Elastic Load Balancing

網路負載平衡器

Elastic Load Balancing: 網路負載平衡器

Table of Contents

What is a 網路負載平衡器?

Elastic Load Balancing 支援以下類型的負載平衡器：Application Load Balancer、網路負載平衡器 和 Classic Load Balancer。本指南將討論 網路負載平衡器。如需其他負載平衡器的詳細資訊，請參閱《Application Load Balancer 使用者指南》及《Classic Load Balancer 使用者指南》。

網路負載平衡器 components

A load balancer 作爲客戶的單點聯繫人。負載平衡器會將傳入的流量分散到多個目標，例如 Amazon EC2 執行個體。這會提高您應用程式的可用性。您要為負載平衡器添加一個或多個接聽程式。

A listener 使用您配置的協議和端口來檢查客戶端的連接請求，並將請求轉發到目標組。

每個 target group 使用TCP協議和指定的端口號，將請求路由到一個或多個已註冊目標（例如ec2實例）。您可以向多個目標群組註冊任一目標。您可以針對每個目標群組設定運作狀態檢查。凡已註冊至負載平衡器的接聽程式規則中指定之目標群組的所有目標，系統將對其執行運作狀態檢查。

如需詳細資訊，請參閱下列文件。

- Load Balancers (p. 9)
- Listeners (p. 17)
- Target Groups (p. 28)

網路負載平衡器 overview

網路負載平衡器 是在開放系統互相連線 (OSI) 模型的第四層運作。每秒可以處理數百萬個請求。負載平衡器接收到連線請求後，將依預設規則從目標群組中選取一個目標。負載平衡器會嘗試開啟接聽程式設定中指定之連接埠上所選目標的 TCP 連線。

當您為負載平衡器啟用某個可用區域時，Elastic Load Balancing 會在該可用區域內建立一個負載平衡器節點。預設情況下，每個負載平衡器節點只會將流量分布到其可用區域中的登錄目標。若您啟用跨區域負載平衡功能，每個負載平衡器節點會將流量分布至所有可用區域內已登錄的目標。如需更多詳細資訊，請參閱「Availability Zones (p. 10)」。

如果您為負載平衡器啟用多個可用區域，並確保每個目標群組在各個已啟用的可用區域內皆至少有一個目標，便能提高應用程式的容錯能力。例如，若一個或多個目標群組在某個可用區域內沒有運作狀態良好的目標，我們將從 DNS 移除相應子網路的 IP 地址，但其他可用區域內的負載平衡器節點仍然可供用於路由流量。如有用戶端未遵守存留時間 (TTL) 而將請求傳送至已從 DNS 移除的 IP 地址，其請求即會失敗。

若是 TCP 流量，負載平衡器將根據通訊協定、來源 IP 地址、來源連接埠、目的地 IP 地址、目的地連接埠和 TCP 序號，使用流程雜湊演算法選取目標。來自用戶端的 TCP 連線具有不同的來源連接埠和序號，可以路由至不同的目標。每一單獨的 TCP 連線在該連線的有效期內都將路由至單個目標。

若是 UDP 流量，負載平衡器將根據通訊協定、來源 IP 地址、來源連接埠、目的地 IP 地址和目的地連接埠，使用流程雜湊演算法選取目標。UDP 流程有相同的來源和目的地，所以能夠在其生命期間一致地路由到單一目標。不同 UDP 流程有不同的來源 IP 地址和連接埠，因此可以將他們路由到不同的目標。

Elastic Load Balancing 會為您所啟用的每個可用區域建立網路介面。可用區域中的每個負載平衡器節點皆使用此網路界面來取得靜態 IP 地址。當您建立面向網際網路的負載平衡器時，您可以選擇連結每個子網路的一組彈性 IP 地址。

建立目標群組時，您會指定其目標類型，此類型會決定是否根據執行個體 ID 或 IP 地址來註冊目標。如果根據執行個體 ID 註冊目標，用戶端的來源 IP 地址將保留並提供予您的應用程式。如果使用 IP 地址註冊目標，來源 IP 地址即是負載平衡器節點的私有 IP 地址。

當您需要進行變更時，您可以從負載平衡器新增和移除目標，而不需中斷應用程式的請求整體流程。Elastic Load Balancing 擴展您的負載平衡器做為應用程式流量的變化。Elastic Load Balancing 可以自動擴展至多數工作負載。

您可以設定運作狀態檢查，用於監控已註冊目標的運作狀態，使負載平衡器只能傳送請求至運作狀態良好的目標。

有關詳細信息，請參閱 如何 Elastic Load Balancing 工作 在 Elastic Load Balancing 使用者指南.

Benefits of migrating from a Classic Load Balancer

使用 網路負載平衡器 替代 Classic Load Balancer 的優點如下：

- Ability to handle volatile workloads and scale to millions of requests per second.
- Support for static IP addresses for the load balancer. You can also assign one Elastic IP address per subnet enabled for the load balancer.
- Support for registering targets by IP address, including targets outside the VPC for the load balancer.
- Support for routing requests to multiple applications on a single EC2 instance. You can register each instance or IP address with the same target group using multiple ports.
- Support for containerized applications. Amazon Elastic Container Service (Amazon ECS) can select an unused port when scheduling a task and register the task with a target group using this port. This enables you to make efficient use of your clusters.
- Support for monitoring the health of each service independently, as health checks are defined at the target group level and many Amazon CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand.

如需各種負載平衡器類型支援的功能詳細資訊，請參閱 Elastic Load Balancing 產品比較。

How to get started

若要建立 網路負載平衡器，請選擇下列其中一項教學課程：

- Getting started with 網路負載平衡器 (p. 3)
- Tutorial: Create a 網路負載平衡器 using the AWS CLI (p. 6)

如需常見負載平衡器組態的示範，請參閱 Elastic Load Balancing 示範。

Pricing

如需詳細資訊，請參閱 網路負載平衡器 定價。

Getting started with 網路負載平衡器

本教學課程提供透過 AWS 管理主控台 Web 界面的 網路負載平衡器 實作簡介。若要建立您的第一個 網路負載平衡器，請完成以下步驟。

任務

或者，創建 Application Load Balancer，參見 開始使用 Application Load Balancer 在 Application Load Balancer 使用者指南。創建 Classic Load Balancer，參見 創建 Classic Load Balancer 在 Classic Load Balancer 使用者指南.

如需常見負載平衡器組態的示範，請參閱 Elastic Load Balancing 示範。

Before you begin

- Decide which Availability Zones you will use for your EC2 instances. Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones. These public subnets are used to configure the load balancer. You can launch your EC2 instances in other subnets of these Availability Zones instead.
- Launch at least one EC2 instance in each Availability Zone. Ensure that the security groups for these instances allow TCP access from clients on the listener port and health check requests from your VPC. For more information, see 目標安全群組 (p. 40).

Step 1: Choose a load balancer type

Elastic Load Balancing 支援三種類型的負載平衡器：本教學課程將要建立 網路負載平衡器。

建立 網路負載平衡器

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 於導覽列上，為負載平衡器選擇一個區域。請務必選擇您用於 EC2 執行個體的同一區域。
3. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
4. 選擇 Create Load Balancer (建立負載平衡器)。
5. 針對 網路負載平衡器 選擇 Create (建立)。

Step 2: Configure your load balancer and listener

在 Configure Load Balancer (設定負載平衡器) 頁面上，完成以下程序。

設定負載平衡器和接聽程式

1. 針對 Name (名稱)，輸入負載平衡器的名稱。

   在區域的 Application Load Balancer 和 網路負載平衡器 組合中，網路負載平衡器 的名稱必須獨一無二，其字元數上限為 32 個，只能包含英數字元與連字號，但不能以連字號開頭或結尾，且不能以 "internal-" 開頭。
2. 針對 Scheme (配置)，請維持預設值 internet-facing。
3. 針對 Listeners (接聽程式)，維持預設值，即接聽程式會接受連接埠 80 的 TCP 流量。
4. 針對 Availability Zones (可用區域)，選取您用於 EC2 執行個體的 VPC。針對用於啟動 EC2 執行個體的各個可用區域，先選取可用區域，接著選取該可用區域的一個公有子網路。

   在預設情況下，AWS 會從每個負載平衡器節點可用區域的子網路將 IPv4 地址指派到每個負載平衡器節點。或者，當您建立面向網際網路的負載平衡器，您可以為每個可用區域選取一個彈性 IP 地址。這可為您的負載平衡器提供靜態 IP 地址。
5. 選擇 Next (下一步)。配置路由.

Step 3: Configure your target group

建立目標群組以用於請求路由。接聽程式的規則會將請求路由至此目標群組中的已註冊目標。負載平衡器會使用您為目標群組定義的運作狀態檢查設定，檢查此目標群組中各目標的運作狀態。在 Configure Routing (設定路由) 頁面上，完成以下程序。

設定目標群組

1. 針對 Target group (目標群組)，保留預設值 New target group (新目標群組)。
2. 針對 Name (名稱)，輸入新目標群組的名稱。
3. 維持 Protocol (通訊協定) 為 TCP，Port (連接埠) 為 80，Target type (目標類型) 為執行個體。
4. 針對 Health checks (運作狀態檢查)，保留預設通訊協定。
5. 選擇 Next (下一步)。註冊目標.

Step 4: Register targets with your target group

在 Register Targets (註冊目標) 頁面上，完成以下程序。

向目標群組註冊目標

1. 從 Instances (執行個體)，選取一個或多個執行個體。
2. 保留預設連接埠 80，然後選擇 Add to registered (新增至已註冊)。
3. 完成選擇實例後，選擇 下一步: 檢閱

Step 5: Create and test your load balancer

建立負載平衡器之前，請先檢閱您的設定。建立負載平衡器之後，確認其是否會將流量傳送到您的 EC2 執行個體。

建立和測試負載平衡器

1. 在 Review (檢閱) 頁面上，選擇 Create (建立)。

2. 系統通知您已成功建立負載平衡器之後，選擇 Close (關閉)。
3. 在導覽窗格，LOAD BALANCING (負載平衡) 中，選擇 Target Groups (目標群組)。
4. 選取新建立的目標群組。
5. 選擇 Targets (目標) 並確認您的執行個體已就緒。若執行個體的狀態為 `initial`，原因可能是執行個體仍在進行註冊，或者未通過可視為運作狀態良好的運作狀態檢查次數下限。當至少有一個執行個體處於 `healthy` 狀態後，您即可測試您的負載平衡器。
6. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
7. 選取新建立的負載平衡器。
8. 選擇 Description (描述)，然後複製負載平衡器的 DNS 名稱 (例如 my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com)。將此 DNS 名稱貼至已連接網際網路的 web 瀏覽器的網址欄位。如果一切正常，瀏覽器會顯示您的伺服器的預設頁面。

Step 6: Delete your load balancer (optional)

在您的負載平衡器可用後，將會根據持續執行時間收取一小時或不足一小時的費用。當您已不再需要負載平衡器時，便可將其刪除。刪除負載平衡器後，便會停止收取費用。請注意，刪除負載平衡器並不會影響已向該負載平衡器註冊的目標。例如，您的 EC2 執行個體將繼續運作。

刪除負載平衡器

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Actions (動作)、Delete (刪除)。
4. 出現確認提示時，選擇 Yes, Delete (是，刪除)。

Tutorial: Create a 網路負載平衡器 using the AWS CLI

本教學課程提供透過 AWS CLI 演練 網路負載平衡器 的實作簡介。

Before you begin

- Install the AWS CLI or update to the current version of the AWS CLI if you are using a version that does not support 網路負載平衡器. For more information, see Installing the AWS Command Line Interface in the AWS Command Line Interface 使用者指南.
- Decide which Availability Zones you will use for your EC2 instances. Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones.
- Launch at least one EC2 instance in each Availability Zone. Ensure that the security groups for these instances allow TCP access from clients on the listener port and health check requests from your VPC. For more information, see 目標安全群組 (p. 40).

Create your load balancer

完成以下步驟，建立您的第一個負載平衡器。

建立負載平衡器

1. 使用 create-load-balancer 命令建立負載平衡器，為您在其中啟動執行個體的各個可用區域指定公有子網路。每個可用區域只能指定一個子網路。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-12345678
```

其輸出將包含負載平衡器的 Amazon Resource Name (ARN)，格式如下：

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

2. 使用 create-target-group 命令建立目標群組，指定您用於 EC2 執行個體的相同 VPC：

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-12345678
```

其輸出將包含目標群組的 ARN，格式如下：

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

3. 使用 register-targets 命令向目標群組註冊您的執行個體：

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets Id=i-12345678
 Id=i-23456789
```

4. 使用 create-listener 命令為您的負載平衡器建立具有預設規則以轉送請求至目標群組的接聽程式：

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

其輸出將包含接聽程式的 ARN，格式如下：

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

5. (選用) 您可以使用 describe-target-health 命令驗證目標群組已註冊目標的運作狀態，如下所示：

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

Specify an Elastic IP address for your load balancer

建立 網路負載平衡器 時，您可以使用子網路對應，為每個子網路指定一個彈性 IP 地址。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \
--subnet-mappings SubnetId=subnet-12345678,AllocationId=eipalloc-12345678
```

Add targets using port overrides

如果您有微服務架構由單一執行個體提供多項服務，則每項服務將透過不同的連接埠接受連線。您可以多次向目標群組註冊執行個體，每次使用不同的連接埠。

使用連接埠覆寫新增目標

1. 使用 create-target-group 命令建立目標群組。

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 \
--vpc-id vpc-12345678
```

2. 使用 register-targets 命令向目標群組註冊您的執行個體：請注意，每個容器的執行個體 ID 皆相同，但連接埠不同。

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-12345678,Port=80 Id=i-12345678,Port=766
```

3. 使用 create-listener 命令為您的負載平衡器建立具有預設規則以轉送請求至目標群組的接聽程式：

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

Delete your load balancer

當您已不再需要負載平衡器和目標群組時，便可將其刪除，如下所示：

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

網路負載平衡器

A load balancer 作爲客戶的單點聯繫人。用戶端將請求傳送到負載平衡器，而負載平衡器將請求傳送到目標，例如在一或多個可用區域內的 EC2 執行個體。

若要設定您的負載平衡器，您需要建立目標群組 (p. 28)，然後使用您的目標群組來登錄目標。如果您確認每個已啟用的可用區域擁有至少一個登錄的目標，您的負載平衡器會展現最高效率。您也可以建立接聽程式 (p. 17)來檢查來自用戶端的連線請求，並路由來自用戶端的請求到目標群組中的目標。

網路負載平衡器 支援 VPC 對等、AWS 受管 VPN、AWS Direct Connect 和第三方 VPN 解決方案的用戶端連線。

內容

Load balancer state

負載平衡器可以是以下其中一個狀態：

`provisioning`

正在設定負載平衡器。

`active`

負載平衡器已設定完成並準備好路由流量。

`failed`

無法設定的負載平衡器。

Load balancer attributes

以下是負載平衡器屬性：

`deletion_protection.enabled`

表示是否已啟用刪除保護 (p. 11)。(預設為 `false`.)

`load_balancing.cross_zone.enabled`

表示是否已啟用跨區域負載平衡 (p. 10)。(預設為 `false`.)

