Classic Load Balancer

Elastic Load Balancing

Elastic Load Balancing: Classic Load Balancer

Table of Contents

什麼是 Classic Load Balancer？

Elastic Load Balancing 會在一或多個可用區域中自動將傳入流量分配到多個目標，例如EC2執行個體、容器和 IP 位址。其會監控已註冊目標的運作狀態，並且僅將流量路由至運作狀態良好的目標。當傳入流量隨著時間發生變化，Elastic Load Balancing 會擴展您的負載平衡器。他可以自動擴展以因應絕大多數的工作負載。

Elastic Load Balancing 支援下列負載平衡器：Application Load Balancer、Network Load Balancer、Gateway Load Balancer 和 Classic Load Balancer。您可以選取最符合您需要的負載平衡器類型。本指南主要探討 Classic Load Balancer。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》、《Network Load Balancer 使用者指南》和《Gateway Load Balancer 使用者指南》。

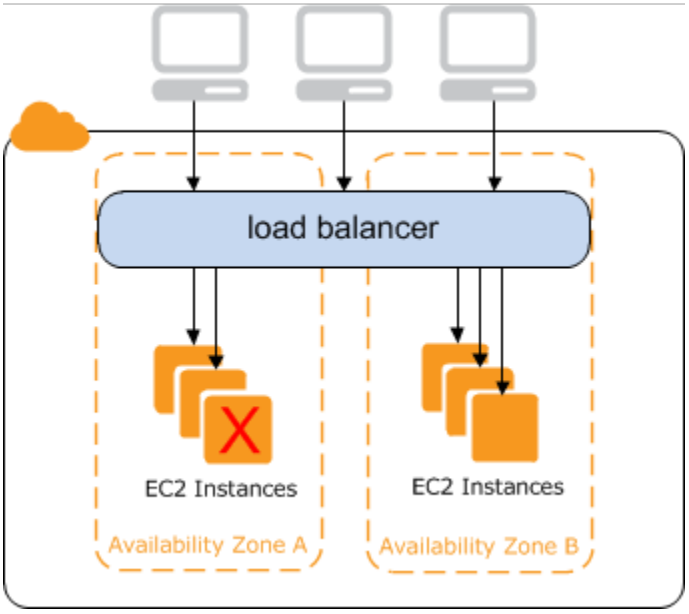
Classic Load Balancer 概觀

負載平衡器會將傳入的應用程式流量分散到多個可用區域的多個EC2執行個體。這可提高應用程式的容錯能力。Elastic Load Balancing 會偵測運作狀態不佳的執行個體，並僅將流量路由至運作狀態良好的執行個體。

您的負載平衡器做為用戶端的單一聯絡窗口。這會提高您應用程式的可用性。您可以依據需求變化，為負載平衡器新增和移除執行個體，而不需中斷應用程式的整體請求流程。當應用程式的流量隨著時間發生變化，Elastic Load Balancing 會擴展您的負載平衡器。Elastic Load Balancing 能夠自動擴展以因應絕大多數的工作負載。

接聽程式會使用您設定的通訊協定和連接埠，檢查來自用戶端的連線請求，並使用您設定的通訊設定和的連接埠號碼，將請求轉送至一或多個已註冊執行個體。您要為負載平衡器添加一個或多個接聽程式。

您可以設定運作狀態檢查，其被用於監控已註冊執行個體的運作狀態，使負載平衡器只能傳送請求至運作狀態良好的執行個體。



為了確保您的已註冊執行個體能夠在每個可用區域處理請求負載，請務必保留和每個可用區域中大約相同數量的執行個體 (已向負載平衡器註冊)。例如，如果您有 10 個執行個體在可用區域 us-west-2a，兩個執行個體在 us-west-2b，請求會平均分佈在兩個可用區域之間。因此，兩個在 us-west-2b 的執行個體所服務的流程，和在 us-west-2a 的十個執行個體提供流量相同。反之，您每個可用區域中應該有六個執行個體。

根據預設，負載平衡器橫跨您為負載平衡器啟用的可用區域平均分派流量。若要在所有啟用之可用區域內跨所有已註冊執行個體平均分佈流量，請在負載平衡器上啟用跨區域負載平衡功能。不過，我們仍然建議您維持大約同等號碼在每個可用區域的執行個體以獲得更優的容錯能力。

如需詳細資訊，請參閱 Elastic Load Balancing 使用者指南中的 Elastic Load Balancing的運作方式 。

優勢

使用 Classic Load Balancer (而非 Application Load Balancer) 具有下列優點：

- Support TCP 和SSL聽眾
- 使用應用程式產生的 Cookie 支援黏性工作階段

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。

如何開始

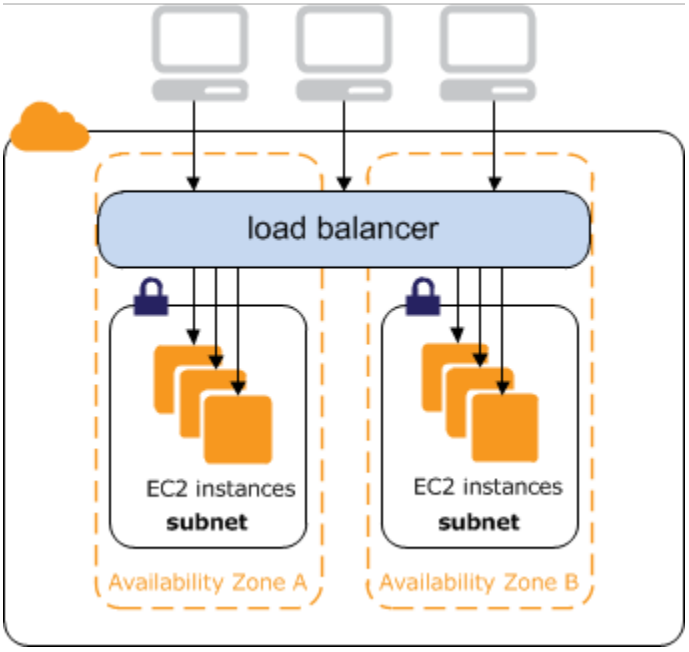
- 若要瞭解如何建立 Classic Load Balancer 並向其註冊EC2執行個體，請參閱建立面向網際網路的 Classic Load Balancer。
- 若要瞭解如何建立HTTPS負載平衡器並向其註冊EC2執行個體，請參閱使用HTTPS接聽程式建立 Classic Load Balancer 。
- 若要瞭解如何使用傳統負載平衡器支援的各種功能，請參閱設定 Classic Load Balancer。

定價

使用負載平衡器時，您只需按實際用量付費。如需詳細資訊，請參閱「Elastic Load Balancing 定價」。

面向網際網路的 Classic Load Balancer

建立 Classic Load Balancer 時，您可以將其設為內部負載平衡器或網際網路對向的負載平衡器。面向網際網路的負載平衡器具有可公開解析的DNS名稱，因此它可以透過網際網路將來自用戶端的要求路由到在負載平衡器註冊的EC2執行個體。



內部負載平衡器的DNS名稱可公開解析為節點的私有 IP 位址。因此，內部負載平衡器只能路由來自具有負載平衡器存取權的VPC用戶端的要求。如需詳細資訊，請參閱內部負載平衡器。

