Wenn Ihr Load Balancer korrekt funktioniert, sehen Sie die Standardseite Ihres Servers.

16. Delete (optional) (Löschen (optional))

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

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

    c. Wählen Sie den Load Balancer aus.

    d. Wählen Sie den Load Balancer aus und klicken Sie auf Actions (Aktionen) und dann auf Delete load balancer (Load Balancer löschen).

    e. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie `confirm` ein und wählen Sie dann Delete (Löschen) aus.

f. Nachdem Sie einen Load Balancer gelöscht haben, werden die EC2 Instances, die beim Load Balancer registriert wurden, weiter ausgeführt. Ihnen wird jede teilweise oder ganze Stunde in Rechnung gestellt, in der sie weiterlaufen. Wenn Sie eine EC2 Instance nicht mehr benötigen, können Sie sie beenden oder beenden, um zusätzliche Kosten zu vermeiden.

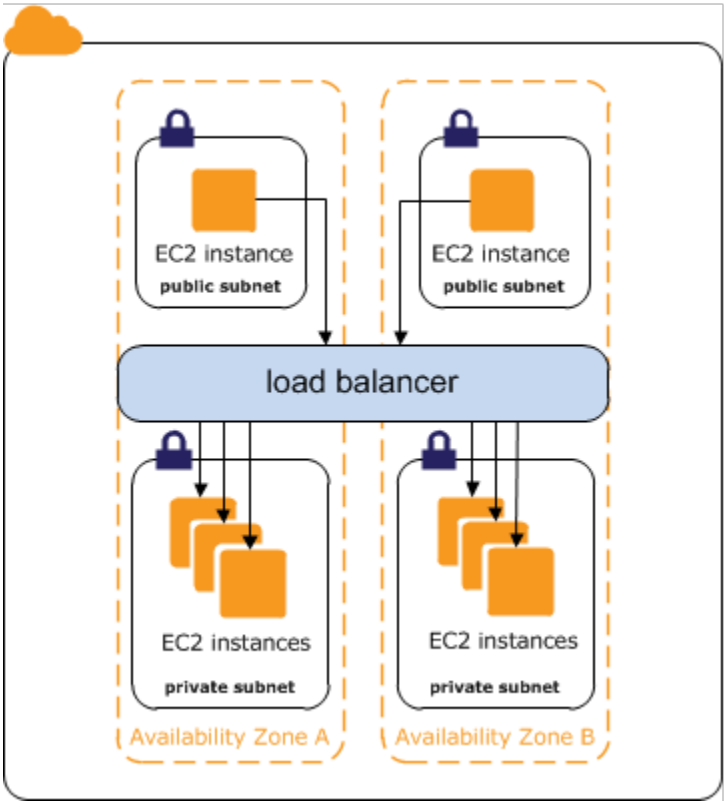
Interne Classic Load Balancer

Wenn Sie einen Load Balancer erstellen, müssen Sie entscheiden, ob es ein interner Load Balancer oder ein mit dem Internet verbundener Load Balancer werden soll.

Die Knoten eines mit dem Internet verbundenen Load Balancers haben öffentliche IP-Adressen. Der DNS-Name eines mit dem Internet verbundenen Load Balancers ist öffentlich zu den öffentlichen IP-Adressen der Knoten auflösbar. Daher können mit dem Internet verbundene Load Balancer Anfragen von Clients über das Internet weiterleiten. Weitere Informationen finden Sie unter Mit dem Internet verbundene Classic Load Balancer.

Die Knoten eines internen Load Balancers haben nur private IP-Adressen. Der DNS-Name eines internen Load Balancers ist öffentlich zu den privaten IP-Adressen der Knoten auflösbar. Daher kann der interne Load Balancer nur Anforderungen von Clients mit Zugriff auf die VPC für den Load Balancer weiterleiten.

Wenn Ihre Anwendung mehrere Stufen hat, z. B. Webserver, die mit dem Internet verbunden sein müssen, und Datenbank-Server, die nur eine Verbindung zum Webserver haben, können Sie eine Architektur einrichten, die sowohl interne als auch mit dem Internet verbundene Load Balancer verwendet. Erstellen Sie einen mit dem Internet verbundenen Load Balancer und registrieren Sie die Webserver bei ihm. Erstellen Sie einen internen Load Balancer und registrieren Sie die Datenbankserver bei ihm. Die Webserver empfangen Anforderungen von dem mit dem Internet verbundenen Load Balancer und senden die Anforderungen für den Datenbankserver an den internen Load Balancer. Die Datenbankserver empfangen Anfragen vom internen Load Balancer.



Inhalt

Öffentlicher DNS-Name für Ihren Load Balancer

Wenn ein interner Load Balancer erstellt wird, erhält er einen öffentlichen DNS-Namen im folgenden Format:

```
internal-name-123456789.region.elb.amazonaws.com
```

Die DNS-Server lösen den DNS-Namen Ihres Load Balancer in die privaten IP-Adressen der Load Balancer-Knoten für Ihren internen Load Balancer auf. Jeder Load Balancer-Knoten ist mithilfe von Elastic Network-Schnittstellen mit den privaten IP-Adressen der Back-End-Instances verbunden. Wenn zonenübergreifendes Load Balancing aktiviert ist, ist jeder Knoten unabhängig von der Availability Zone mit jeder Back-End-Instance verbunden. Andernfalls ist jeder Knoten nur mit den Instances verbunden, die sich in derselben Availability Zone befinden.

Erstellen eines internen Classic Load Balancer

Sie können einen internen Load Balancer erstellen, um Traffic von Clients mit Zugriff auf die VPC für den Load Balancer an Ihre EC2 Instances zu verteilen.

Inhalt

Voraussetzungen

- Wenn Sie noch keine VPC für Ihren Load Balancer erstellt haben, müssen Sie diese erstellen, bevor Sie beginnen. Weitere Informationen finden Sie unter Empfehlungen für Ihre VPC.
- Starten Sie die EC2 Instances, die Sie bei Ihrem internen Load Balancer registrieren möchten. Stellen Sie sicher, dass Sie diese in privaten Subnetzen im VPC für den Load Balancer starten.

Erstellen Sie mithilfe der Konsole einen internen Load Balancer

Gehen Sie wie folgt vor, um einen internen Classic Load Balancer zu erstellen. Geben Sie grundlegende Konfigurationsinformationen für Ihren Load Balancer an, z. B. einen Namen und ein Schema. Geben Sie anschließend Informationen über Ihr Netzwerk und den Listener an, der den Datenverkehr an Ihre Instances weiterleitet.

So erstellen Sie einen internen Classic Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste eine Region für Ihren Load Balancer aus. Achten Sie darauf, dieselbe Region auszuwählen, die Sie für Ihre EC2 Instances ausgewählt haben.
3. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
4. Wählen Sie Load Balancer erstellen aus.
5. Erweitern Sie den Abschnitt Classic Load Balancer und wählen Sie dann Create (Erstellen) aus.
6. Basiskonfiguration

a. Geben Sie im Feld Load balancer name (Name des Load Balancers) einen Namen für Ihren Load Balancer ein.

   Der Name des Classic Load Balancers muss innerhalb Ihrer Gruppe mit Classic Load Balancern für die Region eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen sowie Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.

b. Wählen Sie für Scheme (Schema) die Option Internal (Intern) aus.

7. Netzwerkzuordnung

   a. Wählen Sie im Feld VPC die VPC aus, die Sie für Ihre Instances verwendet haben.

   b. Wählen Sie für Mappings (Zuordnungen) zunächst eine Availability Zone und dann ein Subnetz aus den verfügbaren Subnetzen aus. Sie können nur ein Subnetz pro Availability Zone auswählen. Zur Verbesserung der Verfügbarkeit Ihrer Load Balancer wählen Sie mehr als eine Availability Zone und ein Subnetz aus.

8. Wählen Sie für Security groups (Sicherheitsgruppen) eine vorhandene Sicherheitsgruppe aus, die so konfiguriert ist, dass sie den erforderlichen HTTP-Verkehr auf Port 80 zulässt. Oder Sie können eine neue Sicherheitsgruppe erstellen, wenn Ihre Anwendung unterschiedliche Protokolle und Ports verwendet.

9. Listener und Routing

   a. Stellen Sie für Listener sicher, dass das Protokoll `HTTP` und der Port `80` ist.

   b. Stellen Sie für Instance sicher, dass das Protokoll `HTTP` und der Port `80` ist.

10. Health checks (Zustandsprüfungen)

    a. Für das Ping Protocol(Ping-Protokoll) ist die Standardeinstellung `HTTP`.

    b. Für Ping Port (Ping-Port) ist der Standardwert `80`.

    c. Für Ping Path (Ping-Pfad) ist der Standardwert `/`.

    d. Verwenden Sie für die Advanced health check settings (Erweiterte Einstellungen für die Zustandsprüfung) die Standardwerte oder geben Sie anwendungsspezifische Werte ein.

11. Instances

    a. Wählen Sie Add instances (Instances hinzufügen) aus, um den Bildschirm zur Instance-Auswahl aufzurufen.

b. Unter Available instances (Verfügbare Instances) können Sie basierend auf den zuvor gewählten Netzwerkeinstellungen aus den aktuellen Instances auswählen, die für den Load Balancer verfügbar sind.

c. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Confirm (Bestätigen) aus, um die zu registrierenden Instances zum Load Balancer hinzuzufügen.

12. Attribute

- Behalten Sie für Enable cross-zone load balancing (Zonenübergreifendes Load Balancing aktivieren), Enable connection draining (Connection Draining aktivieren) und Timeout (draining interval) (Timeout (Draining-Intervall)) die Standardwerte bei.

13. Load balancer tags (optional) (Load-Balancer-Tags (optional))

a. Das Feld Key (Schlüssel) ist ein Pflichtfeld.

b. Das Feld Value (Wert) ist optional.

c. Um ein weiteres Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) aus und geben Sie dann Ihre Werte in das Feld Key (Schlüssel) und optional in das Feld Value (Wert) ein.

d. Um ein vorhandenes Tag zu entfernen, wählen Sie neben dem zu entfernenden Tag die Option Remove (Entfernen).

14. Summary and creation (Zusammenfassung und Erstellung)

a. Wenn Sie Einstellungen ändern müssen, wählen Sie neben der Einstellung, die geändert werden muss, Edit (Bearbeiten) aus.

b. Wenn Sie mit allen in der Zusammenfassung angezeigten Einstellungen zufrieden sind, wählen Sie Create load balancer (Load Balancer erstellen) aus, um mit der Erstellung Ihres Load Balancers zu beginnen.

c. Wählen Sie auf der letzten Erstellungsseite Load Balancer anzeigen aus, um Ihren Load Balancer in der EC2 Amazon-Konsole anzuzeigen.

15. Verify

a. Wählen Sie den neuen Load Balancer aus.

b. Überprüfen Sie auf der Registerkarte Target instances (Ziel-Instances) die Spalte Health status (Zustandsstatus). Sobald mindestens eine Ihrer EC2 Instances in Betrieb ist, können Sie Ihren Load Balancer testen.

c. Kopieren Sie im Abschnitt Details den DNS name (DNS-Namen) des Load Balancers, der etwa wie `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com` aussehen würde.

d. Fügen Sie den DNS name (DNS-Namen) Ihres Load Balancers in das Adressfeld eines öffentlichen Webbrowsers mit Internetanschluss ein. Wenn Ihr Load Balancer korrekt funktioniert, sehen Sie die Standardseite Ihres Servers.

16. Delete (optional) (Löschen (optional))

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

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

c. Wählen Sie den Load Balancer aus.

d. Wählen Sie den Load Balancer aus und klicken Sie auf Actions (Aktionen) und dann auf Delete load balancer (Load Balancer löschen).

e. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie `confirm` ein und wählen Sie dann Delete (Löschen) aus.

f. Nachdem Sie einen Load Balancer gelöscht haben, werden die EC2 Instances, die beim Load Balancer registriert wurden, weiter ausgeführt. Ihnen wird jede teilweise oder ganze Stunde in Rechnung gestellt, in der sie weiterlaufen. Wenn Sie eine EC2 Instance nicht mehr benötigen, können Sie sie beenden oder beenden, um zusätzliche Kosten zu vermeiden.

Erstellen Sie einen internen Load Balancer mit dem AWS CLI

Elastic Load Balancing erstellt standardmäßig einen mit dem Internet verbundenen Load Balancer. Gehen Sie wie folgt vor, um einen internen Load Balancer zu erstellen und Ihre EC2 Instances beim neu erstellten internen Load Balancer zu registrieren.

Erstellen eines internen Load Balancer

1. Verwenden Sie den create-load-balancerBefehl, bei dem die `--scheme` Option auf gesetzt ist`internal`, wie folgt:

```
aws elb create-load-balancer --load-balancer-name my-internal-loadbalancer --
listeners Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80
```

```
 --subnets subnet-4e05f721 --scheme internal --security-groups sg-b9ffedd5
```

Nachfolgend finden Sie eine Beispielantwort. Beachten Sie, dass der Name darauf hinweist, dass es sich hierbei um einen internen Load Balancer handelt.

```
{
    "DNSName": "internal-my-internal-loadbalancer-786501203.us-
west-2.elb.amazonaws.com"
}
```

2. Verwenden Sie den folgenden Befehl register-instances-with-load-balancer, um Instanzen hinzuzufügen:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-internal-
loadbalancer --instances i-4f8cf126 i-0bb7ca62
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

3. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um den internen Load Balancer zu überprüfen:

```
aws elb describe-load-balancers --load-balancer-name my-internal-loadbalancer
```

Die Antwort enthält die Felder `DNSName` und `Scheme`, die angeben, dass es sich hierbei um einen internen Load Balancer handelt.

```
{
    "LoadBalancerDescriptions": [
        {
```

```
            ...
            "DNSName": "internal-my-internal-loadbalancer-1234567890.us-
west-2.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-b9ffedd5"
            ],
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": []
            },
            "LoadBalancerName": "my-internal-loadbalancer",
            "CreatedTime": "2014-05-22T20:32:19.920Z",
            "AvailabilityZones": [
                "us-west-2a"
            ],
            "Scheme": "internal",
            ...
        }
    ]
}
```

Konfigurieren Ihres Classic Load Balancers

Nachdem Sie einen Classic Load Balancer erstellt haben, können Sie dessen Konfiguration ändern. Sie können beispielsweise die Attribute, Subnetze und Sicherheitsgruppen des Load Balancers aktualisieren.

Load Balancer-Attribute

Verbindung wird schwächer

Wenn diese Option aktiviert ist, ermöglicht der Load Balancer das Abschließen vorhandener Anforderungen, bevor der Load Balancer den Datenverkehr weg von einer abgemeldeten oder fehlerhaften Instance leitet.

Zonenübergreifendes Load Balancing

Wenn diese Option aktiviert ist, leitet der Load Balancer den Anforderungsdatenverkehr gleichmäßig auf alle Instances unabhängig von den Availability Zones um.

Desync-Migrationsmodus

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

Timeout im Leerlauf

Wenn diese Option aktiviert ist, lässt der Load Balancer zu, dass die Verbindungen für die angegebene Dauer im Leerlauf ausgeführt werden können (keine Daten werden über diese Verbindung gesendet). Standardmäßig ist ein Zeitraum von 60 Sekunden festgelegt.

Sticky Sessions

Classic Load Balancer unterstützen sowohl die Dauer als auch die Anwendungsabhängigkeit von Sitzungen.

Einzelheiten zum Load Balancer

Sicherheitsgruppen

Die Sicherheitsgruppen für Ihren Load Balancer müssen Datenverkehr auf den Listener- und Integritätsprüf-Ports zulassen.

Subnets

Sie können die Fähigkeiten Ihres Load Balancers auf zusätzliche Subnetze erweitern.

Proxy-Protokoll

Wenn diese Option aktiviert ist, fügen wir einen Header mit Verbindungsinformationen hinzu, die an die Instance gesendet werden.

Tags

Sie können Tags hinzufügen, um Ihre Load Balances zu kategorisieren.

Konfigurieren des Leerlaufverbindungszeitlimits für Ihren Classic Load Balancer

Für jede Anforderung, die ein Client über einen Classic Load Balancer sendet, hält der Load Balancer zwei Verbindungen aufrecht. Es besteht eine Front-End-Verbindung zwischen dem Client und dem Load Balancer. Die Back-End-Verbindung besteht zwischen dem Load Balancer und einer registrierten Instance. EC2 Der Load Balancer verfügt über ein konfiguriertes Leerlauf-Timeout, das für seine Verbindungen gilt. Wenn bis zum Ablauf des Leerlaufzeitlimits keine Daten versandt oder empfangen wurden, schließt der Load Balancer die Verbindung. Um sicherzustellen, dass langwierige Vorgänge wie z. B. Datei-Uploads genügend Zeit haben, senden Sie mindestens 1 Datenbyte vor Ablauf jeder Leerlaufzeitüberschreitung und erhöhen Sie die Länge des Timeoutlimits bei Bedarf.

Wenn Sie HTTP- und HTTPS-Listener verwenden, sollten Sie die HTTP-Keepalive-Option für Ihre Instances aktivieren. Sie können Keepalive in den Webserver-Einstellungen für Ihre Instances aktivieren. Wenn Keep-Alive aktiviert ist, kann der Load Balancer Back-End-Verbindungen erneut verwenden, bis das Keep-Alive-Timeout abläuft. Stellen Sie die HTTP-Keep-Alive-Zeit höher als das für den Load Balancer konfigurierte Leerlaufzeitlimit ein, um sicherzustellen, dass der Load Balancer für das Schließen von Verbindungen mit Ihrer Instance zuständig ist.

Beachten Sie, dass TCP-Keepalive-Prüfpunkte das Schließen von Verbindungen durch den Load Balancer nicht verhindern, da sie keine Nutzlastdaten senden.

Inhalt

Konfigurieren des Leerlaufzeitlimits mithilfe der Konsole

Elastic Load Balancing setzt das Leerlaufzeitlimit für Ihren Load Balancer standardmäßig auf 60 Sekunden. Gehen Sie folgendermaßen vor, um einen anderen Wert für das Leerlaufzeitlimit festzulegen.

Um die Einstellung für das Leerlauf-Timeout für Ihren Load Balancer mithilfe der Konsole zu konfigurieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Geben Sie auf der Seite Edit load balancer attributes (Attribute des Load Balancer bearbeiten) im Abschnitt Traffic configuration (Konfiguration des Datenverkehrs) einen Wert für Idle Timeout (Timeout-Leerlauf) ein. Der Bereich für das Leerlaufzeitlimit ist 1 bis 4,000 Sekunden.
6. Wählen Sie Änderungen speichern aus.

Konfigurieren des Leerlaufzeitlimits mit der AWS CLI

Verwenden Sie den folgenden modify-load-balancer-attributesBefehl, um das Leerlauf-Timeout für Ihren Load Balancer festzulegen:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionSettings\":{\"IdleTimeout\":30}}"
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "LoadBalancerAttributes": {
        "ConnectionSettings": {
            "IdleTimeout": 30
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Konfigurieren des zonenübergreifenden Load Balancing für Ihren Classic Load Balancer

Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Load Balancer-Knoten für Ihren Classic Load Balancer Anfragen gleichmäßig auf die registrierten Instances in allen aktivierten Availability Zones. Wenn zonenübergreifendes Load Balancing deaktiviert ist, verteilt jeder Load Balancer-Knoten Anfragen gleichmäßig nur auf die registrierten Instances in seiner aktivierten Availability Zone. Weitere Informationen finden Sie unter Zonenübergreifender Load Balancing im Benutzerhandbuch für Elastic Load Balancing.

Beim zonenübergreifenden Load Balancing muss nicht mehr die gleiche Anzahl von Instances in jeder aktivierten Availability Zone vorhanden sein, und die Anwendung kann den Verlust von einer oder mehreren Instances besser bewältigen. Für eine bessere Fehlertoleranz sollte allerdings dennoch etwa die gleiche Anzahl von Instances in jeder aktivierten Availability Zone vorhanden sein.

In Umgebungen, in denen Clients DNS-Suchvorgänge zwischenspeichern, können eingehende Anforderungen eine der Availability Zones bevorzugen. Wenn Sie zonenübergreifendes Load Balancing verwenden, wird dieses Ungleichgewicht der Anforderungslast auf alle verfügbaren Instances in der Region verteilt, sodass die Auswirkungen durch fehlerhafte Clients reduziert werden.

Wenn Sie einen Classic Load Balancer erstellen, hängt die Voreinstellung für zonenübergreifendes Load Balancing davon ab, wie Sie den Load Balancer erstellen. Mit der API oder CLI wird das zonenübergreifende Load Balancing standardmäßig deaktiviert. Bei der ist die AWS Management Console Option zur Aktivierung des zonenübergreifenden Lastenausgleichs standardmäßig ausgewählt. Nachdem Sie einen Classic Load Balancer erstellt haben, können Sie zonenübergreifendes Load Balancing jederzeit aktivieren oder deaktivieren.

Inhalt

Aktivieren von zonenübergreifendem Load Balancing

Sie können das zonenübergreifende Load Balancing jederzeit für Ihren Classic Load Balancer aktivieren.

Aktivieren des zonenübergreifenden Load Balancing mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Aktivieren Sie auf der Seite Edit load balancer attributes (Load-Balancer-Attribute bearbeiten) im Abschnitt Availability Zone Routing configuration (Routing-Konfiguration der Availability Zone) die Option Cross-zone load balancing (Zonenübergreifendes Load Balancing).
6. Wählen Sie Änderungen speichern aus.

Um den zonenübergreifenden Load Balancing zu aktivieren, verwenden Sie AWS CLI

1. Verwenden Sie den folgenden modify-load-balancer-attributesBefehl, um das `CrossZoneLoadBalancing` Attribut Ihres Load Balancers auf festzulegen: `true`

   ```
   aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --
   load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":true}}"
   ```

   Nachfolgend finden Sie eine Beispielantwort:

   ```
   {
      "LoadBalancerAttributes": {
        "CrossZoneLoadBalancing": {
            "Enabled": true
          }
      },
      "LoadBalancerName": "my-loadbalancer"
    }
   ```

2. (Optional) Verwenden Sie den folgenden describe-load-balancer-attributesBefehl, um zu überprüfen, ob der zonenübergreifende Load Balancing für Ihren Load Balancer aktiviert ist:

   ```
   aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
   ```

   Nachfolgend finden Sie eine Beispielantwort:

   ```
   {
   ```

```
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
}
```

Deaktivieren des zonenübergreifenden Load Balancing

Sie können die Option zonenübergreifendes Load Balancing jederzeit für Ihren Load Balancer deaktivieren.

Deaktivieren des zonenübergreifenden Load Balancing mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Deaktivieren Sie auf der Seite Edit load balancer attributes (Load-Balancer-Attribute bearbeiten) im Abschnitt Availability Zone Routing configuration (Routing-Konfiguration der Availability Zone) die Option Cross-zone load balancing (Zonenübergreifendes Load Balancing).
6. Wählen Sie Änderungen speichern aus.

Um das zonenübergreifende Load Balancing zu deaktivieren, setzen Sie das Attribut `CrossZoneLoadBalancing` Ihres Load Balancer auf `false`.

Um den zonenübergreifenden Load Balancing zu deaktivieren, verwenden Sie AWS CLI

1. Verwenden Sie den folgenden modify-load-balancer-attributes-Befehl:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":false}}"
```

   Nachfolgend finden Sie eine Beispielantwort:

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": false
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Optional) Verwenden Sie den folgenden describe-load-balancer-attributesBefehl, um zu überprüfen, ob der zonenübergreifende Lastenausgleich für Ihren Load Balancer deaktiviert ist:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

   Nachfolgend finden Sie eine Beispielantwort:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": false
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
```

```
}
```

Konfigurieren des Connection Draining für Ihren Classic Load Balancer

Verwenden Sie den Connection Draining, um sicherzustellen, dass der Classic Load Balancer aufhört, Anforderungen an Instances zu senden, deren Registrierung aufgehoben werden soll oder die fehlerhafte sind, und vorhandene Verbindungen bestehen bleiben. Auf diese Weise kann der Load Balancer aktive Anforderungen an Instances mit aufgehobener Registrierung oder fehlerhafte Instances abschließen.

Wenn Sie den Connection Draining aktivieren, können Sie eine maximale Zeitspanne angeben, während der der Load Balancer die Verbindungen aufrecht erhält, bevor er die Registrierung der Instance als aufgehoben meldet. Die maximale Timeout-Wert kann zwischen 1 und 3.600 Sekunden liegen (der Standardwert beträgt 300 Sekunden). Wenn das maximale Zeitlimit überschritten wird, schließt der Load Balancer die Verbindungen zu der Instance, deren Registrierung aufgehoben werden soll.

Wenn eine Instance, deren Registrierung aufgehoben wird, keine laufenden Anfragen und keine aktiven Verbindungen hat, schließt Elastic Load Balancing den Abmeldevorgang sofort ab.

Während aktive Anforderungen bearbeitet werden, gibt der Load Balancer den Status einer Instance, deren Registrierung aufgehoben werden soll, als `InService: Instance deregistration currently in progress` aus. Wenn die Instance, deren Registrierung aufgehoben werden soll, alle aktiven Anforderungen bearbeitet hat oder das maximale Zeitlimit erreicht wurde, gibt der Load Balancer den Status der Instance als `OutOfService: Instance is not currently registered with the LoadBalancer` aus.

Wenn eine Instance fehlerhaft wird, gibt der Load Balancer den Status der Instance als `OutOfService` aus. Wenn laufende Anforderungen an die fehlerhafte Instance vorliegen, werden diese abgeschlossen. Das maximale Zeitlimit gilt nicht für Verbindungen zu fehlerhaften Instances.

Wenn Ihre Instances zu einer Auto-Scaling-Gruppe gehören und der Connection Draining für Ihren Load Balancer aktiviert ist, wartet Auto Scaling, bis die laufenden Anforderungen abgeschlossen werden oder das maximale Zeitlimit abgelaufen ist, bevor die Instances aufgrund eines Skalierungsereignisses oder einer Ersatzzustandsprüfung beendet werden.

Sie können den Connection Draining deaktivieren, wenn Sie möchten, dass Ihr Load Balancer sofort Verbindungen zu den Instances schließt, deren Registrierung aufgehoben werden soll oder die fehlerhaft geworden sind. Wenn der Connection Draining deaktiviert ist, werden alle laufenden Anforderungen an die Instances, deren Registrierung aufgehoben werden soll oder die fehlerhaft sind, nicht abgeschlossen.

Inhalt

Aktivieren von Connection Draining

Sie können den Connection Draining für Ihren Load Balancer jederzeit aktivieren.

Aktivieren von Connection Draining mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Wählen Sie auf der Seite Edit load balancer attributes (Load-Balancer-Attribute bearbeiten) im Abschnitt Traffic configuration (Konfiguration des Datenverkehrs) die Option Enable connection draining (Connection Draining aktivieren) aus.
6. (Optional) Geben Sie für Timeout (draining interval) (Timeout (Draining-Intervall)) einen Wert zwischen 1 und 3 600 Sekunden ein. Andernfalls wird der Standardwert von 300 Sekunden verwendet.
7. Wählen Sie Änderungen speichern aus.

Um den Verbindungsabbau mit dem zu aktivieren AWS CLI

Verwenden Sie den folgenden modify-load-balancer-attributes-Befehl:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":true,\"Timeout\":300}}"
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": true,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Deaktivieren von Connection Draining

Sie können den Connection Draining für Ihren Load Balancer jederzeit deaktivieren.

Deaktivieren von Connection Draining mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Deaktivieren Sie auf der Seite Edit load balancer attributes (Load-Balancer-Attribute bearbeiten) im Abschnitt Traffic configuration (Konfiguration des Datenverkehrs) die Option Enable connection draining (Connection Draining aktivieren).
6. Wählen Sie Änderungen speichern aus.

Um den Verbindungsabbau zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den folgenden modify-load-balancer-attributes-Befehl:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":false}}"
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
```

```
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Konfigurieren von Sticky Sessions für Ihren Classic Load Balancer

Standardmäßig leitet ein Classic Load Balancer jede Anforderung getrennt an die registrierte Instance mit der kleinsten Last weiter. Sie können jedoch das Feature Sticky Session (auch als gebundene Sitzungen bezeichnet) verwenden, damit der Load Balancer die Sitzung eines Benutzers an eine bestimmte Instance binden kann. So wird sichergestellt, dass alle Anforderungen, die während der Sitzung vom Benutzer gesendet werden, an dieselbe Instance weitergeleitet werden.

Bei der Verwaltung von Sticky Sessions ist es besonders wichtig festzulegen, wie lange der Load Balancer die Anforderung des Benutzers an die gleiche Instance leiten soll. Wenn Ihre Anwendung über ein eigenes Sitzungscookie verfügt, können Sie den Elastic Load Balancing so konfigurieren, dass das Sitzungscookie die durch das Sitzungscookie der Anwendung festgelegte Dauer einhält. Wenn Ihre Anwendung nicht über ein eigenes Sitzungscookie verfügt, können Sie den Elastic Load Balancing so konfigurieren, dass Sie selbst ein Sitzungscookie erstellen, indem Sie eine Dauer für die Sticky Sessions angeben.

Elastic Load Balancing erstellt ein Cookie mit dem Namen AWSELB, das verwendet wird, um die Sitzung der Instanz zuzuordnen.

Voraussetzungen

- Ein HTTP/HTTPS-Load Balancer.
- Mindestens eine funktionierende Instance in jeder Availability Zone.

Kompatibilität

- Beim RFC für die Pfadeigenschaften eines Cookies sind Unterstriche erlaubt. Die Elastic-Load-Balancing-URI kodiert Unterstriche jedoch als `%5F`, da für einige Browser, wie zum Beispiel Internet Explorer 7, URI-kodierte Unterstriche wie `%5F` erforderlich sind. Da derzeit betriebsfähige Browser anderenfalls beeinträchtigt werden können, setzt der Elastic Load Balancing die URI-Kodierung von Unterstrichen fort. Besitzt ein Cookie beispielsweise die Eigenschaft `path=/my_path`, ändert der Elastic Load Balancing diese Eigenschaft in der weitergeleiteten Anforderungen zu `path=/my%5Fpath`.

- Sie können das `secure`-Flag oder `HttpOnly`-Flag nicht für Cookies für Sticky Sessions auf Basis der Dauer festlegen. Diese Cookies enthalten jedoch keine sensiblen Daten. Beachten Sie, dass, wenn Sie das `secure` Flag oder das `HttpOnly` Flag für ein anwendungsgesteuertes Session-Stickiness-Cookie setzen, es auch für das Cookie gesetzt wird. AWSELB
- Wenn sich im Bereich `Set-Cookie` eines Anwendungs-Cookies ein abschließendes Semikolon befindet, ignoriert der Load Balancer das Cookie.

Inhalt

Sticky Sessions auf Basis der Dauer

Der Load Balancer verwendet ein spezielles Cookie, AWSELB, um die Instanz für jede Anfrage an jeden Listener zu verfolgen. Wenn der Load Balancer eine Anforderung empfängt, prüft er zunächst, ob dieses Cookie in der Anforderung vorhanden ist. Wenn ja, wird die Anforderung an die im Cookie angegebene Instance gesendet. Wenn kein Cookie vorhanden ist, wählt der Load Balancer eine Instance basierend auf dem vorhandenen Load Balancing-Algorithmus aus. Ein Cookie wird in die Antwort eingefügt, um nachfolgende Anforderungen von demselben Benutzer an diese Instance zu binden. Mit der Konfiguration der Richtlinie für Sticky Sessions wird ein Cookie-Ablauf definiert, der die Dauer der Gültigkeit für jedes Cookie festlegt. Der Load Balancer aktualisiert die Ablaufzeit des Cookies nicht und überprüft nicht, ob das Cookie abgelaufen ist, bevor er es verwendet. Nachdem ein Cookie abgelaufen ist, ist die Sitzung nicht mehr gebunden. Der Client muss das Cookie nach Ablauf aus seinem Cookiespeicher entfernen.

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

Wenn eine Instance ausfällt oder fehlerhaft ist, leitet der Load Balancer keine Anforderungen mehr an diese Instance weiter und wählt basierend auf dem bestehenden Load Balancing-Algorithmus eine neue funktionierende Instance. Die Anforderung wird an die neue Instance geleitet, als ob kein Cookie vorhanden wäre, und die Sitzung ist nicht gebunden.

Wenn ein Client zu einem Listener mit einem anderen Backend-Port wechselt, ist die Sitzung nicht mehr gebunden.

Aktivieren von Sticky Sessions auf Basis der Dauer für einen Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listeners (Listener) die Option Manage listeners (Listener verwalten) aus.
5. Suchen Sie auf der Seite Manage listeners (Listener verwalten) den Listener, der aktualisiert werden soll und wählen Sie unter Cookie stickiness (Cookie-Stickiness) die Option Edit (Bearbeiten) aus.
6. Wählen Sie im Popup-Fenster „Cookie-Stickiness-Einstellung bearbeiten“ die Option Generiert vom Load Balancer aus.
7. (Optional) Geben Sie für Expiration Period (Verfallsdatum) den Ablaufzeitraum für Cookies, in Sekunden, ein. Wenn Sie keinen Ablaufzeitraum angeben, dauert die Sticky Session solange wie die Browsersitzung.
8. Wählen Sie Änderungen speichern, um das Popup-Fenster zu schließen.
9. Wählen Sie Änderungen speichern, um zur Seite mit den Load Balancer-Details zurückzukehren.

Aktivieren von Sticky Sessions auf Basis der Dauer für einen Load Balancer mit der AWS CLI

1. Verwenden Sie den folgenden Befehl create-lb-cookie-stickiness-policy, um eine vom Load Balancer generierte Cookie-Stickiness-Richtlinie mit einer Cookie-Ablaufzeit von 60 Sekunden zu erstellen:

```
aws elb create-lb-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-duration-cookie-policy --cookie-expiration-period 60
```

2. Verwenden Sie den folgenden Befehl set-load-balancer-policies-of-listener, um Session Stickiness für den angegebenen Load Balancer zu aktivieren:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-duration-cookie-policy
```

> **Note**
>
> Der Befehl `set-load-balancer-policies-of-listener` ersetzt die Richtlinien, die aktuell dem angegebenen Load Balancer-Port zugeordnet sind. Geben Sie jedes Mal, wenn Sie diesen Befehl verwenden, die Option `--policy-names` an, um alle Richtlinien für die Aktivierung aufzulisten.

3. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die Richtlinie aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Die Antwort umfasst die folgenden Informationen, was bedeutet, dass die Richtlinie für den Listener auf dem angegebenen Port aktiviert ist:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-duration-cookie-policy",
                        "ELBSecurityPolicy-TLS-1-2-2017-01"
                    ]
                },
                ...
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [
                 {
```

```
                        "PolicyName": "my-duration-cookie-policy",
                        "CookieExpirationPeriod": 60
                    }

                ],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": [
                    "ELBSecurityPolicy-TLS-1-2-2017-01"
                ]
            },
            ...
        }
    ]
}
```

Anwendungsgesteuerte Sticky Sessions

Der Load Balancer verwendet ein spezielles Cookie, um die Sitzung mit der Instance zu verknüpfen, die die ursprüngliche Anforderung verarbeitet hat, folgt jedoch der Lebensdauer des in der Richtlinienkonfiguration angegebenen Anwendungs-Cookies. Der Load Balancer fügt nur eine neues Cookie für Sticky Sessions ein, wenn die Anwendungsantwort ein neues Anwendungs-Cookie enthält. Das Load Balancer-Cookie für Sticky Sessions wird nicht mit jeder Anforderung aktualisiert. Wenn das Anwendungs-Cookie explizit entfernt wird oder abläuft, ist die Sitzung nicht mehr gebunden, bis ein neues Anwendungs-Cookie ausgegeben wird.