Availability Zones

建立您的負載平衡器時，啟用一個或多個可用區域。如果您為您的負載平衡器啟用多個可用區域，將會提高應用程式的容錯能力。建立 網路負載平衡器 之後，您無法停用可用區域，但可以啟用其他可用區域。

當您啟用可用區域時，從該可用區域中指定一個子網路。Elastic Load Balancing 在可用區域中建立一個負載平衡器節點以及子網路的網路界面 (說明以「ELB 網路」為開頭並包含負載平衡器的名稱)。可用區域中的每個負載平衡器節點皆使用此網路界面來取得 IPv4 地址。請注意，您可以查看此網路界面，但您無法修改。

當您建立面向網際網路的負載平衡器時，您可以選擇每個子網路指定一個彈性 IP 地址。如果您沒有選擇其中一個自己的彈性 IP 地址，Elastic Load Balancing 會為您在每個子網路提供一個彈性 IP 地址。這些彈性 IP 地址為您的負載平衡器提供靜態 IP 地址，這些地址在負載平衡器的生命週期內不會變更。建立負載平衡器之後，您無法變更這些彈性 IP 地址。

當您建立內部負載平衡器時，您可以選擇每個子網路指定一個彈性 IP 地址。如果您沒有從子網路指定 IP 地址，Elastic Load Balancing 會為您選擇一個地址。這些私有 IP 地址為您的負載平衡器提供靜態 IP 位址，這些地址在負載平衡器的生命週期內不會變更。建立負載平衡器之後，您無法變更這些私有 IP 位址。

Requirements

- For internet-facing load balancers, the subnets that you specify must have at least 8 available IP addresses. For internal load balancers, this is only required if you let AWS select a private IPv4 address from the subnet.
- You can't specify a subnet in a constrained Availability Zone. The error message is "Load balancers with type 'network' are not supported in az_name". You can specify a subnet in another Availability Zone that is not constrained and use cross-zone load balancing to distribute traffic to targets in the constrained Availability Zone.
- You can't specify a subnet in a Local Zone.

當您啟用可用區域之後，負載平衡器會開始將請求路由到該可用區域內已註冊的目標。如果您確認每個已啟用的可用區域擁有至少一個登錄的目標，您的負載平衡器會展現最高效率。

使用主控台新增可用區域

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器。
4. 在 Description (描述) 標籤的 Basic Configuration (基本組態) 下方，選擇 Edit subnets (編輯子網路)。
5. 若要啟用可用區域，請選取該可用區域的核取方塊。如果該可用區域有一個子網路，則會選取該子網路。如果該可用區域有多個子網路，則請選取其中一個子網路。請注意，一個可用區域只能選取一個子網路。

   對於面向網際網路的負載平衡器，您可以為每個可用區域選取一個彈性 IP 地址。對於內部負載平衡器，您可以從每個子網路的 IPv4 範圍指派私有 IP 地址，而不是讓 Elastic Load Balancing 指派。
6. 選擇 Save (儲存)。

使用 AWS CLI 新增可用區域

使用 set-subnets 命令。

Cross-zone load balancing

預設情況下，每個負載平衡器節點只會將流量分布到其可用區域中的登錄目標。若您啟用跨區域負載平衡功能，每個負載平衡器節點會將流量分布至所有可用區域內已登錄的目標。有關詳細信息，請參閱 跨區負載平衡 在 Elastic Load Balancing 使用者指南.

使用主控台啟用跨區域負載平衡

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器。
4. 依序選擇 Description (說明)、Edit attributes (編輯屬性)。
5. 在 Edit load balancer attributes (編輯負載平衡器屬性) 頁面上，選擇 Cross-Zone Load Balancing (跨區負載平衡) 的 Enable (啟用)，然後選擇 Save (儲存)。

使用 AWS CLI 啟用跨區域負載平衡

以 `load_balancing.cross_zone.enabled` 屬性來使用 modify-load-balancer-attributes 命令。

Deletion protection

為避免您的負載平衡器上遭意外刪除，您可以啟用刪除保護。您的負載平衡器的刪除保護預設為停用。

如果您為負載平衡器啟用刪除保護，則必須先停用才可刪除負載平衡器。

使用主控台來啟用刪除保護

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器。
4. 依序選擇 Description (說明)、Edit attributes (編輯屬性)。
5. 在 Edit load balancer attributes (編輯負載平衡器屬性) 頁面上，選擇 Delete Protection (刪除保護) 的 Enable (啟用)，然後選擇 Save (儲存)。

使用主控台來停用刪除保護

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器。
4. 依序選擇 Description (說明)、Edit attributes (編輯屬性)。
5. 在 Edit load balancer attributes (編輯負載平衡器屬性) 頁面上，清除 Enable delete protection (啟用刪除保護)，然後選擇 Save (儲存)。

使用 AWS CLI 來啟用或停用刪除保護

以 `deletion_protection.enabled` 屬性來使用 modify-load-balancer-attributes 命令。

Connection idle timeout

對於用戶端透過 網路負載平衡器 做出的每個 TCP 請求，將會追蹤該連線的狀態。若在比閒置逾時更長的時間內沒有由用戶端或目標透過連線傳送的資料，連線將關閉。如果用戶端或目標閒置逾時時間經過後傳送資料，就會收到一個 TCP RST 封包，表示連線不再有效。

Elastic Load Balancing 會將 TCP 流程的閒置逾時值設為 350 秒。您無法修改此值。用戶端或目標可以使用 TCP 保持連線封包來重設閒置逾時。

雖然 UDP 是無連線的，負載平衡器會根據來源和目的地 IP 地址和連接埠來維護 UDP 流程狀態，以確保會持續將屬於相同流程的封包傳送到相同目標。閒置逾時期間經過之後，負載平衡器會將傳入的 UDP 套件視為新的流程，並將其路由到新的目標。Elastic Load Balancing 會將 UDP 流程的閒置逾時值設為 120 秒。

EC2 執行個體必須在 30 秒內回應新的請求，才能建立傳回路徑。

DNS name

每個 網路負載平衡器 接收包含以下語法的默認域名系統(DNS)名稱: *name*-*id*elb*region*.amazonaws.com。例如，My-Load-Balancer-1234567890ABCDEF.ELB。us-east-2.amazonaws.com.

如果您偏好使用更易於記住的 DNS 名稱，您可以建立自訂網域名稱，並將其與負載平衡器的 DNS 名稱建立關聯。當用戶端使用此自訂網域名稱發出請求時，DNS 伺服器為您的負載平衡器解析 DNS 名稱。

首先，向取得認證的網域名稱註冊商註冊網域名稱。接著，使用您的 DNS 服務 (例如您的網域註冊商) 建立 CNAME 記錄，以便將請求路由到您的負載平衡器。如需詳細資訊，請參閱您的 DNS 服務文件。例如，您可以使用 Amazon Route 53 做為 DNS 服務。有關詳細信息，請參閱 將流量路由到ELB負載均衡器 在 Amazon Route 53 開發人員指南.

負載平衡器在每個已啟用的可用區域都有一個 IP 地址。這些是負載平衡器節點的地址。負載平衡器的 DNS 名稱解析為這些地址。例如，假設負載均衡器的自定義域名爲 `example.networkloadbalancer.com`。使用以下內容 dig 或 nslookup 用於確定負載均衡器節點的IP地址的命令。

Linux or Mac

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

Windows

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

負載平衡器具有其負載平衡器節點的 DNS 記錄。您可以使用DNS名稱來確定負載均衡器節點的IP地址: *az*.*name*-*id*elb*region*.amazonaws.com.

Linux or Mac

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

Windows

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

Create a 網路負載平衡器

負載平衡器會從用戶端取得請求，然後分布到目標群組的目標，例如，EC2 執行個體。

開始之前，請確保您負載平衡器的虛擬私有雲端 (VPC) 在目標所在的每個可用區域中至少有一個公有子網路。

若要使用 AWS CLI 來建立負載平衡器，請參閱Tutorial: Create a 網路負載平衡器 using the AWS CLI (p. 6)。

若要使用 AWS 管理主控台來建立負載平衡器，請完成下列工作。

任務

Step 1: Configure a load balancer and a listener

首先，提供您負載平衡器的一些基本組態資訊，例如名稱、網路和一個或多個接聽程式。接聽程式是檢查連線請求的程序。使用通訊協定以及連接埠為用戶端與負載平衡器間的連線進行設定。如需受支援的通訊協定與連接埠之詳細資訊，請參閱Listener configuration (p. 17)。

設定負載平衡器和接聽程式

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選擇 Create Load Balancer (建立負載平衡器)。
4. 針對 網路負載平衡器 選擇 Create (建立)。
5. 針對 Name (名稱)，輸入負載平衡器的名稱。例如：**my-nlb**。
6. 針對 Scheme (機制)，面對網際網路的負載平衡器會透過網際網路將用戶端的請求路由至目標。內部負載平衡器會使用私有 IP 地址將請求路由至目標。
7. 針對 Listeners (接聽程式)，預設值是接受連接埠 80 上之 TCP 流量的接聽程式。您可以保留預設接聽程式設定、修改通訊協定或修改連接埠。選擇 Add (新增) 來新增另一個接聽程式。
8. 針對 Availability Zones (可用區域)，選取您用於 EC2 執行個體的 VPC。而針對用來啟動 EC2 執行個體的各個可用區域，則先選取可用區域，接著選取該可用區域的公有子網路。

   在預設情況下，AWS 會從每個負載平衡器節點可用區域的子網路將 IPv4 地址指派到每個負載平衡器節點。或者，如果您建立面向網際網路的負載平衡器，您可以為每個可用區域選取一個彈性 IP 地址。這可為您的負載平衡器提供靜態 IP 地址。如果您建立內部負載平衡器，您可以從每個子網路的 IPv4 範圍指派私有 IP 地址，而不是讓 AWS 指派。
9. 選擇 Next (下一步)。配置路由.

Step 2: Configure a target group

您向目標群組登錄目標 (例如 EC2 執行個體)。您在此步驟設定的目標群組是用作接聽程式規則中的目標群組，藉以將請求轉送至目標群組。如需更多詳細資訊，請參閱「 的目標群組網路負載平衡器 (p. 28)」。

設定目標群組

1. 針對 Target group (目標群組)，保留預設值 New target group (新目標群組)。
2. 針對 Name (名稱)，輸入目標群組的名稱。
3. 對於 Protocol (通訊協定)，請如下所示選擇通訊協定：

   - If the listener protocol is TCP, choose TCP or TCP_UDP.
   - If the listener protocol is TLS, choose TCP or TLS.
   - If the listener protocol is UDP, choose UDP or TCP_UDP.
   - If the listener protocol is TCP_UDP, choose TCP_UDP.
4. (選用) 視需要設定 Port (連接埠)。
5. 針對 Target type (目標類型)，選擇 `instance` 來根據執行個體 ID 指定目標，或選擇 `ip` 來根據 IP 地址指定目標。如果目標群組通訊協定是 UDP 或 TCP_UDP，您必須選取 `instance`。

6. 針對 Health checks (運作狀態檢查)，保留預設運作狀態檢查設定。
7. 選擇 Next (下一步)。註冊目標.

Step 3: Register targets with the target group

您可以在目標群組中將 EC2 執行個體登錄為目標。

根據執行個體 ID 來登錄目標

1. 從 Instances (執行個體)，選取一個或多個執行個體。
2. 保留預設執行個體接聽程式連接埠或者輸入新連接埠並選擇 Add to registered (新增到已登錄)。
3. 完成註冊實例後，選擇 下一步: 檢閱

根據 IP 地址來登錄目標

1. 對於每個要登錄的 IP 地址，請執行下列動作：
   a. 對於 Network (網路)，若 IP 地址來自目標群組 VPC 的子網路，請選擇 VPC。否則，請選取 Other private IP address (其他私有 IP 地址)。
   b. 對於 Availability Zone (可用區域)，請選取可用區域或 all (全部)。這將決定目標是否只會接收來自指定可用區域中負載平衡器節點的流量，或者來自所有已啟用的可用區域。若您正從 VPC 登錄 IP 地址，將不會顯示此欄位。在這種情況下，將自動偵測到的可用區域。
   c. 對於 IP，請輸入地址。
   d. 對於 Port (連接埠)，請輸入連接埠。
   e. 選擇 Add to list (新增到清單)。
2. 當您完成向列表添加IP地址時，選擇 下一步: 檢閱

Step 4: Create the load balancer

在建立您的負載平衡器後，您可以確認您的 EC2 執行個體已通過最初運作狀態檢查，然後測試該負載平衡器正在傳送流量到您的 EC2 執行個體。完成負載平衡器使用後，即可刪除。如需更多詳細資訊，請參閱「Delete a 網路負載平衡器 (p. 15)」。

建立負載平衡器

1. 在 Review (檢閱) 頁面上，選擇 Create (建立)。
2. 建立網路負載平衡器之後，選擇 Close (關閉)。
3. 在導覽窗格的 LOAD BALANCING (負載平衡) 中，選擇 Target Groups (目標群組)。
4. 選取新建立的目標群組。
5. 選擇 Targets (目標) 並確認您的執行個體已就緒。若執行個體的狀態為 `initial`，原因可能是執行個體仍在進行註冊，或者未通過可視為運作狀態良好的運作狀態檢查次數下限。至少有一個執行個體的運作狀態為健康之後，您可以測試您的負載平衡器。

Tags for your 網路負載平衡器

標籤可幫助您以不同的方式來將負載平衡器分類，例如，根據目的、擁有者或環境。

您可以在每個負載平衡器中加入多個標籤。每個負載平衡器的標籤索引鍵必須是唯一的。如果所新增的標籤，其索引鍵已經與負載平衡器相關聯，則此動作會更新該標籤的值。

使用標籤完成負載平衡器使用後，可將其自負載平衡器中移除。

Restrictions

- Maximum number of tags per resource—50
- Maximum key length—127 Unicode characters
- Maximum value length—255 Unicode characters
- Tag keys and values are case-sensitive. Allowed characters are letters, spaces, and numbers representable in UTF-8, plus the following special characters: + - = . _ : / @. Do not use leading or trailing spaces.
- Do not use the `aws:` prefix in your tag names or values because it is reserved for AWS use. You can't edit or delete tag names or values with this prefix. Tags with this prefix do not count against your tags per resource limit.

使用主控台來更新負載平衡器的標籤

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器。
4. 選擇 Tags (標籤)、Add/Edit Tags (新增/編輯標籤)，然後執行一項或多項下列動作：
   a. 若要更新標籤，請編輯 Key (索引鍵) 和 Value (值) 的值。
   b. 若要新增新標籤，請選擇 Create Tag (建立標籤)。在 Key (索引鍵) 和 Value (值) 欄位中輸入值。
   c. 若要刪除標籤，請選擇標籤旁的刪除圖示 (X)。
5. 完成更新標籤的作業時，請選擇 Save (儲存)。

使用 AWS CLI 來更新負載平衡器的標籤

使用 add-tags 和 remove-tags 指令。

Delete a 網路負載平衡器

在您的負載平衡器可用後，將會根據持續執行時間收取一小時或不足一小時的費用。當您不再需要負載平衡器時，可以將它刪除。刪除負載平衡器後，便會停止收取費用。

如果已啟用刪除保護，則無法刪除負載平衡器。如需更多詳細資訊，請參閱「Deletion protection (p. 11)」。

如果負載平衡器正由其他服務使用，則無法刪除負載平衡器。例如，如果負載平衡器與 VPC 端點服務相關聯，您必須先刪除端點服務組態，才能刪除相關聯的負載平衡器。

若刪除負載平衡器，接聽程式也會一併刪除。刪除負載平衡器不會影響其登錄目標。例如，您的 EC2 執行個體將繼續執行，且仍會登錄到他們的目標群組。若要刪除您的目標群組，請參閱刪除目標群組 (p. 45)。

使用主控台來刪除負載平衡器

1. 若您的網域有指向負載平衡器的 CNAME 記錄，請指向新位置並等待 DNS 變更發生效用，之後再刪除負載平衡器。
2. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
3. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
4. 選取負載平衡器。
5. 選擇 Actions (動作)、Delete (刪除)。

6. 出現確認提示時，選擇 Yes, Delete (是，刪除)。

使用 AWS CLI 來刪除負載平衡器

使用 delete-load-balancer 指令。

Listeners for your 網路負載平衡器

在您開始使用 網路負載平衡器，您必須添加一個或多個 listeners。偵聽程序是使用您配置的協議和端口檢查連接請求的過程。您為接聽程式定義的規則將決定負載平衡器路由請求到一個或多個目標群主中之目標的方法。

有關詳細信息，請參閱 請求路由 在 Elastic Load Balancing 使用者指南.