目錄

負載平衡器的公用DNS名稱

建立負載平衡器時，它會收到用戶端可用來傳送要求的公用DNS名稱。DNS伺服器會將負載平衡器的DNS名稱解析為負載平衡器之負載平衡器節點的公用 IP 位址。每個負載平衡器節點連接到使用私有 IP 地址的後端執行個體。

主控台會以下列格式顯示公用DNS名稱：

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

建立面向網際網路的 Classic Load Balancer

建立負載平衡器時，您可以設定接聽程式、設定健全狀況檢查，以及註冊後端執行個體。您透過指定一個前端 (用戶端到負載平衡器) 連線的通訊協定和連接埠，以及後端 (負載平衡器到後端執行個體) 連線的通訊協定和連接埠來設定接聽程式。您可以為您的負載平衡器設定多個接聽程式。

本教學課程透過 Web 型介面提供傳統負載平衡器的 AWS Management Console實際操作簡介。您將建立負載平衡器，以接收公共HTTP流量並將其傳送至您的EC2執行個體。

若要使用接聽程式建立負載平衡HTTPS器，請參閱使用HTTPS接聽程式建立 Classic Load Balancer。

任務

- 開始之前
- 使用建立 Classic Load Balancer AWS Management Console

開始之前

- 建立虛擬私有雲 (VPC)。如需詳細資訊，請參閱為您的建議 VPC。
- 啟動您計劃向負載平衡器註冊的EC2執行個體。請確定這些執行個體的安全性群組允許在連接埠 80 上HTTP存取。
- 在每個執行個體上安裝網頁伺服器 (例如 Apache 或 Internet 資訊服務 (IIS)，在連線至網際網路之網頁瀏覽器的位址欄位中輸入其DNS名稱，然後確認瀏覽器是否顯示伺服器的預設頁面。

使用建立 Classic Load Balancer AWS Management Console

使用下列程序建立您的 Classic Load Balancer。提供您負載平衡器的基本組態資訊，例如名稱和結構描述。然後提供您網路的相關資訊，以及將流量路由至您執行個體的接聽程式資訊。

使用主控台建立 Classic Load Balancer

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 於導覽列上，為負載平衡器選擇一個區域。請務必選取您為EC2執行個體選取的相同區域。
3. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
4. 選擇 Create Load Balancer (建立負載平衡器)。
5. 展開 Classic Load Balancer 區段，然後選擇建立。

6. 基本組態

   a. 針對負載平衡器名稱，輸入負載平衡器的名稱。

      在區域的 Classic Load Balancer 組合中，您的 Classic Load Balancer 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，但開頭或結尾都不可為連字號。

   b. 針對結構描述，選取面向網際網路。

7. 網路映射

   a. 對於 VPC，選取您為執行個體選取的相同VPC項目。

   b. 針對映射，先選取可用區域，然後從可用子網路中選擇公有子網路。一個可用區域只能選取一個子網路。為了提高您的負載平衡器可用性，可選取一個以上的可用區域和子網路。

8. 安全群組

   - 針對安全性群組，選取設定為允許連接埠 80 上所需HTTP流量的現有安全性群組。

9. 接聽程式和路由

   a. 針對接聽程式，請確定通訊協定為 HTTP，且連接埠為 80。

   b. 針對執行個體，請確定通訊協定為 HTTP，且連接埠為 80。

10. 運作狀態檢查

    a. 針對 Ping 通訊協定，請確定通訊協定為 HTTP。

    b. 針對 Ping 連接埠，請確定連接埠為 80。

    c. 針對 Ping路徑，請確定路徑為 /。

    d. 針對進階運作狀態檢查設定，請使用預設值。

11. 執行個體

    a. 選取新增執行個體以開啟執行個體選取畫面。

    b. 在可用執行個體下方，您可以根據目前的網路設定，選取目前可用於負載平衡器的執行個體。

    c. 當您對您的選項感到滿意時，請選取確認，將要註冊的執行個體新增至負載平衡器。

12. Attributes

    - 針對啟用跨區域負載平衡、啟用連接耗盡和逾時 (耗盡間隔)，請保留預設值。

13. 負載平衡器標籤 (選用)

    a. 索引鍵欄位為必填。

b. 值欄位為選填。

c. 若要新增另一個標籤，請選取新增標籤，然後輸入索引鍵欄位值，並選擇性地填寫值欄位。

d. 若要移除現有的標籤，請在要移除的標籤旁選取移除。

14. 摘要和建立

a. 如果您需要變更任何設定，請在需要變更的設定旁選取編輯。

b. 如果您對摘要中顯示的所有設定感到滿意，請選取建立負載平衡器，開始建立您的負載平衡器。

c. 在最後建立頁面上，選取檢視負載平衡器以在 Amazon EC2 主控台中檢視負載平衡器。

15. 確認

a. 選取新的負載平衡器。

b. 在目標執行個體索引標籤中，檢查運作狀態欄位。至少有一個EC2執行個體處於服務中之後，您可以測試負載平衡器。

c. 在 [詳細資料] 區段中，複製負載平衡器DNS名稱，看起來類似於`my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`。

d. 將您的負載平衡器DNS名稱粘貼到公共互聯網連接的 Web 瀏覽器的地址字段中。如果負載平衡器運作正常，您會看到伺服器的預設頁面。

16. 刪除 (選用)

a. 如果您的網域有指向負載平衡器的CNAME記錄，請將其指向新位置，並等待DNS變更生效，然後再刪除負載平衡器。

b. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。

c. 選取負載平衡器。

d. 選擇動作、刪除負載平衡器。

e. 出現確認提示時，請輸入 `confirm`，然後選取刪除。

f. 刪除負載平衡器之後，向負載平衡器註冊的EC2執行個體會繼續執行。系統將根據執行個體繼續執行的時間，按每小時或不足一小時的時數計費。當您不再需要EC2執行個體時，您可以停止或終止執行個體，以避免產生額外費用。