Die folgenden Attribute, die von Back-End-Instances festgelegt werden, werden an Clients im Cookie gesendet:`path`, `port`, `domain`, `secure`, `httponly`, `discard`, `max-age`, `expires`, `version`, `comment`, `commenturl` und `samesite`.

Wenn eine Instance ausfällt oder fehlerhaft ist, leitet der Load Balancer keine Anforderungen mehr an diese Instance weiter und wählt basierend auf dem bestehenden Load Balancing-Algorithmus eine neue funktionierende Instance. Der Load Balancer behandelt die Sitzung jetzt als der neuen funktionierenden Instance „angeheftet“ und leitet Anforderungen auch dann an diese Instance, wenn die ausgefallene Instance wieder funktionsfähig ist.

Aktivieren anwendungsgesteuerter Sticky Sessions mithilfe der Konsole

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

3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listeners (Listener) die Option Manage listeners (Listener verwalten) aus.
5. Suchen Sie auf der Seite Manage listeners (Listener verwalten) den Listener, der aktualisiert werden soll und wählen Sie unter Cookie stickiness (Cookie-Stickiness) die Option Edit (Bearbeiten) aus.
6. Wählen Sie Generated by application (Von der Anwendung generiert) aus.
7. Geben Sie unter Cookie Name den Namen Ihres Anwendungscookies ein.
8. Wählen Sie Änderungen speichern aus.

Um die anwendungsgesteuerte Sitzungsabhängigkeit zu aktivieren, verwenden Sie AWS CLI

1. Verwenden Sie den folgenden Befehl create-app-cookie-stickiness-policy, um eine von der Anwendung generierte Cookie-Stickiness-Richtlinie zu erstellen:

```
aws elb create-app-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-app-cookie-policy --cookie-name my-app-cookie
```

2. Verwenden Sie den folgenden Befehl set-load-balancer-policies-of-listener, um Session Stickiness für einen Load Balancer zu aktivieren:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-app-cookie-policy
```

> **Note**
>
> Der Befehl `set-load-balancer-policies-of-listener` ersetzt die Richtlinien, die aktuell dem angegebenen Load Balancer-Port zugeordnet sind. Geben Sie jedes Mal, wenn Sie diesen Befehl verwenden, die Option `--policy-names` an, um alle Richtlinien für die Aktivierung aufzulisten.

3. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die Sticky-Policy aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

4. Die Antwort umfasst die folgenden Informationen, was bedeutet, dass die Richtlinie für den Listener auf dem angegebenen Port aktiviert ist:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-app-cookie-policy",
                        "ELBSecurityPolicy-TLS-1-2-2017-01"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "TCP",
                        "InstanceProtocol": "TCP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [
                {
                        "PolicyName": "my-app-cookie-policy",
                        "CookieName": "my-app-cookie"
                    }

                ],
                "OtherPolicies": [
```

```
                    "ELBSecurityPolicy-TLS-1-2-2017-01"
                ]
            },
            ...
        }
    ]
}
```

Konfigurieren Sie den Desync-Mitigationsmodus für Ihren Classic Load Balancer

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

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

Inhalt

> **Tip**
>
> Diese Konfiguration gilt nur für Classic Load Balancer. Informationen zu Application Load Balancer finden Sie unter Desync-Minderungsmodus für Application Load Balancers.

Klassifizierungen

Diese Klassifizierungen lauten wie folgt:

- Konform – Die Anforderung entspricht RFC 7230 und stellt keine bekannten Sicherheitsbedrohungen dar.
- Akzeptabel – Die Anforderung entspricht nicht RFC 7230, stellt jedoch keine bekannten Sicherheitsbedrohungen dar.
- Mehrdeutig – Die Anforderung entspricht nicht RFC 7230, stellt jedoch ein Risiko dar, da verschiedene Webserver und Proxys sie unterschiedlich behandeln könnten.
- Schwerwiegend – Die Anforderung stellt ein hohes Sicherheitsrisiko dar. Der Load Balancer blockiert die Anforderung, sendet dem Client eine 400-Antwort und schließt die Client-Verbindung.

In den folgenden Listen werden die Probleme für jede Klassifizierung beschrieben.

Akzeptabel

- Ein Header enthält ein Nicht-ASCII- oder Steuerzeichen.
- Die Anforderungsversion enthält einen ungültigen Wert.
- Es gibt einen Content-Length-Header mit dem Wert 0 für eine GET- oder HEAD-Anfrage.
- Die Anforderungs-URI enthält ein Leerzeichen, das nicht URL-codiert ist.

Mehrdeutig

- Die Anforderungs-URI enthält Steuerzeichen.
- Die Anfrage enthält sowohl einen Transfer-Encoding-Header als auch einen Content-Length-Header.
- Es gibt mehrere Content-Length-Header mit demselben Wert.
- Eine Kopfzeile ist leer oder es gibt eine Zeile mit nur Leerzeichen.
- Es gibt einen Header, der mithilfe gängiger Textnormalisierungstechniken auf Transfer-Encoding oder Content-Length normalisiert werden kann.
- Es gibt einen Content-Length-Header für eine GET- oder HEAD-Anfrage.
- Es gibt einen Transfer-Encoding-Header für eine GET- oder HEAD-Anfrage.

Schwerwiegend

- Die Anforderungs-URI enthält ein Nullzeichen oder ein Zeilenumkehrzeichen.
- Der Content-Length-Header enthält einen Wert, der nicht analysiert werden kann oder der keine gültige Zahl ist.
- Ein Header enthält ein Nullzeichen oder ein Zeilenumkehrzeichen.
- Der Transfer-Encoding-Header enthält einen ungültigen Wert.
- Die Anforderungsmethode ist schlecht geformt.
- Die Anforderungsversion ist schlecht geformt.
- Es gibt mehrere Content-Length-Header mit verschiedenen Werten.
- Es gibt mehrere Transfer-Encoding: chunked Header.

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

Modi

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

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

[1] Leitet die Anfragen weiter, schließt aber die Client- und Zielverbindungen.

Desynchronen Mitigationsmodus ändern

So aktualisieren Sie den Desync-Mitigation-Modus über die Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Wählen Sie auf der Seite Edit load balancer attributes (Load-Balancer-Attribute bearbeiten) unter Traffic configuration (Konfiguration des Datenverkehrs) die Optionen Defensive - recommended (Defensiv – empfohlen), Strictest (Strikteste) oder Monitor (Überwachen) aus.
6. Wählen Sie Änderungen speichern aus.

Um den Desync-Minimationsmodus zu aktualisieren, verwenden Sie AWS CLI

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

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer --load-
balancer-attributes file://attribute.json
```

Im Folgenden sehen Sie den Inhalt von `attribute.json`.

```
{
    "AdditionalAttributes": [
        {
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }
    ]
}
```

Konfigurieren Sie das Proxyprotokoll für Ihren Classic Load Balancer

Proxy-Protokoll ist ein Internetprotokoll, das verwendet wird, um Verbindungsinformationen von der Quelle, die die Verbindung anfragt, zum Ziel, für das die Verbindung angefragt wurde, überträgt. Elastic Load Balancing verwendet die Proxy-Protokoll-Version 1 in einem visuell lesbaren Header-Format.

Wenn Sie Transmission Control Protocol (TCP) für Frontend- und Backend-Verbindungen verwenden, überträgt Ihr Classic Load Balancer standardmäßig Anforderungen an die Instances, ohne die Anforderungs-Header zu ändern. Wenn Sie Proxy-Protokoll aktivieren, wird ein visuell lesbarer Header mit Verbindungsinformationen, wie z. B. Quell-IP-Adresse, Ziel-IP-Adresse und Portnummern, zum Anforderungs-Header hinzugefügt. Der Header wird dann als Teil der Anforderung zu der Instance gesandt.

> **Note**
>
> Das AWS Management Console unterstützt die Aktivierung des Proxyprotokolls nicht.

Inhalt

Proxy-Protokoll-Header

Anhand des Proxy-Protokoll-Headers können Sie die IP-Adresse eines Clients identifizieren, wenn Sie über einen Load Balancer verfügen, der für Backend-Verbindungen TCP verwendet. Da Load Balancers Datenverkehr zwischen Clients und Ihren Backend-Instances abfangen, enthalten die Zugriffsprotokolle von Ihrer Backend-Instance die IP-Adresse des Load Balancer statt des ursprünglichen Clients. Sie können die erste Zeile der Anforderung parsen, um die IP-Adresse Ihres Clients und die Portnummer abzurufen.

Die Adresse des Proxys im Header für IPv6 ist die öffentliche IPv6 Adresse Ihres Load Balancers. Diese IPv6 Adresse entspricht der IP-Adresse, die aus dem DNS-Namen Ihres Load Balancers aufgelöst wird, der entweder mit oder `ipv6` beginnt. `dualstack` Wenn der Client eine Verbindung herstellt IPv4, ist die Adresse des Proxys im Header die private IPv4 Adresse des Load Balancers, die nicht durch eine DNS-Suche aufgelöst werden kann.

Die Proxy-Protokoll-Zeile ist eine einzelne Zeile, die mit einem Wagenrücklauf und Zeilenvorschub endet (`"\r\n"`) und in der folgenden Form vorliegt:

```
PROXY_STRING + single space + INET_PROTOCOL + single space + CLIENT_IP + single space +
 PROXY_IP + single space + CLIENT_PORT + single space + PROXY_PORT + "\r\n"
```

Beispiel: IPv4

Im Folgenden finden Sie ein Beispiel für die Proxy-Protokollzeile für. IPv4

```
PROXY TCP4 198.51.100.22 203.0.113.7 35646 80\r\n
```

Voraussetzungen für die Aktivierung des Proxy-Protokolls

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Vergewissern Sie sich, dass Ihr Load Balancer sich nicht hinter einem Proxy-Server mit aktiviertem Proxy-Protokoll befindet. Wenn Proxy-Protokoll sowohl für den Proxy-Server als auch den Load Balancer aktiviert ist, fügt der Load Balancer einen weiteren Header zu der Anforderung hinzu, die bereits über einen Header vom Proxy-Server verfügt. Abhängig von der Konfiguration Ihrer Instance kann diese Duplikation zu Fehlern führen.
- Vergewissern Sie sich, dass Ihre Instances die Proxy-Protokoll-Informationen verarbeiten können.
- Vergewissern Sie sich, dass Ihre Listener-Einstellungen Proxy-Protokoll unterstützen. Weitere Informationen finden Sie unter Listener-Konfigurationen für Classic Load Balancer.

Aktivieren von Proxy-Protokoll mit der AWS CLI

Sie müssen eine Richtlinie des Typs `ProxyProtocolPolicyType` erstellen und diese Richtlinie dann auf dem Instance-Port aktivieren, um Proxy-Protokoll zu aktivieren.

Nutzen Sie die folgende Vorgehensweise, um eine neue Richtlinie für Ihren Load Balancer des Typs `ProxyProtocolPolicyType` zu erstellen. Legen Sie die neu erstellte Richtlinie für die Instance von Port `80` fest und stellen Sie sicher, dass die Richtlinie aktiviert ist.

Aktivieren von Proxy-Protokoll für Ihren Load Balancer

1. (Optional) Verwenden Sie den folgenden Befehl describe-load-balancer-policy-types, um die von Elastic Load Balancing unterstützten Richtlinien aufzulisten:

```
aws elb describe-load-balancer-policy-types
```

   Die Antwort enthält die Namen und Beschreibungen der unterstützten Richtlinientypen. Das folgende Beispiel zeigt die Ausgabe für den `ProxyProtocolPolicyType`-Typ:

```
{
    "PolicyTypeDescriptions": [
        ...
        {
            "PolicyAttributeTypeDescriptions": [
                {
                    "Cardinality": "ONE",
                    "AttributeName": "ProxyProtocol",
                    "AttributeType": "Boolean"
                }
            ],
            "PolicyTypeName": "ProxyProtocolPolicyType",
            "Description": "Policy that controls whether to include the IP address
 and port of the originating
request for TCP messages. This policy operates on TCP/SSL listeners only"
        },
        ...
    ]
}
```

2. Verwenden Sie den folgenden create-load-balancer-policyBefehl, um eine Richtlinie zu erstellen, die das Proxy-Protokoll aktiviert:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-ProxyProtocol-policy --policy-type-name ProxyProtocolPolicyType --policy-
attributes AttributeName=ProxyProtocol,AttributeValue=true
```

3. Verwenden Sie den folgenden for-backend-server Befehl set-load-balancer-policies-, um die neu erstellte Richtlinie für den angegebenen Port zu aktivieren. Beachten Sie, dass dieser Befehl die aktuell aktivierten Richtlinien ersetzt. Daher müssen in der Option `--policy-names` sowohl die Richtlinie, die Sie zur Liste hinzufügen (zum Beispiel `my-ProxyProtocol-policy`) als auch alle Richtlinien, die aktuell aktiviert sind (zum Beispiel `my-existing-policy`) angegeben werden.

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-ProxyProtocol-policy my-existing-policy
```

4. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob das Proxyprotokoll aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Die Antwort enthält die folgenden Informationen, was bedeutet, dass die Richtlinie `my-ProxyProtocol-policy` Port `80` zugeordnet ist.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "BackendServerDescriptions": [
                {
                    "InstancePort": 80,
                    "PolicyNames": [
                        "my-ProxyProtocol-policy"
                    ]
                }
            ],
            ...
        }
    ]
}
```

Deaktivieren von Proxy-Protokoll mit der AWS CLI

Sie können die mit Ihrer Instance verknüpften Richtlinien deaktivieren und zu einem späteren Zeitpunkt wieder aktivieren.

Deaktivieren der Proxy-Protokoll-Richtlinie

1. Verwenden Sie den folgenden for-backend-server Befehl set-load-balancer-policies-, um die Proxyprotokollrichtlinie zu deaktivieren, indem Sie sie aus der `--policy-names` Option weglassen, aber die anderen Richtlinien einbeziehen, die aktiviert bleiben sollen (z. B.). `my-existing-policy`

   ```
   aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-existing-policy
   ```

   Wenn keine anderen Richtlinien zum Aktivieren vorhanden sind, geben Sie mit der Option `--policy-names` eine leere Zeichenfolge an:

   ```
   aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names "[]"
   ```

2. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die Richtlinie deaktiviert ist:

   ```
   aws elb describe-load-balancers --load-balancer-name my-loadbalancer
   ```

   Die Antwort enthält die folgenden Informationen, was bedeutet, dass keine Ports mit der Richtlinie verknüpft sind.

   ```
   {
       "LoadBalancerDescriptions": [
           {
               ...
               "BackendServerDescriptions": [],
               ...
           }
       ]
   }
   ```

Kennzeichnen Ihres Classic 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 Classic Load Balancer hinzufügen. Tag-Schlüssel müssen für jeden 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 von Ihrem Load Balancer entfernen.

Inhalt

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

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

Hinzufügen eines Tags

Sie können jederzeit Tags zu Ihrem Load Balancer hinzufügen.

Hinzufügen eines Tags mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Tags die Option Manage tags (Tags verwalten).
5. Wählen Sie auf der Seite Manage tags (Tags verwalten) für jeden Tag die Option Add new tag (Neuen Tag hinzufügen) und geben Sie dann einen Schlüssel und einen Wert an.
6. Wenn Sie fertig mit dem Hinzufügen der Tags sind, wählen Sie Save changes (Änderungen speichern).

Um ein Tag hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den folgenden Befehl add-tags, um das angegebene Tag hinzufügen:

```
aws elb add-tags --load-balancer-name my-loadbalancer --tag "Key=project,Value=lima"
```

Entfernen eines Tags

Sie können Tags von Ihrem Load Balancer entfernen, wenn Sie sie nicht mehr benötigen.

Entfernen eines Tags mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Tags die Option Manage tags (Tags verwalten).
5. Wählen Sie auf der Seite Manage tags (Tags verwalten) neben jedem Tag, den Sie entfernen möchten, Remove (Entfernen) aus.
6. Nachdem Sie alle Tags entfernt haben, wählen Sie Save changes (Änderungen speichern).

Um ein Tag mit dem zu entfernen AWS CLI

Verwenden Sie den folgenden Befehl remove-tags, um das Tag mit dem angegebenen Schlüssel zu entfernen:

```
aws elb remove-tags --load-balancer-name my-loadbalancer --tag project
```

Konfigurieren Sie Subnetze für Ihren Classic Load Balancer

Wenn Sie ein Subnetz zu Ihrem Load Balancer hinzufügen, erstellt Elastic Load Balancing einen Load-Balancer-Knoten in der Availability Zone. Load Balancer-Knoten akzeptieren Datenverkehr von Clients und leiten Anfragen an die fehlerfreien registrierten Instances in einer oder mehreren Availability Zones weiter. Wir empfehlen, dass Sie für mindestens zwei Availability Zones ein Subnetz pro Availability Zone hinzufügen. Auf diese Weise wird die Verfügbarkeit Ihres Load Balancer verbessert. Beachten Sie, dass Sie die Subnetze für Ihren Load Balancer jederzeit ändern können.

Wählen Sie Subnetze aus denselben Availability Zones wie Ihre Instances aus. Wenn es sich bei Ihrem Load Balancer um einen mit dem Internet verbundenen Load Balancer handelt, müssen Sie öffentliche Subnetze auswählen, damit Ihre Backend-Instances Datenverkehr vom Load Balancer erhalten (auch wenn sich die Backend-Instances in privaten Subnetzen befinden). Wenn es sich bei Ihrem Load Balancer um einen internen Load Balancer handelt, empfehlen wir, private Subnetze auszuwählen. Weitere Informationen zu Subnetzen für den Load Balancer finden Sie unter Empfehlungen für Ihre VPC.

Um ein Subnetz hinzuzufügen, registrieren Sie die Instances in der Availability Zone beim Load Balancer und fügen Sie dann ein Subnetz aus dieser Availability Zone mit dem Load Balancer hinzu. Weitere Informationen finden Sie unter Registrieren Sie Instances mit Ihrem Classic Load Balancer.

Nachdem Sie ein Subnetz hinzugefügt haben, beginnt der Load Balancer mit der Weiterleitung von Anfragen an die registrierten Instances in der entsprechenden Availability Zone. Der Load Balancer leitet Anfragen standardmäßig gleichmäßig an die Availability Zones für deren Subnetze weiter. Um Anforderungen gleichmäßig an die registrierten Instances in den Availability Zones weiterzuleiten, aktivieren Sie für deren Subnetze zonenübergreifendes Load Balancing. Weitere Informationen finden Sie unter Konfigurieren des zonenübergreifenden Load Balancing für Ihren Classic Load Balancer.

Sie können ein Subnetz aus Ihrem Load Balancer vorübergehend entfernen, wenn die entsprechende Availability Zone keine fehlerfreien registrierten Instances enthält oder wenn Sie Fehler bei den registrierten Instances beheben oder diese aktualisieren möchten. Nachdem Sie ein Subnetz entfernt haben, leitet der Load Balancer keine Anfragen mehr an die registrierten Instances in der entsprechenden Availability Zone weiter. Anfragen werden aber weiterhin an die registrierten Instances in den Availability Zones für die verbleibenden Subnetze weitergeleitet. Beachten Sie, dass nach dem Entfernen eines Subnetzes die Instances in diesem Subnetz weiterhin beim Load Balancer

registriert sind. Sie können sie aber auch abmelden, wenn Sie möchten. Weitere Informationen finden Sie unter Registrieren Sie Instances mit Ihrem Classic Load Balancer.

Inhalt

Voraussetzungen

Wenn Sie die Subnetze für Ihren Load Balancer aktualisieren, müssen Sie die folgenden Anforderungen erfüllen:

- Der Load Balancer muss ständig über mindestens ein Subnetz verfügen.
- Sie können je Availability Zone höchstens ein Subnetz hinzufügen.
- Sie können kein lokales Zonen-Subnetz hinzufügen.

Da es separate Subnetze gibt APIs , die einem Load Balancer hinzugefügt und daraus entfernt werden können, müssen Sie die Reihenfolge der Vorgänge sorgfältig abwägen, wenn Sie die aktuellen Subnetze gegen neue Subnetze austauschen, um diese Anforderungen zu erfüllen. Außerdem müssen Sie vorübergehend ein Subnetz aus einer anderen Availability Zone hinzufügen, wenn Sie alle Subnetze für Ihren Load Balancer austauschen müssen. Beispiel: Wenn Ihr Load Balancer eine einzige Availability Zone hat und Sie das Subnetz gegen ein anderes Subnetz austauschen müssen, müssen Sie zuerst ein Subnetz aus einer zweiten Availability Zone hinzufügen. Anschließend können Sie das Subnetz aus der ursprünglichen Availability Zone entfernen (ohne die Anforderung von einem Subnetz zu unterschreiten), neues Subnetz aus der ursprünglichen Availability Zone hinzufügen (ohne die Anforderung von einem Subnetz zu überschreiten), und dann das Subnetz aus der zweiten Availability Zone entfernen (wenn es benötigt wird, um den Tausch vorzunehmen).

Konfigurieren Sie Subnetze mithilfe der Konsole

Gehen Sie wie folgt vor, um Subnetze mithilfe der Konsole hinzuzufügen oder zu entfernen.

So konfigurieren Sie Subnetze mit der Konsole

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

2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Network mapping (Netzwerkzuordnung) die Option Edit subnets (Subnetze bearbeiten) aus.
5. Fügen Sie auf der Seite Subnetze bearbeiten im Abschnitt Netzwerkzuordnung nach Bedarf Subnetze hinzu und entfernen Sie sie.
6. Klicken Sie auf Save changes (Änderungen speichern), wenn Sie fertig sind.

Konfigurieren Sie Subnetze mit der CLI

Verwenden Sie die folgenden Beispiele, um Subnetze mithilfe von hinzuzufügen oder zu entfernen. AWS CLI

Hinzufügen eines Subnetzes zu Ihrem Load Balancer mithilfe der CLI

Verwenden Sie den folgenden Befehl attach-load-balancer-to-subnets, um Ihrem Load Balancer zwei Subnetze hinzuzufügen:

```
aws elb attach-load-balancer-to-subnets --load-balancer-name my-load-balancer --
subnets subnet-dea770a9 subnet-fb14f6a2
```

In der Antwort werden alle Subnetze für den Load Balancer aufgelistet. Zum Beispiel:

```
{
    "Subnets": [
        "subnet-5c11033e",
        "subnet-dea770a9",
        "subnet-fb14f6a2"
    ]
}
```

Um ein Subnetz zu entfernen, verwenden Sie AWS CLI

Verwenden Sie den folgenden Befehl detach-load-balancer-from-subnets, um die angegebenen Subnetze aus dem angegebenen Load Balancer zu entfernen:

```
aws elb detach-load-balancer-from-subnets --load-balancer-name my-loadbalancer --
subnets subnet-450f5127
```

In der Antwort werden die verbleibenden Subnetze für den Load Balancer aufgelistet. Zum Beispiel:

```
{
    "Subnets": [
        "subnet-15aaab61"
    ]
}
```

Konfigurieren von Sicherheitsgruppen für Ihren Classic Load Balancer

Wenn Sie den verwenden AWS Management Console , um einen Load Balancer zu erstellen, können Sie eine vorhandene Sicherheitsgruppe auswählen oder eine neue erstellen. Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss sie für den Load Balancer in beide Richtungen zum Listener-Port und zum Zustandsprüfung-Port Datenverkehr zulassen. Wenn Sie eine Sicherheitsgruppe erstellen möchten, fügt die Konsole automatisch Regeln hinzu, um den gesamten Datenverkehr auf diesen Ports zuzulassen.

[Nicht standardmäßige VPC] Wenn Sie die AWS CLI oder -API verwenden, einen Load Balancer in einer nicht standardmäßigen VPC erstellen, aber keine Sicherheitsgruppe angeben, wird Ihr Load Balancer automatisch der Standardsicherheitsgruppe für die VPC zugeordnet.

[Standard-VPC] Wenn Sie die API AWS CLI oder verwenden, um einen Load Balancer in Ihrer Standard-VPC zu erstellen, können Sie keine bestehende Sicherheitsgruppe für Ihren Load Balancer auswählen. Stattdessen bietet Elastic Load Balancing eine Sicherheitsgruppe mit Regeln, um an den für den Load Balancer angegebenen Ports den gesamte Datenverkehr zuzulassen. Elastic Load Balancing erstellt nur eine solche Sicherheitsgruppe pro AWS Konto mit einem Namen in der Form default_elb_ *id* (z. B.). `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE` Nachfolgende Load Balancer, die Sie in der Standard-VPC erstellen, verwenden auch diese Sicherheitsgruppe. Lesen Sie die Sicherheitsgruppenregeln, um sicherzustellen, dass sie für den neuen Load Balancer Datenverkehr auf dem Listener-Port und dem Zustandsprüfungs-Ports zulassen. Wenn Sie Ihren Load Balancer löschen, wird diese Sicherheitsgruppe nicht automatisch gelöscht.

Wenn Sie einen Listener zu einem bestehenden Load Balancer hinzufügen, müssen Sie Ihre Sicherheitsgruppen überprüfen, um sicherzustellen, dass sie am neuen Listener-Port Datenverkehr in beide Richtungen zulassen.

Inhalt

Empfohlene Regeln für Load-Balancer-Sicherheitsgruppen

Die Sicherheitsgruppen für Ihre Load Balancer müssen ihnen erlauben, mit Ihren Instances zu kommunizieren. Die empfohlenen Regeln hängen vom Typ des Load Balancers ab, ob mit dem Internet verbunden oder intern.

Mit dem Internet verbundener Load Balancer

Die folgende Tabelle zeigt die empfohlenen Regeln für eingehenden Datenverkehr für einen mit dem Internet verbundenen Load Balancer.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
0.0.0.0/0	TCP	*listener*	Allen eingehenden Datenverkehr auf dem Load Balancer Listener-Port erlauben

Die folgende Tabelle zeigt die empfohlenen Regeln für ausgehenden Datenverkehr für einen mit dem Internet verbundenen Load Balancer.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
instance security group	TCP	*instance listener*	Ausgehenden Datenverkehr an Instances auf dem Instance-Listener-Port erlauben
instance security group	TCP	*health check*	Ausgehenden Datenverkehr an Instances auf dem Zustandsp rüfungsport erlauben

Interne Load Balancer

Die folgende Tabelle zeigt die empfohlenen Regeln für eingehenden Datenverkehr für einen internen Load Balancer.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	TCP	*listener*	Eingehenden Datenverkehr aus dem VPC CIDR auf dem Load Balancer-Listener-Port erlauben

Die folgende Tabelle zeigt die empfohlenen Regeln für ausgehenden Datenverkehr für einen internen Load Balancer.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
instance security group	TCP	*instance listener*	Ausgehenden Datenverkehr an Instances auf dem Instance-Listener-Port erlauben
instance security group	TCP	*health check*	Ausgehenden Datenverkehr an Instances auf dem Zustandsprüfungsport erlauben

Weisen Sie Sicherheitsgruppen mithilfe der Konsole zu

Gehen Sie wie folgt vor, um die mit Ihrem Load Balancer verknüpften Sicherheitsgruppen zu ändern.

So aktualisieren Sie eine Ihrem Load Balancer zugewiesene Sicherheitsgruppe mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Security (Sicherheit) die Option Edit (Bearbeiten) aus.

5. Fügen Sie auf der Seite Sicherheitsgruppen bearbeiten unter Sicherheitsgruppen nach Bedarf Sicherheitsgruppen hinzu oder entfernen Sie sie.

   Sie können bis zu 5 Sicherheitsgruppen hinzufügen.

6. Klicken Sie auf Save changes (Änderungen speichern), wenn Sie fertig sind.

Weisen Sie Sicherheitsgruppen zu, indem Sie AWS CLI

Verwenden Sie den folgenden Befehl apply-security-groups-to-load-balancer, um eine Sicherheitsgruppe einem Load Balancer zuzuordnen. Die angegebenen Sicherheitsgruppen setzen die vorher zugewiesenen Sicherheitsgruppen außer Kraft.

```
aws elb apply-security-groups-to-load-balancer --load-balancer-name my-loadbalancer --
security-groups sg-53fae93f
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
  "SecurityGroups": [
     "sg-53fae93f"
  ]
}
```

Netzwerk ACLs für Ihren Classic Load Balancer konfigurieren

Die standardmäßige Netzwerkzugriffskontrollliste (ACL) für eine VPC erlaubt den gesamten ein- und ausgehenden Datenverkehr. Wenn Sie ein benutzerdefiniertes Netzwerk erstellen ACLs, müssen Sie Regeln hinzufügen, die die Kommunikation zwischen dem Load Balancer und den Instances ermöglichen.

Die empfohlenen Regeln für das Subnetz Ihres Load Balancers hängen vom Typ des Load Balancers ab, ob mit dem Internet verbunden oder intern.

Mit dem Internet verbundener Load Balancer

Im Folgenden finden Sie die empfohlenen Regeln für eingehende Nachrichten für einen mit dem Internet verbundenen Load Balancer.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
0.0.0.0/0	TCP	*listener*	Allen eingehenden Datenverkehr auf dem Load Balancer Listener-Port erlauben
VPC CIDR	TCP	1024 - 65535	Eingehenden Datenverkehr vom VPC CIDR an den flüchtigen Ports zulassen

Im Folgenden sind die empfohlenen Regeln für ausgehende Nachrichten für einen mit dem Internet verbundenen Load Balancer aufgeführt.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	TCP	*instance listener*	Gesamten ausgehenden Datenverkehr am Listener-Port der Instance zulassen
VPC CIDR	TCP	*health check*	Gesamten ausgehenden Datenverkehr am Zustandsprüfungs-Port zulassen
0.0.0.0/0	TCP	1024 - 65535	Gesamten ausgehenden Datenverkehr an den flüchtigen Ports zulassen

Interner Load Balancer

Im Folgenden sind die empfohlenen Regeln für eingehenden Datenverkehr für einen internen Load Balancer aufgeführt.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	TCP	*listener*	Eingehenden Datenverkehr aus dem VPC CIDR auf dem Load Balancer-Listener-Port erlauben
VPC CIDR	TCP	1024 - 65535	Eingehenden Datenverkehr vom VPC CIDR an den flüchtigen Ports zulassen

Im Folgenden sind die empfohlenen Regeln für ausgehenden Datenverkehr für einen internen Load Balancer aufgeführt.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	TCP	*instance listener*	Ausgehenden Datenverkehr zu den VPC CIDR am Listener-Port der Instance zulassen
VPC CIDR	TCP	*health check*	Ausgehenden Datenverkehr zum VPC CIDR am Zustandsprüfungs-Port zulassen
VPC CIDR	TCP	1024 - 65535	Ausgehenden Datenverkehr zum VPC CIDR an den flüchtigen Ports zulassen

Konfigurieren eines benutzerdefinierten Domainnamens für Ihren Classic Load Balancer

Jeder Classic Load Balancer erhält einen Standard-DNS-Namen (Domain Name System). Dieser DNS-Name enthält den Namen der AWS Region, in der der Load Balancer erstellt wurde. Wenn Sie beispielsweise einen Load Balancer mit dem Namen `my-loadbalancer` in der

Region USA West (Oregon) erstellen, erhält Ihr Load Balancer einen DNS-Namen wie `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com`. Fügen Sie diesen DNS-Namen in das Adressfeld von einem Webbrowser ein, um auf die Website auf Ihren Instances zuzugreifen. Diesen DNS-Name können Ihre Kunden jedoch nicht leicht behalten und verwenden.

Wenn Sie anstatt des Standard-DNS-Namen lieber einen praktischen DNS-Namen für Ihren Load Balancer verwenden möchten, wie zum Beispiel `www.example.com`, können Sie einen benutzerdefinierten Domainnamen erstellen und diesen mit dem DNS-Namen für Ihren Load Balancer verknüpfen. Wenn ein Client eine Anforderung mit diesem benutzerdefinierten Domainnamen sendet, löst der DNS-Server diesen Namen in den DNS-Namen für Ihren Load Balancer auf.

Inhalt

Verknüpfen eines benutzerdefinierten Domainnamens mit Ihrem Load Balancer-Namen

Registrieren Sie Ihren Domainnamen, falls noch nicht geschehen. Die ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet Domain-Namen im Internet. Sie registrieren einen Domain-Namen über eine Vergabestelle für Domain-Namen, eine von der ICANN autorisierte Organisation, die die Registrierung von Domain-Namen verwaltet. Die Website für Ihre Vergabestelle enthält genaue Anweisungen und Preise für die Registrierung des Domain-Namens. Weitere Informationen finden Sie in den folgenden Ressourcen:

- Um Amazon Route 53 zur Registrierung eines Domain-Namens zu verwenden, siehe Registrieren von Domain-Namen mit Route 53 im Amazon Route 53-Entwicklerhandbuch.
- Eine Liste der akkreditierten Registrare finden Sie in der Liste der akkreditierten Registrare.

Verwenden Sie dann Ihren DNS-Service, wie zum Beispiel Ihre Domainvergabestelle, um einen CNAME-Datensatz zur Weiterleitung von Abfragen an Ihren Load Balancer zu erstellen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem DNS-Service.

Alternativ dazu können Sie Route 53 als Ihren DNS-Service verwenden. Sie erstellen eine gehostete Zone, die Informationen darüber, wie Datenverkehr im Internet für Ihre Domain weitergeleitet wird, und einen Aliasressourcendatensatz enthält, der Abfragen für Ihren Domainnamen an Ihren Load Balancer weiterleitet. In Route 53 werden keine Kosten für die DNS-Abfragen für Aliasdatensätze erstattet, und Sie können Aliasdatensätze verwenden, um DNS-Abfragen für den Zone Apex Ihrer Domain an Ihren Load Balancer weiterzuleiten (zum Beispiel `example.com`). Weitere Informationen zum Übertragen von DNS-Services für vorhandene Domains in Route 53 finden Sie unter Konfigurieren von Route 53 als DNS-Service im Amazon-Route-53-Entwicklerhandbuch.