內容

Listener configuration

接聽程式支援下列通訊協定與連接埠：

- Protocols: TCP, TLS, UDP, TCP_UDP
- Ports: 1-65535

您可以使用 TLS 接聽程式來將加密和解密的工作卸載到您的負載平衡器，使得您的應用程式可以專注在商業邏輯上。如果接聽程式的通訊協定是 TLS，您必須在接聽程式確切部署一個 SSL 伺服器憑證。如需更多詳細資訊，請參閱「TLS listeners for your Network Load Balancer (p. 18)」。

若要在相同的連接埠上同時支援 TCP 和 UDP，請建立 TCP_UDP 接聽程式。TCP_UDP 接聽程式的目標群組必須使用 TCP_UDP 通訊協定。

您可以透過接聽程式來使用 WebSocket。

傳送至設定之接聽程式的所有網路流量皆分類為預期流量。對於已設定的接聽程式，任何不匹配的網路流量皆分類為非預期流量。類型 3 以外的 ICMP 請求也視為非預期流量。網路負載平衡器 會捨棄非預期流量，而不轉送到任何目標。傳送至接聽程式連接埠的 TCP 資料封包會遭到 TCP 重設 (RST) 拒絕，該接聽程式連接埠適用的已設定接聽程式不是新連線或作用中 TCP 連線一部分。

Listener rules

當您建立接聽程式後，可指定路由請求的規則。此規則將轉發請求到指定的目標群組。若要更新此規則，請參閱 Update a listener for your 網路負載平衡器 (p. 24)。

Create a listener for your 網路負載平衡器

接聽程式是檢查連線請求的程序。您在建立負載平衡器時定義接聽程式，之後可隨時將接聽程式新增到您的負載平衡器。

Prerequisites

- You must specify a target group for the listener rule. For more information, see 為 建立目標群組網路負載平衡器 (p. 34).
- You must specify an SSL certificate for a TLS listener. The load balancer uses the certificate to terminate the connection and decrypt requests from clients before routing them to targets. For more information, see Server certificates (p. 19).

Add a listener

您使用用戶端與負載平衡器間連線的通訊協定與連接埠來設定接聽程式，並為預設接聽程式規則設定目標群組。如需更多詳細資訊，請參閱「Listener configuration (p. 17)」。

使用主控台來新增接聽程式

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 選擇 Add listener (新增接聽程式)。
5. 對於 Protocol : port (通訊協定：連接埠)，選擇 TCP (TCP)、UDP (UDP)、TCP_UDP (TCP_UDP) 或 TLS (TLS)。保持預設連接埠或輸入不同的連接埠。
6. [TLS 接聽程式] 若為 ALPN policy (ALPN 政策)，請選擇要啟用 ALPN 的政策，或選擇 None (無) 停用 ALPN。如需更多詳細資訊，請參閱「ALPN policies (p. 23)」。
7. 對於 Default actions (預設動作)，選擇 Add action (新增操作)、Forward to (轉送至)，然後選擇可用的目標群組。
8. [TLS 接聽程式] 針對 Security policy (安全政策)，建議您保留預設的安全政策。
9. [TLS 接聽程式] 針對 Default SSL certificate (預設 SSL 憑證)，執行以下其中一項：
   - If you created or imported a certificate using AWS Certificate Manager, choose From ACM and choose the certificate.
   - If you uploaded a certificate using IAM, choose From IAM and choose the certificate.
10. 選擇 Save (儲存)。
11. [TLS 接聽程式] 若要新增用於 SNI 通訊協定的選用憑證清單，請參閱Add certificates to the certificate list (p. 25)。

使用 AWS CLI 來新增接聽程式

使用 create-listener 命令來建立接聽程式。

TLS listeners for your Network Load Balancer

若要使用 TLS 接聽程式，您必須在負載平衡器上部署至少一個伺服器憑證。負載平衡器使用伺服器憑證終止前端連接，然後解密用戶端的請求，再將它們傳送到目標。

Elastic Load Balancing 使用 TLS 交涉組態 (稱為安全政策)，在用戶端與負載平衡器之間交涉 TLS 連線。安全政策為通訊協定與加密的組合。通訊協定會在用戶端與伺服器之間建立安全連線，並確保在用戶端與負載平衡器之間傳遞的所有資料為私有。隨碼是一項加密演算法，使用加密金鑰來建立編碼的訊息。通訊協定使用多個加密來加密透過網際網路的資料。在連線交涉程序期間，用戶端與負載平衡器會出示它們分別支援的加密和通訊協定的清單 (以偏好的順序)。系統會針對安全連線選取伺服器清單上符合任何用戶端加密的第一個加密。

網路負載平衡器 不支援 TLS 重新交涉。

若要建立 TLS 接聽程式，請參閱Add a listener (p. 18)。如需相關示範，請參閱 網路負載平衡器 上的 TLS 支援及 網路負載平衡器 上的 SNI 支援。

Server certificates

負載平衡器需要 X.509 憑證 (伺服器憑證)。憑證為憑證授權機構 (CA) 發出的數位形式身分證明。憑證包含識別資訊、有效期間、公有金鑰、序號和發行者的數位簽章。

建立憑證以搭配您的負載平衡器使用時，您必須指定網域名稱。

建議您使用 AWS Certificate Manager (ACM) 為負載平衡器建立憑證。ACM 會與 Elastic Load Balancing 整合，使得您可以在負載平衡器上部署憑證。如需更多詳細資訊，請參閱 AWS Certificate Manager 使用者指南。

或者，您可以使用 TLS 工具來建立憑證簽署請求 (CSR)、取得由 CA 簽署的憑證 CSR 產生的憑證，然後匯入到 ACM 或上傳憑證為 AWS Identity and Access Management (IAM)。有關詳細信息，請參閱 導入證書 在 AWS Certificate Manager 使用者指南 或 使用服務器證書 在 IAM 使用者指南.

> Important
>
> 您無法在 網路負載平衡器 安裝具有大於 2048 位元 RSA 金鑰或 EC 金鑰的憑證。

Default certificate

建立 TLS 接聽程式時，您必須指定剛好一個憑證。此證書被稱爲 default certificate。您可以在創建TLS偵聽程序之後替換默認證書。如需更多詳細資訊，請參閱「Replace the default certificate (p. 25)」。

如果您在憑證清單 (p. 19)中指定額外憑證，只有當用戶端連接時未使用伺服器名稱指示 (SNI) 通訊協定來指定主機名稱，或憑證清單中沒有相符的憑證時，才會使用預設憑證。

如果您不指定額外憑證，但需要透過單一負載平衡器來託管多個安全應用程式，您可以使用萬用字元憑證，或將每個額外網域的主體別名 (SAN) 新增至憑證。

Certificate list

TLS 接聽程式建立之後具有預設憑證和空的憑證清單。您可以選擇性將憑證新增至接聽程式的憑證清單。使用憑證清單可讓負載平衡器在相同連接埠上支援多個網域，並為每個網域提供不同的憑證。如需更多詳細資訊，請參閱「Add certificates to the certificate list (p. 25)」。

負載平衡器使用支援 SNI 的智慧憑證選擇演算法。如果用戶端提供的主機名稱符合憑證清單中的單一憑證，負載平衡器會選取此憑證。如果用戶端提供的主機名稱符合憑證清單中的多個憑證，負載平衡器會選取用戶端可支援的最佳憑證。憑證選擇是根據採用下列順序的以下條件：

- Public key algorithm (prefer ECDSA over RSA)
- Hashing algorithm (prefer SHA over MD5)
- Key length (prefer the largest)
- Validity period

負載平衡器存取日誌項目會指出用戶端指定的主機名稱和向用戶端出示的憑證。如需更多詳細資訊，請參閱「存取日誌項目 (p. 54)」。

Certificate renewal

每個憑證均附帶有效期間。您必須確保在有效期間結束之前，續約或更換負載平衡器的每個憑證。這包括預設憑證和憑證清單中的憑證。續約或更換憑證不會影響負載平衡器節點收到並且等待路由到運作狀態良好目標的傳輸中請求。續約憑證之後，新請求會使用續約的憑證。更換憑證之後，新請求會使用新的憑證。

您可以如下所示管理憑證續約和更換：

- Certificates provided by AWS Certificate Manager and deployed on your load balancer can be renewed automatically. ACM attempts to renew certificates before they expire. For more information, see Managed renewal in the AWS Certificate Manager 使用者指南.
- If you imported a certificate into ACM, you must monitor the expiration date of the certificate and renew it before it expires. For more information, see Importing certificates in the AWS Certificate Manager 使用者指南.
- If you imported a certificate into IAM, you must create a new certificate, import the new certificate to ACM or IAM, add the new certificate to your load balancer, and remove the expired certificate from your load balancer.

Security policies

建立 TLS 接聽程式時，您必須選取安全政策。您可以視需要更新安全政策。如需更多詳細資訊，請參閱「Update the security policy (p. 26)」。

您可以選擇用於前端連線的安全政策。`ELBSecurityPolicy-2016-08` 安全政策一律用於後端連線。網路負載平衡器 不支援自訂安全政策。

Elastic Load Balancing 為 網路負載平衡器 提供以下安全政策：

- `ELBSecurityPolicy-2016-08` (default)
- `ELBSecurityPolicy-TLS-1-0-2015-04`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-FS-2018-06`
- `ELBSecurityPolicy-FS-1-1-2019-08`
- `ELBSecurityPolicy-FS-1-2-2019-08`
- `ELBSecurityPolicy-FS-1-2-Res-2019-08`
- `ELBSecurityPolicy-2015-05` (identical to `ELBSecurityPolicy-2016-08`)

為了相容，我們建議 `ELBSecurityPolicy-2016-08` 政策。如果您需要遠期保密 (FS)，則可以使用其中一個 `ELBSecurityPolicy-FS` 政策。您可以使用其中一個 `ELBSecurityPolicy-TLS` 政策，以滿足需要停用特定 TLS 通訊協定版本的合規和安全標準，或是支援需要已淘汰加密的舊版用戶端。網際網路用戶端中只有一小部分百分比需要 TLS 版本 1.0。若要檢視對您的負載平衡器的請求 TLS 通訊協定版本，請為您的負載平衡器啟用存取記錄並檢查存取日誌。如需詳細資訊，請參閱存取日誌 (p. 53)。

下表說明預設政策和 `ELBSecurityPolicy-TLS` 政策。

安全政策	預設值：	TLS 1.0 †	TLS 1.1	TLS 1.2	TLS 1.2 ext
TLS Protocols					
Protocol-TLSv1	♦	♦			
Protocol-TLSv1.1	♦	♦	♦		
Protocol-TLSv1.2	♦	♦	♦	♦	♦
TLS Ciphers					

安全政策	預設值：	TLS 1.0 †	TLS 1.1	TLS 1.2	TLS 1.2 ext
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256 *	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA *	♦	♦	♦		♦
ECDHE-RSA-AES128-SHA	♦	♦	♦		♦
ECDHE-ECDSA-AES256-GCM-SHA384 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA	♦	♦	♦		♦
ECDHE-ECDSA-AES256-SHA *	♦	♦	♦		♦
AES128-GCM-SHA256	♦	♦	♦	♦	♦
AES128-SHA256	♦	♦	♦	♦	♦
AES128-SHA	♦	♦	♦		♦

安全政策	預設值：	TLS 1.0 †	TLS 1.1	TLS 1.2	TLS 1.2 ext
AES256-GCM-SHA384	♦	♦	♦	♦	♦
AES256-SHA256	♦	♦	♦	♦	♦
AES256-SHA *	♦	♦	♦		♦
DES-CBC3-SHA		♦			

† 請勿使用此政策，除非您必須支援需要 DES-CBC3-SHA 加密 (一種弱式加密) 的傳統用戶端。

下表說明預設政策和 `ELBSecurityPolicy-FS` 政策。

安全政策	預設值：	FS	FS 1.1	FS 1.2	FS 1.2 res
TLS Protocols					
Protocol-TLSv1	♦	♦			
Protocol-TLSv1.1	♦	♦	♦		
Protocol-TLSv1.2	♦	♦	♦	♦	♦
TLS Ciphers					
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256 *	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA *	♦	♦	♦	♦	
ECDHE-RSA-AES128-SHA	♦	♦	♦	♦	
ECDHE-ECDSA-	♦	♦	♦	♦	♦

安全政策	預設值：	FS	FS 1.1	FS 1.2	FS 1.2 res
AES256-GCM-SHA384 *					
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384 *	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA	♦	♦	♦	♦	
ECDHE-ECDSA-AES256-SHA *	♦	♦	♦	♦	
AES128-GCM-SHA256	♦				
AES128-SHA256	♦				
AES128-SHA	♦				
AES256-GCM-SHA384	♦				
AES256-SHA256	♦				
AES256-SHA *	♦				

若要使用 AWS CLI 來檢視負載平衡器適用的安全政策的組態，請使用 describe-ssl-policies 命令。

ALPN policies

應用程式層通訊協定交涉 (ALPN) 是在初始 TLS 信號交換您好訊息上傳送的 TLS 延伸。ALPN 使應用程式層能夠協商哪些通訊協定的使用透過安全的連接 (如 HTTP/1 和 HTTP/2) 來進行。

當用戶端起始 ALPN 連線時，負載平衡器會將用戶端 ALPN 喜好設定清單與其 ALPN 政策進行比較。如果用戶端支援來自 ALPN 政策的通訊協定，則負載平衡器會根據 ALPN 政策的喜好設定清單來建立連線。否則，負載平衡器不會使用 ALPN。

Requirements

- TLS listener
- TLS target group

支援的 ALPN 政策

以下是支援的 ALPN 政策：

`HTTP1Only`

只交涉 HTTP/1.*。ALPN 喜好設定清單為 http/1.1、http/1.0。

`HTTP2Only`

只協商 HTTP/2。ALPN 喜好設定清單為 h2。

`HTTP2Optional`

偏好 HTTP/1.*，而不是 HTTP/2 (這對於 HTTP/2 測試可能有用)。ALPN 喜好設定清單包括：http/1.1、http/1.0、h2。

`HTTP2Preferred`

偏好 HTTP/2，而不是 HTTP/1.*。ALPN 喜好設定清單是 h2、http/1.1、http/1.0。

`None`

不要交涉 ALPN。(此為預設值)。

啟用 ALPN 連線

您可以在建立或修改 TLS 接聽程式時啟用 ALPN 連線。如需詳細資訊，請參閱 Add a listener (p. 18) 及 Update the ALPN policy (p. 27)。

Update a listener for your 網路負載平衡器

您可以更新接聽程式連接埠、接聽程式通訊協定或預設的接聽程式規則。

預設的接聽程式規則將轉發請求到指定的目標群組。

如果通訊協定從 TCP 或 UDP 變更為 TLS，您必須指定安全政策和伺服器憑證。如果通訊協定從 TLS 變更為 TCP 或 UDP，安全政策和伺服器憑證將被移除。

使用主控台更新您的接聽程式

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 選取接聽程式的核取方塊，並選擇 Edit (編輯)。
5. (選用) 變更 Protocol : port (通訊協定：連接埠) 的指定值。
6. (選用) 按一下鉛筆圖示，為 Default action (預設動作) 選取不同的目標群組。
7. 選擇 Update (更新)。