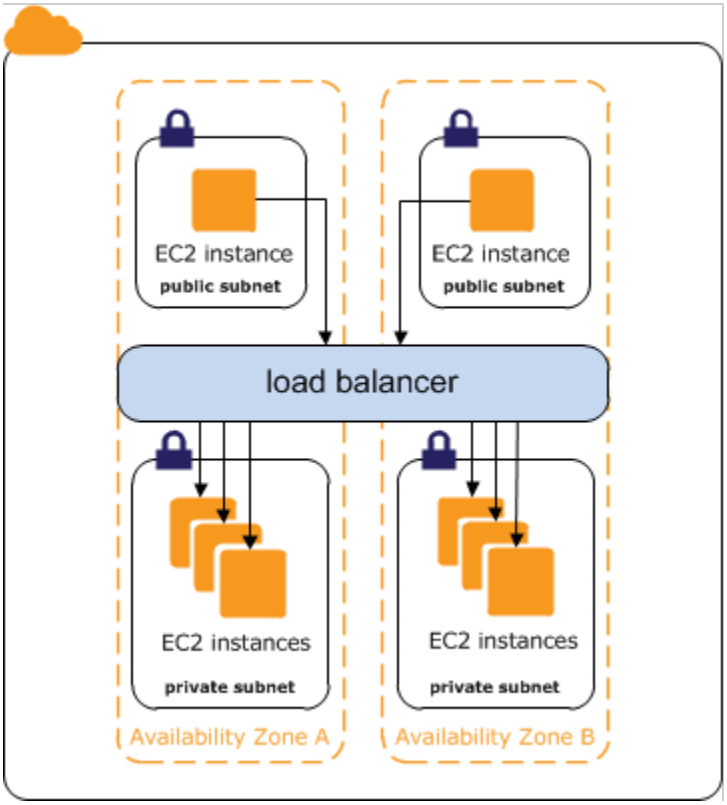
內部 Classic Load Balancer

當您建立負載平衡器時，您必須選擇將它當做內部負載平衡器或面向網際網路的負載平衡器。

面向網際網路負載平衡器的節點具有公有 IP 地址。面向網際網路的負載平衡器的DNS名稱可公開解析為節點的公用 IP 位址。因此，面向網際網路的負載平衡器可透過網際網路來路由用戶端請求。如需詳細資訊，請參閱面向網際網路的 Classic Load Balancer。

內部負載平衡器的節點僅具有私有 IP 地址。內部負載平衡器的DNS名稱可公開解析為節點的私有 IP 位址。因此，內部負載平衡器只能路由來自具有負載平衡器存取權的VPC用戶端的要求。

如果您的應用程式有多個層級 (例如，必須連接到網際網路的 Web 伺服器，以及只連接到 Web 伺服器的資料庫伺服器)，您可以設計架構來同時使用內部與面向網際網路的負載平衡器。建立面向網際網路的負載平衡器，並向它註冊 Web 伺服器。建立內部負載平衡器，並向它註冊資料庫伺服器。Web 伺服器會從面向網際網路的負載平衡器接收請求，並將對於資料庫伺服器的請求傳送到內部負載平衡器。資料庫伺服器會接收來自內部負載平衡器的請求。



目錄

負載平衡器的公用DNS名稱

建立內部負載平衡器時，會收到具有下列格式的公用DNS名稱：

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

DNS伺服器會將負載平衡器的DNS名稱解析為內部負載平衡器節點的私有 IP 位址。每個負載平衡器節點連接到使用彈性網路界面之後端執行個體的私有 IP 地址。如果啟用跨區域負載平衡，每個節點都會連接到每個後端執行個體，無論可用區域為何。否則，每個節點僅連接在其可用區域中的執行個體。

建立內部 Classic Load Balancer

您可以建立內部負載平衡器，將流量從具有負載平衡器存取權的用戶端分配VPC給EC2執行個體。

目錄

必要條件

- 如果尚未VPC為負載平衡器建立，則必須在開始之前建立它。如需詳細資訊，請參閱為您的建議VPC。
- 啟動您計劃向內部負載平衡器註冊的EC2執行個體。請務必在用於負載平衡器的私人子網路中VPC啟動它們。

使用主控台建立內部負載平衡器

使用下列程序建立您的內部 Classic Load Balancer。提供您負載平衡器的基本組態資訊，例如名稱和結構描述。然後提供您網路的相關資訊，以及將流量路由至您執行個體的接聽程式資訊。

使用主控台建立內部 Classic Load Balancer

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 於導覽列上，為負載平衡器選擇一個區域。請務必選取您為EC2執行個體選取的相同區域。
3. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。

4. 選擇 Create Load Balancer (建立負載平衡器)。
5. 展開 Classic Load Balancer 區段，然後選擇建立。
6. 基本組態
   a. 針對負載平衡器名稱，輸入負載平衡器的名稱。

      在區域的 Classic Load Balancer 組合中，您的 Classic Load Balancer 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，但開頭或結尾都不可為連字號。
   b. 針對結構描述，選取內部。
7. 網路映射
   a. 對於 VPC，選取您為執行個體選取的相同VPC項目。
   b. 針對映射，先選取可用區域，然後從可用子網路中選擇子網路。一個可用區域只能選取一個子網路。為了提高您的負載平衡器可用性，可選取一個以上的可用區域和子網路。
8. 針對安全性群組，選取設定為允許連接埠 80 上所需HTTP流量的現有安全性群組。或者，如果您的應用程式使用不同的通訊協定和連接埠，您也可以建立新的安全群組。
9. 接聽程式和路由
   a. 針對接聽程式，請確定通訊協定為 HTTP，且連接埠為 80。
   b. 針對執行個體，請確定通訊協定為 HTTP，且連接埠為 80。
10. 運作狀態檢查
    a. Ping 通訊協定預設為 HTTP。
    b. Ping 連接埠預設為 80。
    c. Ping 路徑預設為 /。
    d. 針對進階運作狀態檢查設定，請使用預設值或輸入您應用程式特定的值。
11. 執行個體
    a. 選取新增執行個體以開啟執行個體選取畫面。
    b. 在可用執行個體下方，您可以根據先前選取的網路設定，選取目前可用於負載平衡器的執行個體。
    c. 當您對您的選項感到滿意時，請選取確認，將要註冊的執行個體新增至負載平衡器。
12. Attributes
    - 針對啟用跨區域負載平衡、啟用連接耗盡和逾時 (耗盡間隔)，請保留預設值。

13. 負載平衡器標籤 (選用)
    a. 索引鍵欄位為必填。
    b. 值欄位為選填。
    c. 若要新增另一個標籤，請選取新增標籤，然後輸入索引鍵欄位值，並選擇性地填寫值欄位。
    d. 若要移除現有的標籤，請在要移除的標籤旁選取移除。
14. 摘要和建立
    a. 如果您需要變更任何設定，請在需要變更的設定旁選取編輯。
    b. 如果您對摘要中顯示的所有設定感到滿意，請選取建立負載平衡器，開始建立您的負載平衡器。
    c. 在最後建立頁面上，選取檢視負載平衡器以在 Amazon EC2 主控台中檢視您的負載平衡器。
15. 確認
    a. 選取新的負載平衡器。
    b. 在目標執行個體索引標籤中，檢查運作狀態欄位。至少有一個EC2執行個體處於服務中之後，您可以測試負載平衡器。
    c. 在 [詳細資料] 區段中，複製負載平衡器DNS名稱，看起來類似於`my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`。
    d. 將您的負載平衡器DNS名稱粘貼到公共互聯網連接的 Web 瀏覽器的地址字段中。如果負載平衡器運作正常，您會看到伺服器的預設頁面。
16. 刪除 (選用)
    a. 如果您的網域有指向負載平衡器的CNAME記錄，請將其指向新位置，並等待DNS變更生效，然後再刪除負載平衡器。
    b. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
    c. 選取負載平衡器。
    d. 選擇動作、刪除負載平衡器。
    e. 出現確認提示時，請輸入 `confirm`，然後選取刪除。
    f. 刪除負載平衡器之後，向負載平衡器註冊的EC2執行個體會繼續執行。系統將根據執行個體繼續執行的時間，按每小時或不足一小時的時數計費。當您不再需要EC2執行個體時，您可以停止或終止執行個體，以避免產生額外費用。