Erstellen Sie schließlich eine gehostete Zone und einen Alias-Datensatz für Ihre Domain mit Route 53. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr an einen Load Balancer im Entwicklerhandbuch von Amazon Route 53.

Verwenden des Route-53-DNS-Failover für Ihren Load Balancer

Wenn Sie mithilfe von Route 53 DNS-Abfragen an Ihren Load Balancer leiten, können Sie mithilfe von Route 53 auch DNS-Failover für Ihren Load Balancer konfigurieren. In einer Failover-Konfiguration überprüft Route 53 den Zustand der registrierten EC2 Instances für den Load Balancer, um festzustellen, ob sie verfügbar sind. Wenn beim Load Balancer keine fehlerfreien EC2 Instances registriert sind oder wenn der Load Balancer selbst fehlerhaft ist, leitet Route 53 den Verkehr an eine andere verfügbare Ressource weiter, z. B. einen fehlerfreien Load Balancer oder eine statische Website in Amazon S3.

Beispiel: Sie haben eine Webanwendung `www.example.com` und möchten, dass redundante Instances hinter zwei Load Balancers in verschiedenen Regionen laufen. Sie möchten, dass der Datenverkehr in erster Linie auf den Load Balancer in einer Region weitergeleitet wird, und der Load Balancer in der anderen Region soll bei Ausfällen als Sicherung dienen. Wenn Sie DNS Failover konfigurieren, können Sie einen primären und einen sekundären (Sicherung) Load Balancer festlegen. Route 53 leitet den Datenverkehr direkt zum primären Load Balancer, und wenn dieser nicht verfügbar ist, wird der Datenverkehr zum sekundären Load Balancer geleitet.

Verwenden von „Zielintegrität auswerten“

- Wenn die Option „Zielintegrität auswerten“ für einen Aliaseintrag für einen Classic Load Balancer auf `Yes` festgelegt ist, wertet Route 53 die Integrität der durch den `alias target`-Wert angegebenen Ressource aus. Für einen Classic Load Balancer verwendet Route 53 die mit dem Load Balancer verknüpften Zustandsprüfungen für Instances.
- Wenn mindestens eine der registrierten Instances in einem Classic Load Balancer fehlerfrei ist, markiert Route 53 den Aliasdatensatz als fehlerfrei. Route 53 gibt dann Datensätze gemäß Ihrer

Routing-Richtlinie zurück. Wenn die Failover-Routing-Richtlinie verwendet wird, gibt Route 53 den primären Datensatz zurück.

- Wenn alle der registrierten Instances für einen Classic Load Balancer fehlerhaft sind, markiert Route 53 den Aliasdatensatz als fehlerhaft. Route 53 gibt dann Datensätze gemäß Ihrer Routing-Richtlinie zurück. Wenn die Failover-Routing-Richtlinie verwendet wird, gibt Route 53 dann den sekundären Datensatz zurück.

Weitere Informationen finden Sie unter Konfigurieren von DNS-Failover im Entwicklerhandbuch für Amazon Route 53.

Trennen des benutzerdefinierten Domainnamens von Ihrem Load Balancer

Sie können den benutzerdefinierten Domainnamen von einer Load Balancer-Instance trennen, indem Sie zuerst die Ressourcendatensätze in Ihrer gehosteten Zone und dann die gehostete Zone löschen. Weitere Informationen finden Sie unter Bearbeiten von Datensätzen und Löschen einer öffentlichen gehosteten Zone im Entwicklerhandbuch für Amazon Route 53.

Listener für Ihren Classic Load Balancer

Bevor Sie mit der Nutzung von Elastic Load Balancing beginnen, müssen Sie einen oder mehrere Listener für Ihren Classic Load Balancer konfigurieren. Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Er wird mit einem Protokoll und einem Port für Frontend-Verbindungen (Client zu Load Balancer) sowie einem Protokoll und einem Port für Backend-Verbindungen (Load Balancer zu Backend-Instance) konfiguriert.

Elastic Load Balancing unterstützt die folgenden Protokolle:

- HTTP
- HTTPS (sicheres HTTP)
- TCP
- SSL (sicheres TCP)

Das HTTPS-Protokoll verwendet das SSL-Protokoll, um sichere Verbindungen über den HTTP-Layer aufzubauen. Sie können auch das SSL-Protokoll verwenden, um sichere Verbindungen über den TCP-Layer aufzubauen.

Wenn die Frontend-Verbindung TCP oder SSL verwendet, können Ihre Backend-Verbindungen entweder TCP oder SSL verwenden. Wenn die Frontend-Verbindung HTTP oder HTTPS verwendet, können Ihre Backend-Verbindungen entweder HTTP oder HTTPS verwenden.

Backend-Instances können auf den Ports 1-65535 lauschen.

Load Balancer können auf den folgenden Ports lauschen: 1-65535

Inhalt

Protokolle

Kommunikation für eine typische Webanwendung wird durch Hardware- und Software-Layer geleitet. Jeder Layer bietet eine spezifische Kommunikationsfunktion. Die Kontrolle über die Kommunikationsfunktion wird nacheinander von einem Layer zum nächsten übergeben. Die Open System Interconnection (OSI) definiert ein Modell für die Implementierung eines Standardformats für die Kommunikation, das in diesen Layern als Protokoll bezeichnet wird. Weitere Informationen finden Sie unter OSI-Modell in Wikipedia.

Wenn Sie Elastic Load Balancing verwenden, müssen Sie über ein grundlegendes Verständnis von Layer 4 und Layer 7 verfügen. Layer 4 ist die Transportschicht, die die Transmission Control Protocol (TCP)-Verbindung zwischen dem Client und Ihrer Backend-Instance über den Load Balancer beschreibt. Layer 4 ist die niedrigste Ebene, die für Ihren Load Balancer konfiguriert werden kann. Layer 7 ist die Anwendungsebene, die die Verwendung von Hypertext Transfer Protocol (HTTP) und HTTPS (sicheres HTTP)-Verbindungen von den Clients zum Load Balancer und vom Load Balancer zur Backend-Instance beschreibt.

Das SSL-Protokoll (Secure Sockets Layer) wird in erster Linie für die Verschlüsselung vertraulicher Daten über unsichere Netzwerke wie das Internet verwendet. Das SSL-Protokoll stellt eine sichere Verbindung zwischen einem Client und dem Backend-Server her und stellt sicher, dass alle Daten zwischen Ihrem Client und Ihrem Server privat und integriert sind.

TCP/SSL-Protokoll

Wenn Sie TCP (Layer 4) für Frontend- und Backend-Verbindungen verwenden, leitet Ihr Load Balancer die Anforderung an die Backend-Instances weiter, ohne die Header zu ändern. Nachdem der Load Balancer die Anforderung empfangen hat, versucht er, eine TCP-Verbindung zu der Backend-Instance auf dem in der Listener-Konfiguration spezifizierten Port zu öffnen.

Da Load Balancer Datenverkehr zwischen Clients und Ihren Backend-Instances abfangen, enthalten die Zugriffsprotokolle für Ihre Backend-Instance die IP-Adresse des Load Balancer statt des ursprünglichen Clients. Sie können Proxy-Protokoll aktivieren, damit ein Header mit den Verbindungsinformationen des Clients, wie z. B. die Quell-IP-Adresse, Ziel-IP-Adresse und Port-Nummern, hinzugefügt wird. Der Header wird im Rahmen der Anforderung dann wieder an die Backend-Instance gesendet. Sie können die erste Zeile in der Anforderung parsen, um die Verbindungsinformationen abzurufen. Weitere Informationen finden Sie unter Konfigurieren Sie das Proxyprotokoll für Ihren Classic Load Balancer.

Mit dieser Konfiguration erhalten Sie keine Cookies für Sticky Sessions oder X-Forwarded-Header.

HTTP/HTTPS-Protokoll

Wenn Sie HTTP (Layer 7) sowohl für Front-End- als auch für Back-End-Verbindungen verwenden, analysiert Ihr Load Balancer die Header in der Anfrage, bevor er die Anfrage an die Back-End-Instances sendet.

Für jede registrierte und fehlerfreie Instanz, die hinter einer Anfrage steht. HTTP/HTTPS load balancer, Elastic Load Balancing opens and maintains one or more TCP connections. These connections ensure that there is always an established connection ready to receive HTTP/HTTPS

Die HTTP-Anforderungen und -Antworten verwenden Header-Felder, um Informationen über HTTP-Nachrichten zu senden. Elastic Load Balancing unterstützt `X-Forwarded-For`-Header. Da Load Balancer Datenverkehr zwischen Clients und Servern abfangen, enthalten Ihre Server-Zugriffsprotokolle nur die IP-Adresse des Load Balancer. Verwenden Sie den `X-Forwarded-For`-Anforderungs-Header, um die IP-Adresse des Clients anzuzeigen. Weitere Informationen finden Sie unter X-Forwarded-For.

Wenn Sie HTTP/HTTPS verwenden, können Sie Sticky Sessions auf Ihrem Load Balancer aktivieren. Eine Sticky Session bindet eine Benutzersitzung an eine bestimmte Backend-Instance. So wird sichergestellt, dass alle Anforderungen, die während der Sitzung vom Benutzer gesendet werden, an dieselbe Backend-Instance weitergeleitet werden. Weitere Informationen finden Sie unter Konfigurieren von Sticky Sessions für Ihren Classic Load Balancer.

Der Load Balancer unterstützt nicht alle HTTP-Erweiterungen. Sie benötigen möglicherweise einen TCP-Listener, wenn der Load Balancer nicht in der Lage ist, die Anforderung zu beenden, da unerwartete Methoden, Antwortcodes oder andere Nicht-Standard-HTTP 1.0/1.1-Implementierungen vorliegen.

HTTPS/SSL-Listener

Sie können einen Load Balancer mit den folgenden Sicherheitsfunktionen erstellen.

SSL-Serverzertifikate

Wenn Sie HTTPS oder SSL für Ihre Frontend-Verbindungen verwenden, müssen Sie ein X.509-Zertifikat (SSL-Server-Zertifikat) auf Ihrem Load Balancer bereitstellen. Der Load Balancer entschlüsselt Anforderungen von Clients, bevor er sie an die Backend-Instances zurücksendet (auch als SSL-Terminierung bezeichnet). Weitere Informationen finden Sie unter SSL/TLS-Zertifikate für Classic Load Balancer.

Wenn Sie nicht möchten, dass der Load Balancer den SSL-Abschluss (auch als SSL-Auslagerung bezeichnet) übernimmt, können Sie TCP für die Frontend- und Backend-Verbindungen verwenden und Zertifikate auf den registrierten Instances, die die Anforderungen bearbeiten, bereitstellen.

SSL-Aushandlung

Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen, die als Verschlüsselungen bezeichnet werden. Bei manchen Anwendungsfällen müssen alle Daten im Netzwerk verschlüsselt werden, und es werden nur bestimmte Verschlüsselungen zugelassen. Einige Sicherheits-Compliance-Standards (z. B. PCI, SOX usw.) erfordern möglicherweise bestimmte Protokolle und Verschlüsselungen von Clients, um sicherzustellen, dass die Sicherheitsstandards erfüllt werden. In diesen Fällen können Sie eine benutzerdefinierte SSL-Aushandlungskonfiguration basierend auf Ihren spezifischen Anforderungen erstellen. Ihre Verschlüsselungen und Protokolle sollten innerhalb von 30 Sekunden wirksam werden. Weitere Informationen finden Sie unter SSL-Aushandlungskonfigurationen für Classic Load Balancer.

Backend-Serverauthentifizierung

Wenn Sie HTTPS oder SSL für Ihre Backend-Verbindungen verwenden, können Sie die Authentifizierung Ihrer registrierten Instances aktivieren. Sie können dann das Authentifizierungsverfahren verwenden, um sicherzustellen, dass die Instances nur verschlüsselte Kommunikation akzeptieren und jede registrierte Instance den richtigen öffentlichen Schlüssel besitzt.

Weitere Informationen finden Sie unter Konfigurieren der Backend-Authentifizierung.

Listener-Konfigurationen für Classic Load Balancer

In der folgenden Tabelle werden mögliche Konfigurationen für HTTP- und HTTPS-Listener für einen Classic Load Balancer beschrieben.

Anwendungsfall	Frontend-Protokoll	Frontend-Optionen	Backend-Protokoll	Backend-Optionen	Hinweise
Allgemeiner HTTP-Load Balancer	HTTP	N/A	HTTP	N/A	• Unterstützt die X-Forwarded-Header
Sichere Website oder Anwendung, die Elastic Load Balancing verwendet, um die SSL-Entschlüsselung auszulagern	HTTPS	SSL-Aushandlung	HTTP	N/A	• Unterstützt die X-Forwarded-Header • Auf dem Load Balancer muss ein SSL-Zertifikat bereitgestellt werden.
Sichere Website oder Anwendung mithilfe von Verschlüsselung end-to-end	HTTPS	SSL-Aushandlung	HTTPS	Backend-Authentifizierung	• Unterstützt die X-Forwarded-Header • Auf dem Load Balancer und den registrierten Instances muss ein SSL-Zertifikat

Anwendungsfall	Frontend-Protokoll	Frontend-Optionen	Backend-Protokoll	Backend-Optionen	Hinweise
					bereitgestellt werden.

In der folgenden Tabelle werden mögliche Konfigurationen für TCP- und SSL-Listener für einen Classic Load Balancer beschrieben.

Anwendungsfall	Frontend-Protokoll	Frontend-Optionen	Backend-Protokoll	Backend-Optionen	Hinweise
Allgemeiner TCP-Load Balancer	TCP	N/A	TCP	N/A	• Unterstützt den Proxy-Protokoll-Header
Sichere Website oder Anwendung, die Elastic Load Balancing verwendet, um die SSL-Entschlüsselung auszulagern	SSL	SSL-Aushandlung	TCP	N/A	• Auf dem Load Balancer muss ein SSL-Zertifikat bereitgestellt werden. • Unterstützt den Proxy-Protokoll-Header
Sichere Website oder Anwendung mithilfe von end-to-end	SSL	SSL-Aushandlung	SSL	Backend-Authentifizierung	• Auf dem Load Balancer und den registrie

Anwendungsfall	Frontend-Protokoll	Frontend-Optionen	Backend-Protokoll	Backend-Optionen	Hinweise
Verschlüsselung mit Elastic Load Balancing					rten Instances muss ein SSL-Zertifikat bereitgestellt werden. • Bei Backend-SSL-Verbindungen werden keine SNI-Header eingefügt. • Der Proxy-Protokoll-Header wird nicht unterstützt

HTTP-Header und Classic Load Balancer

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

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

Voraussetzungen

- Vergewissern Sie sich, dass Ihre Listener-Einstellungen die X-Forwarded-Header unterstützten. Weitere Informationen finden Sie unter Listener-Konfigurationen für Classic Load Balancer.
- Konfigurieren Sie Ihren Webserver, um Client-IP-Adressen zu protokollieren.

X-Forwarded-Header

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

X-Forwarded-For

Der `X-Forwarded-For`-Anforderungs-Header wird automatisch hinzugefügt und hilft Ihnen, die IP-Adresse eines Clients zu identifizieren, wenn Sie einen HTTP- oder HTTPS-Load-Balancer verwenden. Da Load Balancer Datenverkehr zwischen Clients und Servern abfangen, enthalten Ihre Server-Zugriffsprotokolle nur die IP-Adresse des Load Balancer. Verwenden Sie den `X-Forwarded-For`-Anforderungs-Header, um die IP-Adresse des Clients anzuzeigen. Elastic Load Balancing speichert die IP-Adresse des Clients im `X-Forwarded-For`-Anforderungs-Header und übergibt den Header an Ihren Server. Wenn der `X-Forwarded-For`-Anforderungsheader nicht in der Anforderung enthalten ist, erstellt der Load Balancer einen Header mit der Client-IP-Adresse als Anforderungswert. Andernfalls fügt der Load Balancer die Client-IP-Adresse dem vorhandenen Header hinzu und leitet den Header dann an Ihren Server weiter. Der `X-Forwarded-For`-Anforderungsheader kann mehrere IP-Adressen enthalten, die durch Kommas getrennt sind. Die Adresse ganz links ist die Client-IP, über die die Anforderung zuerst gestellt wurde. Darauf folgen alle nachfolgenden Proxy-Bezeichner in einer Kette.

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

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

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

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

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

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

X-Forwarded-Proto

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

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

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

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

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

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

X-Forwarded-Port

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

HTTPS-Listener für Ihren Classic Load Balancer

Sie können einen Load Balancer erstellen, der das SSL-/TLS-Protokoll für verschlüsselte Verbindungen verwendet (auch als SSL-Offload bezeichnet). Diese Funktion ermöglicht die Verschlüsselung des Datenverkehrs zwischen Ihrem Load Balancer und den Clients, die HTTPS-Sitzungen initiieren, sowie für Verbindungen zwischen Ihrem Load Balancer und Ihren Instances. EC2

Elastic Load Balancing verwendet Secure Sockets Layer (SSL)-Aushandlungskonfigurationen, auch bekannt als Sicherheitsrichtlinien, um Verbindungen zwischen Clients und dem Load Balancer zu verhandeln. Wenn Sie HTTPS/SSL für Ihre Frontend-Verbindungen verwenden, können Sie entweder eine vordefinierte Sicherheitsrichtlinie oder eine benutzerdefinierte Sicherheitsrichtlinie verwenden. Sie müssen ein SSL-Zertifikat auf dem Load Balancer bereitstellen. Der Load Balancer verwendet dieses Zertifikat, um die Verbindung zu beenden und dann Anfragen von Clients zu entschlüsseln, bevor er sie an die Instances sendet. Der Load Balancer verwendet eine statische Verschlüsselungssammlung für Backend-Verbindungen. Sie können optional festlegen, dass Authentifizierung auf Ihren Instances aktiviert wird.

Classic Load Balancers unterstützt keine Servernamensanzeige (Server Name Indication, SNI) auf Ihrem Load Balancer. Sie können stattdessen eine der folgenden Alternativen verwenden:

- Stellen Sie ein Zertifikat auf dem Load Balancer bereit und fügen Sie für jede weitere Website einen Subject Alternative Name (SAN) hinzu. SANs ermöglicht es Ihnen, mehrere Hostnamen mit einem einzigen Zertifikat zu schützen. Erkundigen Sie sich bei Ihrem Zertifikatsanbieter nach weiteren Informationen darüber, wie viele Zertifikate pro Zertifikat unterstützt werden und wie Sie SANs diese hinzufügen und entfernen können SANs.
- Verwenden Sie TCP-Listener an Port 443 für die Frontend- und Backend-Verbindungen. Der Load Balancer leitet die Anfrage unverändert weiter, sodass Sie die HTTPS-Terminierung auf der EC2 Instance handhaben können.

Classic Load Balancer unterstützen keine gegenseitige TLS-Authentifizierung (mTLS). Für mTLS-Unterstützung erstellen Sie einen TCP-Listener. Der Load Balancer leitet die Anfrage unverändert weiter, sodass Sie mTLS auf der Instance implementieren können. EC2

Inhalt

SSL/TLS-Zertifikate für Classic Load Balancer

Wenn Sie HTTPS (SSL oder TLS) für Ihre Frontend-Listener verwenden, müssen Sie ein SSL/TLS-Zertifikat auf dem Load Balancer bereitstellen. Der Load Balancer verwendet das Zertifikat, um die Verbindung zu beenden und dann Anfragen von Clients zu entschlüsseln, bevor er sie an die Instances sendet.

Die SSL- und TLS-Protokolle verwenden ein X.509-Zertifikat (SSL/TLS-Serverzertifikat) zum Authentifizieren von Client und Backend-Anwendung. Ein X.509-Zertifikat ist eine digitale Form der Identifikation, die von einer Zertifizierungsstelle (CA) ausgestellt wurde und Informationen zur Identifizierung, einer Gültigkeitsdauer, einen öffentlichen Schlüssel, einer Seriennummer und die digitale Signatur des Ausstellers enthält.

Sie können ein Zertifikat mit AWS Certificate Manager oder einem Tool erstellen, das die SSL- und TLS-Protokolle unterstützt, z. B. OpenSSL. Sie legen dieses Zertifikat beim Erstellen oder Aktualisieren eines HTTPS-Listeners für Ihren Load Balancer fest. Wenn Sie ein Zertifikat zur Verwendung mit Ihrem Load Balancer erstellen, müssen Sie einen Domainnamen angeben.

Wenn Sie ein Zertifikat zur Verwendung mit Ihrem Load Balancer erstellen, müssen Sie einen Domainnamen angeben. Der Domainname auf dem Zertifikat muss mit dem Datensatz für den benutzerdefinierten Domainnamen übereinstimmen. Wenn sie nicht übereinstimmen, wird der Datenverkehr nicht verschlüsselt, da die TLS-Verbindung nicht verifiziert werden kann.

Sie müssen einen vollqualifizierten Domainnamen (Fully Qualified Domain Name, FQDN) für Ihr Zertifikat wie `www.example.com` oder einen Apex-Domainnamen wie `example.com` angeben. Sie können auch ein Sternchen (*) als Platzhalter verwenden, um mehrere Websitenamen in derselben Domain zu schützen. Wenn Sie ein Platzhalter-Zertifikat anfordern, muss sich das Sternchen (*) ganz links im Domainnamen befinden und es kann nur eine Subdomain-Ebene geschützt werden. `*.example.com` schützt beispielsweise `corp.example.com` und `images.example.com`, aber es kann `test.login.example.com` nicht schützen. Beachten Sie außerdem, dass `*.example.com`

nur die Subdomains von `example.com` schützt, jedoch nicht die „Bare“- oder „Apex“-Domain (`example.com`). Der Platzhaltername wird im Feld Subject (Betreff) und in der Erweiterung Subject Alternative Name (Alternativer Name des Betreffs) des Zertifikats angezeigt. Weitere Informationen zum Anfordern öffentlicher Zertifikate finden Sie unter Anfordern eines öffentlichen Zertifikats im AWS Certificate Manager -Benutzerhandbuch.

Erstellen oder importieren Sie ein SSL/TLS-Zertifikat mit AWS Certificate Manager

Wir empfehlen, dass Sie AWS Certificate Manager (ACM) verwenden, um Zertifikate für Ihren Load Balancer zu erstellen oder zu importieren. ACM lässt sich in Elastic Load Balancing integrieren, sodass Sie das Zertifikat in Ihrem Load Balancer bereitstellen können. Um ein Zertifikat auf dem Load Balancer bereitzustellen, muss sich das Zertifikat in derselben Region wie der Load Balancer befinden. Weitere Informationen finden Sie unter Anfordern eines öffentlichen Zertifikats oder Importieren von Zertifikaten im AWS Certificate Manager -Benutzerhandbuch.

Um einem Benutzer die Bereitstellung des Zertifikats auf Ihrem Load Balancer mithilfe der AWS Management Console zu ermöglichen, müssen Sie den Zugriff auf die ACM `ListCertificates`-API-Aktion erlauben. Weitere Informationen finden Sie unter Auflisten von Zertifikaten im AWS Certificate Manager -Benutzerhandbuch.

> **Important**
>
> Sie können Zertifikate mit 4096-Bit-RSA-Schlüsseln oder EC-Schlüsseln nicht durch Integration in ACM auf Ihrem Load Balancer installieren. Sie müssen Zertifikate mit 4096-Bit-RSA-Schlüsseln oder EC-Schlüsseln zu IAM hochladen, um sie mit Ihrem Load Balancer verwenden zu können.

Importieren eines SSL-/TLS-Zertifikats mithilfe von IAM

Wenn Sie nicht mit ACM arbeiten, können Sie mit SSL/TLS-Tools, wie OpenSSL, eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) erstellen, die CSR dann von einer CA signieren lassen, um ein Zertifikat zu erstellen, und das Zertifikat zu IAM hochladen. Weitere Informationen finden Sie unter Arbeiten mit Serverzertifikaten im IAM-Benutzerhandbuch.

SSL-Aushandlungskonfigurationen für Classic Load Balancer

Elastic Load Balancing verwendet eine Secure Socket Layer (SSL)-Aushandlungskonfiguration, die als Sicherheitsrichtlinie bezeichnet wird, um SSL-Verbindungen zwischen einem Client und dem Load Balancer auszuhandeln. Eine Sicherheitsrichtlinie ist eine Kombination von SSL-Protokollen, SSL-Verschlüsselung und der Präferenz für die Serverreihenfolge. Weitere Informationen über die Konfiguration einer SSL-Verbindung für Ihren Load Balancer finden Sie unter Listener für Ihren Classic Load Balancer.

Inhalt

Sicherheitsrichtlinien

Eine Sicherheitsrichtlinie bestimmt, welche Verschlüsselungen und Protokolle während der SSL-Aushandlungen zwischen einem Client und einem Load Balancer unterstützt werden. Sie können Ihre Classic Load Balancer so konfigurieren, dass sie entweder vordefinierte oder benutzerdefinierte Sicherheitsrichtlinien verwenden.

Beachten Sie, dass ein von AWS Certificate Manager (ACM) bereitgestelltes Zertifikat einen öffentlichen RSA-Schlüssel enthält. Daher müssen Sie eine Cipher Suite (Verschlüsselungssammlung) zu Ihrer Sicherheitsrichtlinie hinzufügen, die RSA verwendet, wenn Sie ein Zertifikat von ACM verwenden, da andernfalls die TLS-Verbindung fehlschlägt.

Vordefinierte Sicherheitsrichtlinien

Die Namen der neuesten vordefinierten Sicherheitsrichtlinien enthalten Informationen basierend auf dem Jahr und Monat, in dem sie veröffentlicht wurden. Die vordefinierte Standardsicherheitsrichtlinie ist beispielsweise `ELBSecurityPolicy-2016-08`. Jedes Mal, wenn eine neue vordefinierte Sicherheitsrichtlinie veröffentlicht wird, können Sie Ihre Konfiguration aktualisieren, um diese zu verwenden.

Weitere Informationen über die Protokolle und Verschlüsselungen für die vordefinierten Sicherheitsrichtlinien finden Sie unter Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer.

Benutzerdefinierte Sicherheitsrichtlinien

Sie können eine benutzerdefinierte Aushandlungskonfiguration mit den benötigten Verschlüsselungen und Protokollen erstellen. Beispielsweise erfordern einige Sicherheits-Compliance-Standards (z. B. PCI, SOC usw.) bestimmte Protokolle und Verschlüsselungen von Clients, um sicherzustellen, dass die Sicherheitsstandards erfüllt werden. In solchen Fällen können Sie eine benutzerdefinierte Sicherheitsrichtlinie erstellen, um diese Standards zu erfüllen.

Weitere Informationen zum Erstellen einer benutzerdefinierten Sicherheitsrichtlinie finden Sie unter Aktualisieren der SSL-Aushandlungskonfiguration Ihres Classic Load Balancers.

SSL-Protokolle

Das SSL-Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her und stellt sicher, dass alle Daten, die zwischen dem Client und Ihrem Load Balancer übertragen werden, privat sind.

Secure Sockets Layer (SSL) und Transport Layer Security (TLS) sind kryptografische Protokolle, die für die Verschlüsselung vertraulicher Daten über unsichere Netzwerke wie das Internet verwendet werden. Das TLS-Protokoll ist eine neuere Version des SSL-Protokolls. In der Dokumentation zu Elastic Load Balancing bezeichnen wir sowohl SSL- als auch TLS-Protokolle als SSL-Protokoll.

Empfohlenes Protokoll

Wir empfehlen TLS 1.2, das in der vordefinierten Sicherheitsrichtlinie ELBSecurity Policy-TLS-1-2-2017-01 verwendet wird. Sie können TLS 1.2 auch in Ihren benutzerdefinierten Sicherheitsrichtlinien verwenden. Die Standard-Sicherheitsrichtlinie unterstützt sowohl TLS 1.2 als auch frühere Versionen von TLS und ist daher weniger sicher als Policy-TLS-1-2-2017-01. ELBSecurity

Veraltete Protokolle

Wenn Sie das SSL-2.0-Protokoll in einer benutzerdefinierten Richtlinie aktiviert haben, empfehlen wir, dass Sie Ihre Sicherheitsrichtlinie auf eine der vordefinierten Sicherheitsrichtlinien aktualisieren.

Präferenz für die Serverreihenfolge

Elastic Load Balancing unterstützt die Option Präferenz für die Serverreihenfolge für das Aushandeln von Verbindungen zwischen einem Client und einem Load Balancer. Während der SSL-Verbindungsaushandlung präsentieren der Client und der Load Balancer eine Liste von Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Standardmäßig wird für die SSL-Verbindung die erste Verschlüsselung auf der Liste des Clients ausgewählt, die mit einem der Verschlüsselungsverfahren des Load Balancers übereinstimmt. Wenn der Load Balancer zur Unterstützung der Präferenz für die Serverreihenfolge konfiguriert ist, wählt der Load Balancer die erste Verschlüsselung in der Liste aus, die auch in der Client-Verschlüsselungsliste enthalten ist. Auf diese Weise wird sichergestellt, dass der Load Balancer bestimmt, welche Verschlüsselung für die SSL-Verbindung verwendet wird. Wenn Sie die Präferenz für die Serverreihenfolge nicht aktivieren, wird die vom Client angebotene Reihenfolge der Verschlüsselung zum Aushandeln der Verbindungen zwischen dem Client und dem Load Balancer verwendet.

SSL-Verschlüsselungsverfahren

Ein SSL-Verschlüsselungsverfahren ist ein Algorithmus, der eine kodierte Nachricht mithilfe von Verschlüsselungsschlüsseln erstellt. SSL-Protokolle verwenden mehrere SSL-Verschlüsselungsverfahren zum Verschlüsseln von Daten über das Internet.

Beachten Sie, dass ein von AWS Certificate Manager (ACM) bereitgestelltes Zertifikat einen öffentlichen RSA-Schlüssel enthält. Daher müssen Sie eine Cipher Suite (Verschlüsselungssammlung) zu Ihrer Sicherheitsrichtlinie hinzufügen, die RSA verwendet, wenn Sie ein Zertifikat von ACM verwenden, da andernfalls die TLS-Verbindung fehlschlägt.

Elastic Load Balancing unterstützt die folgenden Verschlüsselungen für die Verwendung mit Classic Load Balancern. Ein Teil dieser Verschlüsselungen wird von den vordefinierten SSL-Richtlinien verwendet. Alle diese Verschlüsselungen sind für die Verwendung in einer benutzerdefinierten Richtlinie verfügbar. Wir empfehlen, dass Sie nur die Verschlüsselungen in der Standardsicherheitsrichtlinie (mit einem Sternchen gekennzeichnet) verwenden. Viele der anderen Verschlüsselungen sind nicht sicher und erfolgen auf eigenes Risiko.

Verschlüsselungen

- ECDHE-ECDSA- -GCM- * AES128 SHA256
- ECDHE-RSA- AES128 -GCM- * SHA256

- ECDHE-ECDSA- AES128 - * SHA256
- ECDHE-RSA- AES128 - * SHA256
- AES128ECDHE-ECDSA-SHA *
- AES128ECDHE-RSA-SHA *
- AES128DHE-RSA-SHA
- ECDHE-ECDSA- -GCM- * AES256 SHA384
- ECDHE-RSA- AES256 -GCM- * SHA384
- ECDHE-ECDSA- AES256 - * SHA384
- ECDHE-RSA- AES256 - * SHA384
- ECDHE-RSA- AES256 -SHA *
- AES256ECDHE-ECDSA-SHA *
- AES128-GCM- * SHA256
- AES128-SHA256 *
- AES128-SCHA *
- AES256-GCM- * SHA384
- AES256-SHA256 *
- AES256-SCHA *
- DHE-DSS-SHA AES128
- CAMELLIA128-SCHA
- EDH-RSA-DES-SHA CBC3
- DES- CBC3 -SHA
- ECDHE-RSA-SHA RC4
- RC4-SCHA
- ECDHE-ECDSA- -SHA RC4
- DHE-DSS-GCM- AES256 SHA384
- DHE-RSA- AES256 -GCM- SHA384
- DHE-RSA- AES256 - SHA256
- DHE-DSS- AES256 - SHA256
- AES256DHE-RSA-SHA

- AES256DHE-DSS-SHA
- CAMELLIA256DHE-RSA-SHA
- CAMELLIA256DHE-DSS-SHA
- CAMELLIA256-SCHA
- EDH-DSS-DES-SHA CBC3
- AES128DHE-DSS-GCM- SHA256
- DHE-RSA- AES128 -GCM- SHA256
- DHE-RSA- AES128 - SHA256
- DHE-DSS- AES128 - SHA256
- CAMELLIA128DHE-RSA-SHA
- CAMELLIA128DHE-DSS-SHA
- ADH- AES128 -GCM- SHA256
- ADH- -SHA AES128
- ADH- - AES128 SHA256
- ADH- AES256 -GCM- SHA384
- ADH- -SHA AES256
- ADH- - AES256 SHA256
- ADH- CAMELLIA128 -SHA
- ADH- -SHA CAMELLIA256
- ADH-DES-SHA CBC3
- ADH-DES-CBC-SHA
- ADH- - RC4 MD5
- ADH-SEED-SHA
- DES-CBC-SHA
- DHE-DSS-SEED-SHA
- DHE-RSA-SEED-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- IDEA-CBC-SHA
- RC4-MD5

- SEED-SHA
- DES- CBC3 - MD5
- DES-CBC- MD5
- RC2-CBC- MD5
- PSK- -CBC-SHA AES256
- PSK-3DES-EDE-CBC-SHA
- KRB5-DES- CBC3 -SHA
- KRB5-DES- - CBC3 MD5
- PSK- -CBC-SHA AES128
- PSK- RC4 -SHA
- KRB5- -SCHA RC4
- KRB5-RC4-MD5
- KRB5-DES-CBC-SHA
- KRB5-DES-CBC- MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-ADH-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP- -CBC- RC2 MD5
- EXP- - -CBC-SHA KRB5 RC2
- EXP- KRB5 -DES-CBC-SHA
- EXP- - -CBC- KRB5 RC2 MD5
- EXP- -DES-CBC- KRB5 MD5
- RC4EXP-ADH- - MD5
- EXP- - RC4 MD5
- EXP- - -SHA KRB5 RC4
- EXP- - - KRB5 RC4 MD5

* Dies sind die Chiffren, die in der Standardsicherheitsrichtlinie Policy-2016-08 enthalten sind.
ELBSecurity

Cipher Suite für Back-End-Verbindungen

Classic Load Balancers verwendet eine statische Verschlüsselungssuite für Back-End-Verbindungen. Wenn Ihr Classic Load Balancer und registrierte Instances keine Verbindung aushandeln können, fügen Sie eine der folgenden Chiffren hinzu.