使用 AWS CLI 更新您的接聽程式

使用 modify-listener 命令。

Update a TLS listener for your 網路負載平衡器

建立 TLS 接聽程式之後，您可以取代預設憑證、從憑證清單新增或移除憑證、更新安全性政策，或更新 ALPN 政策。

限制

您無法在 網路負載平衡器 安裝具有大於 2048 位元 RSA 金鑰或 EC 金鑰的憑證。

任務

Replace the default certificate

您可以使用以下程序，更換 TLS 接聽程式的預設憑證。如需更多詳細資訊，請參閱「Default certificate (p. 19)」。

使用主控台取代預設憑證

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 選取接聽程式的核取方塊，並選擇 Edit (編輯)。
5. 針對 Default SSL certificate (預設 SSL 憑證)，執行下列其中一項作業：
   - If you created or imported a certificate using AWS Certificate Manager, choose From ACM and choose the certificate.
   - If you uploaded a certificate using IAM, choose From IAM and choose the certificate.
6. 選擇 Update (更新)。

使用 AWS CLI 取代預設憑證

使用 modify-listener 命令搭配 --certificates 選項。

Add certificates to the certificate list

您可以使用以下程序，將憑證新增至接聽程式的憑證清單。當您最初建立 TLS 接聽程式時，憑證清單是空的。您可以新增一或多個憑證。您可以選擇性新增預設憑證，以確保此憑證即使更換為預設憑證，也會搭配 SNI 通訊協定一起使用。如需更多詳細資訊，請參閱「Certificate list (p. 19)」。

使用主控台將憑證新增至憑證清單

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 若要讓 HTTPS 接聽程式更新，請選擇 View/edit certificates (檢視/編輯憑證)，這會顯示預設的憑證，接著是您新增到接聽程式的任何其他憑證。
5. 選擇功能表列中的 Add certificates (新增憑證) 圖示 (加號)，這會顯示預設的憑證，接著是 ACM 和 IAM 管理的任何其他憑證。如果您已新增憑證到接聽程式，則會選取其核取方塊並停用。
6. 若要新增已由 ACM 或 IAM 管理的憑證，請選取憑證的核取方塊，然後選擇 Add (新增)。
7. 如果您有未由 ACM 或 IAM 管理的憑證，請將它匯入到 ACM，並將它新增至您的接聽程式，如下所示：

a. 選擇 Import certificate (匯入憑證)。
b. 對於 Certificate private key (憑證私有金鑰)，貼上憑證的 PEM 編碼、未加密私有金鑰。
c. 對於 Certificate body (憑證內文)，貼上 PEM 編碼憑證。
d. (選用) 對於 Certificate chain (憑證鏈)，貼上 PEM 編碼的憑證鏈。
e. 選擇 Import (匯入)。新匯入的憑證會顯示在可用的憑證清單中，並且選取。
f. 選擇新增。

8. 若要離開此畫面，請選取功能表列上的 Back to the load balancer (返回負載平衡器) 圖示 (返回按鈕)。

使用 AWS CLI 將憑證新增至憑證清單

使用 add-listener-certificates 命令。

Remove certificates from the certificate list

您可以使用以下程序，從 TLS 接聽程式的憑證清單中移除憑證。若要移除 TLS 接聽程式的預設憑證，請參閱Replace the default certificate (p. 25)。

使用主控台從憑證清單中移除憑證

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 若要讓接聽程式更新，請選擇 View/edit certificates (檢視/編輯憑證)，這會顯示預設的憑證，接著是您新增到接聽程式的任何其他憑證。
5. 選擇功能表列中的 Remove certificates (移除憑證) 圖示 (減號)。
6. 選取憑證的核取方塊，然後選擇 Remove (移除)。
7. 若要離開此畫面，請選取功能表列上的 Back to the load balancer (返回負載平衡器) 圖示 (返回按鈕)。

使用 AWS CLI 從憑證清單中移除憑證

使用 remove-listener-certificates 命令。

Update the security policy

建立 TLS 接聽程式時，您可以選取符合您的需求的安全政策。新增新的安全政策時，您可以更新您的 TLS 接聽程式，以使用新的安全政策。網路負載平衡器 不支援自訂安全政策。如需更多詳細資訊，請參閱「Security policies (p. 20)」。

使用主控台更新安全政策

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 選取 TLS 接聽程式的核取方塊，並選擇 Edit (編輯)。
5. 針對 Security policy (安全政策)，選擇安全政策。
6. 選擇 Update (更新)。

使用 AWS CLI 更新安全政策

使用 modify-listener 命令搭配 --ssl-policy 選項。

Update the ALPN policy

您可以使用下列程序更新 TLS 接聽程式的 ALPN 政策。如需更多詳細資訊，請參閱「ALPN policies (p. 23)」。

使用主控台更新 ALPN 政策

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。
4. 選取 TLS 接聽程式的核取方塊，並選擇 Edit (編輯)。
5. 若為 ALPN policy (ALPN 政策)，請選擇要啟用 ALPN 的政策，或選擇 None (無) 停用 ALPN。
6. 選擇 Update (更新)。

若要更新 ALPN 政策，請使用 AWS CLI

使用 modify-listener 命令搭配 --alpn-policy 選項。

Delete a listener for your 網路負載平衡器

您可隨時刪除接聽程式。

使用主控台刪除接聽程式

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 LOAD BALANCING (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取負載平衡器，然後選擇 Listeners (接聽程式)。選取接聽程式的核取方塊，並選擇 Delete (刪除)。
4. 出現確認提示時，選擇 Yes, Delete (是，刪除)。

使用 AWS CLI 來刪除接聽程式

使用 delete-listener 命令。

的目標群組網路負載平衡器

每個 目標組 用於將請求路由至一個或多個已註冊目標。當您建立接聽程式時，可以為其預設動作指定一個目標群組。流量會轉送至接聽程式規則中指定的目標群組。您可以針對不同類型的請求，建立不同的目標群組。例如，針對一般請求建立一個目標群組，然後再針對應用程式微型服務的請求，建立其他的目標群組。如需詳細資訊，請參閱網路負載平衡器 components (p. 1).

您可以針對每個目標群組，指定負載平衡器的運作狀態檢查設定。除非您在建立目標群組時覆寫這些設定，或是在之後修改設定，否則每個目標群組都會使用預設的運作狀態檢查設定。當您在接聽程式的規則中指定目標群組後，負載平衡器會針對自己已啟用可用區域中的目標群組，持續地監控透過該目標群組註冊的所有目標，以了解目標的運作狀態。負載平衡器會將請求路由至運作狀態良好的已註冊目標。如需詳細資訊，請參閱目標群組運作狀態檢查 (p. 35).

內容

路由組態

根據預設，負載平衡器會使用您在建立目標群組時所指定的通訊協定和埠號，來將請求路由至其目標。或者，您可以在使用目標群組來註冊目標時，覆寫用來將流量轉送到目標的連接埠。

目標組 網路負載平衡器 支持以下協議和端口:

- 通訊協定: TCP、TLS、UDP、TCP_UDP
- 連接埠: 1 到 65535

如果使用 TLS 通訊協定設定目標群組，則負載平衡器會使用您在目標上安裝的憑證，與目標建立 TLS 連線。負載平衡器不會驗證這些憑證。因此，您可以使用自我簽署的憑證或已過期的憑證。由於負載平衡器位於 Virtual Private Cloud (VPC)，系統會在封包層級對負載平衡器與目標之間的流量進行驗證，因此即使目標上的憑證無效，也不會遭受中間人攻擊或詐騙的風險。

下表總結接聽程式通訊協定和目標群組設定的支援組合。

接聽程式通訊協定	目標群組通訊協定	目標群組類型	運作狀態檢查通訊協定
TCP	TCP | TCP_UDP	執行個體 | ip	HTTP | HTTPS | TCP

接聽程式通訊協定	目標群組通訊協定	目標群組類型	運作狀態檢查通訊協定
TLS	TCP | TLS	執行個體 | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	執行個體 | ip	HTTP | HTTPS | TCP
TCP_UDP	TCP_UDP	執行個體 | ip	HTTP | HTTPS | TCP

Target type (目標類型)

在建立目標群組時，您會指定其目標類型，這會決定您指定其目標的方式。目標群組建立之後，您就無法更改其目標類型。

下列是可能的目標類型：

`instance`

以執行個體 ID 來指定目標。

`ip`

以 IP 地址來指定目標。

如果目標類型是 `ip`，您可以從下列其中一個 CIDR 區塊指定 IP 地址：

- 目標群組 VPC 的子網路
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Important

您無法指定可公開路由傳送的 IP 地址。

這些支持的CIDR塊使您能夠與目標組註冊以下內容: ClassicLink實例、IP地址和端口可尋址的AWS資源（例如，數據庫）以及與AWS相關聯的本地資源 AWS Direct Connect 或軟件VPN連接。

若目標類型是 `ip`，負載平衡器可支援 55,000 條同時連線，或每分鐘 55,000 條連線連至唯一目標 (IP 地址和連接埠)。若超過上述連線數量，將提高連接埠配置錯誤機率。若發生連接埠配置錯誤，請將更多目標新增至目標群組。

網路負載平衡器 不支持 `lambda` 目標類型，僅限 Application Load Balancer 支持 `lambda` 目標類型。有關詳細信息，請參閱 Lambda功能作爲目標 在 Application Load Balancer 使用者指南.

請求路由與 IP 地址

如果使用執行個體 ID 來指定目標，會利用在執行個體的主要網路界面中，所指定的主要私有 IP 地址，來將流量轉送到執行個體。負載平衡器會重新寫入資料封包的目的地 IP 地址，再轉送至目標執行個體。

如果使用 IP 地址來指定目標，您可以利用來自一個或多個網路界面的任何私有 IP 地址，將流量轉送到執行個體。這可讓執行個體上的多個應用程式，使用相同的連接埠。請注意，每個網路界面都可以有自己的安全群組。負載平衡器會先重新寫入目的地 IP 地址，再轉送至目標。

如需允許流量進入執行個體的詳細資訊，請參閱 目標安全群組 (p. 40).

來源 IP 保留

如果您按實例ID指定目標，將保留客戶端的源IP地址，並將其提供給應用程序。

如果您按IP地址指定目標，源IP地址取決於目標組的協議，如下所示:

- TCP和TLS: 源IP地址是負載均衡器節點的專用IP地址。如果您需要客戶端的IP地址，請啓用 代理協議 (p. 31) 並從代理協議標題獲取客戶端IP地址。
- UDP和TCP_UDP: 源IP地址是客戶端的IP地址。

如果您在使用 網路負載平衡器 登錄的執行個體上擁有微型服務，除非負載平衡器是連線到網際網路，或執行個體是依 IP 地址登錄，否則您無法使用負載平衡器來在這兩者之間提供通訊。如需詳細資訊，請參閱Connections time out for requests from a target to its load balancer (p. 62).

已登記的目標

您的負載平衡器可做為用戶端的單一聯絡窗口，並將傳入的流量分配到各個運作狀態良好的已登錄目標。在負載平衡器能夠使用的每個可用區域中，每個目標群組都必須擁有至少一個已登錄的目標。您可以利用一個或多個群組來登錄每個目標。您可以使用不同的連接埠，使用同一個目標群組來註冊每個 EC2 執行個體或 IP 地址多次，讓負載平衡器將請求轉送到微型服務。

如果對應用程式的需求增加，您可以利用一個或多個目標群組來登錄額外的目標，來應付需求。只要登錄程序一完成，負載平衡器就會開始將流量轉傳到新登錄的目標。

如果對您應用程式的需求減少，或者您需要為目標提供服務，可以從目標群組取消目標的登錄。取消目標的登錄，會將該目標從目標群組中移除，但不會影響到目標。取消目標的登錄之後，負載平衡器就會立即停止將流量轉傳到目標。目標會進入 `draining` 狀態，直到處理中的請求已完成。當您準備讓目標再繼續接收流量時，可以將目標登錄到目標群組。

如果是根據執行個體 ID 來註冊目標，您可以使用負載平衡器搭配 Auto Scaling 群組。在您將目標組附加到 Auto Scaling 組， Auto Scaling 在啓動目標組時，將目標註冊爲目標組。有關詳細信息，請參閱 將負載平衡器附加到您的 Auto Scaling 組 在 Amazon EC2 Auto Scaling 使用者指南.

Requirements

- 如果使用以下實例類型之一，則無法按實例ID註冊實例:
  C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3或T1。
- 如果VPC處於負載均衡器VPC（相同區域或不同區域）的虛擬機中，則無法按實例ID註冊實例。您可以依照 IP 地址來註冊這些執行個體。
- 如果您依照 IP 地址註冊目標，且 IP 地址與負載平衡器位於相同的 VPC 中，則負載平衡器會驗證它來自於其可連上的子網路。
- 對於UDP和TCP_UDP目標組，如果IP地址位於負載均衡器VPC以外或如果使用以下實例類型之一，請勿通過IP地址寄存實例: C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3或T1。駐留在負載均衡器VPC以外的目標或使用不支持的實例類型可能能夠接收負載均衡器的流量，但無法響應。

目標群組屬性

下列是目標群組的屬性：

`deregistration_delay.timeout_seconds`

的時間 Elastic Load Balancing 要在更改已從 `draining` 至 `unused`...範圍爲0-3600秒。預設值為 300 秒。

`proxy_protocol_v2.enabled`

顯示是否已啟用 Proxy Protocol 第 2 版。預設會停用 Proxy Protocol。

`stickiness.enabled`

指出是否已啟用黏性工作階段。

`stickiness.type`

黏性的類型。可能的值為 `source_ip`.

取消登記的延遲

將執行個體取消登錄時，負載平衡器會停止建立執行個體的新連線。負載平衡器會以連接耗盡功能，來確保傳輸中流量在現有連線上完成。如果取消登錄的執行個體保持良好的狀態，且現有連線未閒置，負載平衡器可以繼續傳送流量至執行個體。若要確保現有連線關閉，您可以在取消登錄執行個體之前確保該執行個體運作不良，或您可以定期關閉用戶端連線。

刪除目標的初始狀態爲 `draining`...默認情況下，負載均衡器將已刪除目標狀態更改爲 `unused` 300秒後。若要變更負載平衡器在將取消登錄目標的狀態變更成 `unused` 之前的等候時間，請更新取消登錄的延遲的值。我們建議您指定的值至少 120 秒，以確保完成該請求。

New console

如何使用新控制檯更新DeregistrationDelay值

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 在 組詳情 頁面， 屬性 部分，選擇 編輯.
5. 在 編輯屬性 頁面，更改 Deregistrationdelay（DeregistrationDelay） 根據需要。
6. 選擇 保存更改.

Old console

如何使用舊控制檯更新DeregistrationDelay值

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選取目標群組。
4. 選擇 描述， 編輯屬性.
5. 更改 Deregistrationdelay（DeregistrationDelay） 根據需要，然後選擇 保存.

使用 來更新取消登錄的延遲值AWS CLI

使用 修改-目標組屬性 命令。

Proxy Protocol (代理通訊協定)

網路負載平衡器 會使用 Proxy Protocol 第 2 版來傳送額外的連線資訊，例如來源和目的地。Proxy Protocol 第 2 版提供 Proxy Protocol 標頭的二進位編碼。負載平衡器會在 TCP 資料前面加上 Proxy Protocol 標頭。

它不會捨棄或覆寫現有資料，包括用戶端傳送的 proxy protocol 標頭或網路路徑中的其他代理程式、負載平衡器或伺服器。因此，可能接收多個 proxy protocol 標頭。此外，若有 網路負載平衡器 以外的其他網路路徑連至目標，第一個 proxy protocol 標頭可能並非來自您的 。網路負載平衡器.