使用建立內部負載平衡器 AWS CLI

在預設情況下，Elastic Load Balancing 建立面向網際網路的負載平衡器。使用下列程序建立內部負載平衡器，並向新建立的內部負載平衡器註冊EC2執行個體。

建立內部負載平衡器

1. 在將`--scheme`選項設定為的情況下使用create-load-balancer指令`internal`，如下所示：

```
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
```

以下是回應範例。請注意，從名稱可看出這是內部負載平衡器。

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

2. 使用下列 register-instances-with-load-平衡器命令新增執行個體：

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

以下是回應範例：

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

3. (選擇性) 使用下列describe-load-balancers命令驗證內部負載平衡器：

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

回應包含 DNSName 和 Scheme 欄位，這表示這是內部負載平衡器。

```
{
    "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",
            ...
        }
    ]
}
```

設定 Classic Load Balancer

建立 Classic Load Balancer 後，您可以變更其組態。例如，您可以更新負載平衡器屬性、子網路和安全群組。

負載平衡器屬性

連線耗盡

如啟用，則負載平衡器允許先完成現有的請求，再從已取消註冊或狀態不佳的執行個體轉移流量。

跨區域負載平衡

如果啟用，負載平衡器會將請求流量平均路由到所有執行個體，不論可用區域。

Desync 遷移模式

決定負載平衡器如何處理可能對應用程式造成安全風險的請求。可能的值為 `monitor`、`defensive` 和 `strictest`。預設值為 `defensive`。

閒置逾時

如果啟用，則負載平衡器允許連線在指定的期間保持閒置 (不透過此連線傳送資料)。預設值為 60 秒。

黏性工作階段

Classic Load Balancer 支援持續時間型和應用程式型工作階段黏性。

負載平衡器詳細資訊

安全群組

負載平衡器的安全群組必須允許接聽程式和運作狀態檢查連接埠上的流量。

子網

您可以將負載平衡器的功能擴展到其他子網路。

Proxy Protocol (代理通訊協定)

如果啟用，我們會新增一個標頭，其中包含傳送至執行個體的連線資訊。

Tags (標籤)

您可以新增標籤來分類負載平衡。

為 Classic Load Balancer 設定閒置連線逾時

對於用戶端透過 Classic Load Balancer 提出的每個請求，負載平衡器會維持兩個連線。前端連線是在用戶端和負載平衡器之間。後端連線位於負載平衡器和已註冊EC2執行個體之間。負載平衡器具有適用於其連線的已設定閒置逾時期間。如果截至閒置逾時的時間過後都沒有傳送或接收的資料，負載平衡器會關閉連線。為了確保冗長的操作 (例如檔案上傳) 有時間完成，請在每個閒置逾時期間過去之前傳送至少 1 位元組的資料，並視需要增加閒置逾時期間的長度。

如果您使用 HTTP和 HTTPS 接聽程式，建議您為執行個體啟用HTTP保持連線選項。您可以在 Web 伺服器設定中為您的執行個體啟用保持連線。啟用保持連線後，會啟用負載平衡器以重複使用後端連線，直到保持連線逾時過期。為確保負載平衡器負責關閉與執行個體的連線，請確定您為HTTP保持連線時間設定的值大於為負載平衡器設定的閒置逾時設定。

請注意，TCP保持連線探查不會阻止負載平衡器終止連線，因為它們不會在承載中傳送資料。

目錄

使用主控台設定閒置逾時

預設情況下，Elastic Load Balancing 會將負載平衡器的閒置逾時設為 60 秒。請使用下列程序來設定不同的閒置逾時值。

使用主控台設定負載平衡器的閒置逾時設定

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的流量組態區段，輸入閒置逾時的值。閒置逾時的範圍是從 1 到 4,000 秒。

6. 選擇 Save changes (儲存變更)。

使用 AWS CLI設定閒置逾時

使用下列modify-load-balancer-attributes命令來設定負載平衡器的閒置逾時：

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

以下是回應範例：

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

為 Classic Load Balancer 設定跨區域負載平衡。

若使用跨區域負載平衡，Classic Load Balancer 的每個負載平衡器節點會將請求平均分配到所有已啟用可用區域中已註冊的執行個體。若顯示跨區域負載平衡，每個負載平衡器節點會平均地將請求僅分配到其可用區域中已註冊的執行個體。如需詳細資訊，請參閱 Elastic Load Balancing 使用者指南中的跨區域負載平衡。

跨區域負載平衡可減少需要維護同等號碼在每個可用區域的執行個體啟用，並改善您的應用程式能夠處理一個或多個執行個體的遺失。不過，我們仍然建議您維持大約同等號碼在每個已啟用可用區域的執行個體以獲得更高的容錯能力。

對於用戶端快取DNS查詢的環境，傳入的請求可能會偏好其中一個可用區域。使用跨區域負載平衡的負載，這個需求負載的不平衡會分配至所有區域中可用的執行個體，降低行為不當用戶端的影響。

當您建立 Classic Load Balancer 時，跨區域負載平衡的預設值取決於您如何建立負載平衡器。使用 API或 時CLI，跨區域負載平衡預設為停用。使用 時 AWS Management Console，預設會選取啟用跨區域負載平衡的選項。建立 Classic Load Balancer 後，您隨時可以啟用或停用跨區域負載平衡。

目錄

- 啟用跨區域負載平衡
- 停用跨區域負載平衡

啟用跨區域負載平衡

您可以隨時為 Classic Load Balancer 啟用跨區域負載平衡。

使用主控台啟用跨區域負載平衡

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的可用區域路由組態區段，啟用跨區域負載平衡。
6. 選擇 Save changes (儲存變更)。

若要使用 啟用跨區域負載平衡 AWS CLI

1. 使用下列modify-load-balancer-attributes命令，將負載平衡器的`CrossZoneLoadBalancing`屬性設定為 `true`：

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

   以下是回應範例：

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

2. （選用）使用下列describe-load-balancer-attributes命令來確認您的負載平衡器已啟用跨區域負載平衡：

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

以下是回應範例：

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

停用跨區域負載平衡

您可以在任何時間停用您的負載平衡器跨區域負載平衡選項。

停用主控台啟用跨區域負載平衡

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的可用區域路由組態區段，停用跨區域負載平衡。
6. 選擇 Save changes (儲存變更)。

若要停用跨區域負載平衡的負載平衡器，設定您的負載平衡器的 `CrossZoneLoadBalancing` 屬性至 `false`。

若要使用 停用跨區域負載平衡 AWS CLI

1. 使用下列 modify-load-balancer-attributes 命令：

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

以下是回應範例：

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

2. （選用）使用下列describe-load-balancer-attributes命令來確認您的負載平衡器已停用跨區域負載平衡：

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

以下是回應範例：

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

```
}
```

為 Classic Load Balancer 設定連接耗盡

為了確保 Classic Load Balancer 停止傳送請求給取消註冊或運作狀態不佳的執行個體，並保留現有的連線開放，請使用連接耗盡。這可讓負載平衡器完成取消註冊或運作狀態不佳的執行個體的處理中請求。