- AES256-GCM- SHA384
- AES256-SHA256
- AES256-SCHA
- CAMELLIA256-SCHA
- AES128-GCM- SHA256
- AES128-SHA256
- AES128-SCHA
- CAMELLIA128-SCHA
- RC4-SCHA
- DES-SHA CBC3
- DES-CBC-SHA
- DHE-DSS-GCM- AES256 SHA384
- DHE-RSA- AES256 -GCM- SHA384
- DHE-RSA- AES256 - SHA256
- DHE-DSS- AES256 - SHA256
- AES256DHE-RSA-SHA
- AES256DHE-DSS-SHA
- CAMELLIA256DHE-RSA-SHA
- CAMELLIA256DHE-DSS-SHA
- AES128DHE-DSS-GCM- SHA256
- DHE-RSA- AES128 -GCM- SHA256
- DHE-RSA- AES128 - SHA256
- DHE-DSS- AES128 - SHA256
- AES128DHE-RSA-SHA
- AES128DHE-DSS-SHA
- CAMELLIA128DHE-RSA-SHA

- CAMELLIA128DHE-DSS-SHA
- CBC3EDH-RSA-DES-SHA
- CBC3EDH-DSS-DE-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA

Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer

Sie können eine der vordefinierten Sicherheitsrichtlinien für Ihre HTTPS/SSL-Listener auswählen. Sie können eine der `ELBSecurityPolicy-TLS`-Richtlinien zur Erfüllung von Compliance- und Sicherheitsstandards verwenden, welche die Deaktivierung bestimmter TLS-Protokollversionen erfordern. Alternativ können Sie eine benutzerdefinierte Sicherheitsrichtlinie erstellen. Weitere Informationen finden Sie unter Aktualisieren der SSL-Aushandlungskonfiguration.

Die RSA- und DSA-basierten Verschlüsselungen gelten speziell für den Signaturalgorithmus zum Erstellen von SSL-Zertifikaten. Stellen Sie sicher, dass Sie ein SSL-Zertifikat mit dem Signaturalgorithmus erstellen, der auf Verschlüsselungen basiert, die für Ihre Sicherheitsrichtlinie aktiviert sind.

Wenn Sie eine Richtlinie auswählen, für die Präferenz für die Serverreihenfolge aktiviert ist, verwendet der Load Balancer die Verschlüsselungen in der Reihenfolge, in der sie hier angegeben sind, um die Verbindungen zwischen dem Client und dem Load Balancer auszuhandeln. Andernfalls verwendet der Load Balancer die Verschlüsselungen in der Reihenfolge, in der sie vom Client angeboten werden.

In den folgenden Abschnitten werden die neuesten vordefinierten Sicherheitsrichtlinien für Classic Load Balancer beschrieben, einschließlich der aktivierten SSL-Protokolle und SSL-Verschlüsselungen. Sie können die vordefinierten Richtlinien auch mit dem Befehl beschreiben. describe-load-balancer-policies

> **Tip**
>
> Diese Informationen gelten nur für Classic Load Balancers. Informationen, die für andere Load Balancer gelten, finden Sie unter Sicherheitsrichtlinien für Ihren Application Load Balancer und Sicherheitsrichtlinien für Ihren Network Load Balancer.

Inhalt

Protokolle nach Richtlinien

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

Sicherheitsrichtlinien	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS-1-2-2017-01	Ja	Nein	Nein
ELBSecurityRichtlinie-TLS-1-1-2017-01	Ja	Ja	Nein
ELBSecurityPolitik-2016-08	Ja	Ja	Ja
ELBSecurityPolitik-2015-05	Ja	Ja	Ja
ELBSecurityPolitik-2015-03	Ja	Ja	Ja
ELBSecurityPolitik-2015-02	Ja	Ja	Ja

Chiffren nach Richtlinien

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

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

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

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik 2015-05	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA • DES-SHA CBC3

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityRichtlinie 2015-03	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA • DHE-RSA-SHA AES128 • AES128DHE-DSS-SHA • CBC3DES-SHA

Sicherheitsrichtlinie	Verschlüsselungen
ELBSecurityPolitik 2015-02	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES128 - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA-SHA AES128 • ECDHE-RSA-SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDHE-RSA- AES256 -GCM- SHA384 • ECDHE-ECDSA- AES256 - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA-SHA AES256 • ECDHE-RSA-SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SCHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SCHA • DHE-RSA-SHA AES128 • AES128DHE-DSS-SHA

Richtlinien nach Chiffre

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

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-ECDSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c02b
OpenSSL — ECDHE-RSA-AES 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c02f
OpenSSL — ECDHE-ECDSA-AES 128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c023
OpenSSL — ECDHE-RSA-AES 128-SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01	c027

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	
OpenSSL — 128-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c009
OpenSSL — 128-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c013
OpenSSL — ECDHE-ECDSA-AES 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c02c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — ECDHE-RSA-AES 256-GCM- SHA384 IANA — TLS_ECCHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c030
OpenSSL — ECDHE-ECDSA-AES 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c024
OpenSSL — ECDHE-RSA-AES 256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c028

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — 256-SHA ECDHE-ECDSA-AES IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c014
OpenSSL — 256-SHA ECDHE-RSA-AES IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	c00a
OpenSSL — AES128 -GCM- SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	9c

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — - AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	3c
OpenSSL — -SHA AES128 IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	2f
OpenSSL — AES256 -GCM- SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	9d

Name der Chiffre	Sicherheitsrichtlinien	Verschlüsselungssuite
OpenSSL — - AES256 SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityRichtlinie-TLS-1-2-2017-01 • ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	3d
OpenSSL — -SHA AES256 IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityRichtlinie-TLS-1-1-2017-01 • ELBSecurityPolitik-2016-08 • ELBSecurityPolitik-2015-05 • ELBSecurityPolitik-2015-03 • ELBSecurityPolitik-2015-02	35
OpenSSL — 128-SHA DHE-RSA-AES IANA — TLS_DHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie 2015-03 • ELBSecurityPolitik-2015-02	33
OpenSSL — 128-SHA DHE-DSS-AES IANA — TLS_DHE_DSS_WITH_AES_128_CBC_SHA	• ELBSecurityRichtlinie 2015-03 • ELBSecurityPolitik-2015-02	32
OpenSSL — DES-SHA CBC3 IANA — TLS_RSA_WITH_3DES_EDE_CBC_SHA	• ELBSecurityRichtlinie 2015-05 • ELBSecurityPolitik-2015-03	0a

Erstellen eines Classic Load Balancers mit einem HTTPS-Listener

Ein Load Balancer nimmt Anfragen von Clients entgegen und verteilt sie auf die EC2 Instances, die beim Load Balancer registriert sind.

Sie können einen Load Balancer erstellen, der die Ports HTTP (80) und HTTPS (443) überwacht. Wenn Sie angeben, dass der HTTPS-Listener Anforderungen an die Instances auf Port 80 sendet, beendet der Load Balancer die Anforderungen und die Kommunikation über den Load Balancer an die Instances ist nicht verschlüsselt. Wenn der HTTPS-Listener Anforderungen an die Instances auf Port 443 sendet, ist die Kommunikation über den Load Balancer an die Instances verschlüsselt.

Wenn Ihr Load Balancer eine verschlüsselte Verbindung verwendet, um mit den Instances zu kommunizieren, können Sie optional die Authentifizierung der Instances aktivieren. Auf diese Weise wird sichergestellt, dass der Load Balancer mit einer Instance nur dann kommuniziert, wenn der öffentliche Schlüssel mit dem angegebenen Schlüssel, den Sie zu diesem Zweck auf dem Load Balancer angegeben haben, übereinstimmt.

Weitere Informationen über das Hinzufügen von HTTPS-Listenern zu einem vorhandenen Load Balancer finden Sie unter Konfigurieren eines HTTPS-Listeners für Ihren Classic Load Balancer.

Inhalt

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Führen Sie die Schritte unter Empfehlungen für Ihre VPC aus.
- Starten Sie die EC2 Instances, die Sie bei Ihrem Load Balancer registrieren möchten. Die Sicherheitsgruppen für diese Instances müssen den Datenverkehr aus dem Load Balancer zulassen.
- Die EC2 Instances müssen auf das Ziel der Zustandsprüfung mit dem HTTP-Statuscode 200 antworten. Weitere Informationen finden Sie unter Zustandsprüfungen für die Instances für Ihren Classic Load Balancer.

- Wenn Sie die Keep-Alive-Option auf Ihren EC2 Instances aktivieren möchten, empfehlen wir Ihnen, die Keep-Alive-Einstellungen auf mindestens die Leerlauf-Timeout-Einstellungen Ihres Load Balancers festzulegen. Wenn Sie sicherstellen möchten, dass der Load Balancer für das Schließen von Verbindungen mit Ihrer Instance zuständig ist, stellen Sie die Keepalive-Zeit auf der Instance höher als das Load Balancer-Leerlaufzeitlimit ein. Weitere Informationen finden Sie unter Konfigurieren des Leerlaufverbindungszeitlimits für Ihren Classic Load Balancer.
- Wenn Sie einen sicheren Listener erstellen, müssen Sie ein SSL-Zertifikat auf dem Load Balancer Server bereitstellen. Der Load Balancer verwendet das Zertifikat zum Beenden und entschlüsselt dann Anforderungen vor der Übermittlung an die Instances. Wenn Sie nicht über ein SSL-Zertifikat verfügen, können Sie eins erstellen. Weitere Informationen finden Sie unter SSL/TLS-Zertifikate für Classic Load Balancer.

Erstellen Sie mithilfe der Konsole einen HTTPS-Load Balancer

In diesem Beispiel konfigurieren Sie zwei Listener für Ihren Load Balancer. Der erste Listener akzeptiert HTTP-Anforderungen auf Port 80 und sendet diese über HTTP auf Port 80 an die Instances. Der zweite Listener akzeptiert HTTPS-Anforderungen auf Port 443 und sendet diese mittels HTTP auf Port 80 (oder unter Verwendung von HTTPS auf Port 443, wenn Sie Backend-Instance-Authentifizierung konfigurieren möchten) an die Instances.

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Er wird mit einem Protokoll und einem Port für Frontend-Verbindungen (Client zu Load Balancer) sowie einem Protokoll und einem Port für Backend-Verbindungen (Load Balancer zu Instance) konfiguriert. Weitere Informationen zu den von Elastic Load Balancing unterstützten Ports, Protokollen und Listener-Konfigurationen finden Sie unter Listener für Ihren Classic Load Balancer.

So erstellen Sie Ihren sicheren Classic Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste eine Region für Ihren Load Balancer aus. Achten Sie darauf, dieselbe Region auszuwählen, die Sie für Ihre EC2 Instances ausgewählt haben.
3. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
4. Wählen Sie Load Balancer erstellen aus.
5. Erweitern Sie den Abschnitt Classic Load Balancer und wählen Sie dann Create (Erstellen) aus.
6. Basiskonfiguration

a. Geben Sie im Feld Load balancer name (Name des Load Balancers) einen Namen für Ihren Load Balancer ein.

   Der Name des Classic Load Balancers muss innerhalb Ihrer Gruppe mit Classic Load Balancern für die Region eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen sowie Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.

b. Wählen Sie für Scheme (Schema) die Option Internet-facing (Internet verbunden) aus.

7. Netzwerkzuordnung

   a. Wählen Sie im Feld VPC die VPC aus, die Sie für Ihre Instances verwendet haben.

   b. Wählen Sie für Mappings (Zuordnungen) zunächst eine Availability Zone und dann ein öffentliches Subnetz aus den verfügbaren Subnetzen aus. Sie können nur ein Subnetz pro Availability Zone auswählen. Zur Verbesserung der Verfügbarkeit Ihrer Load Balancer wählen Sie mehr als eine Availability Zone und ein Subnetz aus.

8. Sicherheitsgruppen

   • Wählen Sie für Security groups (Sicherheitsgruppen) eine vorhandene Sicherheitsgruppe aus, die so konfiguriert ist, dass sie den erforderlichen HTTP-Verkehr auf Port 80 und HTTPS-Verkehr auf Port 443 zulässt.

     Wenn keine vorhanden ist, können Sie eine neue Sicherheitsgruppe mit den erforderlichen Regeln erstellen.

9. Listener und Routing

   a. Behalten Sie die Standardeinstellungen für den Standard-Listener bei und wählen Sie Add listener (Listener hinzufügen) aus.

   b. Wählen Sie für Listener auf dem neuen Listener `HTTPS` als Protokoll aus, und der Port wird auf `443` aktualisiert. Standardmäßig verwendet Instance das `HTTP`-Protokoll auf dem Port `80`.

   c. Wenn eine Backend-Authentifizierung erforderlich ist, ändern Sie das Instance-Protokoll auf `HTTPS`. Auf diese Weise wird auch der Instance-Port auf `443` aktualisiert

10. Secure listener settings (Sichere Listener-Einstellungen)

    Wenn Sie HTTPS oder SSL für Ihre Frontend-Listener verwenden, müssen Sie ein SSL-Zertifikat auf dem Load Balancer bereitstellen. Der Load Balancer verwendet das Zertifikat, um die

Verbindung zu beenden und dann Anfragen von Clients zu entschlüsseln, bevor er sie an die Instances sendet. Sie müssen auch eine Sicherheitsrichtlinie angeben. Elastic Load Balancing bietet Sicherheitsrichtlinien mit vordefinierten SSL-Aushandlungskonfigurationen, oder Sie können Ihre eigenen benutzerdefinierten Sicherheitsrichtlinien erstellen. Wenn Sie HTTPS/SSL für die Backend-Verbindung konfiguriert haben, können Sie die Authentifizierung Ihrer Instances aktivieren.

a. Als Sicherheitsrichtlinie empfehlen wir, immer die neueste vordefinierte Sicherheitsrichtlinie zu verwenden oder eine benutzerdefinierte Richtlinie zu erstellen. Siehe Aktualisieren der SSL-Aushandlungskonfiguration.

b. Für Default SSL/TLS certificate (Standard-SSL-/TLS-Zertifikat) sind die folgenden Optionen verfügbar:

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

c. (Optional) Wenn Sie den HTTPS-Listener für die Kommunikation mit den Instances über eine verschlüsselte Verbindung eingerichtet haben, können Sie optional die Authentifizierung der Instances unter Backend authentication certificate (Backend-Authentifizierungszertifikat) einrichten.

> **Note**
>
> Wenn Sie den Abschnitt Backend authentication certificate (Backend-Authentifizierungszertifikat) nicht sehen, kehren Sie zu Listeners and routing (Listeners und Routing) zurück und wählen Sie HTTPS als Protokoll für Instance aus.

i. Geben Sie für Certificate name den Namen des öffentlichen Schlüsselzertifikats ein.

ii. Kopieren Sie für Certificate Body (PEM encoded) (Zertifizierungsstelle (PEM-codiert)) den Inhalt des Zertifikats und fügen Sie ihn ein. Der Load Balancer kommuniziert mit einer Instanz nur dann, wenn der öffentliche Schlüssel diesem Schlüssel entspricht.

iii. Um ein weiteres Zertifikat hinzuzufügen, wählen Sie Add new backend certificate (Neues Backend-Zertifikat hinzufügen). Das Limit liegt bei fünf.

11. Health checks (Zustandsprüfungen)

    a. Wählen Sie im Abschnitt Ping target (Ping-Ziel) ein Ping Protocol (Ping-Protokoll) und einen Ping Port (Ping-Port) aus. Ihre EC2 Instances müssen Datenverkehr über den angegebenen Ping-Port akzeptieren.

    b. Stellen Sie für Ping Port sicher, dass der Port `80` ist.

    c. Ersetzen Sie den Standardwert für Ping Path (Ping-Pfad) durch einen Schrägstrich (`/`). Dadurch wird Elastic Load Balancing angewiesen, Zustandsprüfungsanfragen an die Standardstartseite Ihres Webservers, z. B. `index.html`, zu senden.

    d. Verwenden Sie für die Advanced health check settings (Einstellungen für erweiterte Zustandsprüfungen) die Standardwerte.

12. Instances

    a. Wählen Sie Add instances (Instances hinzufügen) aus, um den Bildschirm zur Instance-Auswahl aufzurufen.

    b. Unter Available instances (Verfügbare Instances) können Sie basierend auf den zuvor gewählten Netzwerkeinstellungen aus den aktuellen Instances auswählen, die für den Load Balancer verfügbar sind.

    c. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Confirm (Bestätigen) aus, um die zu registrierenden Instances zum Load Balancer hinzuzufügen.

13. Attribute

    - Behalten Sie für Enable cross-zone load balancing (Zonenübergreifendes Load Balancing aktivieren), Enable connection draining (Connection Draining aktivieren) und Timeout (draining interval) (Timeout (Draining-Intervall)) die Standardwerte bei.

14. Load balancer tags (optional) (Load-Balancer-Tags (optional))

    a. Das Feld Key (Schlüssel) ist ein Pflichtfeld.

b. Das Feld Value (Wert) ist optional.

c. Um ein weiteres Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) aus und geben Sie dann Ihre Werte in das Feld Key (Schlüssel) und optional in das Feld Value (Wert) ein.

d. Um ein vorhandenes Tag zu entfernen, wählen Sie neben dem zu entfernenden Tag die Option Remove (Entfernen).

15. Summary and creation (Zusammenfassung und Erstellung)

    a. Wenn Sie Einstellungen ändern müssen, wählen Sie neben der Einstellung, die geändert werden muss, Edit (Bearbeiten) aus.

    b. Wenn Sie mit allen in der Zusammenfassung angezeigten Einstellungen zufrieden sind, wählen Sie Create load balancer (Load Balancer erstellen) aus, um mit der Erstellung Ihres Load Balancers zu beginnen.

    c. Wählen Sie auf der letzten Erstellungsseite Load Balancer anzeigen aus, um Ihren Load Balancer in der EC2 Amazon-Konsole anzuzeigen.

16. Verify

    a. Wählen Sie den neuen Load Balancer aus.

    b. Überprüfen Sie auf der Registerkarte Target instances (Ziel-Instances) die Spalte Health status (Zustandsstatus). Sobald mindestens eine Ihrer EC2 Instances in Betrieb ist, können Sie Ihren Load Balancer testen.

    c. Kopieren Sie im Abschnitt Details den DNS name (DNS-Namen) des Load Balancers, der etwa wie `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com` aussehen würde.

    d. Fügen Sie den DNS name (DNS-Namen) Ihres Load Balancers in das Adressfeld eines öffentlichen Webbrowsers mit Internetanschluss ein. Wenn Ihr Load Balancer korrekt funktioniert, sehen Sie die Standardseite Ihres Servers.

17. Delete (optional) (Löschen (optional))

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

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

    c. Wählen Sie den Load Balancer aus.

d. Wählen Sie den Load Balancer aus und klicken Sie auf Actions (Aktionen) und dann auf Delete load balancer (Load Balancer löschen).

e. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie `confirm` ein und wählen Sie dann Delete (Löschen) aus.

f. Nachdem Sie einen Load Balancer gelöscht haben, werden die EC2 Instances, die beim Load Balancer registriert wurden, weiter ausgeführt. Ihnen wird jede teilweise oder ganze Stunde in Rechnung gestellt, in der sie weiterlaufen. Wenn Sie eine EC2 Instance nicht mehr benötigen, können Sie sie beenden oder beenden, um zusätzliche Kosten zu vermeiden.

Erstellen Sie einen HTTPS-Load Balancer mit dem AWS CLI

Verwenden Sie die folgenden Anweisungen zum Erstellen eines HTTPS/SSL-Load Balancers mithilfe der AWS CLI.

Aufgaben

Schritt 1: Konfigurieren von Listenern

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Er wird mit einem Protokoll und einem Port für Frontend-Verbindungen (Client zu Load Balancer) sowie einem Protokoll und einem Port für Backend-Verbindungen (Load Balancer zu Instance) konfiguriert. Weitere Informationen zu den von Elastic Load Balancing unterstützten Ports, Protokollen und Listener-Konfigurationen finden Sie unter Listener für Ihren Classic Load Balancer.

In diesem Beispiel konfigurieren Sie zwei Listener für Ihren Load Balancer, indem Sie die Ports und Protokolle für die Frontend- und Backend-Verbindungen angeben. Der erste Listener akzeptiert HTTP-Anforderungen auf Port 80 und sendet die Anforderungen über HTTP auf Port 80 an

die Instances. Der zweite Listener akzeptiert HTTPS-Anforderungen auf Port 443 und sendet Anforderungen über HTTP auf Port 80 an Instances.

Da der zweite Listener HTTPS für die Frontend-Verbindung verwendet, müssen ein SSL-Serverzertifikat auf dem Load Balancer bereitstellen. Der Load Balancer verwendet das Zertifikat zum Beenden und entschlüsselt dann Anforderungen vor der Übermittlung an die Instances.

So konfigurieren Sie Listener für Ihren Load Balancer

1. Rufen Sie den Amazon-Ressourcennamen (ARN) des SSL-Zertifikats ab. Zum Beispiel:

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

   ```
   arn:aws:iam::123456789012:server-certificate/my-server-certificate
   ```

2. Verwenden Sie den folgenden create-load-balancerBefehl, um den Load Balancer mit den beiden Listenern zu konfigurieren:

   ```
   aws elb create-load-balancer --load-balancer-name my-load-balancer --listeners
    "Protocol=http,LoadBalancerPort=80,InstanceProtocol=http,InstancePort=80"
    "Protocol=https,LoadBalancerPort=443,InstanceProtocol=http,InstancePort=80,SSLCertificateI
    --availability-zones us-west-2a
   ```

   Nachfolgend finden Sie eine Beispielantwort:

   ```
   {
     "DNSName": "my-loadbalancer-012345678.us-west-2.elb.amazonaws.com"
   }
   ```

3. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um die Details Ihres Load Balancers anzuzeigen:

   ```
   aws elb describe-load-balancers --load-balancer-name my-load-balancer
   ```

Schritt 2: Konfigurieren der SSL-Sicherheitsrichtlinie

Sie können eine der vordefinierten Sicherheitsrichtlinien auswählen oder Ihre eigene benutzerdefinierte Sicherheitsrichtlinie erstellen. Andernfalls konfiguriert Elastic Load Balancing Ihren Load Balancer mit der standardmäßigen vordefinierten Sicherheitsrichtlinie `ELBSecurityPolicy-2016-08`. Weitere Informationen finden Sie unter SSL-Aushandlungskonfigurationen für Classic Load Balancer.

So stellen Sie sicher, dass der Load Balancer der Standardsicherheitsrichtlinie zugeordnet ist

Verwenden Sie den folgenden describe-load-balancers-Befehl:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Nachfolgend finden Sie eine Beispielantwort. Beachten Sie, dass `ELBSecurityPolicy-2016-08` dem Load Balancer auf Port 443 zugeordnet ist.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
```

```
                }
            ],
            ...
        }
    ]
}
```

Wenn Sie möchten, können Sie die SSL-Sicherheitsrichtlinie für Ihren Load Balancer anstelle der Standardsicherheitsrichtlinie verwenden.

(Optional) Verwendung einer vordefinierten SSL-Sicherheitsrichtlinie

1. Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um die Namen der vordefinierten Sicherheitsrichtlinien aufzulisten:

   ```
   aws elb describe-load-balancer-policies
   ```

   Informationen über die Konfiguration mit vordefinierten Sicherheitsrichtlinien finden Sie unter Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer.

2. Verwenden Sie den folgenden create-load-balancer-policyBefehl, um eine SSL-Verhandlungsrichtlinie mithilfe einer der vordefinierten Sicherheitsrichtlinien zu erstellen, die Sie im vorherigen Schritt beschrieben haben:

   ```
   aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
   --policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
   --policy-attributes AttributeName=Reference-Security-
   Policy,AttributeValue=predefined-policy
   ```

3. (Optional) Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um zu überprüfen, ob die Richtlinie erstellt wurde:

   ```
   aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
   policy-name my-SSLNegotiation-policy
   ```

   Die Antwort enthält die Beschreibung der Richtlinie.

4. Verwenden Sie den folgenden Befehl set-load-balancer-policies-of-listener, um die Richtlinie auf dem Load Balancer-Port 443 zu aktivieren:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Der Befehl `set-load-balancer-policies-of-listener` ersetzt die aktuellen Richtlinien für den angegebenen Load Balancer-Port durch die angegebenen Richtlinien. Die Liste `--policy-names` muss alle zu aktivierenden Richtlinien enthalten. Wenn Sie eine Richtlinie auslassen, die derzeit aktiviert ist, wird sie deaktiviert.

5. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die Richtlinie aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Es folgt ein Beispiel für eine Antwort, die zeigt, dass die Richtlinie auf Port 443 aktiviert ist.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
```

```
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie erstellen, müssen Sie mindestens ein Protokoll und eine Verschlüsselung aktivieren. Die DSA- und RSA-Verschlüsselungen gelten speziell für den Signaturalgorithmus zum Erstellen von SSL-Zertifikaten. Wenn Sie bereits über ein SSL-Zertifikat verfügen, müssen Sie die Verschlüsselung aktivieren, mit der das Zertifikat erstellt wurde. Der Name der benutzerdefinierten Richtlinie darf nicht mit `ELBSecurityPolicy-` oder `ELBSample-` beginnen, da diese Präfixe für die Namen der vordefinierten Sicherheitsrichtlinien definiert sind.

(Optional) Verwendung einer benutzerdefinierten SSL-Sicherheitsrichtlinie

1. Verwenden Sie den create-load-balancer-policyBefehl, um eine SSL-Verhandlungsrichtlinie mithilfe einer benutzerdefinierten Sicherheitsrichtlinie zu erstellen. Zum Beispiel:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
 --policy-name my-SSLNegotiation-policy --policy-type-name
 SSLNegotiationPolicyType
 --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
 AttributeName=Protocol-TLSv1.1,AttributeValue=true
 AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
 AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

2. (Optional) Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um zu überprüfen, ob die Richtlinie erstellt wurde:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

   Die Antwort enthält die Beschreibung der Richtlinie.

3. Verwenden Sie den folgenden Befehl set-load-balancer-policies-of-listener, um die Richtlinie auf dem Load Balancer-Port 443 zu aktivieren:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Der Befehl `set-load-balancer-policies-of-listener` ersetzt die aktuellen Richtlinien für den angegebenen Load Balancer-Port durch die angegebenen Richtlinien. Die Liste `--policy-names` muss alle zu aktivierenden Richtlinien enthalten. Wenn Sie eine Richtlinie auslassen, die derzeit aktiviert ist, wird sie deaktiviert.

4. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die Richtlinie aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Es folgt ein Beispiel für eine Antwort, die zeigt, dass die Richtlinie auf Port 443 aktiviert ist.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
```

```
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Schritt 3: Konfigurieren der Backend-Instance-Authentifizierung (optional)

Wenn Sie HTTPS/SSL für die Backend-Verbindung eingerichtet haben, können Sie optional die Authentifizierung Ihrer Instances einrichten.

Wenn Sie Backend-Instance-Authentifizierung eingerichtet haben, erstellen Sie eine Richtlinie mit öffentlichem Schlüssel. Anschließend verwenden Sie diese Richtlinie mit öffentlichem Schlüssel zum Erstellen einer Backend-Instance-Authentifizierungsrichtlinie. Abschließend legen Sie den Instance-Port für das HTTPS-Protokoll der Backend-Instance-Authentifizierungsrichtlinie fest.

Der Load Balancer kommuniziert mit einer Instance nur dann, wenn der öffentliche Schlüssel, den die Instance dem Load Balancer bietet, einem öffentlichen Schlüssel in der Authentifizierungsrichtlinie für Ihren Load Balancer entspricht.

So konfigurieren Sie Backend-Instance-Authentifizierung

1. Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel abzurufen:

```
openssl x509 -in your X509 certificate PublicKey -pubkey -noout
```

2. Verwenden Sie den folgenden create-load-balancer-policyBefehl, um eine Richtlinie für öffentliche Schlüssel zu erstellen:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-PublicKey-policy \
--policy-type-name PublicKeyPolicyType --policy-attributes
 AttributeName=PublicKey,AttributeValue=MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
```

```
WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
3rrszlaEXAMPLE=
```

> **Note**
>
> Wenn Sie einen öffentlichen Schlüssel für `--policy-attributes` angeben, entfernen Sie die ersten und letzten Zeilen des öffentlichen Schlüssels (die Zeilen mit "`-----BEGIN PUBLIC KEY-----`" und "`-----END PUBLIC KEY-----`"). Der AWS CLI akzeptiert keine Leerzeichen in`--policy-attributes`.

3. Verwenden Sie den folgenden create-load-balancer-policyBefehl, um eine Authentifizierungsrichtlinie für Back-End-Instanzen mithilfe von `my-PublicKey-policy` zu erstellen.

```
aws elb create-load-balancer-policy --load-balancer-name my-
loadbalancer --policy-name my-authentication-policy --policy-type-
name BackendServerAuthenticationPolicyType --policy-attributes
 AttributeName=PublicKeyPolicyName,AttributeValue=my-PublicKey-policy
```

   Sie haben auch die Möglichkeit, verschiedene Richtlinien mit öffentlichem Schlüssel zu verwenden. Der Load Balancer versucht nacheinander alle Schlüssel. Wenn der von einer Instance angebotene öffentliche Schlüssel mit einem dieser öffentlichen Schlüssel übereinstimmt, ist die Instance authentifiziert.

4. Verwenden Sie den folgenden for-backend-server Befehl set-load-balancer-policies-, `my-authentication-policy` um den Instanzport für HTTPS festzulegen. In diesem Beispiel ist der Instance-Port 443.