如果您按照IP地址指定目標，則提供給應用程序的源IP地址取決於目標組的協議，如下所示:

- TCP和TLS: 源IP地址是負載均衡器節點的專用IP地址。如果您需要用戶端的 IP 地址，請啟用 Proxy Protocol，並從 Proxy Protocol 標頭取得用戶端的 IP 地址。
- UDP和TCP_UDP: 源IP地址是客戶端的IP地址。

如果使用執行個體 ID 來指定目標，則提供給應用程式的來源 IP 地址，會是用戶端的 IP 地址。不過，如果您需要的話，可以啟用 Proxy Protocol，並從 Proxy Protocol 標頭取得用戶端的 IP 地址。

運作狀態檢查連線

啟用 Proxy Protocol 之後，在與負載平衡器的運作狀態檢查連線中，也會包含 Proxy Protocol 標頭。不過，如果有運作狀態檢查連線，在 Proxy Protocol 的標頭中就不會傳送用戶端的連線資訊。

VPC 端點服務 ()

對於從服務消費者到客戶的流量 VPC端點服務，嚮應用程序提供的源IP地址是負載均衡器節點的專用IP地址。如果應用程式需要服務消費者的 IP 地址，請啟用 Proxy Protocol，並且從 Proxy Protocol 標頭取得這些地址。

Proxy Protocol 標頭也包含了端點的 ID。這項資訊是使用自訂的 Type-Length-Value (類型/長度/值，TLV) 向量進行編碼。

欄位	長度 (單位：octet (八位元組))	描述：
類型	1.	PP2_TYPE_AWS (0xEA)
Length (長度)	2	值的長度
數值	1.	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	變數 (值的長度減 1)	端點的 ID

如需解析TLV型號0xEA的示例，請參閱 https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot.

啟用 Proxy Protocol

在針對目標群組啟用 Proxy Protocol 之前，請確定應用程式可處理和剖析 Proxy Protocol 第 2 版的標頭，否則應用程式可能會當機。有關詳細信息，請參閱 代理協議版本1和2.

New console

使用新控制檯啓用代理協議v2

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱，打開其詳細信息頁面。

4. 在 組詳情 頁面， 屬性 部分，選擇 編輯.
5. 在 編輯屬性 頁面，選擇 代理協議v2.
6. 選擇 保存更改.

Old console

使用舊控制檯啓用代理協議v2

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選取目標群組。
4. 選擇 描述， 編輯屬性.
5. 對於 代理協議v2，選擇 啓用.
6. 選擇 保存.

使用 來啟用 Proxy Protocol 第 2 版AWS CLI

使用 修改-目標組屬性 命令。

黏性工作階段

黏性工作階段是將用戶端流量路由到目標群組中相同目標的機制。這對於維護狀態資訊以便為用戶端提供持續體驗的伺服器來說很實用。

Considerations

- 使用粘性工作階段會導致連線和流程分配不均，因而可能會影響目標的可用性。例如，相同 NAT 裝置後面的所有用戶端都有相同的來源 IP 地址。因此，來自這些用戶端的所有流量都會路由到相同的目標。
- 如果目標群組之任何目標的運作狀態發生變更，或者如果您向目標群組註冊或取消註冊目標，則負載平衡器可能會重設該目標群組的粘性工作階段。
- TLS 接聽程式和 TLS 目標群組不支援相黏工作階段。

New console

如何使用新控制檯啓用粘滯會話

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 在 組詳情 頁面， 屬性 部分，選擇 編輯.
5. 在 編輯屬性 頁面，選擇 粘性.
6. 選擇 保存更改.

Old console

如何使用舊控制檯啓用粘滯會話

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選取目標群組。
4. 選擇 描述， 編輯屬性.
5. 對於 粘性，選擇 啓用.
6. 選擇 保存.

使用 啟用黏性工作階段AWS CLI

使用 修改-目標組屬性 使用 `stickiness.enabled` 屬性。

為 建立目標群組網路負載平衡器

您會透過目標群組來登錄 網路負載平衡器 的目標。根據預設，負載平衡器會使用您針對目標群組所指定的埠號和通訊協定，來將請求傳送到登錄的目標。在透過目標群組來註冊每個目標時，您可以覆寫此埠號。

在建立目標群組之後，您可以新增標籤。

若要將流量轉傳到目標群組中的目標，請建立接聽程式，並且在接聽程式的預設動作中，指定該目標群組。如需詳細資訊，請參閱Listener rules (p. 17).

您可以隨時從目標群組新增或移除目標。如需詳細資訊，請參閱透過目標群組來登記目標 (p. 39). 您也可以修改目標群組的運作狀態檢查設定。如需詳細資訊，請參閱修改目標群組的運作狀態檢查設定 (p. 39).

New console

如何使用新控制檯創建目標組

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇 創建目標組.
4. 對於 選擇目標類型，選擇 實例 按實例ID或 IP地址 按IP地址註冊目標。
5. 對於 目標組名稱，鍵入目標組的名稱。此名稱在每個帳戶的每個區域中都必須是唯一的，其長度上限為 32 個字元，並且必須僅包含英數字元或連字號，且開頭或結尾不可以是連字號。
6. 對於 協議，選擇如下方案:
   - 如果偵聽程序協議是TCP，請選擇 TCP 或 TCP_UDP.
   - 如果偵聽程序協議爲TLS，請選擇 TCP 或 TLS.
   - 如果偵聽程序協議爲UDP，請選擇 UDP 或 TCP_UDP.
   - 如果偵聽程序協議是TCP_UDP，請選擇 TCP_UDP.
7. （可選）端口，根據需要修改默認值。
8. 對於 VPC，選擇虛擬私有云(VPC)。
9. （可選）運行狀況檢查 部分，根據需要修改默認設置。
10. (選用) 新增一個或多個標籤，如下所示：
    a. 擴展 標籤 第節。
    b. 選擇 添加標籤.
    c. 輸入標籤密鑰和標記值。
11. 選擇 下一步.

12. （可選）添加一個或多個目標，如下所示:
    - 如果目標類型爲 實例，選擇一個或多個實例，輸入一個或多個端口，然後選擇 包括在下面的待處理中.
    - 如果目標類型爲 IP地址，選擇網絡，輸入IP地址和端口，然後選擇 包括在下面的待處理中.
13. 選擇 創建目標組.
14. (選用) 您可以在預設接聽程式規則中指定目標群組。有關詳細信息，請參閱 創建傾聽者 (p. 17) 和 更新偵聽者 (p. 24).

Old console

如何使用舊控制檯創建目標組

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇 創建目標組.
4. 對於 目標組名稱，鍵入目標組的名稱。此名稱在每個帳戶的每個區域中都必須是唯一的，其長度上限為 32 個字元，並且必須僅包含英數字元或連字號，且開頭或結尾不可以是連字號。
5. 對於 協議，選擇如下方案:
    - 如果偵聽程序協議是TCP，請選擇 TCP 或 TCP_UDP.
    - 如果偵聽程序協議爲TLS，請選擇 TCP 或 TLS.
    - 如果偵聽程序協議爲UDP，請選擇 UDP 或 TCP_UDP.
    - 如果偵聽程序協議是TCP_UDP，請選擇 TCP_UDP.
6. （可選）端口，根據需要修改默認值。
7. 對於 目標類型，選擇 `instance` 按實例ID或 `ip` 按IP地址指定目標。
8. 對於 VPC，選擇虛擬私有云(VPC)。
9. （可選）運行狀況檢查設置 和 高級運行狀況檢查設置，根據需要修改默認設置。選擇 創建.
10. (選用) 新增一個或多個標籤，如下所示：
    a. 選取新建立的目標群組。
    b. 選擇 標籤， 添加/編輯標籤.
    c. 在 添加/編輯標籤 頁面，對於您添加的每個標籤，請選擇 創建標籤 然後指定標籤密鑰和標記值。添加標籤後，選擇 保存.
11. (選用) 若要在目標群組中加入目標，請參閱透過目標群組來登記目標 (p. 39).
12. (選用) 您可以在預設接聽程式規則中指定目標群組。有關詳細信息，請參閱 創建傾聽者 (p. 17) 和 更新偵聽者 (p. 24).

使用 來建立目標群組AWS CLI

使用 創建目標組 命令來創建目標組， 添加標籤 命令標記您的目標組，以及 寄存器目標 添加目標的命令。

目標群組運作狀態檢查

您可以利用一個或多個群組來登錄目標。只要登錄程序一完成，負載平衡器就會開始將請求路由到新登錄的目標。註冊程序可能需要幾分鐘的時間才能完成，並開始運作狀態檢查。

網路負載平衡器 使用主動和被動的運作狀態檢查，以判定目標是否可用於處理請求。預設情況下，每個負載平衡器節點只會將請求路由至其可用區域內運作狀態良好的目標。若您啟用跨區域負載平衡功能，每個負載

平衡器節點則會將請求路由至所有已啟用的可用區域內運作狀態良好的目標。如需詳細資訊，請參閱Cross-zone load balancing (p. 10).

憑藉主動的運作狀態檢查，負載平衡器將定期向每個已註冊目標傳送請求以檢查其狀態。每個負載平衡器節點會使用各目標註冊所屬目標群組的運作狀態檢查設定，檢查該目標的運作狀態。每次運作狀態檢查完成後，負載平衡器節點即會關閉其為執行運作狀態檢查而建立的連線。

憑藉被動的運作狀態檢查，負載平衡器將觀察各目標回應連線的情形。被動的運作狀態檢查使負載平衡器得以在主動的運作狀態檢查回報某目標運作狀態不佳之前即偵測出其運作狀態不佳。您無法停用、設定或監控被動的運作狀態檢查。不支援對 UDP 流量進行被動運作狀態檢查。

如果目標變得狀態不良，負載平衡器會針對在與目標相關聯的用戶端連線上接收的封包傳送 TCP RST。

如果一個或多個目標群組在已啟用的可用區域內沒有運作狀態良好的目標，我們將從 DNS 移除相應子網路的 IP 地址，以使請求無法路由至該可用區域內的目標。如果每個目標群組中無任何已啟用的可用區域具有運作狀態良好的目標，請求便會路由至所有已啟用的可用區域內的目標。

對於 HTTP 或 HTTPS 運作狀態檢查請求，主機標頭會包含負載平衡器節點的 IP 位址和接聽程式連接埠 (而不是目標的 IP 位址和運作狀態檢查連接埠)。

如果您新增 TLS 接聽程式至 網路負載平衡器，我們會執行接聽程式連線測試。TLS 終止也會中斷 TCP 連線，此時您的負載平衡器和目標之間會建立新的 TCP 連線。因此，您可能看到此測試的 TCP ping 從負載平衡器傳送至目標 (這些目標已向 TLS 接聽程式註冊)。您可以識別這些 TCP ping，因為他們具有 網路負載平衡器 的來源 IP 地址，而且連線不包含資料封包。

若是 UDP 服務，則會、則會使用導向您目標上 TCP 連接埠的 TCP 有效運作狀態檢查來測試可用性。您可以在目標上使用任何 TCP 連接埠來驗證 UDP 服務的可用性。如果接聽運作狀態檢查連接埠的服務失敗，您的目標是被視為無法使用。為了改善 UDP 服務運作狀態檢查的準確性，將接聽運作狀態檢查連接埠的服務設定為追蹤 UDP 服務的狀態，若服務無法使用則關閉運作狀態檢查連接埠。

運作狀態檢查設定

您將使用以下設定，為目標群組中的目標設定主動的運作狀態檢查。如果運行狀況檢查超過 未運行閾值計數 連續失敗，負載均衡器將目標停止服務。當運行狀況檢查超過 HealthyThreshold計數 連續成功後，負載均衡器將目標放回服務。

設定	描述：
HealthCheckProtocol	負載平衡器對目標執行運作狀態檢查時使用的通訊協定。可能的通訊協定包括 HTTP、HTTPS 和 TCP。預設為 TCP 通訊協定。
HealthCheckPort	負載平衡器對目標執行運作狀態檢查時使用的連接埠。預設為使用每個目標從負載平衡器接收流量的連接埠。
HealthCheckPath	[HTTP/HTTPS 運作狀態檢查] 執行運作狀態檢查的目標其目的地 ping 路徑。 預設值為 。
HealthCheckTimeoutSeconds	以秒為單位的時間長度，若目標在此期間內毫無回應即表示運作狀態檢查失敗。這個值在檢查 HTTP 運作狀態時一定為 6 秒，在檢查 TCP 和 HTTPS 運作狀態時為 10 秒。
HealthCheckIntervalSeconds	個別目標每次執行運作狀態檢查的大約間隔時間，以秒為單位。此值可以是 10 秒或 30 秒。預設為 30 秒。

設定	描述：
	Important 運行狀況檢查 網路負載平衡器 分佈並使用共識機制確定目標健康。因此，目標會接收超過所設定次數的運作狀態檢查。為了減輕對目標造成的影響，如果您使用 HTTP 運作狀態檢查，請在目標上使用較簡易的目的地，例如靜態 HTML 檔案，或是改為 TCP 運作狀態檢查。
HealthyThresholdCount	將運作狀態不佳的目標視為運作狀態良好之前，運作狀態檢查需連續成功的次數。範圍介於 2 至 10 之間。預設為 3。
UnhealthyThresholdCount	將目標視為運作狀態不佳之前，運作狀態檢查需連續失敗的次數。此值必須與運作狀態良好閾值計數相同。
Matcher	[HTTP/HTTPS 運作狀態檢查] 檢查來自目標的成功回應時所使用的 HTTP 代碼。此值必須為 200 至 399。

目標運作狀態

在負載平衡器向目標傳送運作狀態檢查請求之前，您必須向目標群組註冊該目標，由接聽程式規則中指定其目標群組，並確保負載平衡器已啟用該目標的可用區域。

下表說明已註冊目標的運作狀態可能的值。

數值	描述：
`initial`	負載平衡器正在註冊目標或對目標執行初始運作狀態檢查。 相關原因代碼: `Elb.RegistrationInProgress` || `Elb.InitialHealthChecking`
`healthy`	目標的運作狀態良好。 相關原因代碼: 無.
`unhealthy`	目標未回應運作狀態檢查或未通過運作狀態檢查。 相關原因代碼：`Target.FailedHealthChecks`
`unused`	目標未向目標群組註冊、未在接聽程式規則中使用目標群組、目標位於未啟用的可用區域，或目標處於已停止或已終止狀態。 相關原因代碼: `Target.NotRegistered` || `Target.NotInUse` || `Target.InvalidState` || `Target.IpUnusable`
`draining`	目標正在取消註冊，連接耗盡作業進行中。 相關原因代碼：`Target.DeregistrationInProgress`

數值	描述：
`unavailable`	目標健全狀態無法使用。 相關原因代碼：`Elb.InternalError`

運作狀態檢查原因代碼

如果目標的狀態是 `Healthy` 以外的任何值，API 將傳回問題的原因代碼和描述，而且主控台會以工具提示顯示同樣的描述。請注意，以 `Elb` 起始於負載均衡器側和原因代碼，以 `Target` 源於目標端。

原因代碼	描述：
`Elb.InitialHealthChecking`	初始運作狀態檢查正進行中
`Elb.InternalError`	運作狀態檢查由於內部錯誤而失敗
`Elb.RegistrationInProgress`	目標註冊正進行中
`Target.DeregistrationInProgress`	目標取消註冊正進行中
`Target.FailedHealthChecks`	運作狀態檢查失敗
`Target.InvalidState`	目標處於停止狀態 目標處於終止狀態 目標處於終止或停止狀態 目標處於無效狀態
`Target.IpUnusable`	IP 地址不能做為目標，因為負載平衡器正在使用它
`Target.NotInUse`	目標群組未設定為接收來自負載平衡器的流量 目標位於負載平衡器未啟用的可用區域
`Target.NotRegistered`	目標未向目標群組註冊

檢查目標的運作狀態

您可以檢查已向目標群組註冊的各個目標的運作狀態。

New console

使用新控制檯檢查目標的運行狀況

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 在 目標 選項卡， 狀態 列表示每個目標的狀態。
5. 如果目標狀態是以外的任何值 `Healthy`、 狀態詳情 列包含更多信息。

Old console

使用舊控制檯檢查目標的運行狀況

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中，負載平衡，選擇 目標組.
3. 選取目標群組。
4. 選擇 目標，並查看每個目標的狀態 狀態 列。若狀態為 `Healthy` 以外的任何值，檢視工具提示可獲取詳細資訊。

使用 檢查目標的運作狀態AWS CLI

使用 描述-目標-健康 命令。此命令的輸出包含目標的運作狀態。若狀態為 以外的任何值，其將附上原因代碼。`Healthy`.