當您啟用連接耗盡時，您可以指定一個最長的時間，讓連線的負載平衡器在報告取消註冊執行個體前持續作用。最長逾時值可以設在 1 和 3,600 秒之間 (預設為 300 秒)。當達到最長時間限制，負載平衡器強制關閉連線到取消註冊的執行個體。

當提供了需求中的請求，負載平衡器報告正在取消註冊執行個體的 `InService: Instance deregistration currently in progress` 狀態。當取消註冊的執行個體完成服務中的所有請求，或是當達到限制的最長逾時，負載平衡器報告執行個體的狀態為 `OutOfService: Instance is not currently registered with the LoadBalancer`。

如果執行個體運作狀態不佳，負載平衡器報告狀態為 `OutOfService`。如果有運作中狀態不佳的執行個體所做的處理中請求，會將它們完成。最長逾時限制不適用於連線到運作狀態不佳的執行個體。

如果您的執行個體是 Auto Scaling 群組的一部分且您的負載平衡器已啟用連接耗盡，在終止執行個體之前，由於擴展事件或運作狀態檢查替換，Auto Scaling 會等待傳送中的請求完成，或最長逾時過期。

如果您希望立即關閉連接到執行個體運作狀態不佳或取消註冊，您可以停用連接耗盡的負載平衡器。當停用連接耗盡時，任何處理中的請求的取消註冊或運作狀態不佳的執行個體都沒有完成。

目錄

啟用連接耗盡

您可以於任何時間啟用您的負載平衡器的連接耗盡。

使用主控台來啟用連接耗盡

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

2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的流量組態區段中，選取啟用連接耗盡。
6. (選用) 對於逾時 (耗盡間隔)，輸入 1 到 3,600 秒之間的值。否則，系統會使用 300 秒的預設值。
7. 選擇 Save changes (儲存變更)。

若要使用 啟用連線排放 AWS CLI

使用下列 modify-load-balancer-attributes 命令：

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

以下是回應範例：

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

停用連接耗盡

您可以於任何時間停用您的負載平衡器的連接耗盡。

使用主控台來停用連接耗盡

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。

5. 在編輯負載平衡器屬性頁面的流量組態區段中，取消選取啟用連接耗盡。
6. 選擇 Save changes (儲存變更)。

使用 停用連線耗電 AWS CLI

使用下列 modify-load-balancer-attributes 命令：

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

以下是回應範例：

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

為 Classic Load Balancer 設定黏性工作階段

Classic Load Balancer 預設會以最小的負載，將每個請求獨立路由至已註冊的執行個體。不過，您可以使用黏性工作階段功能 (也稱為工作階段親和性)，它能讓負載平衡器將使用者的工作階段繫結到特定執行個體。這樣能確保該工作階段期間所有的使用者請求都能傳送到相同的執行個體。

管理黏性工作階段的金鑰是決定您的負載平衡器應該持續將使用者請求路由到同一個執行個體的時間。如果您的應用程式有其自己的工作階段 Cookie，則您可以設定 Elastic Load Balancing，因此工作階段 Cookie 遵循應用程式的工作階段 Cookie 指定的持續時間。如果您的應用程式沒有自己的工作階段 Cookie，則您可用指定自己的黏性持續時間來設定 Elastic Load Balancing，以建立工作階段 Cookie。

Elastic Load Balancing 會建立名為 的 Cookie AWSELB，用於將工作階段映射至執行個體。

要求

- HTTP/HTTPS 負載平衡器。

- 在各個可用區域內啟動至少一個正常運作的執行個體。

相容性

- Cookie RFC 路徑屬性的 可允許底線。不過，Elastic Load Balancing URI 會將底線字元編碼為 ，`%5F`因為某些瀏覽器，例如 Internet Explorer 7，預期底線會URI編碼為 `%5F`。由於可能影響目前運作中的瀏覽器，Elastic Load Balancing URI 會持續編碼底線字元。例如，如果 Cookie 有屬性 `path=/my_path`，Elastic Load Balancing 會變更轉發請求至 `path=/my%5Fpath` 的屬性。
- 您無法設定 `secure` 旗標或 `HttpOnly` 旗標在您的持續時間為基礎的工作階段黏著 Cookie。不過，這些 Cookie 不包含機密資料。請注意，如果您在應用程式控制的工作階段黏性 Cookie 上設定`secure`旗標或`HttpOnly`旗標，也會在 AWSELB Cookie 上設定。
- 如果您有一個在 `Set-Cookie` 欄位在應用程式 Cookie 結尾的分號，則負載平衡器忽略 Cookie。

目錄

持續時間為基礎的工作階段黏著

負載平衡器使用特殊 Cookie AWSELB來追蹤每個請求給每個接聽程式的執行個體。當負載平衡器收到請求時，首先會檢查此 Cookie 是否存在於請求中。若是，此請求會傳送至 Cookie 中指定的執行個體。若 Cookie 不存在，則負載平衡器會根據現有負載平衡演算法選擇執行個體。回應會插入 Cookie，藉此將後續來自相同使用者的請求繫結至該執行個體。黏性政策設定可定義 Cookie 過期時間，用來建立每個 Cookie 有效期。負載平衡器在使用之前，不會重新整理 Cookie 的過期時間也不會檢查 Cookie 是否過期。在 Cookie 過期之後，工作階段不再有黏性。用戶端應該從其 Cookie 存放在到期移除 Cookie。

透過 CORS（跨來源資源共用）請求，某些瀏覽器需要`SameSite=None; Secure`啟用黏性。在此情況下，Elastic Load Balancing 會建立第二個黏性 Cookie AWSELBCORS，其中包含與原始黏性 Cookie 相同的資訊，以及此`SameSite`屬性。用戶端會同時收到這兩個 Cookie。

如果執行個體發生失敗或變成運作狀態不佳，負載平衡器停止路由請求到該執行個體，並根據現有的負載平衡演算法選擇新的運作狀態良好的執行個體。如果沒有 Cookie，而且工作階段不再有黏性，該請求路由到新的執行個體。

如果用戶端切換到具備不同的後端連接埠的接聽程式，黏著性遺失。

若要使用主控台的負載平衡器啟用持續時間為基礎的黏性工作階段

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在接聽程式索引標籤中，選擇管理接聽程式。
5. 在管理接聽程式頁面上找到要更新的接聽程式，然後選擇 Cookie 黏性下方的編輯。
6. 在編輯 Cookie 黏性設定快顯視窗上，選取依負載平衡器產生 。
7. (選用) 對於過期期間，輸入 Cookie 過期期間 (以秒為單位)。如果您不指定過期時段，黏性工作階段持續在瀏覽器工作階段。
8. 選擇儲存變更以關閉快顯視窗。
9. 選擇儲存變更以返回負載平衡器詳細資訊頁面。

若要 AWS CLI的負載平衡器啟用持續時間為基礎的黏性工作階段

1. 使用下列 create-lb-cookie-stickiness-policy 命令來建立負載平衡器產生的 Cookie 黏性政策，其 Cookie 過期期間為 60 秒：

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

2. 使用下列 set-load-balancer-policies-of-listener 命令，為指定的負載平衡器啟用工作階段黏性：

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

> **Note**
>
> 此 `set-load-balancer-policies-of-listener` 命令會取代目前的政策與指定的負載平衡器連接埠相關聯。每當您使用此命令，指定 `--policy-names` 選項列出所有政策以啟用。