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-
loadbalancer --instance-port 443 --policy-names my-authentication-policy
```

5. (Optional) Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um alle Richtlinien für Ihren Load Balancer aufzulisten:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer
```

6. (Optional) Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um Details der Richtlinie anzuzeigen:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-names my-authentication-policy
```

Schritt 4: Konfigurieren von Zustandsprüfungen (optional)

Elastic Load Balancing überprüft regelmäßig den Zustand jeder registrierten EC2 Instance auf der Grundlage der von Ihnen konfigurierten Integritätsprüfungen. Wenn Elastic Load Balancing eine fehlerhafte Instance erkennt, wird der Datenverkehr nicht mehr an diese Instance gesendet und stattdessen an die fehlerfreien Instances geleitet. Weitere Informationen finden Sie unter Zustandsprüfungen für die Instances für Ihren Classic Load Balancer.

Wenn Sie Ihren Load Balancer erstellen, verwendet Elastic Load Balancing die Standardeinstellungen für die Zustandsprüfungen. Wenn Sie möchten, können Sie die Zustandsprüfungskonfiguration für Ihren Load Balancer ändern, anstatt die Standardeinstellungen zu verwenden.

So konfigurieren Sie die Zustandsprüfungen für Ihre Instances

Verwenden Sie den folgenden configure-health-check-Befehl:

```
aws elb configure-health-check --load-balancer-name my-loadbalancer --health-check
 Target=HTTP:80/ping,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/ping",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    }
```

```
}
```

Schritt 5: EC2 Instanzen registrieren

Nachdem Sie Ihren Load Balancer erstellt haben, müssen Sie Ihre EC2 Instances beim Load Balancer registrieren. Sie können EC2 Instances aus einer einzelnen Availability Zone oder mehreren Availability Zones innerhalb derselben Region wie der Load Balancer auswählen. Weitere Informationen finden Sie unter Registrierte Instances pro Classic Load Balancer.

Verwenden Sie den Befehl register-instances-with-load-balancer wie folgt:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

Schritt 6: Überprüfen der Instances

Ihr Load Balancer kann verwendet werden, sobald sich eine der registrierten Instances im Status `InService` befindet.

Verwenden Sie den folgenden Befehl, um den Status Ihrer neu registrierten EC2 Instances zu überprüfen: describe-instance-health

```
aws elb describe-instance-health  --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "InstanceStates": [
        {
            "InstanceId": "i-4f8cf126",
            "ReasonCode": "N/A",
            "State": "InService",
            "Description": "N/A"
        },
        {
            "InstanceId": "i-0bb7ca62",
            "ReasonCode": "Instance",
            "State": "OutOfService",
            "Description": "Instance registration is still in progress"
        }
    ]
}
```

Wenn das Feld `State` für eine Instanz `OutOfService` ist, werden Ihre Instances immer noch registriert. Weitere Informationen finden Sie unter Fehlerbehebung beim Classic Load Balancer: Instance-Registrierung.

Nachdem der Status von mindestens einer Ihrer Instances `InService` ist, können Sie Ihren Load Balancer testen. Zum Testen des Load Balancers kopieren Sie den DNS-Namen des Load Balancers und fügen ihn in das Adressfeld eines mit dem Internet verbundenen Webbrowsers ein. Wenn Ihr Load Balancer verfügbar ist, sehen Sie die Standardseite Ihres HTTP-Servers.

Schritt 7: Löschen des Load Balancers (optional)

Wenn Sie den Load Balancer löschen, wird die Registrierung der zugehörigen EC2 Instances automatisch aufgehoben. Sobald der Load Balancer gelöscht ist, fallen keine weiteren Kosten für diesen Load Balancer mehr an. Die EC2 Instances werden jedoch weiterhin ausgeführt und es fallen weiterhin Gebühren für Sie an.

Verwenden Sie den folgenden delete-load-balancerBefehl, um Ihren Load Balancer zu löschen:

```
aws elb delete-load-balancer --load-balancer-name my-loadbalancer
```

Verwenden Sie den Befehl EC2 stop-instances, um Ihre Instances zu stoppen. Verwenden Sie den Befehl EC2 terminate-instances, um Ihre Instances zu beenden.

Konfigurieren eines HTTPS-Listeners für Ihren Classic Load Balancer

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Er wird mit einem Protokoll und einem Port für Frontend-Verbindungen (Client zu Load Balancer) sowie einem Protokoll und einem Port für Backend-Verbindungen (Load Balancer zu Instance) konfiguriert. Weitere Informationen zu den von Elastic Load Balancing unterstützten Ports, Protokollen und Listener-Konfigurationen finden Sie unter Listener für Ihren Classic Load Balancer.

Wenn Sie einen Load Balancer mit einem Listener haben, der HTTP-Anforderungen auf Port 80 akzeptiert, können Sie einen Listener hinzufügen, der HTTPS-Anforderungen auf Port 443 akzeptiert. Wenn Sie angeben, dass der HTTPS-Listener Anforderungen an die Instances auf Port 80 sendet, beendet der Load Balancer die SSL-Anforderungen und die Kommunikation über den Load Balancer an die Instances ist nicht verschlüsselt. Wenn der HTTPS-Listener Anforderungen an die Instances auf Port 443 sendet, ist die Kommunikation über den Load Balancer an die Instances verschlüsselt.

Wenn Ihr Load Balancer eine verschlüsselte Verbindung verwendet, um mit Instances zu kommunizieren, können Sie optional die Authentifizierung der Instances aktivieren. Auf diese Weise wird sichergestellt, dass der Load Balancer mit einer Instance nur dann kommuniziert, wenn der öffentliche Schlüssel mit dem angegebenen Schlüssel, den Sie zu diesem Zweck auf dem Load Balancer angegeben haben, übereinstimmt.

Weitere Informationen zum Erstellen eines neuen HTTPS-Listeners finden Sie unter Erstellen eines Classic Load Balancers mit einem HTTPS-Listener.

Inhalt

Voraussetzungen

Um die HTTPS-Unterstützung für einen HTTPS-Listener zu aktivieren, müssen Sie ein SSL-Zertifikat auf dem Load Balancer-Server bereitstellen. Der Load Balancer verwendet das Zertifikat zum Beenden und entschlüsselt dann Anforderungen vor der Übermittlung an die Instances. Wenn Sie nicht über ein SSL-Zertifikat verfügen, können Sie eins erstellen. Weitere Informationen finden Sie unter SSL/TLS-Zertifikate für Classic Load Balancer.

Hinzufügen eines HTTPS-Listeners mithilfe der Konsole

Sie können einen HTTPS-Listener zu einem vorhandenen Load Balancer hinzufügen.

Um Ihrem Load Balancer mithilfe der Konsole einen HTTPS-Listener hinzuzufügen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listeners (Listener) die Option Manage listeners (Listener verwalten) aus.
5. Wählen Sie auf der Seite Manage listeners (Listener verwalten) im Abschnitt Listeners (Listener) die Option Add listener (Listener hinzufügen) aus.
6. Wählen Sie für Listener protocol (Listener-Protokoll) die Option HTTPS aus.

   > **Important**
   >
   > Das standardmäßige Instance protocol (Instance-Protokoll) ist HTTP. Wenn Sie Backend-Instance-Authentifizierung einrichten möchten, ändern Sie das Instance protocol (Instance-Protokoll) in HTTPS.

7. Als Sicherheitsrichtlinie empfehlen wir, dass Sie die neueste vordefinierte Sicherheitsrichtlinie verwenden. Wenn Sie eine andere vordefinierte Sicherheitsrichtlinie verwenden möchten oder eine benutzerdefinierte Richtlinie erstellen müssen, finden Sie weitere Informationen unter Aktualisieren der SSL-Aushandlungskonfiguration.
8. Wählen Sie für Default SSL cert (Standard-SSL-Zertifikat) die Option Edit (Bearbeiten) und gehen Sie dann wie folgt vor:

   - Wenn Sie ein Zertifikat mit erstellt oder importiert haben AWS Certificate Manager, wählen Sie Aus ACM, wählen Sie das Zertifikat aus der Liste aus und klicken Sie dann auf Änderungen speichern.

     > **Note**
     >
     > Diese Option ist nur in den Regionen verfügbar, die AWS Certificate Manager unterstützen.

- Wenn Sie ein Zertifikat mit IAM importiert haben, wählen Sie From IAM (Aus IAM), wählen Sie das Zertifikat aus der Liste und wählen Sie dann Save changes (Änderungen speichern).
- Wenn Sie über ein SSL-Zertifikat verfügen, das in ACM importiert werden soll, wählen Sie Import und To ACM (In ACM) aus. Kopieren Sie den Inhalt der PEM-kodierten privaten Schlüsseldatei und fügen Sie ihn in das Feld Certificate private key (Privater Zertifikatsschlüssel) ein. Kopieren Sie den Inhalt der PEM-kodierten öffentlichen Schlüsselzertifikatdatei und fügen Sie ihn in das Feld Certificate body (Zertifikatstext) ein. Kopieren Sie den Inhalt der PEM-kodierten Zertifikatskettendatei und fügen Sie ihn in das Feld Certificate chain - optional (Zertifikats-Kette – optional) ein, es sei denn, Sie verwenden ein selbst signiertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.
- Wenn Sie ein SSL-Zertifikat zum Importieren haben, aber ACM in dieser Region nicht unterstützt wird, wählen Sie Import und To IAM (In ACM) aus. Geben Sie unter Certificate name (Zertifikatsname) den Namen des Zertifikats ein. Kopieren Sie den Inhalt der PEM-kodierten privaten Schlüsseldatei und fügen Sie ihn in das Feld Certificate private key (Privater Zertifikatsschlüssel) ein. Kopieren Sie den Inhalt der PEM-kodierten öffentlichen Schlüsselzertifikatdatei und fügen Sie ihn in das Feld Certificate body (Zertifikatstext) ein. Kopieren Sie den Inhalt der PEM-kodierten Zertifikatskettendatei und fügen Sie ihn in das Feld Certificate chain - optional (Zertifikats-Kette – optional) ein, es sei denn, Sie verwenden ein selbst signiertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.
- Wählen Sie Änderungen speichern aus.

9. Für Cookie stickiness (Cookie-Stickiness) ist die Standardeinstellung Disabled (Deaktiviert). Um dies zu ändern, wählen Sie Edit (Bearbeiten). Wenn Sie Generated by load balancer (Generiert vom Load Balancer) wählen, muss ein Expiration period (Ablaufzeitraum) angegeben werden. Wenn Sie Generated by application (Generiert von der Anwendung) wählen, muss ein Cookie name (Cookie-Name) angegeben werden. Nachdem Sie Ihre Auswahl getroffen haben, wählen Sie Save changes (Änderungen speichern).
10. (Optional) Wählen Sie Add listener (Listener hinzufügen) zum Hinzufügen zusätzlicher Listener.
11. Wählen Sie Save changes (Änderungen speichern) zum Hinzufügen der Listener, die Sie gerade konfiguriert haben.
12. (Optional) Um die Back-End-Instance-Authentifizierung für einen vorhandenen Load Balancer einzurichten, müssen Sie die AWS CLI oder eine API verwenden, da diese Aufgabe über die Konsole nicht unterstützt wird. Weitere Informationen finden Sie unter Konfigurieren der Backend-Instance-Authentifizierung.

Fügen Sie einen HTTPS-Listener hinzu, indem Sie AWS CLI

Sie können einen HTTPS-Listener zu einem vorhandenen Load Balancer hinzufügen.

Um Ihrem Load Balancer einen HTTPS-Listener hinzuzufügen, verwenden Sie AWS CLI

1. Rufen Sie den Amazon-Ressourcennamen (ARN) des SSL-Zertifikats ab. Zum Beispiel:

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

   ```
   arn:aws:iam::123456789012:server-certificate/my-server-certificate
   ```

2. Verwenden Sie den folgenden create-load-balancer-listenersBefehl, um Ihrem Load Balancer einen Listener hinzuzufügen, der HTTPS-Anfragen an Port 443 akzeptiert und die Anfragen über HTTP an die Instances auf Port 80 sendet:

   ```
   aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
   listeners
    Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTP,InstancePort=80,SSLCertificateId
   ```

   Wenn Sie die Backend-Instance-Authentifizierung einrichten möchten, verwenden Sie den folgenden Befehl, um einen Listener hinzuzufügen, der HTTPS-Anforderungen auf Port 443 akzeptiert und die Anforderungen an die Instances auf Port 443 mit HTTPS sendet:

   ```
   aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
   listeners
    Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTPS,InstancePort=443,SSLCertificate
   ```

3. (Optional) Sie können den folgenden describe-load-balancersBefehl verwenden, um die aktualisierten Details Ihres Load Balancers anzuzeigen:

   ```
   aws elb describe-load-balancers --load-balancer-name my-load-balancer
   ```

   Nachfolgend finden Sie eine Beispielantwort:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

4. (Optional) Ihr HTTPS-Listener wurde mithilfe der Standardsicherheitsrichtlinie erstellt. Wenn Sie eine andere vordefinierte Sicherheitsrichtlinie oder eine benutzerdefinierte Sicherheitsrichtlinie angeben möchten, verwenden Sie die Befehle create-load-balancer-policyund set-load-balancer-policies-of-listener. Weitere Informationen finden Sie unter Aktualisieren Sie die Konfiguration der SSL-Aushandlung mithilfe des AWS CLI.
5. (Optional) Verwenden Sie den Befehl -, um die Back-End-Instanzauthentifizierung einzurichten. set-load-balancer-policies for-backend-server Weitere Informationen finden Sie unter Konfigurieren der Backend-Instance-Authentifizierung.

Ersetzen des SSL-Zertifikats für Ihren Classic Load Balancer

Wenn Sie über einen HTTPS-Listener verfügen, haben Sie beim Erstellen des Listeners ein SSL-Serverzertifikat auf dem Load Balancer bereitgestellt. Jedes Zertifikat verfügt über einen Gültigkeitszeitraum. Sie müssen sicherstellen, dass Sie das Zertifikat erneuern oder ersetzen, bevor die Gültigkeitsdauer endet.

Zertifikate, die von Ihrem Load Balancer bereitgestellt AWS Certificate Manager und dort bereitgestellt werden, können automatisch erneuert werden. ACM versucht, die Zertifikate zu verlängern, bevor sie ablaufen. Weitere Informationen finden Sie unter Verwaltete Erneuerung im AWS Certificate Manager -Benutzerhandbuch. Wenn Sie ein Zertifikat in ACM importiert haben, müssen Sie das Ablaufdatum des Zertifikats überwachen und es vor dem Ablauf verlängern. Weitere Informationen finden Sie unter Importieren von Zertifikaten im AWS Certificate Manager -Benutzerhandbuch. Nachdem ein Zertifikat, das auf einem Load Balancer bereitgestellt ist, erneuert wurde, verwenden neue Anforderungen das erneuerte Zertifikat.

Um ein Zertifikat zu ersetzen, müssen Sie zunächst ein neues Zertifikat erstellen, indem Sie die gleichen Schritte ausführen, die Sie verwendet haben, als Sie das aktuelle Zertifikat erstellt haben. Dann können Sie das Zertifikat ersetzen. Nachdem ein Zertifikat, das auf einem Load Balancer bereitgestellt ist, ersetzt wurde, verwenden neue Anforderungen das neue Zertifikat.

Beachten Sie, dass sich das Erneuern oder Ersetzen eines Zertifikats nicht auf Anforderungen auswirkt, die bereits von einem Load Balancer-Knoten empfangen wurden und für die das Routing an ein funktionierendes Ziel aussteht.

Inhalt

Ersetzen des SSL-Zertifikats mithilfe der Konsole

Sie können das auf Ihrem Load Balancer bereitgestellte Zertifikat durch ein Zertifikat von ACM oder ein in IAM hochgeladenes Zertifikat ersetzen.

Um das SSL-Zertifikat für einen HTTPS-Load Balancer mithilfe der Konsole zu ersetzen

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

3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listeners (Listener) die Option Manage listeners (Listener verwalten) aus.
5. Suchen Sie auf der Seite Manage listeners (Listener verwalten) den Listener, der aktualisiert werden soll, wählen Sie unter Default SSL cert (Standard-SSL-Zertifikat) die Option Edit (Bearbeiten) aus und führen Sie einen der folgenden Schritte aus:

   - Wenn Sie ein Zertifikat mit erstellt oder importiert haben AWS Certificate Manager, wählen Sie Aus ACM, wählen Sie das Zertifikat aus der Liste aus und klicken Sie dann auf Änderungen speichern.

     > **Note**
     >
     > Diese Option ist nur in den Regionen verfügbar, die AWS Certificate Manager unterstützen.

   - Wenn Sie ein Zertifikat mit IAM importiert haben, wählen Sie From IAM (Aus IAM), wählen Sie das Zertifikat aus der Liste und wählen Sie dann Save changes (Änderungen speichern).
   - Wenn Sie über ein SSL-Zertifikat verfügen, das in ACM importiert werden soll, wählen Sie Import und To ACM (In ACM) aus. Kopieren Sie den Inhalt der PEM-kodierten privaten Schlüsseldatei und fügen Sie ihn in das Feld Certificate private key (Privater Zertifikatsschlüssel) ein. Kopieren Sie den Inhalt der PEM-kodierten öffentlichen Schlüsselzertifikatdatei und fügen Sie ihn in das Feld Certificate body (Zertifikatstext) ein. Kopieren Sie den Inhalt der PEM-kodierten Zertifikatskettendatei und fügen Sie ihn in das Feld Certificate chain - optional (Zertifikats-Kette – optional) ein, es sei denn, Sie verwenden ein selbst signiertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.
   - Wenn Sie ein SSL-Zertifikat zum Importieren haben, aber ACM in dieser Region nicht unterstützt wird, wählen Sie Import und To IAM (In ACM) aus. Geben Sie unter Certificate name (Zertifikatsname) den Namen des Zertifikats ein. Kopieren Sie den Inhalt der PEM-kodierten privaten Schlüsseldatei und fügen Sie ihn in das Feld Certificate private key (Privater Zertifikatsschlüssel) ein. Kopieren Sie den Inhalt der PEM-kodierten öffentlichen Schlüsselzertifikatdatei und fügen Sie ihn in das Feld Certificate body (Zertifikatstext) ein. Kopieren Sie den Inhalt der PEM-kodierten Zertifikatskettendatei und fügen Sie ihn in das Feld Certificate chain - optional (Zertifikats-Kette – optional) ein, es sei denn, Sie verwenden

ein selbst signiertes Zertifikat und es ist nicht wichtig, dass Browser das Zertifikat implizit akzeptieren.

- Wählen Sie Änderungen speichern aus.

Ersetzen des SSL-Zertifikats mithilfe der AWS CLI

Sie können das auf Ihrem Load Balancer bereitgestellte Zertifikat durch ein Zertifikat von ACM oder ein in IAM hochgeladenes Zertifikat ersetzen.

So ersetzen Sie ein SSL-Zertifikat mit einem Zertifikat von ACM

1. Verwenden Sie den folgenden Befehl request-certificate, um ein neues Zertifikat anzufordern:

```
aws acm request-certificate --domain-name www.example.com
```

2. Verwenden Sie den folgenden Befehl set-load-balancer-listener-ssl-certificate, um das Zertifikat festzulegen:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

So ersetzen Sie ein SSL-Zertifikat mit einem von IAM hochgeladenen Zertifikat

1. Wenn Sie über ein SSL-Zertifikat verfügen, aber es nicht hochgeladen haben, finden Sie weitere Informationen unter Hochladen von Serverzertifikaten im IAM-Benutzerhandbuch.
2. Verwenden Sie den folgenden get-server-certificateBefehl, um den ARN des Zertifikats abzurufen:

```
aws iam get-server-certificate --server-certificate-name my-new-certificate
```

3. Verwenden Sie den folgenden Befehl set-load-balancer-listener-ssl-certificate, um das Zertifikat festzulegen:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:iam::123456789012:server-certificate/my-new-certificate
```

Aktualisieren der SSL-Aushandlungskonfiguration Ihres Classic Load Balancers

Elastic Load Balancing bietet Sicherheitsrichtlinien mit vordefinierten SSL-Aushandlungskonfigurationen zum Aushandeln von SSL-Verbindungen zwischen Clients und Ihrem Load Balancer. Wenn Sie das HTTPS/SSL-Protokoll für Ihren Listener verwenden, stehen zwei vordefinierte Sicherheitsrichtlinien zu Verfügung, oder Sie verwenden Ihre eigenen benutzerdefinierten Sicherheitsrichtlinien.

Weitere Informationen zu den Sicherheitsrichtlinien finden Sie unter SSL-Aushandlungskonfigurationen für Classic Load Balancer. Weitere Informationen über die Konfigurationen der Sicherheitsrichtlinien von Elastic Load Balancing finden Sie unter Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer.

Wenn Sie einen HTTPS/SSL-Listener ohne Zuordnung einer Sicherheitsrichtlinie erstellen, ordnet Elastic Load Balancing Ihrem Load Balancer die vordefinierte Standardsicherheitsrichtlinie `ELBSecurityPolicy-2016-08` zu.

Wenn Sie möchten, können Sie eine benutzerdefinierte Konfiguration erstellen. Wir empfehlen dringend, dass Sie Ihre Sicherheitsrichtlinie testen, bevor Sie Ihre Load Balancer-Konfiguration aktualisieren.

Die folgenden Beispiele zeigen, wie Sie die SSL-Aushandlungskonfiguration für einen HTTPS/SSL-Listener aktualisieren. Beachten Sie, dass die Änderung sich nicht auf Anforderungen auswirkt, die von einem Load Balancer-Knoten empfangen wurden und auf das Routing zu einer funktionierenden Instance warten, sondern die aktualisierte Konfiguration wird für neu empfangene Anforderungen verwendet.

Inhalt

Aktualisieren der SSL-Aushandlungskonfiguration mit der Konsole

Elastic Load Balancing ordnet Ihrem Load Balancer standardmäßig die neueste vordefinierte Richtlinie zu. Wenn eine neue vordefinierte Richtlinie hinzugefügt wird, sollten Sie Ihren Load Balancer mit der neuen vordefinierten Richtlinie aktualisieren. Alternativ können Sie eine andere vordefinierte Sicherheitsrichtlinie auswählen oder eine benutzerdefinierte Richtlinie erstellen.

Um die SSL-Verhandlungskonfiguration für einen HTTPS/SSL-Load Balancer mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Listeners (Listener) die Option Manage listeners (Listener verwalten) aus.
5. Suchen Sie auf der Seite Manage listeners (Listener verwalten) den Listener, der aktualisiert werden soll, und wählen Sie unter Security policy (Sicherheitsrichtlinie) die Option Edit (Bearbeiten) aus. Wählen Sie mithilfe einer der folgenden Optionen eine Sicherheitsrichtlinie aus:
   - Behalten Sie die Standardrichtlinie ELBSecurityPolicy-2016-08 bei und wählen Sie dann Änderungen speichern.
   - Wählen Sie eine andere vordefinierte Richtlinie als die Standardrichtlinie und wählen Sie dann Save changes (Änderungen speichern).
   - Wählen Sie Custom (Benutzerdefiniert) aus und aktivieren Sie mindestens ein Protokoll und eine Verschlüsselung wie folgt:
     a. Wählen Sie für SSL Protocols ein oder mehrere Protokolle zur Aktivierung aus.
     b. Wählen Sie für SSL Options die Option Server Order Preference, um den in der Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer aufgelisteten Auftrag für die SSL-Aushandlung zu verwenden.
     c. Wählen Sie für SSL Ciphers eine oder mehrere Verschlüsselungen zur Aktivierung aus. Wenn Sie bereits ein SSL-Zertifikat haben, müssen Sie die Verschlüsselung aktivieren, mit der das Zertifikat erstellt wurde, da DSA- und RSA-Verschlüsselung spezifisch für den Signaturalgorithmus sind.
     d. Wählen Sie Änderungen speichern aus.

Aktualisieren Sie die Konfiguration der SSL-Aushandlung mithilfe des AWS CLI

Sie können die vordefinierte Standardsicherheitsrichtlinie `ELBSecurityPolicy-2016-08` verwenden, eine andere vordefinierte Sicherheitsrichtlinie oder eine benutzerdefinierte Sicherheitsrichtlinie.

Verwendung einer vordefinierten SSL-Sicherheitsrichtlinie

1. Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um die vordefinierten Sicherheitsrichtlinien aufzulisten, die von Elastic Load Balancing bereitgestellt werden. Die Syntax, die Sie verwenden, ist vom verwendeten Betriebssystem und der Shell abhängig.

   Linux

   ```
   aws elb describe-load-balancer-policies --query 'PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}' --output table
   ```

   Windows

   ```
   aws elb describe-load-balancer-policies --query "PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}" --output table
   ```

   Das Folgende ist Ausgabebeispiel:

   ```
   ----------------------------------------
   |      DescribeLoadBalancerPolicies      |
   +----------------------------------------+
   |               PolicyName               |
   +----------------------------------------+
   |  ELBSecurityPolicy-2016-08             |
   |  ELBSecurityPolicy-TLS-1-2-2017-01     |
   |  ELBSecurityPolicy-TLS-1-1-2017-01     |
   |  ELBSecurityPolicy-2015-05             |
   |  ELBSecurityPolicy-2015-03             |
   |  ELBSecurityPolicy-2015-02             |
   |  ELBSecurityPolicy-2014-10             |
   |  ELBSecurityPolicy-2014-01             |
   |  ELBSecurityPolicy-2011-08             |
   |  ELBSample-ELBDefaultCipherPolicy      |
   |  ELBSample-OpenSSLDefaultCipherPolicy  |
   +----------------------------------------+
   ```

   Um zu bestimmen, welche Verschlüsselungsverfahren für eine Richtlinie aktiviert sind, verwenden Sie den folgenden Befehl:

```
aws elb describe-load-balancer-policies --policy-names ELBSecurityPolicy-2016-08 --
output table
```

Informationen über die Konfiguration mit vordefinierten Sicherheitsrichtlinien finden Sie unter Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer.

2. Verwenden Sie den create-load-balancer-policyBefehl, um eine SSL-Verhandlungsrichtlinie mit einer der vordefinierten Sicherheitsrichtlinien zu erstellen, die Sie im vorherigen Schritt beschrieben haben. Der folgende Befehl verwendet beispielsweise die vordefinierte Standardsicherheitsrichtlinie:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy  --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-
Policy,AttributeValue=ELBSecurityPolicy-2016-08
```

Wenn Sie das Limit für die Anzahl der Richtlinien für den Load Balancer überschreiten, verwenden Sie den delete-load-balancer-policyBefehl, um alle nicht verwendeten Richtlinien zu löschen.

3. (Optional) Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um zu überprüfen, ob die Richtlinie erstellt wurde:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

Die Antwort enthält die Beschreibung der Richtlinie.

4. Verwenden Sie den folgenden Befehl set-load-balancer-policies-of-listener, um die Richtlinie auf dem Load Balancer-Port 443 zu aktivieren:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Der Befehl `set-load-balancer-policies-of-listener` ersetzt die aktuellen Richtlinien für den angegebenen Load Balancer-Port durch die angegebenen Richtlinien.

> Die Liste `--policy-names` muss alle zu aktivierenden Richtlinien enthalten. Wenn Sie eine Richtlinie auslassen, die derzeit aktiviert ist, wird sie deaktiviert.

5. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die neue Richtlinie für den Load Balancer-Port aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Die Antwort zeigt, dass die Richtlinie auf Port 443 aktiviert ist.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
          "InstanceProtocol": "HTTPS"
      },
      "PolicyNames": [
          "my-SSLNegotiation-policy"
      ]
  }
...
```

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie erstellen, müssen Sie mindestens ein Protokoll und eine Verschlüsselung aktivieren. Die DSA- und RSA-Verschlüsselungen gelten speziell für den Signaturalgorithmus zum Erstellen von SSL-Zertifikaten. Wenn Sie bereits über ein SSL-Zertifikat verfügen, müssen Sie die Verschlüsselung aktivieren, mit der das Zertifikat erstellt wurde. Der Name der benutzerdefinierten Richtlinie darf nicht mit `ELBSecurityPolicy-` oder `ELBSample-` beginnen, da diese Präfixe für die Namen der vordefinierten Sicherheitsrichtlinien definiert sind.

Verwendung einer benutzerdefinierten SSL-Sicherheitsrichtlinie

1. Verwenden Sie den create-load-balancer-policyBefehl, um eine SSL-Verhandlungsrichtlinie mithilfe einer benutzerdefinierten Sicherheitsrichtlinie zu erstellen. Zum Beispiel:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
```

```
--policy-name my-SSLNegotiation-policy --policy-type-name
SSLNegotiationPolicyType
--policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
AttributeName=Protocol-TLSv1.1,AttributeValue=true
AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

Wenn Sie das Limit für die Anzahl der Richtlinien für den Load Balancer überschreiten, verwenden Sie den delete-load-balancer-policyBefehl, um alle nicht verwendeten Richtlinien zu löschen.

2. (Optional) Verwenden Sie den folgenden describe-load-balancer-policiesBefehl, um zu überprüfen, ob die Richtlinie erstellt wurde:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

Die Antwort enthält die Beschreibung der Richtlinie.

3. Verwenden Sie den folgenden Befehl set-load-balancer-policies-of-listener, um die Richtlinie auf dem Load Balancer-Port 443 zu aktivieren:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Der Befehl `set-load-balancer-policies-of-listener` ersetzt die aktuellen Richtlinien für den angegebenen Load Balancer-Port durch die angegebenen Richtlinien. Die Liste `--policy-names` muss alle zu aktivierenden Richtlinien enthalten. Wenn Sie eine Richtlinie auslassen, die derzeit aktiviert ist, wird sie deaktiviert.

4. (Optional) Verwenden Sie den folgenden describe-load-balancersBefehl, um zu überprüfen, ob die neue Richtlinie für den Load Balancer-Port aktiviert ist:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Die Antwort zeigt, dass die Richtlinie auf Port 443 aktiviert ist.

```
...
```

```
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
          "InstanceProtocol": "HTTPS"
      },
      "PolicyNames": [
          "my-SSLNegotiation-policy"
      ]
  }
...
```

Registrierte Instances pro Classic Load Balancer

Nachdem Sie Ihren Classic Load Balancer erstellt haben, müssen Sie Ihre EC2 Instances beim Load Balancer registrieren. Sie können EC2 Instances aus einer einzelnen Availability Zone oder mehreren Availability Zones innerhalb derselben Region wie der Load Balancer auswählen. Elastic Load Balancing führt routinemäßig Integritätsprüfungen an registrierten EC2 Instances durch und verteilt eingehende Anfragen an den DNS-Namen Ihres Load Balancers automatisch auf die registrierten, fehlerfreien Instances. EC2

Inhalt

Bewährte Methoden für Ihre Instances

- Sie müssen sicherstellen, dass der Load Balancer mit Ihren Zielen sowohl auf dem Listener-Port als auch auf dem Zustandsprüfungs-Port kommunizieren kann. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsgruppen für Ihren Classic Load Balancer. Die Sicherheitsgruppe für Ihre Instances muss für jedes Subnetz für Ihren Load Balancer in beide Richtungen auf beiden Ports Datenverkehr zulassen.
- Installieren Sie auf allen Instances, die Sie bei Ihrem Load Balancer registrieren möchten, einen Webserver, z. B. Apache oder Internet Information Services (IIS).
- Für HTTP- und HTTPS-Listener empfehlen wir, die Keep-Alive-Option in Ihren EC2 Instances zu aktivieren, sodass der Load Balancer die Verbindungen zu Ihren Instances für mehrere Client-Anfragen wiederverwenden kann. Dadurch wird die Last auf Ihrem Webserver verringert und der Durchsatz des Load Balancer verbessert. Der Keepalive-Timeout sollte mindestens 60 Sekunden betragen, damit der Load Balancer für das Schließen der Verbindung zu Ihrer Instance verantwortlich ist.
- Elastic Load Balancing unterstützt MTU-Discovery (Maximum Transmission Unit, maximale Größe der Übertragungseinheit). Damit Path MTU Discovery ordnungsgemäß ausgeführt werden kann,

müssen Sie sicherstellen, dass die Sicherheitsgruppe für die Instance Nachrichten erlaubt, die ICMP-Fragmentierung erfordern (Typ 3, Code 4). Weitere Informationen finden Sie unter Path MTU Discovery im EC2 Amazon-Benutzerhandbuch.

Empfehlungen für Ihre VPC

Virtual Private Cloud (VPC)

Sofern Sie Ihre VPC nicht AWS-Konto vor 2014 erstellt haben, haben Sie in jeder Region eine Standard-VPC. Sie können eine Standard-VPC für Ihren Load Balancer verwenden, falls Sie eine haben, oder Sie können eine neue VPC erstellen. Weitere Informationen finden Sie im Amazon VPC-Benutzerhandbuch.

Subnetze für Ihren Load Balancer

Damit Ihr Load Balancer ordnungsgemäß skaliert werden kann, stellen Sie sicher, dass jedes Subnetz für Ihren Load Balancer über einen CIDR-Block mit mindestens einer `/27`-Bitmaske (z. B. `10.0.0.0/27`) und über mindestens 8 freie IP-Adressen verfügt. Ihr Load Balancer verwendet diese IP-Adressen, um Verbindungen mit den Instances herzustellen und bei Bedarf zu skalieren. Wenn nicht genügend IP-Adressen vorhanden sind, kann der Load Balancer möglicherweise nicht skalieren, was aufgrund unzureichender Kapazität zu 503-Fehlern führt.

Erstellen Sie ein Subnetz in jeder Availability Zone, in der Sie Instances starten möchten. Abhängig von Ihrer Anwendung können Sie Ihre Instances in öffentlichen Subnetzen, privaten Subnetzen oder einer Kombination aus öffentlichen und privaten Subnetzen starten. Ein öffentliches Subnetz verfügt über eine Route zu einem Internet-Gateway. Beachten Sie, dass standardmäßig VPCs ein öffentliches Subnetz pro Availability Zone vorhanden ist.

Wenn Sie einen Load Balancer erstellen, müssen Sie ein oder mehrere öffentliche Subnetze zum Load Balancer hinzufügen. Wenn sich Ihre Instances in privaten Subnetzen befinden, erstellen Sie öffentliche Subnetze in denselben Availability Zones wie die Subnetze mit Ihren Instances. Sie fügen diese öffentlichen Subnetze zum Load Balancer hinzu.

Netzwerk ACLs

Das Netzwerk ACLs für Ihre VPC muss Datenverkehr in beide Richtungen auf dem Listener-Port und dem Health Check-Port zulassen. Weitere Informationen finden Sie unter Netzwerk ACLs für die Instances für Ihren Classic Load Balancer.

Registrieren Sie Instances mit Ihrem Classic Load Balancer

Durch die Registrierung einer EC2 Instance wird sie Ihrem Load Balancer hinzugefügt. Der Load Balancer überwacht fortlaufend den Zustand registrierter Instances in den aktivierten Availability Zones und leitet Anfragen an die Instances weiter, die fehlerfrei sind. Wenn die Nachfrage nach Ihren Instances steigt, können Sie zusätzliche Instances beim Load Balancer registrieren, um die Nachfrage zu bewältigen.

Wenn Sie eine EC2 Instance deregistrieren, wird sie aus Ihrem Load Balancer entfernt. Der Load Balancer stoppt das Weiterleiten von Anfragen an eine Instance, sobald die Registrierung des Ziels aufgehoben wird. Wenn der Bedarf nachlässt oder Sie Ihre Instances warten müssen, können Sie die Registrierung von Instances beim Load Balancer aufheben. Eine Instance, deren Registrierung aufgehoben wurde, wird weiterhin ausgeführt, erhält aber keinen Datenverkehr mehr vom Load Balancer und Sie können sie erneut beim Load Balancer registrieren, wenn Sie bereit sind.

Wenn Sie die Registrierung einer Instance aufheben, wartet Elastic Load Balancing, bis im Gang befindliche Anforderungen abgeschlossen sind, wenn Connection Draining aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren des Connection Draining für Ihren Classic Load Balancer.

Wenn Ihr Load Balancer mit einer Auto-Scaling-Gruppe verbunden ist, werden Instances in der Gruppe automatisch beim Load Balancer registriert. Wenn Sie einen Load Balancer von Ihrer Auto-Scaling-Gruppe trennen, wird die Registrierung der Instances in der Gruppe aufgehoben.

Elastic Load Balancing registriert Ihre EC2 Instance mithilfe ihrer IP-Adresse bei Ihrem Load Balancer.

[EC2VPC] Wenn Sie eine Instance registrieren, an die ein elastic network interface (ENI) angeschlossen ist, leitet der Load Balancer Anfragen an die primäre IP-Adresse der primären Schnittstelle (eth0) der Instance weiter.

Inhalt

Registrieren einer Instance

Wenn Sie bereit sind, registrieren Sie Ihre Instance bei Ihrem Load Balancer. Wenn sich die Instance in einer Availability Zone befindet, die für den Load Balancer aktiviert ist, ist die Instance bereit, Datenverkehr vom Load Balancer zu erhalten, sobald sie die erforderliche Anzahl von Zustandsprüfungen besteht.

Registrieren Ihrer Instances mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Target instances (Ziel-Instances) die Option Manage instances (Instances verwalten) aus.
5. Wählen Sie auf der Seite Manage instances (Instances verwalten) in der Tabelle Available instances (Verfügbare Instances) die Instances aus, die Sie bei Ihrem Load Balancer registrieren möchten.
6. Stellen Sie sicher, dass die Instances, die registriert werden müssen, nicht in der Tabelle Review selected instances (Ausgewählte Instances überprüfen) aufgeführt sind.
7. Wählen Sie Änderungen speichern.

Um Ihre Instances mit dem zu registrieren AWS CLI

Verwenden Sie den folgenden Befehl register-instances-with-load-balancer:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --
instances i-4e05f721
```

Es folgt ein Beispiel für eine Antwort, in der die beim Load Balancer registrierten Instances aufgelistet werden:

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        },
        {
            "InstanceId": "i-4e05f721"
```

```
        }
    ]
}
```

Zeigen Sie die bei einem Load Balancer registrierten Instances an

Verwenden Sie den folgenden describe-load-balancersBefehl, um die beim angegebenen Load Balancer registrierten Instances aufzulisten:

```
aws elb describe-load-balancers --load-balancer-names my-load-balancer --output text --
query "LoadBalancerDescriptions[*].Instances[*].InstanceId"
```

Das Folgende ist Ausgabebeispiel:

```
i-e905622e
i-315b7e51
i-4e05f721
```

Ermitteln Sie den Load Balancer für eine registrierte Instance

Verwenden Sie den folgenden describe-load-balancersBefehl, um den Namen des Load Balancers abzurufen, bei dem die angegebene Instance registriert ist:

```
aws elb describe-load-balancers --output text --query "LoadBalancerDescriptions[?
Instances[?InstanceId=='i-e905622e']].[LoadBalancerName]"
```

Das Folgende ist Ausgabebeispiel:

```
my-load-balancer
```

Aufheben der Registrierung einer Instance

Sie können die Registrierung einer Instance bei Ihrem Load Balancer aufheben, wenn Sie die Kapazität nicht mehr benötigen oder Sie die Instance warten müssen.