接收有關狀態不良目標的電子郵件通知

使用 CloudWatch 警報觸發A Lambda 發送有關不健康目標詳細信息的函數。有關分步說明，請參閱以下博客帖子: 識別負載均衡器的不健康目標.

修改目標群組的運作狀態檢查設定

您可以修改目標群組的部分運作狀態檢查設定。如果通訊協定的目標群組是 TCP、TLS、UDP 或 TCP_UDP，您無法修改運作狀況檢查協定、間隔、逾時或成功代碼。

New console

如何使用新控制檯修改目標組的運行狀況檢查設置

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中，負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 在 組詳情 選項卡，運行狀況檢查設置 部分，選擇 編輯.
5. 在 編輯運行狀況檢查設置 頁面，根據需要修改設置，然後選擇 保存更改.

Old console

如何使用舊控制檯修改目標組的運行狀況檢查設置

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中，負載平衡，選擇 目標組.
3. 選取目標群組。
4. 選擇 運行狀況檢查，編輯.
5. 在 編輯目標組 頁面，根據需要修改設置，然後選擇 保存.

使用 修改目標群組的運作狀態檢查設定AWS CLI

使用 修改-目標組 命令。

透過目標群組來登記目標

當您的目標準備好處理請求時，可以向一或多個目標群組進行註冊。您可以使用執行個體 ID 或 IP 地址來登錄目標。在註冊程序完成、目標通過初始的運作狀態檢查之後，負載平衡器就會立即開始將請求轉送到目

標。註冊程序可能需要幾分鐘的時間才能完成，並開始運作狀態檢查。如需詳細資訊，請參閱目標群組運作狀態檢查 (p. 35).

如果對目前已註冊目標的需求增加，您可以註冊額外的目標來應付需求。如果對已註冊目標的需求減少，您可以從目標群組取消註冊目標。取消註冊程序可能需要幾分鐘的時間才能完成，而且負載平衡器可能需要幾分鐘才能停止將請求路由到目標。如果之後需求增加，您可以再次向目標群組註冊已取消註冊的目標。如果您需要為目標提供服務，可以取消註冊，然後在服務完成後再次註冊。

當您取消登錄目標時，Elastic Load Balancing 會等到處理中的請求完成。這被稱爲 連接排空. 目標狀態爲 `draining` 連接排空正在進行中。已完成的刪除後，目標更改的狀態爲 `unused`...有關詳細信息，請參閱 取消登記的延遲 (p. 31).

如果是根據執行個體 ID 來註冊目標，您可以使用負載平衡器搭配 Auto Scaling 群組。在您將目標組附加到 Auto Scaling 組和組的擴展， Auto Scaling 組將自動註冊到目標組。如果分離負載平衡器與 Auto Scaling 群組的連結，會自動從該目標群組中取消執行個體的登錄。有關詳細信息，請參閱 將負載平衡器附加到您的 Auto Scaling 組 在 Amazon EC2 Auto Scaling 使用者指南.

目標安全群組

當您將 EC2 執行個體登錄為目標時，必須確定這些執行個體的安全群組，會允許透過接聽程式連接埠和運作狀態檢查通訊埠，來傳送流量。

Limits

- 網路負載平衡器 不具有關聯的安全群組。因此，目標的安全群組必須使用 IP 地址，來允許從負載平衡器傳來的流量。
- 您不能將客戶端的安全組用作目標安全組中的來源。相反，使用客戶端CIDR模塊作爲目標安全組中的源。

適用於執行個體安全群組的建議規則

Inbound			
來源	通訊協定	連接埠範圍	註解
Client IP addresses	*target*	*target*	允許用戶端流量 (`instance` 目標類型)
VPC CIDR	*target*	*target*	允許用戶端流量 (`ip` 目標類型)
VPC CIDR	*health check*	*health check*	允許來自負載平衡器的運作狀態檢查流量

如果您依 IP 位址註冊目標且不想將存取權限授予整個 VPC CIDR，可以將存取權限授予負載平衡器節點所使用的私有 IP 地址。每個負載平衡器子網路都有一個 IP 地址。若要尋找這些地址，請執行下列步驟。

查找用於允許的專用IP地址

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中，選擇 網絡接口.
3. 在搜尋欄位中輸入 的名稱。網路負載平衡器. 每個負載平衡器子網路都有一個網路界面。
4. 在 詳情 每個網絡接口的選項卡，複製地址 主要Ipv4IP.

網路 ACL

當您將 EC2 執行個體登錄為目標時，必須確定執行個體之子網路的網路 ACL，會允許透過接聽程式連接埠和運作狀態檢查通訊埠來傳送流量。VPC 的預設網路存取控制清單 (ACL) 可允許所有傳入和傳出的流量。如果您建立自訂網路 ACL，請確認它們允許適當的流量。

與實例子網相關聯的網絡ACL必須允許面向互聯網的負載均衡器的以下流量。

適用於執行個體子網路的建議規則

Inbound			
來源	通訊協定	連接埠範圍	註解
Client IP addresses	*listener*	*listener*	允許用戶端流量 (instance 目標類型)
VPC CIDR	*listener*	*listener*	允許用戶端流量 (ip 目標類型)
VPC CIDR	*health check*	*health check*	允許來自負載平衡器的運作狀態檢查流量
Outbound			
目的地	通訊協定	連接埠範圍	註解
Client IP addresses	*listener*	*listener*	允許回應用戶端 (instance 目標類型)
VPC CIDR	*listener*	*listener*	允許回應用戶端 (ip 目標類型)
VPC CIDR	*health check*	1024-65535	允許運作狀態檢查流量

與負載平衡器子網相關聯的網絡ACL必須允許面向互聯網的負載均衡器的以下流量。

適用於負載平衡器子網路的建議規則

Inbound			
來源	通訊協定	連接埠範圍	註解
Client IP addresses	*listener*	*listener*	允許用戶端流量 (instance 目標類型)
VPC CIDR	*listener*	*listener*	允許用戶端流量 (ip 目標類型)
VPC CIDR	*health check*	1024-65535	允許運作狀態檢查流量
Outbound			
目的地	通訊協定	連接埠範圍	註解
Client IP addresses	*listener*	*listener*	允許回應用戶端 (instance 目標類型)
VPC CIDR	*listener*	*listener*	允許回應用戶端 (ip 目標類型)

VPC CIDR	*health check*	*health check*	允許運作狀態檢查流量
VPC CIDR	*health check*	1024-65535	允許運作狀態檢查流量

對於內部負載平衡器，您實例和負載平衡器節點的子網的網絡ACL必須允許在偵聽器端口和臨時端口上的VPCCIDR的入站和出站流量同時進行。

登記和取消登記目標

在負載平衡器能夠使用的每個可用區域中，每個目標群組都必須擁有至少一個已登錄的目標。

目標群組的目標類型會決定您向該目標群組註冊目標的方式。如需詳細資訊，請參閱Target type (目標類型) (p. 29).

Requirements

- 如果使用以下實例類型之一，則無法按實例ID註冊實例:
  C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3或T1。
- 如果VPC處於負載均衡器VPC（相同區域或不同區域）的虛擬機中，則無法按實例ID註冊實例。您可以依照 IP 地址來註冊這些執行個體。
- 如果您依照 IP 地址註冊目標，且 IP 地址與負載平衡器位於相同的 VPC 中，則負載平衡器會驗證它來自於其可連上的子網路。
- 對於UDP和TCP_UDP目標組，如果IP地址位於負載均衡器VPC以外或如果使用以下實例類型之一，請勿通過IP地址寄存實例: C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3或T1。駐留在負載均衡器VPC以外的目標或使用不支持的實例類型可能能夠接收負載均衡器的流量，但無法響應。

內容

根據執行個體 ID 來登記或取消登記目標

在註冊時，執行個體必須處於 `running` 狀態。

New console

使用新控制檯通過實例ID註冊或刪除目標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 選擇 目標 選項卡。
5. 要註冊實例，請選擇 註冊目標. 選擇一個或多個實例，根據需要輸入默認實例端口，然後選擇 包括在下面的待處理中. 完成添加實例後，選擇 註冊待定目標.
6. 要取消註冊實例，請選擇實例，然後選擇 德斯托特.

Old console

使用舊控制檯通過實例ID註冊或刪除目標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選取目標群組。
4. 選擇 目標， 編輯.
5. （可選）已註冊實例，選擇要拆除的任何實例，然後選擇 刪除.
6. （可選）實例，選擇要註冊的任何運行實例，根據需要修改默認實例端口，然後選擇 添加至已註冊.
7. 選擇 保存.

根據 IP 地址來登記或取消登記目標

您註冊的 IP 地址必須來自下列其中一個 CIDR 區塊：

- 目標群組 VPC 的子網路
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

New console

使用新控制檯註冊或刪除IP地址的目標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 選擇 目標 選項卡。
5. 要註冊IP地址，請選擇 註冊目標. 對於每個IP地址，請選擇網絡、可用性區、IP地址和端口，然後選擇 包括在下面的待處理中. 完成指定地址後，選擇 註冊待定目標.
6. 要取消註冊IP地址，請選擇IP地址，然後選擇 德斯托特. 如果您擁有多個已登錄的 IP 地址，新增篩選條件或變更排序順序，可能會很有幫助。

Old console

使用舊控制檯註冊或刪除通過IP地址的目標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組並選擇 目標， 編輯.
4. 要註冊IP地址，請選擇 註冊目標 菜單欄中的圖標（加號）。對於每個IP地址，請指定網絡、可用性區、IP地址和端口，然後選擇 添加至列表. 完成指定地址後，選擇 註冊.
5. 要取消註冊IP地址，請選擇 Deregister目標 菜單欄中的圖標（減號）。如果您擁有多個已登錄的 IP 地址，新增篩選條件或變更排序順序，可能會很有幫助。選擇IP地址並選擇 德斯托特.
6. 要離開此屏幕，請選擇 返回目標組 菜單欄中的圖標（“返回”按鈕）。

使用 來登記或取消登記目標AWS CLI

使用 寄存器目標 命令添加目標和 Deregister目標 命令以刪除目標。

目標群組的標籤

標籤可幫助您以不同的方式來將目標群組分類，例如，根據目的、擁有者或環境。

您可以在每個目標群組中加入多個標籤。每個目標群組的標籤索引鍵必須是唯一的。如果所新增的標籤，其索引鍵已經和目標群組具有關聯，則此動作會更新該標籤的值。

當您使用完標籤之後，可以將其移除。

Restrictions

- 每個資源的標籤數上限 —50
- 索引鍵長度上限 — 127 個 Unicode 字元
- 數值長度上限 — 255 個 Unicode 字元
- 標籤索引鍵與值皆區分大小寫。允許的字元包括可用 UTF-8 表示的英文字母、空格和數字，還有以下特殊字元：+ - = . _ : / @。不可使用結尾或前方空格。
- 標籤名稱或值請勿使用 `aws:` 字首，因為它只保留給 AWS 使用。您不可編輯或刪除具此字首的標籤名稱或值。具備此前綴的標籤不會算在每個資源的標籤數限制內。

New console

如何使用新控制檯更新目標組的標記

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組的名稱打開其詳細信息頁面。
4. 在 標籤 選項卡，選擇 管理標籤 並且執行以下一項或多項:
   a. 要更新標記，請輸入新值 關鍵 和 值.
   b. 要添加標記，請選擇 添加標籤 並輸入值 關鍵 和 值.
   c. 要刪除標記，請選擇 刪除 標籤旁邊。
5. 完成標籤更新後，選擇 保存更改.

Old console

使用主控台來更新目標群組的標籤

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選取目標群組。
4. 在 標籤 選項卡，選擇 添加/編輯標籤，然後執行以下一項或多項:
   a. 要更新標記，請編輯 關鍵 和 值.
   b. 要添加新標籤，請選擇 創建標籤 然後輸入值 關鍵 和 值.
   c. 若要刪除標籤，請選擇標籤旁的刪除圖示 (X)。
5. 完成標籤更新後，選擇 保存.

使用 來更新目標群組的標籤AWS CLI

使用 添加標籤 和 刪除標籤 命令。

刪除目標群組

如果未通過任何偵聽程序規則的前進操作引用，可以刪除目標組。刪除目標群組不會影響透過該目標群組登錄的目標。如果不再需要註冊的 EC2 執行個體，則可以停止或終止它。

New console

如何使用新控制檯刪除目標組

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組並選擇 操作， 刪除.
4. 當提示確認時，選擇 是，刪除.

Old console

如何使用舊控制檯刪除目標組

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中， 負載平衡，選擇 目標組.
3. 選擇目標組並選擇 操作， 刪除.
4. 當提示確認時，選擇 是.

使用 來刪除目標群組AWS CLI

使用 刪除-目標組 命令。

監控 網路負載平衡器

您可使用以下功能來監控負載平衡器、分析流量模式並對與負載平衡器和目標相關的問題進行疑難排解。

CloudWatch 指標

您可以使用 Amazon CloudWatch 檢索負載平衡器和目標的數據點數據點，作爲訂單時間序列數據集，稱爲 度量. 您可以使用這些指標來確認您的系統是否依照預期執行。如需詳細資訊，請參閱CloudWatch 用於 的 指標網路負載平衡器 (p. 46).

VPC 流程日誌

您可以使用 VPC Flow Logs 來擷取關於往返 的流量詳細資訊。網路負載平衡器. 有關詳細信息，請參閱 VPC流量日誌 在 Amazon VPC 使用者指南.

為負載平衡器的每個網路界面建立流程日誌。每個負載平衡器子網路都有一個網路界面。為了識別 網路負載平衡器 的網路界面，請在網路界面的描述欄位中尋找負載平衡器名稱。

每個透過 網路負載平衡器 的連線有兩種項目，一個用於用戶端和負載平衡器之間的前端連線，另一個則用於負載平衡器與目標之間的後端連線。如果目標由執行個體 ID 登錄，連線會來自用戶端的連線身分出現於執行個體。如果執行個體的安全群組不允許來自用戶端的連線，但是負載平衡器子網路的網路 ACL 可允許，負載平衡器的網路界面日誌會對前端與後端連線顯示「ACCEPT OK」，而執行個體的網路界面日誌會對連線顯示「REJECT OK」。

存取日誌

您可以使用存取日誌，針對傳送到負載平衡器的 TLS 請求，擷取其詳細資訊。日誌檔案已儲存至 Amazon S3. 您可以使用這些存取日誌來分析流量模式，並排除目標的問題。如需詳細資訊，請參閱 存取日誌網路負載平衡器 (p. 53).

CloudTrail 日誌

您可以使用 AWS CloudTrail 如需獲取有關 Elastic Load Balancing API並將其存儲在 Amazon S3. 您可以使用這些 CloudTrail 日誌來判斷提出了哪些呼叫、提出呼叫的來源 IP 地址、提出呼叫的人員及時間等。如需詳細資訊，請參閱日誌記錄API呼叫 網路負載平衡器 使用 AWS CloudTrail (p. 58).