3. （選用）使用下列describe-load-balancers命令來驗證政策是否已啟用：

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

回應包含下列資訊，其中說明為指定的連接埠上的接聽程式啟用政策：

```
{
    "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"
                ]
            },
            ...
        }
    ]
}
```

應用程式控制工作階段黏著

負載平衡器使用特殊的 Cookie，將工作階段與處理初始請求的執行個體相關聯，但遵循指定在政策組態中應用程式 Cookie 的生命週期。如果應用程式回應包含新應用程式 Cookie，負載平衡器只會插入新的黏性 Cookie。負載平衡器黏性 Cookie 不會隨著每個請求更新。如果應用程式 Cookie 明確移除或過期，工作階段會停止其黏性直到發出新的應用程式 Cookie。

下列由後端執行個體設定的屬性會傳送至 Cookie 中的用戶端：`path`、`port`、`domain`、`secure`、`httponly`、`discard`、`max-age`、`expires`、`version`、`comment`、`commenturl` 和 `samesite`。

如果執行個體發生失敗或變成運作狀態不佳，負載平衡器停止路由請求到該執行個體，並根據現有的負載平衡演算法選擇新的運作狀態良好的執行個體。負載平衡器會將工作階段視為「卡住」到運作狀態良好的執行個體，並持續路由請求到即使失敗的執行個體恢復到該執行個體。

使用主控台來啟用應用程式控制工作階段黏著

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在接聽程式索引標籤中，選擇管理接聽程式。
5. 在管理接聽程式頁面上找到要更新的接聽程式，然後選擇 Cookie 黏性下方的編輯。
6. 選取由應用程式產生。
7. 在 Cookie Name (Cookie 名稱)，輸入您的應用程式名稱。
8. 選擇 Save changes (儲存變更)。

使用 啟用應用程式控制的工作階段黏性 AWS CLI

1. 使用下列 create-app-cookie-stickiness-policy 命令來建立應用程式產生的 Cookie 黏性政策：

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

2. 使用下列 set-load-balancer-policies-of-listener 命令來啟用負載平衡器的工作階段黏性：

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

> **Note**
>
> 此 `set-load-balancer-policies-of-listener` 命令會取代目前的政策與指定的負載平衡器連接埠相關聯。每當您使用此命令，指定 `--policy-names` 選項列出所有政策以啟用。

3. （選用）使用下列describe-load-balancers命令來驗證是否已啟用黏性政策：

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

4. 回應包含下列資訊，其中說明為指定的連接埠上的接聽程式啟用政策：

```
{
    "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"
                ]
            },
            ...
        }
    ]
}
```

為 Classic Load Balancer 設定非同步緩和模式

Desync 緩解模式可保護您的應用程式免受 Desync HTTP 造成的問題。負載平衡器會根據其威脅層級對每個要求進行分類，允許安全要求，然後根據您指定的緩和模式來降低風險。非同步緩和模式分為監控、防禦性和最嚴格。預設值是防禦模式，可提供持久的HTTP去同步緩解，同時維持應用程式的可用性。您可以切換至最嚴格的模式，以確保應用程式僅收到符合 7230 RFC 的請求。

http_desync_guardian 程式庫會分析HTTP請求，以防止 HTTP Desync 攻擊。如需詳細資訊，請參閱 github 上的 HTTP Desync Guardian。

目錄

> **Tip**
>
> 此組態僅適用於 Classic Load Balancer。如需適用於 Application Load Balancer 的資訊，請參閱 Application Load Balancer 的非同步緩和模式。

分類

分類如下。

- 合規 — 請求符合 RFC 7230，不會造成已知的安全威脅。
- 可接受 — 請求不符合 RFC 7230，但不會造成已知的安全威脅。
- 模稜兩可：請求不符合 RFC 7230，但會帶來風險，因為各種 Web 伺服器和代理可能會以不同的方式處理。
- 嚴重 — 要求造成高安全性風險。負載平衡器會封鎖要求，傳送提供 400 回應至用戶端，並關閉用戶端連線。

下列清單說明每個分類的問題。

可接受

- 標頭包含非 ASCII或 控制項字元。
- 要求版本包含錯誤的值。
- GET 或 HEAD請求的 Content-Length 標頭值為 0。
- 請求URI包含未URL編碼的空間。

不明確

- 請求URI包含控制項字元。
- 要求同時包含 Transfer-Encoding 標頭和 Content-Length 標頭。
- 多個 Content-Length 標頭的值相同。
- 標頭空白或標頭列僅含空格。
- 可使用通用文字正規化技術將標頭正規化為 Transfer-Encoding 或 Content-Length。
- GET 或 HEAD請求有一個 Content-Length 標頭。
- GET 或 HEAD請求有一個 Transfer-Encoding 標頭。

嚴重

- 請求URI包含 null 字元或歸位字元。
- Content-Length 標頭包含無法剖析或非有效數字的值。
- 標頭包含空值字元或歸位字元。

- Transfer-Encoding 標頭包含錯誤的值。
- 要求方法格式不正確。
- 要求版本格式不正確。
- 多個 Content-Length 標頭的值不同。
- 有多個 Transfer-Encoding：區塊標頭。

如果請求不符合 RFC 7230，負載平衡器會增加`DesyncMitigationMode_NonCompliant_Request_Count`指標。如需詳細資訊，請參閱Classic Load Balancer 指標。

模式

下表說明 Classic Load Balancers 如何根據模式和分類處理要求。

分類	監控模式	防禦性模式	最嚴格模式
合規	允許	已允許	允許
可接受	允許	允許	封鎖
不明確	允許	允許[1]	封鎖
嚴重	允許	封鎖	封鎖

[1] 路由傳送要求，但關閉用戶端和目標連接。

修改非同步緩和模式

使用主控台更新非同步緩和模式

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的流量組態下方，選擇防禦性 - 建議、最嚴格或監控。
6. 選擇 Save changes (儲存變更)。

使用 更新非同步緩解模式 AWS CLI

使用 `elb.http.desyncmitigationmode` 屬性設定為 `monitor`、 `defensive`或 的 modify-load-balancer-attributes命令`strictest`。

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

`attribute.json` 內容如下。

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

設定 Classic Load Balancer 的代理通訊協定

Proxy Protocol 是一項網際網路協定請求連線的連線資訊從來源到目的地的連線請求。Elastic Load Balancing 使用 Proxy Protocol 版本 1，該版本使用可供人類讀取的標題格式。

根據預設，當您使用傳輸控制通訊協定（TCP）進行前端和後端連線時，Classic Load Balancer 會將請求轉送至執行個體，而不修改請求標頭。如果您啟用 Proxy Protocol，以可供人類讀取的標題新增到請求標題與連線資訊，例如來源 IP 地址、目的地 IP 地址和連接埠號碼。然後標題會做為請求的一部分傳送到執行個體。