Wenn Ihr Load Balancer einer Auto-Scaling-Gruppe zugeordnet ist, wird bei einer Trennung der Instance auch deren Registrierung beim Load Balancer aufgehoben. Weitere Informationen finden Sie unter Trennen von EC2 Instances von Ihrer Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Aufheben der Registrierung Ihrer Instances mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Target instances (Ziel-Instances) die Option Manage instances (Instances verwalten) aus.
5. Heben Sie auf der Seite Manage instances (Instances verwalten) in der Tabelle Available instances (Verfügbare Instances) die Auswahl der Instances auf, die von Ihrem Load Balancer abgemeldet werden sollen.
6. Stellen Sie sicher, dass die Instances, deren Registrierung aufgehoben werden muss, nicht in der Tabelle Review selected instances (Ausgewählte Instances überprüfen) aufgeführt sind.
7. Wählen Sie Änderungen speichern.

Um Ihre Instances abzumelden, verwenden Sie AWS CLI

Verwenden Sie den folgenden Befehl deregister-instances-from-load-balancer:

```
aws elb deregister-instances-from-load-balancer --load-balancer-name my-loadbalancer --instances i-4e05f721
```

Es folgt ein Beispiel für eine Antwort, in der die verbleibenden Instances aufgelistet werden, die beim Load Balancer registriert sind:

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        }
    ]
}
```

Zustandsprüfungen für die Instances für Ihren Classic Load Balancer

Ihr Classic Load Balancer sendet regelmäßig Anforderungen an die registrierten Instances, um deren Status zu überprüfen. Diese Tests werden als Zustandsprüfungen bezeichnet. Der Status der

Instances, die zum Zeitpunkt der Zustandsprüfung fehlerfrei sind, lautet `InService`. Der Status von Instances, die zum Zeitpunkt der Zustandsprüfung fehlerhaft sind, lautet `OutOfService`. Der Load Balancer führt Zustandsprüfungen auf allen registrierten Instances durch, unabhängig davon, ob die Instance einen fehlerfreien oder einen fehlerhaften Zustand aufweist.

Der Load Balancer leitet Anfragen nur an die fehlerfreien Instances weiter. Wenn der Load Balancer feststellt, dass eine Instance fehlerhaft ist, sendet er keine Anfragen mehr an diese Instance. Der Load Balancer sendet wieder Anfragen an die Instance, wenn deren fehlerfreier Zustand wiederhergestellt wurde.

Der Load Balancer prüft den Zustand der registrierten Instances mit der Standard-Zustandsprüfungskonfiguration von Elastic Load Balancing oder mit einer von Ihnen festgelegten Zustandsprüfungskonfiguration.

Wenn Sie Ihre Auto-Scaling-Gruppe mit einem Classic Load Balancer verknüpft haben, können Sie mithilfe der Load Balancer-Zustandsprüfung den Zustand der Instances in Ihrer Auto-Scaling-Gruppe ermitteln. Eine Auto-Scaling-Gruppe ermittelt standardmäßig in regelmäßigen Abständen den Zustand jeder Instance. Weitere Informationen finden Sie unter Hinzufügen von Elastic Load Balancing Balancing-Zustandsprüfungen zu Ihrer Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Inhalt

Zustandsprüfungskonfiguration

Eine Zustandsprüfungskonfiguration enthält die Informationen, die ein Load Balancer verwendet, um den Zustand der registrierten Instances zu bestimmen. Die folgende Tabelle beschreibt die Felder für die Zustandsprüfungskonfiguration.

Feld	Beschreibung
Protokoll	

Feld	Beschreibung
	Das Protokoll, das für die Verbindung zur Instance verwendet werden soll. Gültige Werte: `TCP`, `HTTP`, `HTTPS` und `SSL` Konsolen-Standardeinstellung: `HTTP` CLI/API-Standardeinstellung: `TCP`
Port	Der Port, der als ein `protocol:port` -Paar für die Verbindung zur Instance verwendet werden soll. Wenn der Load Balancer innerhalb des konfigurierten Zeitraums für die Antwort-Zeitüberschreitung am angegebene Port keine Verbindung zur Instance herstellen kann, gilt die Instance als fehlerhaft. Protokolle:`TCP`, `HTTP`, `HTTPS` und `SSL` Port-Bereich: 1 bis 65 535 Konsolen-Standardeinstellung: `HTTP:80` CLI/API-Standardeinstellung: `TCP:80`

Feld	Beschreibung
Pfad	Das Ziel für die HTTP- oder HTTPS-Anfrage. Eine HTTP- oder HTTPS-GET-Anfrage wird an die Instance auf dem Port und dem Pfad ausgegeben. Wenn der Load Balancer innerhalb des Zeitraums für die Antwort-Zeitüberschreitung eine andere Antwort als „200 OK“ erhält, gilt die Instance als fehlerhaft. Wenn die Antwort einen Text enthält, muss Ihre Anwendung entweder den Inhaltslängen-Header auf einen Wert festlegen, der größer oder gleich null ist, oder Transfer-Encoding mit einem auf „Chunked“ festgelegten Wert angeben. Standard: `/index.html`
Reaktions-Timeout	Die Wartezeit in Sekunden, bis eine Antwort von der Zustandsprüfung eingeht. Gültige Werte: 2 bis 60 Standard: 5
HealthCheck Intervall	Der Zeitraum in Sekunden zwischen Zustandsprüfungen einer einzelnen Instance. Gültige Werte: 5 bis 300 Standard: 30

Feld	Beschreibung
Unhealthy Threshold (Schwellenwert für anormalen Zustand)	Die Anzahl der aufeinanderfolgenden fehlgeschlagenen Integritätsprüfungen, die durchgeführt werden müssen, bevor eine EC2 Instance für fehlerhaft erklärt wird. Gültige Werte: 2 bis 10 Standard: 2
Healthy Threshold (Schwellenwert für normalen Zustand)	Die Anzahl der aufeinanderfolgenden erfolgreichen Integritätsprüfungen, die durchgeführt werden müssen, bevor eine EC2 Instance für fehlerfrei erklärt wird. Gültige Werte: 2 bis 10 Standard: 10

Der Load Balancer sendet unter Verwendung des angegeben Ports, Protokolls und Pfads alle `Interval` Sekunden eine Zustandsprüfungs-Anforderung an jede registrierte Instance. Jede Anfrage nach einer Zustandsprüfung ist unabhängig und hält über das gesamte Intervall an. Die Zeit, die die Instance für die Antwort benötigt, hat keinen Einfluss auf das Intervall für die nächste Zustandsprüfung. Wenn die Integritätsprüfungen UnhealthyThresholdCountaufeinanderfolgende Fehler überschreiten, nimmt der Load Balancer die Instance außer Betrieb. Wenn die Zustandsprüfungen HealthyThresholdCountaufeinanderfolgende Erfolge überschreiten, nimmt der Load Balancer die Instance wieder in Betrieb.

Eine HTTP/HTTPS-Zustandsprüfung ist erfolgreich, wenn die Instance innerhalb des Zustandsprüfungsintervalls einen 200-Antwortcode zurückgibt. Eine TCP-Zustandsprüfung ist erfolgreich, wenn die TCP-Verbindung erfolgreich ist. Eine SSL-Zustandsprüfung ist erfolgreich, wenn das SSL-Handshake erfolgreich ist.

Aktualisieren der Zustandsprüfungskonfiguration

Sie können die Zustandsprüfungskonfiguration für Ihren Load Balancer jederzeit aktualisieren.

Aktualisieren der Zustandsprüfungskonfiguration für Ihren Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie in der Registerkarte Health checks (Zustandsprüfungen) die Option Edit (Bearbeiten) aus.
5. Aktualisieren Sie auf der Seite Edit health check settings (Einstellungen für die Zustandsprüfung bearbeiten) unter Health checks (Zustandsprüfungen) die Konfiguration nach Bedarf.
6. Wenn Sie mit Ihren Einstellungen zufrieden sind, klicken Sie auf Save changes (Änderungen speichern).

Um die Health Check-Konfiguration für Ihren Load Balancer zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den folgenden configure-health-check-Befehl:

```
aws elb configure-health-check --load-balancer-name my-load-balancer --health-check
 Target=HTTP:80/path,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Überprüfen des Zustands Ihrer Instances

Sie können den Zustand Ihrer registrierten Instances überprüfen.

Überprüfen des Zustands Ihrer Instances mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Im Abschnitt Details gibt Status an, wie viele Instances in Betrieb sind.
5. Auf der Registerkarte Target instances (Ziel-Instances) in der Tabelle Target instances (Ziel-Instances) gibt die Spalte Health Status (Zustandsstatus) den spezifischen Status jeder registrierten Instance an.

Um den Integritätsstatus Ihrer Instances zu überprüfen, verwenden Sie AWS CLI

Verwenden Sie den folgenden describe-instance-health-Befehl:

```
aws elb describe-instance-health --load-balancer-name my-load-balancer
```

Beheben von Problemen bei Zustandsprüfungen

Es gibt verschiedene Gründe dafür, dass Ihre registrierten Instances die Load Balancer-Zustandsprüfung möglicherweise nicht bestehen. Die häufigsten Gründe dafür, dass eine Zustandsprüfung nicht bestanden wird, liegen darin, dass EC2 Instances die Verbindungen zu Ihrem Load Balancer beenden oder dass bei der Antwort der EC2 Instances ein Timeout auftritt. Weitere Informationen zu potenziellen Ursachen und Schritte zur Behebung der Probleme, die zum Nichtbestehen der Zustandsprüfung führen, finden Sie unter Fehlerbehebung beim Classic Load Balancer: Zustandsprüfungen.

Sicherheitsgruppen für die Instances für Ihren Classic Load Balancer

Eine Sicherheitsgruppe agiert als Firewall, die den zulässigen Verkehr zu und von einer oder mehreren Instances steuert. Wenn Sie eine EC2 Instance starten, können Sie der Instance eine oder mehrere Sicherheitsgruppen zuordnen. Für jede Sicherheitsgruppe fügen Sie eine oder mehrere Regeln hinzu, um Datenverkehr zuzulassen. Diese Regeln können Sie jederzeit ändern, wobei die neuen Regeln automatisch auf alle Instances der Sicherheitsgruppe angewendet werden. Weitere Informationen finden Sie unter EC2 Amazon-Sicherheitsgruppen im EC2 Amazon-Benutzerhandbuch.

Die Sicherheitsgruppen für Ihre Instances müssen ihnen erlauben, mit dem Load Balancer zu kommunizieren. Die folgende Tabelle zeigt die empfohlenen Regeln für eingehenden Datenverkehr.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
load balancer security group	TCP	*instance listener*	Datenverkehr vom Load Balancer auf dem Listener-Port der Instance zulassen
load balancer security group	TCP	*health check*	Datenverkehr vom Load Balancer auf dem Zustandsprüfungs-Port zulassen

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

Netzwerk ACLs für die Instances für Ihren Classic Load Balancer

Eine Netzwerk-Zugriffssteuerungsliste (ACL) erlaubt oder verweigert bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene. Sie können die Standard-Netzwerk-ACL für Ihre VPC verwenden, oder Sie können eine benutzerdefinierte Netzwerk-ACL für Ihre VPC mit Regeln erstellen, die den Regeln für Ihre Sicherheitsgruppen ähneln, um Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen.

Die standardmäßige Netzwerk-ACL für die VPC erlaubt den gesamten ein- und ausgehenden Datenverkehr. Wenn Sie ein benutzerdefiniertes Netzwerk erstellen ACLs, müssen Sie Regeln hinzufügen, die die Kommunikation zwischen dem Load Balancer und den Instances ermöglichen.

Die empfohlenen Regeln für das Subnetz für Ihre Instances hängen davon ab, ob das Subnetz privat oder öffentlich ist. Die folgenden Regeln beziehen sich auf ein privates Subnetz. Wenn sich Ihre Instances in einem öffentlichen Subnetz befinden, ändern Sie Quelle und Ziel vom CIDR der VPC in `0.0.0.0/0`.

Im Folgenden sind die empfohlenen Regeln für eingehenden Datenverkehr aufgeführt.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	TCP	*instance listener*	Eingehenden Datenverkehr vom VPC CIDR am Listener-Port der Instance zulassen
VPC CIDR	TCP	*health check*	Eingehenden Datenverkehr vom VPC CIDR am Zustandsprüfungs-Port zulassen

Im Folgenden sind die empfohlenen Regeln für ausgehenden Datenverkehr aufgeführt.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	TCP	1024 - 65535	Ausgehenden Datenverkehr zum VPC CIDR an den flüchtigen Ports zulassen

Überwachen Ihres Classic Load Balancers

Sie können die folgenden Funktionen verwenden, um Ihre Load Balancer zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihrem Load Balancer und Backend-Instances zu beheben.

CloudWatch Metriken

Elastic Load Balancing veröffentlicht Datenpunkte CloudWatch über Ihre Load Balancer und Back-End-Instances an Amazon. CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, abzurufen. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Classic Load Balancer.

Zugriffsprotokolle für Elastic Load Balancing

Die Zugriffsprotokolle für Elastic Load Balancing erfassen detaillierte Informationen zu Anforderungen an Ihren Load Balancer und speichern diese als Protokolldateien im Amazon-S3-Bucket, den Sie angegeben haben. Jedes Protokoll enthält Detailinformationen wie die Uhrzeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfad und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und für die Fehlerbehebung Ihrer Backend-Anwendungen nutzen. Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihren Classic Load Balancer.

CloudTrail Logs

AWS CloudTrail ermöglicht es Ihnen, die Aufrufe der Elastic Load Balancing API zu verfolgen, die von oder im Namen Ihres AWS Kontos getätigt wurden. CloudTrail speichert die Informationen in Protokolldateien im Amazon S3 S3-Bucket, den Sie angeben. Sie können die betreffenden Protokolldateien zur Überwachung der Aktivitäten Ihrer Load Balancer verwenden, indem Sie bestimmen, welche Anforderungen erfolgt sind, die Quell-IP-Adressen, von denen die Anforderungen kamen, wer die Anforderung gestellt hat, wann die Anforderung erfolgt ist usw. Weitere Informationen finden Sie unter Protokollieren von API-Aufrufen für Elastic Load Balancing mit CloudTrail.

CloudWatch Metriken für Ihren Classic Load Balancer

Elastic Load Balancing veröffentlicht Datenpunkte CloudWatch für Ihre Load Balancer und Ihre Back-End-Instances auf Amazon. CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in

Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Sie können beispielsweise die Gesamtzahl der fehlerfreien EC2 Instances für einen Load Balancer über einen bestimmten Zeitraum überwachen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können beispielsweise einen CloudWatch Alarm erstellen, um eine bestimmte Metrik zu überwachen und eine Aktion einzuleiten (z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb des für Sie akzeptablen Bereichs liegt.

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

Weitere Informationen zu Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Inhalt

Metriken zu Classic Load Balancer

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

Metrik	Beschreibung
`BackendConnectionErrors`	Die Zahl der Verbindungen, die zwischen dem Load Balancer und den registrierten Instances nicht erfolgreich hergestellt wurden. Da der Load Balancer den Verbindungsversuch bei Fehlern wiederholt, kann diese Zahl die Anforderungsrate übersteigen. Diese Zahl

Metrik	Beschreibung
	umfasst außerdem Verbindungsfehler im Zusammenhang mit Zustandsprüfungen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Hinweis: `Average`, `Minimum` und `Maximum` werden pro Load Balancer-Knoten gemeldet und sind nicht immer nützlich. Der Unterschied zwischen dem Mindest- und dem Höchstwert (oder zwischen dem Spitzen- und dem Durchschnittswert bzw. zwischen dem Durchschnitts- und dem Durchsatzwert) kann nützlich sein, um zu bestimmen, ob ein Load Balancer-Knoten ein Ausreißer ist. Beispiel: Angenommen, Ihr Load Balancer verfügt über zwei Instances in us-west-2a und zwei Instances in us-west-2b und Verbindungsversuche mit einer Instance in us-west-2a führen zu Backend-Verbindungsfehlern. Die Summe für us-west-2a umfasst diese Verbindungsfehler, während die Summe für us-west-2b diese nicht enthält. Daher entspricht die Summe für den Load Balancer der Summe für us-west-2a.
`DesyncMitigationMode_NonCompliant_Request_Count`	[HTTP-Listener] Die Anzahl der Anfragen, die nicht RFC 7230 entsprechen. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
`HealthyHostCount`	Die Zahl der fehlerfreien Instances, die mit Ihrem Load Balancer registriert sind. Eine neu registrierte Instance wird als fehlerfrei betrachtet, nachdem sie die erste Zustandsprüfung bestanden hat. Wenn zonenübergreifendes Load Balancing aktiviert ist, wird die Zahl der fehlerfreien Instances für die Dimension `LoadBalancerName` für alle Availability Zones berechnet. Andernfalls wird sie je Availability Zone berechnet. Berichtkriterien: Registrierte Instances Statistiken: Die nützlichsten Statistiken sind `Average` und `Maximum`. Diese Statistiken werden durch die Load Balancer-Knoten bestimmt. Hinweis: Einige Load Balancer-Knoten können feststellen, dass eine Instance für einen kurzen Zeitraum nicht fehlerfrei ist, während andere Knoten ihre Fehlerfreiheit bestätigen. Beispiel: Angenommen, Ihr Load Balancer verfügt über zwei Instances in us-west-2a und zwei Instances in us-west-2b; us-west-2a hat eine nicht fehlerfreie Instance und in us-west-2b sind alle Instances fehlerfrei. Mit der Dimension `AvailabilityZone` ergibt sich ein Durchschnitt von einer fehlerfreien und einer nicht fehlerfreien Instance in us-west-2a sowie ein Durchschnitt von zwei fehlerfreien und null nicht fehlerfreien Instances in us-west-2b.

Metrik	Beschreibung
`HTTPCode_Backend_2XX`, `HTTPCode_Backend_3XX`, `HTTPCode_Backend_4XX`, `HTTPCode_Backend_5XX`	[HTTP-Listener] Die Zahl der HTTP-Antwortcodes, die von registrierten Instances generiert wurden. Diese Zahl umfasst keine Antwortcodes, die vom Load Balancer generiert wurden. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Hinweis: `Minimum`, `Maximum` und `Average` sind alle 1. Beispiel: Angenommen, Ihr Load Balancer verfügt über zwei Instances in us-west-2a und zwei Instances in us-west-2b und Anfragen, die an eine Instance in us-west-2a gesendet wurden, führen zu HTTP-500-Antworten. Die Summe für us-west-2a umfasst diese Fehlerantworten, während die Summe für us-west-2b diese nicht enthält. Daher entspricht die Summe für den Load Balancer der Summe für us-west-2a.
`HTTPCode_ELB_4XX`	[HTTP-Listener] Die Anzahl der vom Load Balancer generierten HTTP 4XX-Client-Fehlercodes Client-Fehler werden generiert, wenn eine Anforderung das falsche Format hat oder unvollständig ist. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Hinweis: `Minimum`, `Maximum` und `Average` sind alle 1. Beispiel: Angenommen, für Ihren Load Balancer sind us-west-2a und us-west-2b aktiviert und Client-Anforderungen umfassen eine falsch formatierte Anforderungs-URL. Dies führt zu einem Client-Fehleranstieg in allen Availability Zones. Die Summe für den Load Balancer ist die Summe der Werte für die Availability Zones.

Metrik	Beschreibung
`HTTPCode_ELB_5XX`	[HTTP-Listener] Die Anzahl der vom Load Balancer generierten HTTP 5XX-Server-Fehlercodes Diese Zahl umfasst keine Antwortcodes, die von den registrierten Instances generiert wurden. Die Metrik wird gemeldet, wenn für den Load Balancer keine fehlerfreien Instances registriert sind oder wenn die Anforderungsrate die Kapazität der Instances (Überlauf) oder des Load Balancers überschreitet. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Hinweis: `Minimum`, `Maximum` und `Average` sind alle 1. Beispiel: Angenommen, für Ihren Load Balancer sind us-west-2a und us-west-2b aktiviert und für Ihre Instances in us-west-2a besteht eine hohe Latenz, sodass sie nur langsam auf Anforderungen antworten. Das führt dazu, dass sich die Anstiegswarteschlange für die Load Balancer-Knoten in us-west-2a füllt und die Clients den Fehler 503 erhalten. Wenn us-west-2b weiterhin normal antwortet, entspricht die Summe für den Load Balancer der Summe für us-west-2a.

Metrik	Beschreibung
`Latency`	[HTTP-Listener] Die gesamte abgelaufene Zeit in Sekunden ab dem Zeitpunkt, zu dem der Load Balancer die Anforderung an eine registrierte Instance gesendet hat, bis zu dem Zeitpunkt, an dem die Instance begann, die Antwort-Header zu senden. [TCP-Listener] Die gesamte abgelaufene Zeit in Sekunden, bis der Load Balancer erfolgreich eine Verbindung zu einer registrierten Instance hergestellt hat. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Average`. Verwenden Sie `Maximum`, um zu bestimmen, ob einige Anforderungen wesentlich länger dauern als der Durchschnitt. Hinweis: `Minimum` ist in der Regel nicht nützlich. Beispiel: Angenommen, Ihr Load Balancer verfügt über zwei Instances in us-west-2a und zwei Instances in us-west-2b und Anforderungen, die an eine Instance in us-west-2a gesendet wurden, weisen eine höhere Latenz auf. Der Durchschnitt für us-west-2a weist einen höheren Wert auf als der Durchschnitt für us-west-2b.

Metrik	Beschreibung
`RequestCount`	Die Zahl der abgeschlossenen Anforderungen oder hergestellten Verbindungen während des angegebenen Intervalls (eine oder fünf Minuten). [HTTP-Listener] Die Zahl der erhaltenen und weitergeleiteten Anforderungen, einschließlich HTTP-Fehlerantworten von den registrierten Instances. [TCP-Listener] Die Zahl der hergestellten Verbindungen mit den registrierten Instances. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben. Beispiel: Angenommen, Ihr Load Balancer verfügt über zwei Instances in us-west-2a und zwei Instances in us-west-2b und 100 Anforderungen werden an den Load Balancer gesendet. 60 Anforderungen werden an us-west-2a gesendet, wobei jede Instance 30 Anforderungen erhält, und 40 Anforderungen an us-west-2b, sodass auf jede Instance 20 Anforderungen entfallen. Mit der Dimension `AvailabilityZone` ergibt sich eine Summe von 60 Anforderungen in us-west-2a und 40 Anforderungen in us-west-2b. Mit der Dimension `LoadBalancerName` beträgt die Summe 100 Anforderungen.

Metrik	Beschreibung
`SpilloverCount`	Die Gesamtanzahl der Anforderungen, die abgelehnt wurden, weil die Anstiegswarteschlange voll ist. [HTTP-Listener] Der Load Balancer gibt einen HTTP 503-Fehlercode zurück. [TCP-Listener] Der Load Balancer schließt die Verbindung. Berichtkriterien: Ein Wert ungleich Null Statistiken: Die nützlichste Statistik ist `Sum`. Hinweis: `Average`, `Minimum` und `Maximum` werden pro Load Balancer-Knoten gemeldet und sind nicht immer nützlich. Beispiel: Angenommen, für Ihren Load Balancer sind us-west-2a und us-west-2b aktiviert und für Ihre Instances in us-west-2a besteht eine hohe Latenz, sodass sie nur langsam auf Anforderungen antworten. Das führt dazu, dass sich die Anstiegswarteschlange für den Load Balancer-Knoten in us-west-2a füllt und ein Überlauf auftritt. Wenn us-west-2b weiterhin normal antwortet, entspricht die Summe für den Load Balancer der Summe für us-west-2a.

Metrik	Beschreibung
SurgeQueueLength	Die Gesamtzahl der Anforderungen (HTTP-Listener) oder Verbindungen (TCP-Listener), deren Weiterleitung an eine fehlerfre ie Instance aussteht. Die maximale Größe der Warteschlange beträgt 1.024. Zusätzliche Anforderungen oder Verbindungen werden abgewiesen, wenn die Warteschlange voll ist. Weitere Informationen finden Sie unter SpilloverCount . Berichtkriterien: Ein Wert ungleich Null. Statistiken: Die nützlichste Statistik ist Maximum, da sie die Spitze der in der Warteschlange befindlichen Anforderungen darstellt . Die Average-Statistik kann in Kombination mit Minimum und Maximum nützlich sein, um den Bereich der in der Warteschlange befindlichen Anforderungen zu bestimmen. Hinweis: Sum ist nicht nützlich. Beispiel: Angenommen, für Ihren Load Balancer sind us-west-2 a und us-west-2b aktiviert und für Ihre Instances in us-west-2a besteht eine hohe Latenz, sodass sie nur langsam auf Anforderu ngen antworten. Das führt dazu, dass sich die Anstiegswarteschla nge für die Load Balancer-Knoten in us-west-2a füllt und sich die Reaktionszeiten der Clients wahrscheinlich verlängern. Wenn diese Situation anhält, treten beim Load Balancer wahrscheinlich Überläufe auf (siehe Metrik SpilloverCount). Wenn us-west-2 b weiterhin normal antwortet, entspricht max für den Load Balancer dem Wert max für us-west-2a.

Metrik	Beschreibung
`UnHealthyHostCount`	Die Zahl der nicht fehlerfreien Instances, die mit Ihrem Load Balancer registriert sind. Eine Instance wird als nicht fehlerfrei betrachtet, sobald sie den für Zustandsprüfungen konfigurierten Unhealthy Threshold (Schwellenwert für anormalen Zustand) überschreitet. Eine nicht fehlerfreie Instance wird wieder als fehlerfrei betrachtet, sobald sie dem für Zustandsprüfungen konfigurierten Healthy Threshold (Schwellenwert für normalen Zustand) entspricht. Berichtkriterien: Registrierte Instances Statistiken: Die nützlichsten Statistiken sind `Average` und `Minimum`. Diese Statistiken werden durch die Load Balancer-Knoten bestimmt. Hinweis: Einige Load Balancer-Knoten können feststellen, dass eine Instance für einen kurzen Zeitraum nicht fehlerfrei ist, während andere Knoten ihre Fehlerfreiheit bestätigen. Beispiel: Siehe `HealthyHostCount` .

Die folgenden Metriken ermöglichen eine Kostenschätzung für die Migration eines Classic Load Balancer auf einen Application Load Balancer. Diese Messwerte sind nur zu Informationszwecken bestimmt, nicht zur Verwendung mit CloudWatch Alarmen. Hinweis: Wenn Ihr Classic Load Balancer über mehrere Listener verfügt, werden diese Metriken über alle Listener hinweg aggregiert.

Diese Schätzungen basieren auf einem Load Balancer mit einer Standardregel und einem Zertifikat mit einer Größe von 2 K. Bei Verwendung eines Zertifikats mit einer Größe von 4 K oder größer empfehlen wir, eine Kostenschätzung wie folgt vorzunehmen: Erstellen Sie einen Application Load Balancer basierend auf Ihrem Classic Load Balancer mit dem Migrationstool und überwachen Sie die Metrik `ConsumedLCUs` für den Application Load Balancer. Weitere Informationen finden Sie unter Migrieren eines Classic Load Balancers im Benutzerhandbuch für Elastic Load Balancing.

Metrik	Beschreibung
`EstimatedALBActive ConnectionCount`	

Metrik	Beschreibung
	Die geschätzte Zahl gleichzeitiger TCP-Verbindungen, die zwischen Clients und Load Balancer und zwischen Load Balancer und Zielen aktiv sind.
`EstimatedALBConsumedLCUs`	Die geschätzte Zahl der von einem Application Load Balancer verwendeten Load-Balancer-Kapazitätseinheiten (LCU). Sie zahlen für die Anzahl dieser Geräte LCUs , die Sie pro Stunde nutzen. Weitere Informationen finden Sie unter Elastic Load Balancing Pricing.
`EstimatedALBNewConnectionCount`	Die geschätzte Zahl neuer TCP-Verbindungen, die zwischen Clients und Load Balancer und zwischen Load Balancer und Zielen hergestellt wurden.
`EstimatedProcessedBytes`	Die geschätzte Zahl der von einem Application Load Balancer verarbeiteten Byte.

Metrik-Dimensionen für Classic Load Balancer

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

Dimension	Beschreibung
`AvailabilityZone`	Filtert die Metrikdaten nach der angegebenen Availability Zone.
`LoadBalancerName`	Filtert die Metrikdaten nach dem angegebenen Load Balancer.

Statistiken für Classic-Load-Balancer-Metriken

CloudWatch stellt Statistiken bereit, die auf den von Elastic Load Balancing veröffentlichten metrischen Datenpunkten basieren. Statistiken sind Metrikdaten-Aggregationen über einen bestimmten Zeitraum. Wenn Sie Statistiken anfordern, wird der zurückgegebene Datenstrom durch den Metriknamen und die Dimension identifiziert. Eine Dimension ist ein name/value Paar, das eine Metrik eindeutig identifiziert. Sie können beispielsweise Statistiken für alle fehlerfreien EC2 Instances anfordern, die hinter einem Load Balancer stehen, der in einer bestimmten Availability Zone gestartet wurde.

Die `Minimum`- und `Maximum`-Statistiken geben die Minimum- und Maximalwerte an, die von den einzelnen Load Balancer-Knoten gemeldet werden. Angenommen, es gibt zwei Load Balancer-Knoten. Ein Knoten hat `HealthyHostCount` mit dem `Minimum`-Wert 2, dem `Maximum`-Wert 10 und dem `Average`-Wert 6, während der andere Knoten `HealthyHostCount` mit dem `Minimum`-Wert 1, dem `Maximum`-Wert 5 und dem `Average`-Wert 3 aufweist. Somit weist der Load Balancer den `Minimum`-Wert 1, den `Maximum`-Wert 10 und den `Average`-Wert von etwa 4 auf.

Die `Sum`-Statistik stellt den Gesamtwert aller Load Balancer-Knoten dar. Da Metriken mehrere Berichte pro Zeitraum umfassen, gilt `Sum` nur für Metriken, die über alle Load Balancer-Knoten aggregiert werden, wie `RequestCount`, `HTTPCode_ELB_XXX`, `HTTPCode_Backend_XXX`, `BackendConnectionErrors` und `SpilloverCount`.

Die `SampleCount`-Statistik ist die Zahl der gemessenen Stichproben. Da Metriken basierend auf Erfassungsintervallen und Ereignissen erfasst werden, ist diese Statistik in der Regel nicht nützlich. Bei `HealthyHostCount` basiert `SampleCount` z. B. auf der Anzahl der Stichproben, die jeder Load Balancer-Knoten meldet, nicht auf der Anzahl fehlerfreier Hosts.

Ein Perzentil gibt die relative Stelle eines Wertes in einem Datensatz an. Sie können ein beliebiges Perzentil mit bis zu zwei Dezimalstellen (z. B. p95,45) angeben. Ein 95. Perzentil bedeutet, dass 95 Prozent der Daten unter diesem Wert und 5 Prozent darüber liegen. Perzentile werden häufig genutzt, um Anomalien zu isolieren. Angenommen, eine Anwendung bedient die meisten Anforderungen aus einem Cache in 1-2 ms, aber benötigt 100 bis 200 ms, wenn der Cache leer ist. Das Maximum spiegelt den langsamsten Fall wider, etwa 200 ms. Der Durchschnitt gibt nicht die Verteilung der Daten an. Perzentile bieten eine aussagekräftigere Darstellung der Anwendungs-Performance. Indem Sie das 99. Perzentil als Auto Scaling-Trigger oder CloudWatch Alarm verwenden, können Sie festlegen, dass die Verarbeitung von nicht mehr als 1 Prozent der Anfragen länger als 2 ms dauert.

CloudWatch Metriken für Ihren Load Balancer anzeigen

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

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

So zeigen Sie Metriken mithilfe der -Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen des Load Balancers aus, um die Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Überwachung.
5. Um eine größere Ansicht einer einzelnen Kennzahl zu erhalten, bewegen Sie den Mauszeiger über das Diagramm und wählen Sie das `Maximize`-Symbol. Die folgenden Metriken sind verfügbar:

   - Fehlerfreie Hosts – `HealthyHostCount`
   - Fehlerhafte Hosts – `UnHealthyHostCount`
   - Durchschnittliche Latenz – `Latency`
   - Anforderungen – `RequestCount`
   - Backend-Verbindungsfehler – `BackendConnectionErrors`
   - Anstiegswarteschlangenlänge – `SurgeQueueLength`
   - Überlaufanzahl – `SpilloverCount`
   - HTTP 2 XXs — `HTTPCode_Backend_2XX`
   - HTTP 3 XXs — `HTTPCode_Backend_3XX`
   - HTTP 4 XXs — `HTTPCode_Backend_4XX`
   - HTTP 5 XXs — `HTTPCode_Backend_5XX`
   - ELB HTTP 4 XXs — `HTTPCode_ELB_4XX`
   - ELB HTTP 5 XXs — `HTTPCode_ELB_5XX`
   - Geschätzte verarbeitete Byte – `EstimatedProcessedBytes`
   - Geschätzter ALB-Verbrauch — LCUs `EstimatedALBConsumedLCUs`

- Geschätzte Anzahl aktiver ALB-Verbindungen – `EstimatedALBActiveConnectionCount`
- Geschätzte Anzahl neuer ALB-Verbindungen – `EstimatedALBNewConnectionCount`

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den ELB-Namespace.
4. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie eine Metrikdimension zum Anzeigen von Metriken nach Load Balancer, nach Availability Zone oder von allen Load Balancern.
   - Um eine Metrik für alle Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.
   - Um die Metriken für einen einzelnen Load Balancer anzuzeigen, geben Sie den Namen in das Suchfeld ein.
   - Um die Metriken für eine einzelne Availability Zone anzuzeigen, geben Sie den Namen in das Suchfeld ein.

Zugriffsprotokolle für Ihren Classic Load Balancer

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen zu Anforderungen erfassen, die an Ihren Load Balancer gesendet werden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembehebung verwenden.

Zugriffsprotokolle sind ein optionales Feature von Elastic Load Balancing, das standardmäßig deaktiviert ist. Nachdem Sie die Zugriffsprotokolle für Ihren Load Balancer aktiviert haben, erfasst Elastic Load Balancing die Protokolle und speichert sie in dem von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Zugriffsprotokollierung jederzeit deaktivieren.

Jede Zugriffsprotokolldatei wird automatisch mit SSE-S3 verschlüsselt, bevor sie im S3-Bucket gespeichert und beim Zugriff auf die Datei entschlüsselt wird. Sie müssen keine Maßnahmen ergreifen. Ver- und Entschlüsselung werden transparent durchgeführt. Jede Protokolldatei ist mit einem eindeutigen Schlüssel verschlüsselt, der wiederum mit einem KMS-Schlüssel verschlüsselt wird, der regelmäßig rotiert wird. Weitere Informationen finden Sie unter Schützen von Daten mithilfe

serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) im Amazon S3 S3-Benutzerhandbuch.