CloudWatch用於 的 指標網路負載平衡器

Elastic Load Balancing 將數據點發布到 Amazon CloudWatch 對於負載平衡器和目標。 CloudWatch 允許您將這些數據點的統計信息檢索爲訂購的時間序列數據集，即 度量. 您可以將指標視為要監控的變數，且資料點是該變數在不同時間點的值。例如，您可以監控負載平衡器在一段指定期間內的運作狀態良好的目標總數量。每個資料點都有關聯的時間戳記和可選的測量單位。

您可以使用指標來確認系統的運作符合預期。例如，若指標超過您認為能夠接受的範圍，您可以建立 CloudWatch 警示來監控指定的指標並採取動作 (例如傳送通知到電子郵件地址)。

Elastic Load Balancing 將度量標準報告給 CloudWatch 只有在請求流過負載平衡器時。如果有請求進出負載平衡器，Elastic Load Balancing 會以 60 秒為間隔來測量並傳送其指標。如果沒有請求流經負載平衡器，或者指標沒有資料，則不會回報該指標。

如需更多詳細資訊，請參閱 Amazon CloudWatch 使用者指南.

內容

Network Load Balancer 指標

TheThethe AWS/NetworkELB Namespace包括以下度量。

指標	描述：
ActiveFlowCount	從用戶端到目標的並行流程 (或連線) 總數。此指標包含處於 SYN_SENT 與 ESTABLISHED 狀態的連線。在負載平衡器上不會終止 TCP 連線，因此開啟 TCP 與目標之連線的用戶端會計算為單一流程。 報告標準: 非零值 統計資料: 最有用的統計數據是 Average， Maximum，和 Minimum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ActiveFlowCount_TCP	從用戶端到目標的並行 TCP 流程 (或連線) 總數。此指標僅包含處於 ESTABLISHED 狀態的連線。在負載平衡器上不會終止 TCP 連線，因此開啟 TCP 與目標之連線的用戶端會計算為單一流程。 報告標準: 非零值 統計資料: 最有用的統計數據是 Average， Maximum，和 Minimum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ActiveFlowCount_TLS	從用戶端到目標的並行 TLS 流程 (或連線) 總數。此指標僅包含處於 ESTABLISHED 狀態的連線。 報告標準: 非零值 統計資料: 最有用的統計數據是 Average， Maximum，和 Minimum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ActiveFlowCount_UDP	從用戶端到目標的並行 UDP 流程 (或連線) 總數。 報告標準: 非零值 統計資料: 最有用的統計數據是 Average， Maximum，和 Minimum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ClientTLSNegotiationErrorCount	在用戶端與 TLS 接聽程式交涉期間失敗的 TLS 交握總數。 報告標準: 非零值

指標	描述：
	統計資料：：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ConsumedLCUs	負載平衡器所使用的負載平衡器容量單位 (LCU) 數目。您需要按每小時使用的 LCU 數目付費。有關詳細信息，請參閱 Elastic Load Balancing 定價. 報告標準: 總是報告 統計資料: 全部 Dimensions • LoadBalancer
ConsumedLCUs_TCP	負載平衡器針對 TCP 所使用的負載平衡器容量單位 (LCU) 數目。您需要按每小時使用的 LCU 數目付費。有關詳細信息，請參閱 Elastic Load Balancing 定價. 報告標準: 總是報告 統計資料: 全部 Dimensions • LoadBalancer
ConsumedLCUs_TLS	負載平衡器針對 TLS 所使用的負載平衡器容量單位 (LCU) 數目。您需要按每小時使用的 LCU 數目付費。有關詳細信息，請參閱 Elastic Load Balancing 定價. 報告標準: 總是報告 統計資料: 全部 Dimensions • LoadBalancer
ConsumedLCUs_UDP	負載平衡器針對 UDP 所使用的負載平衡器容量單位 (LCU) 數目。您需要按每小時使用的 LCU 數目付費。有關詳細信息，請參閱 Elastic Load Balancing 定價. 報告標準: 總是報告 統計資料: 全部 Dimensions • LoadBalancer

指標	描述：
HealthyHostCount	視為健康的目標數目。 報告標準: 如果啓用了運行狀況檢查報告 統計資料: 最有用的統計數據是 Maximum 和 Minimum. Dimensions • LoadBalancer, TargetGroup • AvailabilityZone, LoadBalancer, TargetGroup
NewFlowCount	在期間內，從用戶端到目標建立的新流程 (或連線) 總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
NewFlowCount_TCP	在期間內，從用戶端到目標建立的新 TCP 流程 (或連線) 總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
NewFlowCount_TLS	在期間內，從用戶端到目標建立的新 TLS 流程 (或連線) 總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
NewFlowCount_UDP	在期間內，從用戶端到目標建立的新 UDP 流程 (或連線) 總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer

指標	描述：
ProcessedBytes	負載平衡器所處理的位元組總數，包含 TCP/IP 標頭。此計數包括進出目標的流量 (減去運作狀態檢查流量)。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ProcessedBytes_TCP	TCP 接聽程式所處理的位元組總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ProcessedBytes_TLS	TLS 接聽程式所處理的位元組總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ProcessedBytes_UDP	UDP 接聽程式所處理的位元組總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
TargetTLSNegotiationErrorCount	在 TLS 接聽程式與目標交涉期間失敗的 TLS 交握總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer

指標	描述：
TCP_Client_Reset_Count	從用戶端到目標傳送的重設 (RST) 封包總數。這些重設是由用戶端所產生，並透過負載平衡器進行轉送。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
TCP_ELB_Reset_Count	負載平衡器所產生的重設 (RST) 封包總數。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
TCP_Target_Reset_Count	從目標到用戶端傳送的重設 (RST) 封包總數。這些重設是由目標所產生，並透過負載平衡器進行轉送。 報告標準: 非零值 統計資料: ：最實用的統計資訊是 Sum. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
UnHealthyHostCount	視為不健康的目標數目。 報告標準: 如果啓用了運行狀況檢查報告 統計資料: 最有用的統計數據是 Maximum 和 Minimum. Dimensions • LoadBalancer, TargetGroup • AvailabilityZone, LoadBalancer, TargetGroup

的指標維度網路負載平衡器

若要篩選負載平衡器的指標，請使用下列維度。

維度	描述：
AvailabilityZone	依可用區域篩選指標資料。

維度	描述：
LoadBalancer	依負載平衡器篩選指標資料。按以下方式指定負載均衡器:net/負載平衡器名稱/1234567890123456 （負載均衡器ARN的最後一部分）。
TargetGroup	依目標群組篩選指標資料。按以下方式指定目標組:TargetGroup/目標組名稱/1234567890123456 （目標組ARN的最後一部分）。

統計數據 網路負載平衡器 度量

CloudWatch 根據由 發布的指標資料點提供統計資料。Elastic Load Balancing. 統計資料是隨著指定期間的指標資料彙總。當您請求統計資料時，傳回的資料流是藉由指標名稱和維度做識別。維度是用來單獨辨識指標的名稱/值組。例如，您可以為所有在特定可用區域內啟動的負載平衡器後方之運作狀態良好的 EC2 執行個體請求統計資料。

TheThethe `Minimum` 和 `Maximum` 統計信息反映每個取樣窗口中單個負載均衡器節點報告的數據點的最小值和最大值。最大增加 `HealthyHostCount` 對應於最小值 `UnHealthyHostCount`...因此，我們建議您監控網路負載平衡器 使用 `HealthyHostCount` 或者至少 `UnHealthyHostCount`.

TheThethe `Sum` 統計信息是所有負載均衡器節點的總值。因為指標包和各期間的多個報告，`Sum` 僅可用於來自所有負載平衡器節點的彙總指標。

TheThethe `SampleCount` 統計數量是測量的樣品數。因指標根據範本間隔與事件蒐集而得，此統計資料通常沒有幫助。例如， `HealthyHostCount`， `SampleCount` 基於每個負載均衡器節點報告的樣品數量，而不是健康主機的數量。

檢視負載平衡器的 CloudWatch 指標

您可以查看 CloudWatch 負載平衡器的度量標準 Amazon EC2 控制檯。這些指標會以監控圖表的形式顯示。若啟用負載平衡器並接收請求，監控圖表會顯示資料點。

或者，您可以使用 CloudWatch 主控台來檢視負載平衡器的指標。

使用 Amazon EC2 主控台檢視指標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 若要檢視由目標群組篩選的指標，請執行下列動作：
   a. 在導航窗格中，選擇 目標組.
   b. 選擇您的目標組並選擇 監控.
   c. （可選）要按時間篩選結果，請選擇一個時間範圍 顯示數據.
   d. 若要放大檢視單一指標，請選取它的圖形。
3. 若要檢視由負載平衡器篩選的指標，請執行下列動作：
   a. 在導航窗格中，選擇 負載平衡器.
   b. 選擇您的負載均衡器並選擇 監控.
   c. （可選）要按時間篩選結果，請選擇一個時間範圍 顯示數據.
   d. 若要放大檢視單一指標，請選取它的圖形。

使用 CloudWatch 主控台檢視指標

1. 前往 https://console.aws.amazon.com/cloudwatch/，開啟 CloudWatch 主控台。
2. 在導航窗格中，選擇 度量.
3. 選擇 網絡B namespace。

4. (選用) 若要檢視所有維度的指標，請在搜尋欄位中鍵入其名稱。

若要使用 來檢視指標AWS CLI

使用以下內容 列表度量 命令列出可用度量標準:

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

使用 取得指標的統計資料AWS CLI

使用以下內容 獲取度量標準統計信息 命令獲取指定度量標準和維度的統計信息。請注意，CloudWatch 將把維度的各獨特組合視為個別指標。您無法使用未具體發佈的維度組合來擷取統計資料。您必須指定建立指標時所使用的相同維度。

```
aws cloudwatch get-metric-statistics --namespace AWS/NetworkELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

下列為範例輸出：

```
{
    "Datapoints": [
        {
            "Timestamp": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

存取日誌網路負載平衡器

Elastic Load Balancing 提供存取日誌，可針對傳送到 的 TLS 請求，擷取其詳細資訊。網路負載平衡器. 您可以使用這些存取日誌來分析流量模式和排除問題。

> **Important**
>
> 只有在負載平衡器具有 TLS 接聽程式、且其僅包含 TLS 請求資訊時，才會建立存取日誌。

存取記錄是 Elastic Load Balancing 的選用功能，預設為停用。在啓用負載平衡器的訪問日誌記錄之後，Elastic Load Balancing 將日誌捕獲爲壓縮文件，並將其存儲在 Amazon S3 您指定的桶。您可以隨時停用存取記錄。

如果您透過 Amazon S3 受管加密金鑰 (SSE-S3) 啟用 S3 儲存貯體伺服器端加密，每個存取日誌檔在存放於 S3 儲存貯體之前會自動加密，並於您存取它時解密。存取加密或未加密日誌檔的方式沒有不同，所以您不需要採取任何動作。系統會使用唯一的金鑰來加密每個日誌檔，金鑰本身會以定期輪換的主要金鑰來加密。有關詳細信息，請參閱 使用服務器端加密保護數據 Amazon S3-managedencryptionkeys(SSE-S3) 在 Amazon Simple Storage Service 開發人員指南.

存取日誌無需額外收費。您的存儲成本爲 Amazon S3，但不是用於帶寬的 Elastic Load Balancing 要將日誌文件發送到 Amazon S3. 有關存儲成本的更多信息，請參閱 Amazon S3 定價.

存取日誌檔

Elastic Load Balancing 每 5 分鐘發佈每個負載平衡器節點的日誌檔。日誌傳遞最終會達到一致。負載平衡器可能在相同期間傳遞多個日誌。這通常是在網站的流量很高時才會發生。

存取日誌的檔案名稱使用以下格式：

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-balancer-id_end-time_random-string.log.gz
```

儲存貯體

S3 儲存貯體的名稱。

prefix.

儲存貯體中的字首 (邏輯階層)。如果不指定字首，日誌會放在儲存貯體的根層級。

aws-account-id

擁有者的 AWS 帳戶 ID。

region

負載平衡器和 S3 儲存貯體的區域。

年年年/毫米/DD

傳遞日誌的日期。

load-balancer-id

負載平衡器的資源 ID。如果資源 ID 包含任何斜線 (/)，斜線會換成句點 (.)。

end-time

記錄間隔結束的日期和時間。例如，結束時間 20181220T2340Z 包含在 23:35 和 23:40 之間所提出之請求的項目。

random-string

系統產生的隨機字串。

您可以視需要在儲存貯體存放您的日誌檔，但也可以決定 Amazon S3 生命週期規則，自動封存或刪除日誌檔案。有關詳細信息，請參閱 對象生命週期管理 在 Amazon Simple Storage Service 開發人員指南.

存取日誌項目

下表依序說明存取日誌項目的欄位。所有欄位以空格分隔。引進的新欄位會新增到日誌項目尾端。處理日誌檔案時，您應該忽略日誌項目尾端任何非預期的欄位。

欄位	描述：
類型	接聽程式的類型。支援的值為 `tls`.
version	日誌項目的版本。目前版本是 2.0。
time	在 TLS 連線結束時記錄的時間，採用 ISO 8601 格式。
elb	負載平衡器的資源 ID。

欄位	描述：
接聽程式	適用於連線的 TLS 接聽程式資源 ID。
client:port	用戶端的 IP 地址和連接埠。
destination:port	目的地的 IP 地址和連接埠。如果用戶端直接連線至負載平衡器，則目的地就是接聽程式。如果用戶端使用 VPC 端點服務連線，則目的地就是 VPC 端點。
connection_time	連線從開始到結束的完成時間，以毫秒計。
tls_handshake_time	TCP 連線建立後，TLS 交握完成的總時間，包括用戶端的延遲，以毫秒計。此時間包含在 connection_time 欄位中。
received_bytes	負載平衡器從用戶端接收的解密後位元數。
sent_bytes	負載平衡器向用戶端傳送的加密前位元數。
incoming_tls_alert	負載平衡器從用戶端接收的 TLS 提醒整數值 (若有)。否則，此值設定為 -。
chosen_cert_arn	向用戶端所提供憑證的 ARN。若未傳送有效的用戶端 hello 訊息，則此值設定為 -。
chosen_cert_serial	預留以供日後使用。此值設定為 -。
tls_cipher	與用戶端交涉的密碼套件，採用 OpenSSL 格式。若 TLS 交涉未完成，此值設定為 -。
tls_protocol_version	與用戶端交涉的 TLS 通訊協定，採用字串格式。可能的值是 `tlsv10`，`tlsv11`，和 `tlsv12`...如果TLS談判未完成，此值設置爲-。
tls_named_group	預留以供日後使用。此值設定為 -。
domain_name	server_name 副檔名的值位於用戶端 hello 訊息中。此值為 URL 編碼格式。若未傳送有效的用戶端 hello 訊息或無副檔名，則此值設定為 -。
alpn_fe_protocol	與用戶端交涉的應用程式通訊協定，採用字串格式。可能的值是 `h2`，`http/1.1`，和 `http/1.0`...如果TLS偵聽程序中未配置ALPN策略，則未找到匹配協議，或者未發送有效協議列表，此值設置爲-。
alpn_be_protocol	與目標交涉的應用程式通訊協定，採用字串格式。可能的值是 `h2`，`http/1.1`，和 `http/1.0`...如果TLS偵聽程序中未配置ALPN策略，則未找到匹配協議，或者未發送有效協議列表，此值設置爲-。
alpn_client_preference_list	用戶端您好訊息中的 application_layer_protocol_negotiation 延伸的值。此值為 URL 編碼格式。每個通訊協定用雙引號括起來，並以逗號分隔。如果 TLS 接聽程式中未設定任何 ALPN 政策、未傳送任何有效的用戶端您好訊息，或副檔名不存在，則此值會設定為 -。如果字串長度超過 256 個位元組，則會被截斷。

範例日誌項目

以下為日誌項目範例。請注意，分成多行顯示文字只是為了更輕鬆閱讀。

以下是不含 ALPN 政策的 TLS 接聽程式範例。

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
```

```
- - -
```

以下是具有 ALPN 政策的 TLS 接聽程式範例。

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1"
```

儲存貯體需求

當您啟用存取記錄時，您必須為存取日誌指定 S3 儲存貯體。擁有儲存貯體的帳戶與擁有負載平衡器的帳戶可以不同。儲存貯體必須符合下列需求。

Requirements

- 儲存貯體與負載平衡器必須位於相同的區域。
- 您指定的前綴不能包括Awslogs。我們在您指定的桶名稱和前綴之後以awslogs開頭添加文件名的部分。
- Amazon S3需要 受管加密金鑰 (SSE-S3)。不支援其他加密選項。
- 儲存貯體必須有儲存貯體政策，以授權將存取日誌寫入您的儲存貯體。儲存貯體政策是以存取政策語言所編寫的 JSON 陳述式集合，可定義儲存貯體的存取許可。政策範例如下。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket_name/prefix/AWSLogs/123456789012/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::bucket_name"
    }
  ]
}
```

啟用存取日誌

當您對負載平衡器啟用存取記錄時，您必須指定 S3 儲存貯體的名稱，供負載平衡器存放日誌。如需詳細資訊，請參閱儲存貯體需求 (p. 56).