> **Note**
>
> AWS Management Console 不支援啟用代理通訊協定。

目錄

- 使用 AWS CLI來停用 Proxy Protocol

Proxy Protocol 標題

當您有TCP用於後端連線的負載平衡器時，代理通訊協定標頭可協助您識別用戶端的 IP 地址。因為負載平衡器會攔截用戶端與您的執行個體的流量，所以您的執行個體存取日誌包含負載平衡器的 IP 地址，而不包含來源用戶端。您可以剖析請求中的第一行來擷取您的用戶端 IP 地址和連接埠號碼。

標頭中的代理地址IPv6是負載平衡器的公有IPv6地址。此IPv6地址符合從負載平衡器DNS名稱解析的 IP 地址，其開頭為 `ipv6`或 `dualstack`。如果用戶端與 連線IPv4，則 標頭中的代理地址是負載平衡器的私有IPv4地址，無法透過DNS查詢解決。

Proxy Protocol 列是單一列以換行結束行 (`"\r\n"`)，格式如下：

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

範例： IPv4

以下是 的代理通訊協定行範例IPv4。

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

啟用 Proxy Protocol 先決條件

開始之前，請執行以下動作：

- 確認您的負載平衡器不在啟用 Proxy Protocol 的代理伺服器後方。如果 Proxy Protocol 啟用於代理伺服器和負載平衡器，負載平衡器新增另一個標題到請求，其從代理伺服器已有標題。根據您的執行個體設定方法，這重複可能會導致錯誤。
- 確認您的執行個體可以處理 Proxy Protocol 資訊。
- 確認您的接聽程式設定支援 Proxy Protocol。如需詳細資訊，請參閱Classic Load Balancer 的接聽程式組態。

使用 AWS CLI來啟用 Proxy Protocol

若要啟用 Proxy Protocol ，您需要建立 `ProxyProtocolPolicyType` 類型的政策，然後在執行個體連接埠啟用政策。

請使用下列步驟來建立新的政策，為您的負載平衡器的 `ProxyProtocolPolicyType` 類型，在連接埠 `80` 設定新建立的政策到執行個體，和驗證政策已啟用。

為您的負載平衡器啟用 Proxy Protocol

1. （選用）使用下列 describe-load-balancer-policy-types 命令來列出 Elastic Load Balancing 支援的政策：

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

回應包含名稱和描述支援的政策類型。以下顯示 `ProxyProtocolPolicyType` 類型的輸出：

```
{
    "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. 使用下列create-load-balancer-policy命令來建立啟用代理通訊協定的政策：

```
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. 使用下列 set-load-balancer-policies-for-backend-server 命令，在指定的連接埠上啟用新建立的政策。請注意，這個命令會取代目前組的啟用政策。因此，`--policy-names` 選項必須指定