Es fallen für die Zugriffsprotokolle keine zusätzlichen Gebühren an. Sie zahlen Speicherkosten für Amazon S3, aber Sie zahlen nicht für die Bandbreite, die von Elastic Load Balancing zum Senden von Protokolldateien an Amazon S3 verwendet wird. Weitere Information zu Speicherkosten finden Sie unter Amazon S3 – Preise.

Inhalt

Zugriffsprotokolldateien

Elastic Load Balancing veröffentlicht eine Protokolldatei für jeden Load-Balancer-Knoten in dem von Ihnen angegebenen Intervall. Sie können ein Veröffentlichungsintervall von entweder 5 Minuten oder 60 Minuten festlegen, wenn Sie das Zugriffsprotokoll für Ihren Load Balancer aktivieren. Elastic Load Balancing veröffentlicht Protokolle standardmäßig in einem 60-Minuten-Intervall. Wenn das Intervall 5 Minuten lang ist, werden die Protokolle um 1:05, 1:10, 1:15 usw. veröffentlicht. Der Start der Protokollbereitstellung verzögert sich um bis zu 5 Minuten, wenn das Intervall auf 5 Minuten eingestellt ist, und bis zu 15 Minuten, wenn das Intervall auf 60 Minuten eingestellt ist. Sie können das Veröffentlichungsintervall jederzeit ändern.

Der Load Balancer kann mehrere Protokolle für denselben Zeitraum bereitstellen. Dies passiert in der Regel, wenn die Website hohen Datenverkehr, mehrere Load Balancer-Knoten und ein kurzes Protokollveröffentlichungsintervall hat.

Die Dateinamen der Zugriffsprotokolle verwenden das folgende Format:

```
amzn-s3-demo-loadbalancer-logs[/logging-prefix]/AWSLogs/aws-account-id/
elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-
balancer-name_end-time_ip-address_random-string.log
```

amzn-s3- demo-loadbalancer-logs

Der Name des S3-Buckets.

prefix

(Optional) Das Präfix (logische Hierarchie) für den Bucket. Das von Ihnen angegebene Präfix darf die Zeichenfolge `AWSLogs` nicht enthalten. Weitere Informationen finden Sie unter Organisieren von Objekten mit Präfixen.

`AWSLogs`

Wir fügen den Teil des Dateinamens hinzu, der mit `AWSLogs` nach dem von Ihnen angegebenen Bucket-Namen und dem optionalen Präfix beginnt.

aws-account-id

Die AWS Konto-ID des Besitzers.

Region

Die Region für Ihren Load Balancer und den S3-Bucket.

JJJJ/MM/TT

Das Datum, an dem das Protokoll übermittelt wurde.

load-balancer-name

Der Name des Load Balancers.

end-time

Das Datum und die Uhrzeit, an dem das Protokollierungsintervall endete. Beispiel: Eine Endzeit von 20140215T2340Z enthält Einträge für Anforderungen zwischen 23:35 und 23:40 Uhr, wenn das Veröffentlichungsintervall 5 Minuten beträgt.

ip-address

Die IP-Adresse des Load Balancer-Knotens, der die Anforderung verarbeitet hat. Für einen internen Load Balancer handelt es sich hierbei um eine private IP-Adresse.

random-string

Eine vom System generierte zufällige Zeichenfolge.

Im Folgenden finden Sie ein Beispiel für einen Protokolldateinamen mit dem Präfix „my-app“:

```
s3://amzn-s3-demo-loadbalancer-logs/my-app/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

Im Folgenden finden Sie ein Beispiel für einen Protokolldateinamen ohne Präfix:

```
s3://amzn-s3-demo-loadbalancer-logs/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

Sie können Ihre Protokolldateien beliebig lange im Bucket speichern. Sie können aber auch Amazon S3-Lebenszyklusregeln aufstellen, anhand derer die Protokolldateien automatisch archiviert oder gelöscht werden. Weitere Informationen finden Sie unter Object Lifecycle Management im Amazon S3 S3-Benutzerhandbuch.

Zugriffsprotokolleinträge

Elastic Load Balancing protokolliert Anforderungen, die an den Load Balancer gesendet wurden, einschließlich Anforderungen, die nicht bei den Backend-Instances ankamen. Wenn beispielsweise ein Client eine falsch formatierte Anforderung sendet oder keine fehlerfreie Instance für die Antwort verfügbar ist, werden die Anforderungen trotzdem protokolliert.

> **Important**
>
> Elastic Load Balancing protokolliert Anfragen nach bestmöglichem Bemühen. Wir empfehlen, dass Sie die Zugriffsprotokolle verwende, um die Art der Anforderungen zu verstehen, nicht als eine vollständige Buchführung aller Anforderungen.

Syntax

Jeder Protokolleintrag enthält die Details einer einzelnen Anforderung an den Load Balancer. Alle Felder im Protokolleintrag sind durch Leerzeichen getrennt. Jeder Eintrag in der Protokolldatei weist das folgende Format auf:

```
timestamp elb client:port backend:port request_processing_time backend_processing_time
 response_processing_time elb_status_code backend_status_code received_bytes sent_bytes
 "request" "user_agent" ssl_cipher ssl_protocol
```

Die folgende Tabelle beschreibt die Felder eines Zugriffsprotokolleintrags.

Feld	Beschreibung
time	Die Uhrzeit, zu der der Load Balancer die Anforderung vom Client erhalten hat, im ISO 8601-Format.
elb	Der Name des Load Balancers
client:port	Die IP-Adresse und den Port des anfordernden Clients.
backend:port	Die IP-Adresse und der Port der registrierten Instance, die diese Anfrage verarbeitet hat. Wenn der Load Balancer die Anforderung nicht an eine registrierte Instance senden kann oder die Instance die Verbindung schließt, bevor eine Antwort gesendet werden kann, ist dieser Wert -. Dieser Wert kann auch auf - gesetzt werden, wenn die registrierte Instance nicht vor dem Timeoutwert für die Leerlaufzeit reagiert.
request_processing_time	[HTTP-Listener] Die gesamte abgelaufene Zeit in Sekunden ab dem Zeitpunkt, zu dem der Load Balancer die Anforderung empfangen hat, bis zu dem Zeitpunkt, an dem sie an eine registrierte Instance gesendet wurde. [TCP-Listener] Die gesamte abgelaufene Zeit in Sekunden ab dem Zeitpunkt, zu dem der Load Balancer eine TCP/SSL-Verbindung von einem Client akzeptiert hat, bis zu dem Zeitpunkt, an dem der Load Balancer das erste Datenbyte an eine registrierte Instance gesendet hat. Dieser Wert wird auf -1 festgelegt, wenn der Load Balancer die Anforderung nicht einer registrierten Instance zuteilen kann. Dies kann der Fall sein, wenn die registrierte Instance die Verbindung vor dem Leerlaufzeitlimit schließt oder wenn der Client eine falsch formatierte Anforderung sendet. Bei TCP-Listenern kann dies auch vorkommen, wenn der Client eine Verbindung mit dem Load Balancer herstellt, aber keine Daten sendet.

Feld	Beschreibung
	Dieser Wert kann auch auf `-1` gesetzt werden, wenn die registrierte Instance nicht vor dem Timeoutwert für die Leerlaufzeit reagiert.
backend_processing_time	[HTTP-Listener] Die gesamte abgelaufene Zeit in Sekunden ab dem Zeitpunkt, zu dem der Load Balancer die Anforderung an eine registrierte Instance gesendet hat, bis zu dem Zeitpunkt, an dem die Instance begann, die Antwort-Header zu senden. [TCP-Listener] Die gesamte abgelaufene Zeit in Sekunden, bis der Load Balancer erfolgreich eine Verbindung zu einer registrierten Instance hergestellt hat. Dieser Wert wird auf `-1` festgelegt, wenn der Load Balancer die Anforderung nicht einer registrierten Instance zuteilen kann. Dies kann der Fall sein, wenn die registrierte Instance die Verbindung vor dem Leerlaufzeitlimit schließt oder wenn der Client eine falsch formatierte Anforderung sendet. Dieser Wert kann auch auf `-1` gesetzt werden, wenn die registrierte Instance nicht vor dem Timeoutwert für die Leerlaufzeit reagiert.

Feld	Beschreibung
response_processing_time	[HTTP-Listener] Die gesamte abgelaufene Zeit (in Sekunden) ab dem Zeitpunkt, zu dem der Load Balancer den Antwort-Header von der registrierten Instance erhalten hat, bis zu dem Zeitpunkt, an dem er begonnen hat, die Antwort an den Client zu senden. Dies umfasst sowohl die Wartezeit am Load Balancer als auch die Zeit für die Herstellung der Verbindung vom Load Balancer zum Client. [TCP-Listener] Die gesamte abgelaufene Zeit in Sekunden ab dem Zeitpunkt, zu dem der Load Balancer das erste Byte von der registrierten Instance erhalten hat, bis zu dem Zeitpunkt, an dem er begonnen hat, die Antwort an den Client zu senden. Dieser Wert wird auf `-1` festgelegt, wenn der Load Balancer die Anforderung nicht einer registrierten Instance zuteilen kann. Dies kann der Fall sein, wenn die registrierte Instance die Verbindung vor dem Leerlaufzeitlimit schließt oder wenn der Client eine falsch formatierte Anforderung sendet. Dieser Wert kann auch auf `-1` gesetzt werden, wenn die registrierte Instance nicht vor dem Timeoutwert für die Leerlaufzeit reagiert.
elb_status_code	[HTTP-Listener] Der Statuscode der Antwort vom Load Balancer.
backend_status_code	[HTTP-Listener] Der Statuscode der Antwort von der registrierten Instance.
received_bytes	Die Größe der Anforderung, in Byte, die vom Client (Auftraggeber) eingegangen ist. [HTTP-Listener] Der Wert enthält den Anforderungstext, jedoch nicht die Header. [TCP-Listener] Der Wert enthält den Anforderungstext und den Header.

Feld	Beschreibung
sent_bytes	Die Größe der Antwort, in Byte, die an den Client (Auftraggeber) gesendet wurde. [HTTP-Listener] Der Wert enthält den Antworttext, jedoch nicht die Header. [TCP-Listener] Der Wert enthält den Anforderungstext und den Header.
request	Die Anforderungszeile vom Client in Anführungszeichen und protokoll iert im folgenden Format: HTTP-Methode + Protokoll://Host-Header:Por t + Pfad + HTTP-Version. Der Load Balancer behält die vom Client gesendete URL bei der Aufnahme des Anforderungs-URI unverände rt bei. Es wird kein Inhaltstyp für die Zugriffsprotokolldatei festgelegt. Berücksichtigen Sie bei der Verarbeitung des Feldes, wie der Client die URL gesendet hat. [TCP-Listener] Die URL hat drei Bindestriche, jeweils durch ein Leerzeich en getrennt und endet mit einem Leerzeichen ("- - - ").
user_agent	[HTTP/HTTPS listener] A User-Agent string that identifies the client that originated the request. The string consists of one or more product identifiers, product[/version]. Wenn die Zeichenfolge länger als 8 KB ist, wird sie gekürzt.
ssl_cipher	[Die HTTPS/SSL listener] The SSL cipher. This value is recorded only if the incoming SSL/TLS Verbindung wurde nach einer erfolgreichen Verhandlung hergestellt. Andernfalls wird der Wert auf - festgelegt.
ssl_protocol	[Die HTTPS/SSL listener] The SSL protocol. This value is recorded only if the incoming SSL/TLS Verbindung wurde nach einer erfolgreichen Verhandlung hergestellt. Andernfalls wird der Wert auf - festgelegt.

Beispiele

Beispiel für HTTP-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen HTTP-Listener (Port 80 zu Port 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000073
 0.001048 0.000057 200 200 0 29 "GET http://www.example.com:80/ HTTP/1.1" "curl/7.38.0"
 - -
```

Beispiel für HTTPS-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen HTTPS-Listener (Port 443 zu Port 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80
 0.000086 0.001048 0.001337 200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1"
 "curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2
```

Beispiel für TCP-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen TCP-Listener (Port 8080 zu Port 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001069
 0.000028 0.000041 - - 82 305 "- - - " "-" - -
```

Beispiel für SSL-Eintrag

Es folgt ein Beispiel für einen Protokolleintrag für einen SSL-Listener (Port 8443 zu Port 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001065
 0.000015 0.000023 - - 57 502 "- - - " "-" ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2
```

Verarbeiten von Zugriffsprotokollen

Falls es viele Zugriff auf Ihre Website gibt, kann der Load Balancer Protokolldateien mit mehreren Gigabyte an Daten generieren. Möglicherweise sind Sie nicht in der Lage, eine so große Datenmenge mithilfe von line-by-line Processing zu verarbeiten. Daher müssen Sie möglicherweise Tools zur Datenanalyse verwenden, die parallele Verarbeitungslösungen bieten. Beispielsweise können Sie die folgenden analytischen Tools zum Analysieren und Verarbeiten von Zugriffsprotokollen verwenden:

- Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mit Standard-SQL erleichtert. Weitere Informationen finden Sie unter Abfragen von Classic-Load-Balancer-Protokollen im Benutzerhandbuch zu Amazon Athena.
- Loggly

- Splunk
- Sumo Logic

Aktivieren der Zugriffsprotokolle für Ihren Classic Load Balancer

Um die Zugriffsprotokollierung für Ihren Load Balancer zu aktivieren, müssen Sie den Namen des Amazon-S3-Buckets angeben, in dem der Load Balancer die Protokolle speichert. Außerdem müssen Sie eine Bucket-Richtlinie zu diesem Bucket hinzufügen, der Elastic Load Balancing die Schreibberechtigung für den Bucket erteilt.

Aufgaben

- Schritt 1: Einen S3-Bucket erstellen
- Schritt 2: Hinzufügen von Richtlinien zu Ihrem S3-Bucket
- Schritt 3: Konfigurieren von Zugriffsprotokollen
- Schritt 4: Überprüfen der Bucket-Berechtigungen
- Fehlerbehebung

Schritt 1: Einen S3-Bucket erstellen

Wenn Sie Zugriffsprotokolle aktivieren, müssen Sie einen S3-Bucket für die Zugriffsprotokolldateien angeben. Der Bucket muss die folgenden Anforderungen erfüllen.

Voraussetzungen

- Der Bucket muss sich in derselben Region wie der Load Balancer befinden. Der Bucket und der Load Balancer können verschiedenen Konten gehören.
- Die einzige serverseitige Verschlüsselungsoption, die unterstützt wird, sind von Amazon S3 verwaltete Schlüssel (SSE-S3). Weitere Informationen finden Sie unter Amazon-S3-verwaltete Verschlüsselungsschlüssel (SSE-S3).

Erstellen eines S3-Buckets mithilfe der Amazon-S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Create Bucket (Bucket erstellen) aus.
3. Führen Sie auf der Seite Create bucket (Bucket erstellen) die folgenden Schritte aus:

a. Geben Sie unter Bucket Name (Bucket-Name) einen Namen für den Bucket ein. Dieser Name muss unter den in Amazon S3 vorhandenen Bucket-Namen eindeutig sein. In einigen Regionen kann es zusätzliche Einschränkungen für Bucket-Namen geben. Weitere Informationen finden Sie unter Bucket-Kontingente, Einschränkungen und Einschränkungen im Amazon S3 S3-Benutzerhandbuch.
b. Wählen Sie unter AWS -Region die Region aus, in der Sie Ihren Load Balancer erstellt haben.
c. Wählen Sie für Standardverschlüsselung die Option Von Amazon S3 verwaltete Schlüssel (SSE-S3) aus.
d. Wählen Sie Create Bucket (Bucket erstellen) aus.

Schritt 2: Hinzufügen von Richtlinien zu Ihrem S3-Bucket

Der S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Berechtigung zum Schreiben von Zugriffsprotokollen in den Bucket gewährt. Bucket-Richtlinien sind eine Sammlung von JSON-Anweisungen, die in der Sprache der Zugriffsrichtlinie geschrieben sind, um Zugriffsberechtigungen für Ihre Buckets zu definieren. Jeder Anweisung enthält Informationen über eine einzelne Berechtigung und besteht aus einer Reihe von Elementen.

Wenn Sie einen vorhandenen Bucket verwenden, dem bereits eine Richtlinie angehängt ist, können Sie die Anweisung für Zugriffsprotokolle von Elastic Load Balancing zu der Richtlinie hinzufügen. Wenn Sie dies tun, empfehlen wir, dass Sie eine Beurteilung der daraus resultierenden Berechtigungen vornehmen, um sicherzustellen, dass sie für die Benutzer geeignet sind, die Zugriff auf die Bucket-Zugriffsprotokolle benötigen.

Bucket-Richtlinie

Diese Richtlinie gewährt dem Protokolllieferdienst Berechtigungen.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
```

```
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
    }
  ]
}
```

Geben Sie unter Verwendung des in der Beispielrichtlinie angegebenen Formats den ARN des Speicherorts für die Zugriffsprotokolle ein. `Resource` Geben Sie immer die Konto-ID des Kontos beim Load Balancer in den Ressourcenpfad des S3-Bucket-ARN ein. Dadurch wird sichergestellt, dass nur Load Balancer des angegebenen Kontos Zugriffsprotokolle in den S3-Bucket schreiben können.

Der von Ihnen angegebene ARN hängt davon ab, ob Sie bei der Aktivierung von Zugriffsprotokollen in Schritt 3 ein Präfix angeben möchten.

Beispiel für einen S3-Bucket-ARN mit einem Präfix

Der S3-Bucket-Name ist amzn-s3-demo-logging-bucket und das Präfix istlogging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

[AWS GovCloud (US)] Das folgende Beispiel verwendet die ARN-Syntax für AWS GovCloud (US) Regions.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Beispiel für einen S3-Bucket-ARN ohne Präfix

Der Name des S3-Buckets lautetamzn-s3-demo-logging-bucket. Der S3-Bucket-ARN enthält keinen Präfixteil.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

[AWS GovCloud (US)] Das folgende Beispiel verwendet die ARN-Syntax für AWS GovCloud (US) Regions.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Legacy-Bucket-Richtlinie

Bisher benötigten wir für Regionen, die vor August 2022 verfügbar waren, eine Richtlinie, die Berechtigungen für ein Elastic Load Balancing Balancing-Konto gewährte, das spezifisch für die Region war. Diese alte Richtlinie wird weiterhin unterstützt, wir empfehlen jedoch, sie durch die neuere Richtlinie oben zu ersetzen. Wenn Sie es vorziehen, weiterhin die alte Bucket-Richtlinie zu verwenden, die hier nicht aufgeführt ist, können Sie dies tun.

Als Referenz finden Sie hier die IDs Elastic Load Balancing Balancing-Konten, in denen Sie angeben müssen`Principal`. Beachten Sie, dass Regionen, die nicht in dieser Liste aufgeführt sind, die alte Bucket-Richtlinie nie unterstützt haben.

- USA Ost (Nord-Virginia) – 127311923021
- USA Ost (Ohio) – 033677994240
- USA West (Nordkalifornien) – 027434742980
- USA West (Oregon) – 797873946194
- Afrika (Kapstadt) – 098369216593
- Asien-Pazifik (Hongkong) – 754344448648
- Asien-Pazifik (Jakarta) – 589379963580
- Asien-Pazifik (Mumbai) – 718504428378
- Asien-Pazifik (Osaka) – 383597477331
- Asien-Pazifik (Seoul) – 600734575887
- Asien-Pazifik (Singapur) – 114774131450
- Asien-Pazifik (Sydney) – 783225319266
- Asien-Pazifik (Tokio) – 582318560864
- Kanada (Zentral) – 985666609251
- Europa (Frankfurt) – 054676820928
- Europa (Irland) – 156460612806
- Europa (London) – 652711504416
- Europa (Mailand) – 635631232127
- Europa (Paris) – 009996457667
- Europa (Stockholm) – 897822967062
- Naher Osten (Bahrain) – 076674570225

- Südamerika (São Paulo) – 507241528517
- AWS GovCloud (US-Ost) — 190560391635
- AWS GovCloud (US-West) — 048591011584

Bewährte Methoden für die Gewährleistung der Sicherheit

Um die Sicherheit zu erhöhen, verwenden Sie einen präzisen S3-Bucket. ARNs

- Verwenden Sie den vollständigen Ressourcenpfad, nicht nur den S3-Bucket-ARN.
- Geben Sie den Konto-ID-Teil des S3-Bucket-ARN an.
- Verwenden Sie keine Platzhalter (*) im Konto-ID-Teil des S3-Bucket-ARN.

Nachdem Sie Ihre Bucket-Richtlinie erstellt haben, verwenden Sie eine Amazon S3 S3-Schnittstelle, z. B. die Amazon S3 S3-Konsole oder AWS CLI Befehle, um Ihre Bucket-Richtlinie an Ihren S3-Bucket anzuhängen.

Um Ihre Bucket-Richtlinie mithilfe der Konsole an Ihren Bucket anzuhängen

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, um seine Detailseite zu öffnen.
3. Wählen Sie Berechtigungen und anschließend Bucket-Richtlinie, Bearbeiten aus.
4. Aktualisieren Sie die Bucket-Richtlinie, um die erforderlichen Berechtigungen zu gewähren.
5. Wählen Sie Änderungen speichern aus.

Um Ihre Bucket-Richtlinie mit dem S3-Bucket anzuhängen AWS CLI

Verwenden Sie den put-bucket-policy-Befehl. In diesem Beispiel wurde die Bucket-Richtlinie in der angegebenen JSON-Datei gespeichert.

```
aws s3api put-bucket-policy \
    --bucket amzn-s3-demo-bucket \
    --policy file://access-log-policy.json
```

Schritt 3: Konfigurieren von Zugriffsprotokollen

Verwenden Sie das folgende Verfahren, um Zugriffsprotokolle so zu konfigurieren, dass Anforderungsinformationen erfasst und Protokolldateien an Ihren S3-Bucket gesendet werden.

Voraussetzungen

Der Bucket muss die in Schritt 1 beschriebenen Anforderungen erfüllen und Sie müssen eine Bucket-Richtlinie wie in Schritt 2 beschrieben anhängen. Wenn Sie ein Präfix angeben, darf es die Zeichenfolge "AWSLogs“ nicht enthalten.

So konfigurieren Sie die Zugriffsprotokolle für Ihren Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen Ihres Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).
5. Gehen Sie auf der Seite Edit load balancer attributes (Load Balancer Attribute bearbeiten) im Abschnitt Monitoring (Überwachung) wie folgt vor:
   a. Aktivieren Sie Access logs (Zugriffsprotokolle).
   b. Geben Sie für S3 URI (S3-URI) den S3-URI für Ihre Protokolldateien ein. Der URI, den Sie angeben, hängt davon ab, ob Sie ein Präfix verwenden.
      - URI mit einem Präfix: `s3://amzn-s3-demo-logging-bucket/logging-prefix`
      - URI ohne Präfix: `s3://amzn-s3-demo-logging-bucket`
   c. Behalten Sie das Logging interval (Protokollierungsintervall) bei `60 minutes - default`.
   d. Wählen Sie Änderungen speichern aus.

Um Zugriffsprotokolle für Ihren Load Balancer zu konfigurieren, verwenden Sie AWS CLI

Zuerst erstellen Sie eine .json-Datei zur Erfassung von Protokollen durch Elastic Load Balancing und deren Bereitstellung alle 60 Minuten auf dem S3-Bucket, den Sie für die Protokolle erstellt haben:

```
{
  "AccessLog": {
    "Enabled": true,
    "S3BucketName": "amzn-s3-demo-logging-bucket",
    "EmitInterval": 60,
    "S3BucketPrefix": "my-app"
  }
}
```

Geben Sie als Nächstes die JSON-Datei im modify-load-balancer-attributesBefehl wie folgt an:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes file://my-json-file.json
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
            "EmitInterval": 60,
            "S3BucketName": "amzn-s3-demo-logging-bucket",
            "S3BucketPrefix": "my-app"
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

So verwalten Sie den S3-Bucket für Ihre Zugriffsprotokolle

Stellen Sie sicher, dass Sie die Zugriffsprotokolle deaktivieren, bevor Sie den Bucket löschen, den Sie für Zugriffsprotokolle konfiguriert haben. Andernfalls könnte Elastic Load Balancing die Zugriffsprotokolle für Ihren Load Balancer in AWS-Konto diesen neuen Bucket schreiben, wenn ein neuer Bucket mit demselben Namen und der erforderlichen Bucket-Richtlinie in einem Bucket erstellt wurde, den Sie nicht besitzen.

Schritt 4: Überprüfen der Bucket-Berechtigungen

Nachdem Zugriffsprotokolle für den Load Balancer aktiviert ist, überprüft Elastic Load Balancing den S3-Bucket und erstellt eine Testdatei, um sicherzustellen, dass die Bucket-Richtlinie die erforderlichen Berechtigungen angibt. Sie können die S3-Konsole verwenden, um sicherzustellen, dass die Testdatei erstellt wurde. Die Testdatei ist keine tatsächliche Zugriffsprotokolldatei; sie enthält keine Beispieldatensätze.

So überprüfen Sie, ob Elastic Load Balancing eine Testdatei in Ihrem S3-Bucket erstellt hat

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des S3-Buckets aus, den Sie für Zugriffsprotokolle angegeben haben.

3. Navigieren Sie zur Testdatei, `ELBAccessLogTestFile`. Der Standort hängt davon ab, ob Sie ein Präfix verwenden.

   - Standort mit einem Präfix:*amzn-s3-demo-loadbalancer-logs*/*logging-prefix*/AWSLogs/*123456789012*/ELBAccessLogTestFile
   - Standort ohne Präfix:*amzn-s3-demo-loadbalancer-logs*/AWSLogs/*123456789012*/ELBAccessLogTestFile

Fehlerbehebung

Zugriff verweigert für Bucket:***bucket-name***. Bitte überprüfen Sie die S3bucket-Berechtigung

Wenn Sie diesen Fehler erhalten, kann dies die folgenden möglichen Ursachen haben:

- Die Bucket-Policy gewährt Elastic Load Balancing nicht die Berechtigung, Zugriffsprotokolle in den Bucket zu schreiben. Stellen Sie sicher, dass Sie die richtige Bucket-Richtlinie für die Region verwenden. Stellen Sie sicher, dass der Ressourcen-ARN denselben Bucket-Namen verwendet, den Sie bei der Aktivierung von Zugriffsprotokollen angegeben haben. Stellen Sie sicher, dass der Ressourcen-ARN kein Präfix enthält, wenn Sie bei der Aktivierung von Zugriffsprotokollen kein Präfix angegeben haben.
- Der Bucket verwendet eine nicht unterstützte serverseitige Verschlüsselungsoption. Der Bucket muss von Amazon S3 verwaltete Schlüssel (SSE-S3) verwenden.

Deaktivieren der Zugriffsprotokolle für Ihren Classic Load Balancer

Sie können die Zugriffsprotokolle für Ihren Load Balancer jederzeit deaktivieren. Nachdem Sie Zugriffsprotokolle deaktiviert haben, verbleiben Ihre Zugriffsprotokolle in Ihrem Amazon-S3-Bucket, bis Sie sie löschen. Weitere Informationen finden Sie unter Arbeiten mit S3-Buckets im Amazon S3 S3-Benutzerhandbuch.

So deaktivieren Sie die Zugriffsprotokolle für Ihren Load Balancer mithilfe der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter LOAD BALANCING die Option Load Balancers aus.
3. Wählen Sie den Namen Ihres Load Balancers aus, um die Detailseite zu öffnen.
4. Klicken Sie in der Registerkarte Attributes (Attribute) auf Edit (Bearbeiten).

5. Deaktivieren Sie auf der Seite Edit load balancer attributes (Load Balancer-Attribute bearbeiten) im Abschnitt Monitoring (Überwachung) die Access logs (Zugriffsprotokolle).

Um Zugriffsprotokolle zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den folgenden modify-load-balancer-attributesBefehl, um Zugriffsprotokolle zu deaktivieren:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"AccessLog\":{\"Enabled\":false}}"
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
    "LoadBalancerName": "my-loadbalancer",
    "LoadBalancerAttributes": {
        "AccessLog": {
            "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
            "EmitInterval": 60,
            "Enabled": false,
            "S3BucketPrefix": "my-app"
        }
    }
}
```

Fehlerbehebung bei Ihrem Classic Load Balancer

In der folgenden Tabelle sind die Fehlerbehebungsressourcen aufgelistet, die bei der Arbeit mit dem Classic Load Balancer nützlich sind.

API-Fehler

Fehler
CertificateNotFound: Undefiniert
OutofService: Ein vorübergehender Fehler ist aufgetreten

HTTP-Fehler

Fehler
HTTP 400: BAD_REQUEST
HTTP 405: METHOD_NOT_ALLOWED
HTTP 408: Request Timeout
HTTP 502: Bad Gateway
HTTP 503: Service Unavailable
HTTP 504: Gateway Timeout

Antwortcode-Metriken

Antwortcode-Metrik
HTTPCode_ELB_4XX
HTTPCode_ELB_5XX
HTTPCode_Backend_2xx

Antwortcode-Metrik
HTTPCode_Backend_3xx
HTTPCode_Backend_4xx
HTTPCode_Backend_5xx

Probleme bei der Zustandsprüfung

Problem
Zustandsprüfungs-Zielseitenfehler
Zeitlimit bei der Verbindung zu den Instances ist überschritten
Authentifizierung mit öffentlichem Schlüssel schlägt fehl
Instance empfängt keinen Datenverkehr vom Load Balancer
Ports auf Instance sind nicht offen
Instances in einer Auto-Scaling-Gruppe schlagen bei der ELB-Zustandsprüfung fehl

Probleme mit der Verbindung

Problem
Clients können keine Verbindung zu einem mit dem Internet verbundenen Load Balancer herstellen
Anfragen, die an eine benutzerdefinierte Domain gesendet werden, werden vom Load Balancer nicht empfangen
An den Load Balancer gesendete HTTPS-Anfragen geben „NET::ERR_CERT_COMMON_NAME_INVALID“ zurück

Instance-Registrierungsprobleme

Problem
Die Registrierung einer EC2 Instance dauert zu lange
Instance, die aus einem gebührenpflichtigen AMI gestartet wurde, kann nicht registriert werden

Fehlerbehebung beim Classic Load Balancer: API-Fehler

Nachfolgend finden Sie Fehlermeldungen von der Elastic-Load-Balancing-API, die potenziellen Ursachen und was Sie tun müssen, um das Problem zu lösen.

Fehlermeldungen

- CertificateNotFound: Undefiniert
- OutofService: Ein vorübergehender Fehler ist aufgetreten

CertificateNotFound: Undefiniert

Cause 1 (Ursache 1): Es gibt eine Verzögerung bei der Verbreitung des Zertifikats in alle Regionen, wenn es über die AWS Management Console erstellt wird. Wenn diese Verzögerung auftritt, wird die Fehlermeldung im letzten Schritt im Erstellungsprozess des Load Balancers angezeigt.

Solution 1: Warten Sie etwa 15 Minuten und versuchen Sie es erneut. Falls das Problem weiterhin besteht, rufen Sie das AWS -Support Center auf, um Unterstützung zu erhalten.

Ursache 2: Wenn Sie die API AWS CLI oder direkt verwenden, kann dieser Fehler auftreten, wenn Sie einen Amazon-Ressourcennamen (ARN) für ein Zertifikat angeben, das nicht existiert.

Lösung 2: Verwenden Sie die Aktion AWS Identity and Access Management (IAM) GetServerCertificate, um den Zertifikat-ARN abzurufen und zu überprüfen, ob Sie den richtigen Wert für den ARN angegeben haben.

OutofService: Ein vorübergehender Fehler ist aufgetreten

Cause (Ursache): Es ist ein vorübergehendes internes Problem innerhalb des Elastic-Load-Balancing-Service oder des zugrunde liegenden Netzwerks aufgetreten. Dieses temporäre Problem

kann auch auftreten, wenn Elastic Load Balancing den Zustand des Load Balancers und seiner registrierten Instances abfragt.

Solution: Wiederholen Sie den API-Aufruf. Falls das Problem weiterhin besteht, rufen Sie das AWS - Support Center auf, um Unterstützung zu erhalten.

Fehlerbehebung beim Classic Load Balancer: HTTP-Fehler

Die HTTP-Methode (auch als Verb bezeichnet) bestimmt die Aktion, die auf die Ressource angewendet wird, die eine HTTP-Anforderung empfängt. Die Standardmethoden für HTTP-Anfragen sind in RFC 2616, Methodendefinitionen definiert. Zu den Standardmethoden zählen GET, HEAD, POST, PUT und OPTIONS. Einige Webanwendungen erfordern Methoden (und führen diese manchmal ein), die Erweiterungen der HTTP/1.1-Methoden darstellen. Einige Beispiele für erweiterte HTTP-Methoden sind PATCH, REPORT, MKCOL, PROPFIND, MOVE und LOCK. Elastic Load Balancing akzeptiert alle Standard- und Nicht-Standard-HTTP-Methoden.

HTTP-Anforderungen und -Antworten verwenden Header-Felder, um Informationen per HTTP-Nachricht zu senden. Header-Felder sind durch einen Doppelpunkt getrennte Name/Wert-Paare, die durch eine Zeilenumschaltung und einen Zeilenvorschub getrennt sind. Ein Standardsatz von HTTP-Header-Feldern ist in RFC 2616, Nachrichten-Header definiert. Weitere Informationen finden Sie unter HTTP-Header und Classic Load Balancer.

Wenn ein Load Balancer eine HTTP-Anfrage empfängt, überprüft er diese auf falsch formatierte Anforderungen und die Länge der Methode. Der gesamte Länge der Methode in einer HTTP-Anforderung an einen Load Balancer darf 127 Zeichen nicht überschreiten. Wenn die HTTP-Anfrage beide Prüfungen besteht, sendet der Load Balancer die Anfrage an die EC2 Instance. Falls das Methodenfeld in der Anforderung falsch formatiert ist, reagiert der Load Balancer mit einem HTTP 400: BAD_REQUEST-Fehler. Wenn die Länge der Methode in der Anforderung 127 Zeichen überschreitet, reagiert der Load Balancer mit einem HTTP 405: METHOD_NOT_ALLOWED-Fehler.

Die EC2 Instance verarbeitet eine gültige Anfrage, indem sie die Methode in der Anfrage implementiert und eine Antwort an den Client zurücksendet. Ihre Instances müssen so konfiguriert werden, dass sie unterstützte und nicht unterstützte Methoden verarbeiten können.

Nachfolgend finden Sie mögliche Fehlermeldungen von Ihrem Load Balancer, die potenziellen Ursachen und was Sie tun müssen, um das Problem zu lösen.

Fehlermeldungen

- HTTP 400: BAD_REQUEST

HTTP 400: BAD_REQUEST

Description: Gibt an, dass der Client eine fehlerhafte Anforderung gesendet hat.