使用主控台啟用存取記錄

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中，選擇 負載平衡器.
3. 選取您的負載平衡器。
4. 在 描述 選項卡，選擇 編輯屬性.
5. 在 編輯負載均衡器屬性 頁面，請執行以下操作:
   a. 對於 訪問日誌，選擇 啓用.
   b. 對於 S3位置，鍵入S3桶的名稱，包括任何前綴（例如， `my-loadbalancer-logs/my-app`）。您可以指定現有儲存貯體的名稱，或新儲存貯體的名稱。如果您指定現有的儲存貯體，請確定您擁有該儲存貯體，且已設定所需的儲存貯體政策。
   c. （可選）如果桶不存在，請選擇 爲我創建此位置. 您指定的名稱在 Amazon S3 中的所有現有儲存貯體名稱之間必須是唯一的，且遵循 DNS 命名慣例。有關詳細信息，請參閱 桶命名規則 在 Amazon Simple Storage Service 開發人員指南.
   d. 選擇 保存.

使用 啟用存取記錄AWS CLI

使用 修改負載均衡器屬性 命令。

停用存取記錄

您可以隨時對負載平衡器停用存取記錄。在您停用存取記錄之後，存取日誌會保留在 S3 儲存貯體中，直到您刪除它們。有關詳細信息，請參閱 使用桶 在 Amazon Simple Storage Service 主控台使用者指南.

使用主控台停用存取記錄

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導航窗格中，選擇 負載平衡器.
3. 選取您的負載平衡器。
4. 在 描述 選項卡，選擇 編輯屬性.
5. 對於 訪問日誌，透明 啓用.
6. 選擇 保存.

使用 停用存取記錄AWS CLI

使用 修改負載均衡器屬性 命令。

處理存取日誌檔

存取日誌檔已壓縮。如果您使用 Amazon S3 主控台開啟檔案，則會解壓縮檔案並顯示資訊。如果您下載檔案，則必須先將其解壓縮才能看到資訊。

如果您的網站上有許多需求，負載平衡器產生的日誌檔可能有好幾 GB 的資料。您可能無法逐行處理這麼龐大的資料。因此，您可能需要使用提供平行處理解決方案的分析工具。例如，您可以使用以下分析工具來分析和處理存取日誌：

- Amazon Athena 是互動式查詢服務，可讓您在 Amazon S3 中使用標準 SQL 輕鬆分析資料。有關詳細信息，請參閱 查詢 網路負載平衡器 日誌 在 Amazon Athena 使用者指南.
- Loggly
- Splunk

- Sumo Logic

日誌記錄API呼叫 網路負載平衡器 使用 AWS CloudTrail

Elastic Load Balancing 與 AWS CloudTrail，提供用戶、角色或 AWS 服務 Elastic Load Balancing... CloudTrail 捕獲所有API的呼叫 Elastic Load Balancing 作爲事件。捕獲的呼叫包括來自 AWS 管理主控台和代碼呼叫 Elastic Load Balancing API操作。如果您創建一個跟蹤，可以啓用連續交付 CloudTrail 活動至 Amazon S3 包括 Elastic Load Balancing. 如果不配置跟蹤，您仍可以查看最近的事件 CloudTrail 控制檯 事件歷史記錄. 使用收集的信息 CloudTrail，您可以確定所做的請求 Elastic Load Balancing，提出請求的IP地址、作出請求的人員、在製作的時間以及其他詳細信息。

若要進一步了解 CloudTrail，請參閱。AWS CloudTrail User Guide.

Elastic Load Balancing 中的 資訊CloudTrail

CloudTrail當您建立帳戶時，系統會在您的 AWS 帳戶中啟用 。當活動發生在 Elastic Load Balancing，該活動記錄在 CloudTrail 事件與其他 AWS 服務事件 事件歷史記錄. 您可以檢視、搜尋和下載 AWS 帳戶的最新事件。有關詳細信息，請參閱 查看事件 CloudTrail 事件歷史記錄.

在您的 AWS 賬戶，包括活動 Elastic Load Balancing，創建一個步道。A 追蹤 啓用 CloudTrail 將日誌文件交付給 Amazon S3 桶。依預設，當您在主控台建立追蹤時，該追蹤會套用到所有 AWS 區域。路徑記錄來自 AWS 分區並將日誌文件交付到 Amazon S3 您指定的桶。此外，您還可以配置其他 AWS 服務以進一步分析和採取所收集事件數據的進一步分析和採取行動 CloudTrail 日誌。如需詳細資訊，請參閱下列內容：。

- 建立追蹤的概觀
- CloudTrail 支持的服務和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收 CloudTrail 來自多個區域的日誌文件 和 接收 CloudTrail 來自多個帳戶的日誌文件

全部 Elastic Load Balancing 對於 網路負載平衡器 記錄人 CloudTrail 並記錄在 Elastic Load Balancing API 參考版本 2015-12-01. 例如，呼叫 `CreateLoadBalancer` 和 `DeleteLoadBalancer` 操作在 CloudTrail 日誌文件。

每一筆事件或記錄項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是否使用root根或 AWS Identity and Access Management （ IAM)用戶憑據。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全登入資料。
- 該請求是否由另一項 AWS 服務提出

有關詳細信息，請參閱 CloudTrail 用戶身份元素.

了解 Elastic Load Balancing 日誌檔案項目

跟蹤是一種配置，可以將事件交付到日誌文件中 Amazon S3 您指定的桶。 CloudTrail 日誌文件包含一個或多個日誌條目。事件代表任何來源的單一請求，並包含有關請求的動作、動作的日期和時間、請求參數等資訊。CloudTrail 日誌檔不是公有 API 呼叫的排序堆疊追蹤記錄，因此不會現以任何特定順序顯示。

日誌檔案包含您的 AWS 帳戶的所有 AWS API 呼叫的事件，而不只有 Elastic Load Balancing API 呼叫。您可以找到 Elastic Load Balancing API通過檢查 `eventSource` 帶有價值的元素 `elasticloadbalancing.amazonaws.com`...查看某個特定操作的記錄，例如 `CreateLoadBalancer`，檢查 `eventName` 操作名稱中的元素。

以下是示例 CloudTrail 日誌記錄 Elastic Load Balancing 對於創建A的用戶 網路負載平衡器 然後使用 AWS CLI. 您可以使用 `userAgent` 元素來識別 CLI。您可以使用 `eventName` 元素來識別請求的 API 呼叫。關於用戶的信息 (`Alice`)可在 `userIdentity` 元素。

Example 範例：CreateLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
            "ipAddressType": "ipv4",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example 範例：DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
```

```
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Troubleshoot your 網路負載平衡器

以下資訊有助於您就 網路負載平衡器 的問題進行疑難排解。

A registered target is not in service

如果目標進入 `InService` 狀態所花的時間超過預期，表示該目標可能未通過運作狀態檢查。您的目標將處於非服務中狀態，除非通過一次運作狀態檢查。如需更多詳細資訊，請參閱「目標群組運作狀態檢查 (p. 35)」。

確認您的執行個體是否未通過運作狀態檢查，然後檢查以下各項：

安全群組不允許流量

與執行個體相關聯的安全群組必須允許由負載平衡器使用運作狀態檢查連接埠和運作狀態檢查通訊協定傳來的流量。如需更多詳細資訊，請參閱「目標安全群組 (p. 40)」。

網路存取控制清單 (ACL) 不允許流量

與您的實例子網相關聯的網絡ACL和負載平衡器子網必須允許負載平衡器的流量和運行狀況檢查。如需更多詳細資訊，請參閱「網路 ACL (p. 41)」。

Requests are not routed to targets

檢查以下各項：

安全群組不允許流量

與執行個體相關聯的安全群組必須允許透過接聽程式連接埠來自用戶端 IP 地址的流量 (若目標是由執行個體 ID 指定) 或來自負載平衡器節點的流量 (若目標是由 IP 地址指定)。如需更多詳細資訊，請參閱「目標安全群組 (p. 40)」。

網路存取控制清單 (ACL) 不允許流量

與 VPC 的子網路相關聯的網路 ACL 必須允許負載平衡器和目標透過接聽程式連接埠進行雙向通訊。如需更多詳細資訊，請參閱「網路 ACL (p. 41)」。

目標位於未啟用的可用區域

如果您在某個可用區域內註冊目標但未啟用該可用區域，這些已註冊目標將不會接收來自負載平衡器的流量。

執行個體位於對等的 VPC

如果您在與負載平衡器 VPC 對等的 VPC 中有執行個體，您必須依 IP 地址向負載平衡器註冊這些執行個體，而不是依執行個體 ID。

Targets receive more health check requests than expected

網路負載平衡器 的運作狀態檢查為分散式，採用共識機制判定目標的運作狀態。因此，目標會接收超過由 `HealthCheckIntervalSeconds` 所設定次數的運作狀態檢查。

Targets receive fewer health check requests than expected

檢查是否已啟用 `net.ipv4.tcp_tw_recycle`。此設定已知將導致負載平衡器出問題。使用 `net.ipv4.tcp_tw_reuse` 設定是較為安全的替代方法。

Unhealthy targets receive requests from the load balancer

如果您的負載平衡器至少有一個運作狀態良好的已註冊目標，負載平衡器只會將請求路由至運作狀態良好的已註冊目標。若只有運作狀態不佳的已註冊目標存在，負載平衡器則會將請求路由至所有已註冊目標。

Target fails HTTP or HTTPS health checks due to host header mismatch

運作狀態檢查請求中的 HTTP 主機標頭包含負載平衡器節點的 IP 位址和接聽程式連接埠 (而不是目標的 IP 位址和運作狀態檢查連接埠)。如果您透過主機標頭映射傳入請求，則必須確保運作狀態檢查符合任何 HTTP 主機標頭。另一個選項是在不同的連接埠上新增個別的 HTTP 服務，並將目標群組設定為使用該連接埠進行運作狀態檢查。或者，請考慮使用 TCP 運作狀態檢查。

Connections time out for requests from a target to its load balancer

檢查您是否有內部負載平衡器透過執行個體 ID 註冊目標。內部負載平衡器不支援迴轉傳輸 (Hairpinning) 或回送。透過執行個體 ID 註冊目標時，用戶端的來源 IP 地址將保留。如果執行個體是透過執行個體 ID 註冊為內部負載平衡器的用戶端，則唯有當請求路由至另一執行個體時連線才會成功。否則，來源與目的地 IP 地址將相同，以致連線逾時。

如果執行個體必須傳送請求至其註冊的負載平衡器，請執行以下其中一項操作：

- Register instances by IP address instead of instance ID. When using Amazon Elastic Container Service, use the `awsvpc` network mode with your tasks to ensure that target groups require registration by IP address.
- Ensure that containers that must communicate are on different container instances.
- Use an Internet-facing load balancer.

Performance decreases when moving targets to a 網路負載平衡器

Classic Load Balancer 和 Application Load Balancer 都是使用連線多工處理，但 網路負載平衡器 則不然。因此，您的目標在 網路負載平衡器 後方可能會接收到更多 TCP 連線。請確定您的目標已準備好處理其可能接收到的連線請求量。

Port allocation errors connecting through AWS PrivateLink

如果 網路負載平衡器 與 VPC 端點服務相關聯，它支援對每個唯一的目標 (IP 地址和連接埠) 進行 55,000 個同時連線或每分鐘約 55,000 個連線。若超過上述連線數量，將提高連接埠配置錯誤機率。若發生連接埠配置錯誤，請將更多目標新增至目標群組。

Quotas for your 網路負載平衡器

對於每個 AWS 服務，您的 AWS 帳戶有預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定規定。您可以要求提高某些配額，而其他配額無法提高。

若要檢視 網路負載平衡器 的配額，請開啟Service Quotas 主控台。在導覽窗格中，選擇 AWS services (AWS 服務)，然後選取 Elastic Load Balancing。您也可以針對 Elastic Load Balancing 使用 describe-account-limits (AWS CLI) 命令。

要請求配額增加，請參閱 請求配額增加 在 Service Quotas 使用者指南。如果配額尚未提供 Service Quotas，使用 Elastic Load Balancing 限制增加表格.

您的 AWS 帳戶具有下列與網路負載平衡器相關的配額：

Regional

- 網路負載平衡器 per region: 50
- Target groups per region: 3000 *

Load balancer

- Listeners per load balancer: 50
- Subnets per Availability Zone per load balancer: 1
- [Cross-zone load balancing disabled] Targets per Availability Zone per load balancer: 500
- [Cross-zone load balancing enabled] Targets per load balancer: 500
- Load balancers per target group: 1
- Certificates per load balancer (not counting default certificates): 25

* 此配額由 Application Load Balancer 和 網路負載平衡器 的目標群組共用。

Document history for 網路負載平衡器

下表說明 網路負載平衡器 各版本。

update-history-change	update-history-description	update-history-date
ALPN 政策	此版本新增了對應用程式層通訊協定交涉 (ALPN) 喜好設定清單的支援。	May 27, 2020
黏性工作階段	此版本根據來源 IP 地址和通訊協定新增對黏性工作階段的支援。	February 28, 2020
共用子網路 (p. 65)	此版本新增了對指定由另一個 AWS 帳戶與您共用子網路的支援。	November 26, 2019
私有 IP 地址 (p. 65)	此版本可讓您在啟用內部負載平衡器的可用區域時，從所指定的子網路 IPv4 地址範圍提供私人 IP 地址。	November 25, 2019
新增子網路 (p. 65)	此版本新增讓您在建立負載平衡器後啟用其他可用區域的支援。	November 25, 2019
SNI 支援	此版本增加對伺服器名稱指示 (SNI) 的支援。	September 12, 2019
UDP 通訊協定 (p. 65)	此版本新增 UDP 通訊協定的支援。	June 24, 2019
TLS 協定	此版本新增 TLS 規則的支援。	January 24, 2019
跨區域負載平衡 (Cross-zone load balancing) (p. 65)	此版本新增了支援啟用跨區域負載平衡功能。	February 22, 2018
Proxy Protocol (代理通訊協定)	此版本新增了支援啟用 Proxy Protocol。	November 17, 2017
IP 地址即目標	此版本新增了支援註冊 IP 地址做為目標。	September 21, 2017
新的負載平衡器類型 (p. 65)	此版本的 Elastic Load Balancing 引進了網路負載平衡器。	September 7, 2017

若我們提供該指南英語版本的翻譯，在有任何牴觸的狀況下請以英文版本的指南為主。其透過機器翻譯提供翻譯。