Cause 1 (Ursache 1): Der Client hat eine falsch formatierte Anforderung gesendet, die die HTTP-Spezifikationen nicht erfüllt. Beispielsweise darf eine Anforderung keine Leerzeichen in der URL haben.

Cause 2 (Ursache 2): Der Client verwendet die HTTP-CONNECT-Methode, die von Elastic Load Balancing nicht unterstützt wird.

Solution: Stellen Sie direkt eine Verbindung mit der Instance her und erfassen Sie die Details der Client-Anforderung. Überprüfen Sie die Header und die URL auf falsch formatierte Anforderungen. Überprüfen Sie, ob die Anforderung die HTTP-Spezifikationen erfüllt. Vergewissern Sie sich, dass HTTP-CONNECT nicht verwendet wird.

HTTP 405: METHOD_NOT_ALLOWED

Description: Gibt an, dass die Methodenlänge ungültig ist.

Cause: Die Länge der Methode im Header der Anforderung überschreitet 127 Zeichen.

Solution: Überprüfen Sie die Länge der Methode.

HTTP 408: Request Timeout

Description: Zeigt an, dass der Client die Anforderung storniert oder keine vollständige Anforderung gesendet hat.

Cause 1: Eine Netzwerkunterbrechung oder eine fehlerhafte Anforderungskonstruktion, z. B. ein nur teilweise angegebener Header; die angegebene Inhaltsgröße passt nicht zum tatsächlich übertragenen Inhalt usw.

Solution 1: Untersuchen Sie den Code, der die Anfrage stellt, und versuchen Sie ihn direkt an Ihre registrierten Instances zu senden (oder an eine Entwicklungs-/Testumgebung), in der Sie mehr Kontrolle über die tatsächliche Anforderung haben.

Cause 2: Verbindung zum Client wurde geschlossen (Load Balancer konnte keine Antwort senden)

Solution 2: Überprüfen Sie, ob der Client nicht die Verbindung schließt, bevor eine Antwort gesendet wird, indem Sie einen Packet-Sniffer auf dem Computer verwenden, von dem die Anforderung stammt.

HTTP 502: Bad Gateway

Description: Gibt an, dass der Load Balancer die Antwort von einer registrierten Instance nicht analysieren konnte.

Cause: Falsch formatierte Antwort von der Instance oder möglicherweise ein Problem mit dem Load Balancer.

Solution: Überprüfen Sie, ob die Antwort von der Instance den HTTP-Spezifikationen entspricht. Rufen Sie das AWS -Support Center auf, um Unterstützung zu erhalten.

HTTP 503: Service Unavailable

Description: Zeigt an, dass der Load Balancer oder die registrierten Instances den Fehler verursachen.

Cause 1: Nicht genügend Kapazität auf dem Load Balancer für die Verarbeitung der Anforderung.

Solution 1: Dies ist ein vorübergehendes Problem und sollte nicht länger als ein paar Minuten dauern. Falls es weiterhin besteht, rufen Sie das AWS -Support Center auf, um Unterstützung zu erhalten.

Ursache 2: Es sind keine registrierten Instances vorhanden.

Solution 2: Registrieren Sie mindestens eine Instance in jeder Availability Zone, in welcher der Load Balancer laut Konfiguration antworten soll. Überprüfen Sie dies, indem Sie sich die `HealthyHostCount` Kennzahlen unter ansehen CloudWatch. Wenn Sie nicht sicherstellen können, dass eine Instance in einer Availability Zone registriert ist, empfehlen wir eine zonenübergreifende Lastverteilung. Weitere Informationen finden Sie unter Konfigurieren des zonenübergreifenden Load Balancing für Ihren Classic Load Balancer.

Ursache 3: Es sind keine fehlerfreien Instances vorhanden.

Solution 3: Stellen Sie sicher, dass Sie in jeder Availability Zone über fehlerfreie Instances verfügen, in welcher der Load Balancer laut Konfiguration antworten soll. Überprüfen Sie dies anhand der Metrik `HealthyHostCount`.

Ursache 4: Die Anstiegswarteschlange ist voll.

Lösung 4: Stellen Sie sicher, dass die Kapazität Ihrer Instances zur Verarbeitung dieser Anforderung ausreicht. Überprüfen Sie dies anhand der Metrik `SpilloverCount`.

HTTP 504: Gateway Timeout

Description: Gibt an, dass der Load Balancer eine Verbindung geschlossen hat, da eine Anforderung nicht innerhalb des Zeitraums der Leerlaufzeitüberschreitung abgeschlossen wurde.

Cause 1: Die Anwendung benötigt für die Antwort länger als das konfigurierte Leerlaufzeitlimit.

Solution 1: Überwachen Sie die Metriken `HTTPCode_ELB_5XX` und `Latency`. Wenn es eine Erhöhung dieser Metriken gibt, kann dies daran liegen, dass die Anwendung nicht innerhalb des Leerlaufzeitlimits antwortet. Für detaillierte Informationen über die Zeitüberschreitung bei Anforderungen aktivieren Sie die Zugriffsprotokolle auf dem Load Balancer und überprüfen Sie die 504-Antwortcodes in den Protokollen, die von Elastic Load Balancing generiert wurden. Falls erforderlich, können Sie Ihre Kapazität oder das konfigurierte Leerlaufzeitlimit erhöhen, sodass langwierige Vorgänge (z. B. Hochladen einer großen Datei) abgeschlossen werden können. Weitere Informationen finden Sie unter Konfigurieren des Leerlaufverbindungszeitlimits für Ihren Classic Load Balancer und Wie behebe ich hohe Latenz im Elastic Load Balancing.

Cause 2 (Ursache 2): Registrierte Instances schließen die Verbindung zu Elastic Load Balancing.

Lösung 2: Aktivieren Sie die Keep-Alive-Einstellungen auf Ihren EC2 Instances und stellen Sie sicher, dass das Keep-Alive-Timeout größer ist als die Leerlauf-Timeout-Einstellungen Ihres Load Balancers.

Fehlerbehebung bei einem Classic Load Balancer: Antwortcode-Metriken

Ihr Load Balancer sendet Metriken CloudWatch für die an Clients gesendeten HTTP-Antwortcodes an Amazon und identifiziert dabei entweder den Load Balancer oder die registrierten Instances als Fehlerquelle. Sie können die von Ihrem Load Balancer zurückgegebenen CloudWatch Metriken verwenden, um Probleme zu beheben. Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Classic Load Balancer.

Im Folgenden finden Sie die von CloudWatch Ihrem Load Balancer zurückgegebenen Antwortcode-Metriken, die möglichen Ursachen und die Schritte, die Sie zur Behebung der Probleme ergreifen können.

Antwortcode-Metriken

- HTTPCode_ELB_4XX
- HTTPCode_ELB_5XX
- HTTPCode_Backend_2xx
- HTTPCode_Backend_3xx
- HTTPCode_Backend_4xx
- HTTPCode_Backend_5xx

HTTPCode_ELB_4XX

Cause: Eine falsch formatierte oder stornierte Anforderung vom Client.

Lösungen

- Siehe HTTP 400: BAD_REQUEST.
- Siehe HTTP 405: METHOD_NOT_ALLOWED.
- Siehe HTTP 408: Request Timeout.

HTTPCode_ELB_5XX

Cause: Entweder der Load Balancer oder die registrierte Instance verursacht den Fehler oder der Load Balancer kann die Antwort nicht analysieren.

Lösungen

- Siehe HTTP 502: Bad Gateway.
- Siehe HTTP 503: Service Unavailable.
- Siehe HTTP 504: Gateway Timeout.

HTTPCode_Backend_2xx

Cause: Eine normale, erfolgreiche Antwort von den registrierten Instances.

Solution: Keine.

HTTPCode_Backend_3xx

Cause: Eine umgeleitete Antwort von den registrierten Instances.

Solution: Rufen Sie die Zugriffsprotokolle oder die Fehlerprotokolle auf der Instance auf, um die Ursache zu ermitteln. Senden Sie Ihre Anforderungen direkt an die Instance (unter Umgehung des Load Balancers), um die Antworten zu sehen.

HTTPCode_Backend_4xx

Cause: Eine Client-Fehlerantwort aus den registrierten Instances.

Solution: Rufen Sie die Zugriffsprotokolle oder die Fehlerprotokolle auf den Instances auf, um die Ursache zu ermitteln. Senden Sie Anforderungen direkt an die Instance (unter Umgehung des Load Balancers), um die Antworten zu sehen.

> **Note**
>
> Wenn der Client eine HTTP-Anforderung storniert, die mit einem `Transfer-Encoding: chunked`-Header initiiert wurde, gibt es ein bekanntes Problem, bei dem der Load Balancer die Anforderung an die Instance weiterleitet, obwohl der Client die Anforderung storniert hat. Dies kann zu Backend-Fehlern führen.

HTTPCode_Backend_5xx

Cause: Eine Server-Fehlerantwort aus den registrierten Instances.

Solution: Rufen Sie die Zugriffsprotokolle oder die Fehlerprotokolle auf Ihren Instances auf, um die Ursache zu ermitteln. Senden Sie Anforderungen direkt an die Instance (unter Umgehung des Load Balancers), um die Antworten zu sehen.

> **Note**
>
> Wenn der Client eine HTTP-Anforderung storniert, die mit einem `Transfer-Encoding: chunked`-Header initiiert wurde, gibt es ein bekanntes Problem, bei dem der Load Balancer

die Anforderung an die Instance weiterleitet, obwohl der Client die Anforderung storniert hat. Dies kann zu Backend-Fehlern führen.

Fehlerbehebung beim Classic Load Balancer: Zustandsprüfungen

Ihr Load Balancer prüft den Zustand der registrierten Instances mit der Standard-Zustandsprüfungskonfiguration von Elastic Load Balancing oder mit einer benutzerdefinierten Zustandsprüfungskonfiguration, die Sie angeben. Die Zustandsprüfungskonfiguration enthält Informationen wie Protokoll, Ping-Port, Ping-Pfad, Reaktionszeitüberschreitung und Zustandsprüfungsintervall. Eine Instance wird als fehlerfrei betrachtet, wenn der Antwortcode 200 innerhalb des Zustandsprüfungsintervalls zurückgegeben wird. Weitere Informationen finden Sie unter Zustandsprüfungen für die Instances für Ihren Classic Load Balancer.

Wenn der aktuelle Status einiger oder aller Ihrer Instances `OutOfService` ist und das Beschreibungsfeld folgende Nachricht anzeigt: `Instance has failed at least the Unhealthy Threshold number of health checks consecutively`, sind die Instances bei der Load Balancer-Zustandsprüfung fehlgeschlagen. Nachfolgend finden Sie mögliche Probleme, die potenziellen Ursachen und was Sie tun müssen, um das Problem zu lösen.

Problembereiche

- Zustandsprüfungs-Zielseitenfehler
- Zeitlimit bei der Verbindung zu den Instances ist überschritten
- Authentifizierung mit öffentlichem Schlüssel schlägt fehl
- Instance empfängt keinen Datenverkehr vom Load Balancer
- Ports auf Instance sind nicht offen
- Instances in einer Auto-Scaling-Gruppe schlagen bei der ELB-Zustandsprüfung fehl

Zustandsprüfungs-Zielseitenfehler

Problem: Eine HTTP GET-Anforderung für die Instance auf dem angegebenen Ping-Port und dem Ping-Pfad (z. B. HTTP:80/index.html) erhält einen anderen Antwortcode als 200.

Cause 1: Es ist keine Zielseite in der Instance konfiguriert.

Solution 1: Erstellen Sie eine Zielseite (z. B. `index.html`) auf jeder registrierten Instance und geben Sie den Pfad als Ping-Pfad an.

Cause 2: Der Wert des Inhaltslängen-Headers (Content-Length) ist in der Antwort nicht festgelegt.

Solution 2: Wenn die Antwort einen Textkörper (body) enthält, setzen Sie den Inhaltslängen-Header entweder auf einen Wert größer als oder gleich null oder legen Sie den Wert für „Transfer-Encoding“ auf „Chunked“ fest.

Cause 3: Die Anwendung ist nicht für den Empfang von Anfragen aus dem Load Balancer oder für die Rückgabe eines 200-Antwortcodes konfiguriert.

Solution 3: Überprüfen Sie die Anwendung auf Ihrer Instance, um die Ursache herauszufinden.

Zeitlimit bei der Verbindung zu den Instances ist überschritten

Problem: Bei Anfragen zur Integritätsprüfung von Ihrem Load Balancer an Ihre EC2 Instances kommt es zu Zeitüberschreitungen oder sie schlagen zeitweise fehl.

Überprüfen Sie zunächst das Problem, indem Sie eine direkte Verbindung mit der Instance herstellen. Wir empfehlen, dass Sie eine Verbindung mit Ihrer Instance innerhalb des Netzwerks über die private IP-Adresse der Instance herstellen.

Verwenden Sie den folgenden Befehl für eine TCP-Verbindung:

```
telnet private-IP-address-of-the-instance port
```

Verwenden Sie den folgenden Befehl für eine HTTP- oder HTTPS-Verbindung:

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

Wenn Sie eine HTTP/HTTPS-Verbindung verwenden und eine andere Antwort als 200 erhalten, finden Sie weitere Informationen unter Zustandsprüfungs-Zielseitenfehler. Wenn Sie eine direkte Verbindung mit der Instance herstellen können, überprüfen Sie Folgendes:

Cause 1: Die Instance reagiert nicht innerhalb des konfigurierten Antwort-Zeitüberschreitungslimits.

Solution 1: Passen Sie die Antwort-Zeitüberschreitungseinstellungen in Ihrer Load Balancer-Zustandsprüfungskonfiguration an.

Cause 2: Die Instance ist stark ausgelastet und benötigt länger als das konfigurierte Antwort-Zeitüberschreitungslimit, um zu reagieren.

Lösung 2:

- Überprüfen Sie das Überwachungsdiagramm auf Überlastung der CPU. Weitere Informationen finden Sie unter Sie unter Statistiken für eine bestimmte EC2 Instance abrufen im EC2 Amazon-Benutzerhandbuch.
- Überprüfen Sie die Auslastung anderer Anwendungsressourcen, wie Speicher oder Limits, indem Sie eine Verbindung zu Ihren EC2 Instances herstellen.
- Fügen Sie ggf. weitere Instances hinzu oder aktivieren Sie Auto Scaling. Weitere Informationen finden Sie im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Cause 3: Wenn Sie eine HTTP- oder eine HTTPS-Verbindung verwenden und die Zustandsprüfung auf einer im Ping-Pfad angegebenen Zielseite durchgeführt wird (z. B. `HTTP:80/index.html`), braucht die Zielseite möglicherweise länger als Ihre konfigurierte Zeitüberschreitung.

Solution 3: Verwenden Sie eine einfachere Zustandsprüfungs-Zielseite oder passen Sie das Intervall für die Integritätsprüfungseinstellungen an.

Authentifizierung mit öffentlichem Schlüssel schlägt fehl

Problem: Ein Load Balancer, der zur Verwendung des HTTPS- oder SSL-Protokolls mit aktivierter Backend-Authentifizierung konfiguriert ist, schlägt bei Authentifizierung mit öffentlichem Schlüssel fehl.

Cause: Der öffentliche Schlüssel im SSL-Zertifikat stimmt nicht mit dem öffentlichen Schlüssel auf dem Load Balancer überein. Verwenden Sie den Befehl `s_client`, um die Liste der Serverzertifikate in der Zertifikatkette anzuzeigen. Weitere Informationen finden Sie unter s_client in der OpenSSL-Dokumentation.

Solution: Sie müssen möglicherweise Ihr SSL-Zertifikat aktualisieren. Wenn Ihr SSL-Zertifikat auf dem neuesten Stand ist, versuchen Sie, es erneut auf Ihrem Load Balancer zu installieren. Weitere Informationen finden Sie unter Ersetzen des SSL-Zertifikats für Ihren Classic Load Balancer.

Instance empfängt keinen Datenverkehr vom Load Balancer

Problem: Die Sicherheitsgruppe für die Instance blockiert den Datenverkehr vom Load Balancer.

Führen Sie eine Paketerfassung auf der Instance durch, um das Problem zu bestätigen. Verwenden Sie den folgenden Befehl:

```
# tcpdump port health-check-port
```

Cause 1: Die der Instance zugeordnete Sicherheitsgruppe lässt keinen Datenverkehr vom Load Balancer zu.

Solution 1: Bearbeiten Sie die Instance-Sicherheitsgruppe, um Datenverkehr vom Load Balancer zu ermöglichen. Fügen Sie eine Regel hinzu, die den gesamten Datenverkehr aus der Load Balancer-Sicherheitsgruppe zulässt.

Ursache 2: Die Sicherheitsgruppe für Ihren Load Balancer lässt keinen Datenverkehr zu den EC2 Instances zu.

Lösung 2: Bearbeiten Sie die Sicherheitsgruppe Ihres Load Balancers, um den Datenverkehr zu den Subnetzen und den Instances zuzulassen. EC2

Weitere Informationen über das Verwalten von Sicherheitsgruppen finden Sie unter Konfigurieren von Sicherheitsgruppen für Ihren Classic Load Balancer.

Ports auf Instance sind nicht offen

Problem: Die vom Load Balancer an die EC2 Instance gesendete Integritätsprüfung wird durch den Port oder eine Firewall blockiert.

Überprüfen Sie das Problem, indem Sie den folgenden Befehl eingeben:

```
netstat –ant
```

Cause: Der angegebene Zustandsprüfungs-Port oder der Listener-Port (sofern anders konfiguriert) ist nicht offen. Sowohl der für die Zustandsprüfung angegebene Port als auch der Listener-Port muss geöffnet und im Überwachungsmodus sein.

Solution: Öffnen Sie den Listener-Port und die in der Zustandsprüfung angegebene Port-Konfiguration (falls anders konfiguriert) auf Ihren Instances, um Datenverkehr vom Load Balancer zu erhalten.

Instances in einer Auto-Scaling-Gruppe schlagen bei der ELB-Zustandsprüfung fehl

Problem: Instances in Ihrer Auto Scaling-Gruppe bestehen die standardmäßige Auto-Scaling-Zustandsprüfung, aber nicht die ELB-Zustandsprüfung.

Ursache: Auto Scaling verwendet EC2 Statuschecks, um Hardware- und Softwareprobleme mit den Instances zu erkennen, aber der Load Balancer führt Integritätsprüfungen durch, indem er eine

Anfrage an die Instance sendet und auf einen 200-Antwortcode wartet oder indem er eine TCP-Verbindung (für eine TCP-basierte Zustandsprüfung) mit der Instance herstellt.

Eine Instance kann bei einer ELB-Zustandsprüfung fehlschlagen, weil eine Anwendung, die in der Instance ausgeführt wird, Probleme verursacht, die dazu führen, dass der Load Balancer die Instance außer Betrieb nimmt. Diese Instance könnte die Auto Scaling Scaling-Zustandsprüfung bestehen. Sie würde nicht durch die Auto Scaling Scaling-Richtlinie ersetzt werden, da sie aufgrund der EC2 Statusprüfung als fehlerfrei eingestuft wird.

Solution (Lösung): Verwenden Sie die ELB-Zustandsprüfung für Ihre Auto-Scaling-Gruppe. Wenn Sie die ELB-Zustandsprüfung verwenden, bestimmt Auto Scaling den Zustand Ihrer Instances anhand der Ergebnisse der Instance-Zustandsprüfung und der ELB-Zustandsprüfung. Weitere Informationen finden Sie unter Hinzufügen von Elastic Load Balancing Balancing-Zustandsprüfungen zu Ihrer Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Fehlerbehebung bei Classic Load Balancer: Client-Konnektivität

Clients können keine Verbindung zu einem mit dem Internet verbundenen Load Balancer herstellen

Wenn der Load Balancer auf Anfragen nicht reagiert, überprüfen Sie Folgendes:

Ihr mit dem Internet verbundener Load Balancer ist mit einem privaten Subnetz verbunden.

- Sie müssen öffentliche Subnetze für Ihren Load Balancer angeben. Ein öffentliches Subnetz verfügt über einen Zugang zum Internet-Gateway für Ihre Virtual Private Cloud (VPC).

Eine Sicherheitsgruppe oder Netzwerk-ACL erlaubt keinen Datenverkehr

- Die Sicherheitsgruppe für den Load Balancer und alle Netzwerke ACLs für die Load Balancer-Subnetze müssen eingehenden Datenverkehr von den Clients und ausgehenden Datenverkehr zu den Clients an den Listener-Ports zulassen. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsgruppen für Ihren Classic Load Balancer.

Anfragen, die an eine benutzerdefinierte Domain gesendet werden, werden vom Load Balancer nicht empfangen

Wenn der Load Balancer keine Anfragen empfängt, die an eine benutzerdefinierte Domain gesendet werden, überprüfen Sie Folgendes:

Der benutzerdefinierte Domainname kann nicht in die IP-Adresse des Load Balancers aufgelöst werden

- Bestätigen Sie mithilfe einer Befehlszeilenschnittstelle, auf welche IP-Adresse der benutzerdefinierte Domainname aufgelöst wird.
  - Linux, macOS oder Unix: Sie können den `dig`-Befehl im Terminal verwenden. Beispiel: `dig example.com`
  - Windows: Sie können den `nslookup`-Befehl in der Eingabeaufforderung verwenden. Beispiel: `nslookup example.com`
- Bestätigen Sie die IP-Adresse, zu der der DNS-Name des Load Balancers über eine Befehlszeilenschnittstelle aufgelöst wird.
- Vergleichen Sie die Ergebnisse der beiden Ausgaben. Die IP-Adressen müssen übereinstimmen.

An den Load Balancer gesendete HTTPS-Anfragen geben „NET::ERR_CERT_COMMON_NAME_INVALID“ zurück

Wird auf HTTPS-Anfragen vom Load Balancer `NET::ERR_CERT_COMMON_NAME_INVALID` zurückgegeben, überprüfen Sie die folgenden möglichen Ursachen:

- Der in der HTTPS-Anfrage verwendete Domainname stimmt nicht mit dem im ACM-Zertifikat des Listeners angegebenen alternativen Namen überein.
- Der Standard-DNS-Name des Load Balancers wird verwendet. Der Standard-DNS-Name kann nicht für HTTPS-Anfragen verwendet werden, da für die `*.amazonaws.com`-Domain kein öffentliches Zertifikat angefordert werden kann.

Fehlerbehebung beim Classic Load Balancer: Instance-Registrierung

Wenn Sie eine Instance bei Ihrem Load Balancer registrieren, gibt es eine Reihe von Schritten, die Sie ausführen müssen, bevor der Load Balancer Anforderungen an Ihre Instance senden kann.

Im Folgenden werden Probleme beschrieben, auf die Ihr Load Balancer bei der Registrierung Ihrer EC2 Instances stoßen könnte, die möglichen Ursachen und die Schritte, die Sie ergreifen können, um die Probleme zu lösen.

Problembereiche

Die Registrierung einer EC2 Instance dauert zu lange

Problem: Die Verfügbarkeit registrierter EC2 Instances dauert länger als `InService` erwartet.

Cause: Ihre Instance hat möglicherweise die Zustandsprüfung nicht bestanden. Nach Abschluss der ersten Instance-Registrierungsschritte (kann bis zu ca. 30 Sekunden dauern) startet der Load Balancer das Senden von Zustandsprüfungsanforderungen. Ihre Instance ist erst dann `InService`, nachdem eine Zustandsprüfung erfolgreich ausgeführt wurde.

Solution: Weitere Informationen finden Sie unter Zeitlimit bei der Verbindung zu den Instances ist überschritten.

Instance, die aus einem gebührenpflichtigen AMI gestartet wurde, kann nicht registriert werden

Problem: Elastic Load Balancing kann eine Instance nicht registrieren, die mit einem gebührenpflichtigen AMI gestartet wurde.

Ursache: Ihre Instances wurden möglicherweise mit einem kostenpflichtigen AMI von Amazon gestartet DevPay.

Lösung: Elastic Load Balancing unterstützt nicht die Registrierung von Instances, die mit kostenpflichtigen Zahlungen AMIs von Amazon gestartet wurden DevPay. Beachten Sie, dass Sie Paid AMIs from AWS Marketplace verwenden können. Wenn Sie bereits ein kostenpflichtiges AMI von verwenden AWS Marketplace und eine von diesem kostenpflichtigen AMI gestartete Instance nicht registrieren können, wenden Sie sich an das AWS -Support Center, um Unterstützung zu erhalten.

Kontingente für Ihren Classic Load Balancer

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Um die Quoten für Ihre Classic Load Balancer anzuzeigen, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS services (Dienste) und wählen Sie Elastic Load Balancing aus. Sie können auch den Befehl describe-account-limits(AWS CLI) für Elastic Load Balancing verwenden.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

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

Name	Standard	Anpassbar
Classic Load Balancer pro Region	20	Ja
Listener pro Classic Load Balancer	100	Ja
Registrierte Instances pro Classic Load Balancer	1.000	Ja

Dokumentenverlauf für Classic Load Balancers

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

Änderung	Beschreibung	Datum
Bucket-Richtlinien für Zugriffs- und Verbindungsprotokolle	Vor dieser Version hing die von Ihnen verwendete Bucket-Richtlinie davon ab, ob die Region vor oder nach August 2022 verfügbar war. Mit dieser Version wird die neuere Bucket-Richtlinie in allen Regionen unterstützt. Beachten Sie, dass die alte Bucket-Richtlinie weiterhin unterstützt wird.	10. September 2025
Desynchroner Mitigatio nsmodus	Unterstützung für den desynchronen Mitigatio nsmodus hinzugefügt. Weitere Informationen finden Sie unter Desync-Minimationsmodus für Ihren Classic Load Balancer konfigurieren.	17. August 2020
Klassische Load Balancer	Mit der Einführung von Application Load Balancer und Network Load Balancer werden Load Balancer, die mit der API vom 01.06.201 6 erstellt wurden, jetzt als Classic Load Balancer bezeichnet. Weitere Informati onen zu den Unterschieden zwischen diesen Arten von Load Balancers finden Sie	11. August 2016

	unter Elastic Load Balancing Balancing-Funktionen.	
Support für AWS Certificate Manager (ACM)	Sie können ein SSL/TLS Zertifikat von ACM anfordern und es auf Ihrem Load Balancer bereitstellen. Weitere Informationen finden Sie unter SSL/TLS-Zertifikate für Classic Load Balancers.	21. Januar 2016
Support für zusätzliche Ports	Load Balancer können jeden Port im Bereich 1—65535 abhören. Weitere Informationen finden Sie unter Listener für Ihren Classic Load Balancer.	15. September 2015
Zusätzliche Felder für Zugriffsprotokolleinträge	Felder `user_agent` , `ssl_cipher` und `ssl_protocol` hinzugefügt. Weitere Informationen finden Sie unter Zugriffs-Protokoll dateien.	18. Mai 2015

Support für das Taggen Ihres Load Balancers	Ab dieser Version wurde die Elastic Load Balancing CLI (ELB CLI) durch AWS Command Line Interface (AWS CLI) ersetzt, ein einheitliches Tool zur Verwaltung mehrerer AWS Services. Neue Funktionen, die nach ELB CLI-Version 1.0.35.0 (vom 24.7.14) veröffentlicht werden, sind nur noch in der AWS CLI enthalten. Wenn Sie aktuell die ELB CLI verwenden, empfehlen wir, dass Sie stattdessen die AWS CLI verwenden. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.	11. August 2014
Timeout bei Verbindungen im Leerlauf	Sie können das Leerlauf-Verbindungs-Timeout für Ihren Load Balancer konfigurieren.	24. Juli 2014
Support für die Gewährung von Zugriff auf bestimmte Load Balancer oder API-Aktionen für Benutzer und Gruppen	Sie können eine Richtlinie erstellen, um Benutzern und Gruppen Zugriff auf bestimmte Load Balancer oder API-Aktionen zu gewähren.	12. Mai 2014
Support für AWS CloudTrail	Sie können verwenden CloudTrail , um API-Aufrufe zu erfassen, die von oder in Ihrem Namen AWS-Konto mithilfe der ELB-API, der AWS Management Console, der ELB-CLI oder der getätigt wurden AWS CLI.	4. April 2014

Verbindung wird schwächer	Informationen zu Connection Draining hinzugefügt. Mit diesem Support können Sie Ihren Load Balancer aktivieren, um das Senden von neuen Abfragen an die registrierte Instance stoppen, wenn die Registrierung der Instances aufgehoben wird oder wenn die Instanz fehlerhaft ist. Die vorhandenen Verbindungen bleiben geöffnet. Weitere Informationen finden Sie unter Connection Draining für Ihren Classic Load Balancer konfigurieren.	20. März 2014
Zugriffs-Logs	Sie können Ihren Load Balancer so einrichten, dass er detaillierte Informationen über die an Ihren Load Balancer gesendeten Anfragen erfasst und in einem Amazon S3 S3-Bucket speichert. Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihren Classic Load Balancer.	6. März 2014

Support für TLSv1 1.1-1.2	Es wurden Informationen zur Unterstützung des TLSv1 .1-1.2-Protokolls für Load Balancer hinzugefügt, die mit HTTPS/SSL-Listener n konfiguriert sind. Durch diese Unterstützung aktualisiert Elastic Load Balancing auch die vordefinierten SSL-Aushandlungskonfigurationen. Informationen zu den aktualisierten vordefinierten SSL-Verhandlungskonfigurationen finden Sie unter SSL-Verhandlungskonfigurationen für Classic Load Balancers. Informationen zur Aktualisierung Ihrer aktuellen SSL-Verhandlungskonfiguration finden Sie unter Aktualisieren der SSL-Verhandlungskonfiguration Ihres Classic Load Balancer.	19. Februar 2014
Zonenübergreifendes Load Balancing	Informationen über die zonenübergreifende Lastverteilung für Ihren Load Balancer hinzugefügt. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing für Ihren Classic Load Balancer konfigurieren.	6. November 2013

Zusätzliche Metriken CloudWatch	Informationen über die zusätzlichen Cloudwatch-Metriken von Elastic Load Balancing hinzugefügt. Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Classic Load Balancer.	28. Oktober 2013
Support für das Proxy-Protokoll	Es wurden Informationen zur Unterstützung des Proxyprotokolls für Load Balancer hinzugefügt, die für TCP/SSL Verbindungen konfiguriert sind. Weitere Informationen finden Sie unter Proxy-Protokoll-Header.	30. Juli 2013
Support für DNS-Failover	Es wurden Informationen zur Konfiguration von Amazon Route 53 DNS-Failover für Load Balancer hinzugefügt. Weitere Informationen finden Sie unter Verwenden von Amazon Route 53 DNS-Failover für Ihren Load Balancer.	3. Juni 2013
Konsolenunterstützung für die Anzeige von CloudWatch Metriken und die Erstellung von Alarmen	Es wurden Informationen zum Anzeigen von CloudWatch Metriken und zum Erstellen von Alarmen für einen bestimmten Load Balancer mithilfe der Konsole hinzugefügt. Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Classic Load Balancer.	28. März 2013

Support für die Registrierung von EC2 Instances in einer Standard-VPC	Unterstützung für EC2 Instances hinzugefügt, die in einer Standard-VPC gestartet wurden.	11. März 2013
Interne Load Balancer	Ab dieser Version, kann ein Load Balancer in einer Virtual Private Cloud (VPC) entweder intern oder mit dem Internet verbunden sein. Ein interner Load Balancer verfügt über eine öffentlich auflösbaren DNS-Namen, der in private IP-Adressen aufgelöst wird. Ein mit dem Internet verbunden er Load Balancer verfügt über einen öffentlich auflösbaren DNS-Namen, der in öffentlic he IP-Adressen aufgelöst wird. Weitere Informationen finden Sie unter Erstellen eines internen Classic Load Balancer.	10. Juni 2012
Konsolenunterstützung für die Verwaltung von Listenern, Verschlüsselungseinstellungen und SSL-Zertifikaten	Weitere Informationen finden Sie unter Einen HTTPS-Listener für Ihren Classic Load Balancer konfigurieren und das SSL-Zertifikat für Ihren Classic Load Balancer ersetzen.	18. Mai 2012
Support für Elastic Load Balancing in Amazon VPC	Unterstützung für das Erstellen eines Load Balancers in einer Virtual Private Cloud (VPC) hinzugefügt.	21. November 2011

Amazon CloudWatch	Sie können Ihren Load Balancer überwachen mit. CloudWatch Weitere Informationen finden Sie unter CloudWatch Metriken für Ihren Classic Load Balancer.	17. Oktober 2011
Zusätzliche Sicherheitsfunktionen	Sie können SSL-Verschlüsselungen, Backend-SSL und Backend-Serverauthentifizierung konfigurieren. Weitere Informationen finden Sie unter Classic Load Balancer mit einem HTTPS-Listener erstellen.	30. August 2011
Apex-Domänenname der Zone	Weitere Informationen finden Sie unter Konfigurieren eines benutzerdefinierten Domainnamens für Ihren Classic Load Balancer.	24. Mai 2011

Support für X-Forwarded-Proto und X-Forwarded-Port Header	Der X-Forwarded-Proto Header gibt das Protokoll der ursprünglichen Anfrage an, und der X-Forwarded-Port Header gibt den Port der ursprünglichen Anfrage an. Durch das Hinzufügen dieser Header zu Abfragen können Kunden bestimmen, ob eine eingehende Anforderung an den Load Balancer verschlüs selt ist, und sehen, welcher spezifische Port auf dem Load Balancer die Anforderu ng empfangen hat. Weitere Informationen finden Sie unter HTTP-Header und Classic Load Balancers.	27. Oktober 2010
Support für HTTPS	Mit dieser Version können Sie SSL/TLS das Protokoll zur Verschlüsselung des Datenverkehrs nutzen und die SSL-Verarbeitung von der Anwendungsinstanz auf den Load Balancer auslagern . Dieses Feature ermöglich t außerdem die zentralis ierte Verwaltung von SSL-Zertifikaten auf dem Load Balancer, statt die Zertifikate auf einzelnen Anwendungs-Instances zu verwalten.	14. Oktober 2010
Support für AWS Identity and Access Management (IAM)	IAM wird nun unterstützt.	2. September 2010

Sticky Sessions	Weitere Informationen finden Sie unter Sticky Sessions für Ihren Classic Load Balancer konfigurieren.	7. April 2010
AWS SDK für Java	Unterstützung für SDK für Java hinzugefügt.	22. März 2010
AWS SDK für .NET	Unterstützung für die hinzugefügt SDK für .NET.	11. November 2009
Neuer Service	Erste öffentliche Betaversion von Elastic Load Balancing.	18. Mai 2009

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.