您要加入清單的政策 (例如，my-ProxyProtocol-policy) 和任何目前啟用政策 (例如，my-existing-policy)。

```
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. （選用）使用下列describe-load-balancers命令來確認代理通訊協定已啟用：

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

回應包含下列資訊，其中說明 my-ProxyProtocol-policy 政策與連接埠 80 相關聯。

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

使用 AWS CLI來停用 Proxy Protocol

您可以停用與執行個體關聯的政策，然後讓他們在稍後時間啟用。

停用 Proxy Protocol 政策

1. 使用下列 set-load-balancer-policies-for-backend-server 命令，透過從 --policy-names選項中省略代理通訊協定政策，但包含應保持啟用的其他政策（例如 my-existing-policy），來停用代理通訊協定政策。

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

如果沒有啟用其他政策，以 `--policy-names` 指定空白字串選項，如下所示：

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

2. （選用）使用下列describe-load-balancers命令來驗證政策是否已停用：

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

回應包含下列資訊，其中說明無連接埠與政策相關聯。

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

標記您的 Classic Load Balancer

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。

您可以為每個 Classic Load Balancer 加上多個標籤。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。

目錄

標籤限制

以下基本限制適用於標籤：

- 每一資源標籤數上限：50
- 索引鍵長度上限：127 個 Unicode 字元
- 數值長度上限：255 個 Unicode 字元
- 標籤鍵與值皆區分大小寫。允許字元為字母、空格和數字，以 UTF-8 表示，加上下列特殊字元：+ - = 。_ : / @。不可使用結尾或前方空格。
- 請勿在標籤名稱或值中使用 `aws:` 字首，因為已保留供 AWS 使用。您不可編輯或刪除具此字首的標籤名稱或值。具此字首的標籤，不算在受資源限制的標籤計數內。

新增標籤

您也可以在任何時間內將自己的標籤新增至負載平衡器。

使用主控台新增標籤

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在 Tags (標籤) 索引標籤上，選擇 Manage tags (管理標籤)。
5. 在管理標籤頁面上，針對每個標籤，選擇新增標籤，然後指定索引鍵和值。
6. 當您完成新增標籤的作業後，請選擇儲存變更。

使用 新增標籤 AWS CLI

使用以下 create-tags 命令來新增特定標籤：

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

移除標籤

您可以在您使用完時從負載平衡器刪除標籤。

使用主控台刪除標籤

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在 Tags (標籤) 索引標籤上，選擇 Manage tags (管理標籤)。
5. 在管理標籤頁面上，在每一個您想要移除的標籤旁選擇移除。
6. 當您完成移除標籤的作業後，請選擇儲存變更。

使用 移除標籤 AWS CLI

使用以下 remove-tags 命令刪除具有指定金鑰的標籤：

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

設定 Classic Load Balancer 的子網路

當您新增子網路至負載平衡器時，Elastic Load Balancing 會在該可用區域內建立負載平衡器節點。負載平衡器節點接受來自用戶端的流量，然後將請求轉送到一或多個可用區域中運作狀態良好的已註冊執行個體。我們建議您為每個可用區域新增一個子網路，以用於至少兩個可用區域。這可提高負載平衡器的可用性。請注意您可以隨時為您的負載平衡器修改子網路。

從和您的執行個體相同的可用區域中選取子網路。如果您的負載平衡器是面向網際網路的負載平衡器，您必須選擇公有子網路以便您的後端執行個體接收流量負載平衡器 (即使後端執行個體位於私有子網路)。如果您的負載平衡器是內部負載平衡器，我們建議您選擇私有子網路。負載平衡器的子網路詳細資訊，請參閱為您的建議 VPC。

若要新增子網路，請使用負載平衡器註冊可用區域中的執行個體，然後將子網路從該可用區域連接至負載平衡器。如需詳細資訊，請參閱使用 Classic Load Balancer 註冊執行個體。

當您新增子望路之後，負載平衡器會開始將請求路由傳送到該相關可用區域內已註冊的執行個體。根據預設，負載平衡器會將請求均勻地分散到其子網路的可用區域。若要路由請求均勻地分散到已註冊的子網路可用區域中的執行個體，啟用跨區域負載平衡。如需詳細資訊，請參閱為 Classic Load Balancer 設定跨區域負載平衡。。

您可能想要暫時從您的負載平衡器移除子望路，當您有運作狀態不佳的可用區域或您想進行故障排除或更新註冊執行個體時。您已移除可用區域之後，負載平衡器會停止路由請求至已註冊的執行個體的可用

區域，但持續將請求路由到已註冊的執行個體的剩餘子網路。請注意，移除子網路後，該子網路中的執行個體仍會向負載平衡器註冊，但您可以選擇取消註冊。如需詳細資訊，請參閱使用 Classic Load Balancer 註冊執行個體。

目錄

要求

當您更新您的負載平衡器的子網路，您必須符合下列要求：

- 負載平衡器必須擁有至少一個子網路。
- 一個可用區域最多可新增一個子網路。
- 您無法新增本機區域子網路。

由於從負載平衡器APIs新增和移除子網路是分開的，因此在將目前子網路換成新子網路時，您必須仔細考慮操作順序，才能符合這些需求。此外，您必須從另一個可用區域暫時新增子網路，如果您需要交換所有子網路適用於您的負載平衡器。例如，如果您的負載平衡器有單一可用區域，您需要交換另一個子網路的子網路，您必須先從第二個可用區域。新增另一個子網路。然後，您可以從原始可用區域移除子網路(不用低於一個子網路)、從原始可用區域新增新的子網路 (超出每個可用區域的一個子網路)，然後從第二個可用區域移除子網路 (如果只需要執行交換)。

使用主控台設定子網路

使用下列程序，使用主控台新增或移除子網路。

使用主控台設定子網路

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在網路映射索引標籤中，選擇編輯子網路。
5. 在編輯子網路頁面的網路映射區段中，視需要新增和移除子網路。
6. 完成時，請選擇 Save changes (儲存變更)。

使用 設定子網路 CLI

使用下列範例，使用 新增或移除子網路 AWS CLI。

若要使用 將子網路新增至負載平衡器 CLI

使用下列 attach-load-balancer-to-subnets 命令，將兩個子網路新增至負載平衡器：

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

負載平衡器的所有子網路的回應清單。例如：

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

使用 移除子網路 AWS CLI

使用下列 detach-load-balancer-from-subnets 命令，從指定的負載平衡器移除指定的子網路：

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

負載平衡器的剩餘子網路的回應清單。例如：

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

設定您的 Classic Load Balancer 的安全群組

當您使用 AWS Management Console 建立負載平衡器時，您可以選擇現有的安全群組或建立新的安全群組。如果您選擇現有的安全群組，則必須允許雙向流量至接聽程式和負載平衡器的運作狀態檢查連接埠。如果您選擇建立安全群組，主控台會自動新增規則以允許這些連接埠的所有流量。

【非預設 VPC】 如果您在非預設 中使用 AWS CLI 或API建立負載平衡器VPC，但未指定安全群組，您的負載平衡器會自動與 的預設安全群組建立關聯VPC。

【預設 VPC】 如果您使用 AWS CLI 或 API 在預設 中建立負載平衡器VPC，則無法為負載平衡器選擇現有的安全群組。反之，Elastic Load Balancing 會提供具有規則的安全群組，以允許負載平衡器的指定連接埠上所有流量。Elastic Load Balancing 每個 AWS 帳戶只會建立一個這類安全群組，其名稱為 default_elb_*id*（例如 `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`）。您在預設中建立的後續負載平衡器VPC也會使用此安全群組。請務必檢閱安全群組規則，以確保它們允許流量在適用於新的負載平衡器的接聽程式和運作狀態檢查連接埠。當您刪除負載平衡器時，此安全群組不會自動刪除。

如果您新增接聽程式到現有的負載平衡器，您必須檢閱您的安全群組，以確保它們允許流量在新的雙向接聽連接埠。

目錄

負載平衡器安全群組的建議規則

您的負載平衡器的安全群組必須允許它們與您的執行個體進行通訊。建議的規則取決於負載平衡器的類型、面向網際網路或內部。

面向網際網路的負載平衡器

下表顯示面向網際網路的負載平衡器的建議傳入規則。

來源	通訊協定	連接埠範圍	註解
0.0.0.0/0	TCP	*listener*	在負載平衡器接聽程式連接埠上允許所有傳入流量

下表顯示面向網際網路的負載平衡器的建議傳出規則。

目的地	通訊協定	連接埠範圍	註解
instance security group	TCP	*instance listener*	在執行個體接聽程式連接埠上允許流向執行個體的傳出流量
instance security group	TCP	*health check*	在運作狀態檢查連接埠上允許流向執行個體的傳出流量

內部負載平衡器

下表顯示內部負載平衡器的建議傳入規則。

來源	通訊協定	連接埠範圍	註解
VPC CIDR	TCP	*listener*	允許負載平衡器接聽程式連接埠VPCCIDR上來自 的傳入流量

下表顯示內部負載平衡器的建議傳出規則。

目的地	通訊協定	連接埠範圍	註解
instance security group	TCP	*instance listener*	在執行個體接聽程式連接埠上允許流向執行個體的傳出流量
instance security group	TCP	*health check*	在運作狀態檢查連接埠上允許流向執行個體的傳出流量

使用主控台指派安全群組

使用下列程序變更與負載平衡器相關聯的安全群組。

使用主控台更新指派給負載平衡器的安全群組

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在安全性索引標籤中，選擇編輯。
5. 在編輯安全群組頁面的安全群組 下，視需要新增或移除安全群組。

   您最多可以新增五個安全群組。
6. 完成時，請選擇 Save changes (儲存變更)。

使用 指派安全群組 AWS CLI

使用下列 apply-security-groups-to-load-balancer 命令，將安全群組與負載平衡器建立關聯。指定的安全群組會覆寫先前關聯的安全群組。

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

以下是回應範例：

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

設定 Classic Load Balancer ACLs 的網路

的預設網路存取控制清單 （ACL） VPC 允許所有傳入和傳出流量。如果您建立自訂網路 ACLs，則必須新增允許負載平衡器和執行個體通訊的規則。

負載平衡器子網路的建議規則取決於負載平衡器的類型、面向網際網路或內部。

面向網際網路的負載平衡器

以下是面向網際網路的負載平衡器的建議傳入規則。

來源	通訊協定	連接埠範圍	註解
0.0.0.0/0	TCP	*listener*	在負載平衡器接聽程式連接埠上允許所有傳入流量
VPC CIDR	TCP	1024-65535	允許暫時連接埠VPCCIDR上來自 的傳入流量

以下是面向網際網路的負載平衡器的建議傳出規則。

目的地	通訊協定	連接埠範圍	註解
VPC CIDR	TCP	*instance listener*	允許執行個體接聽程式連接埠上所有傳出流量
VPC CIDR	TCP	*health check*	允許運作狀態檢查連接埠上的所有傳出流量
0.0.0.0/0	TCP	1024-65535	允許暫時性連接埠上所有傳出流量

內部負載平衡器

以下是內部負載平衡器的建議傳入規則。

來源	通訊協定	連接埠範圍	註解
VPC CIDR	TCP	*listener*	允許負載平衡器接聽程式連接埠VPCCIDR上來自 的傳入流量
VPC CIDR	TCP	1024-65535	允許暫時連接埠VPCCIDR上來自 的傳入流量

以下是內部負載平衡器的建議傳出規則。

目的地	通訊協定	連接埠範圍	註解
VPC CIDR	TCP	*instance listener*	允許傳出流量至執行個體接聽程式連接埠VPCCIDR上的
VPC CIDR	TCP	*health check*	允許對運作狀態檢查連接埠VPCCIDR上的 傳出流量
VPC CIDR	TCP	1024-65535	允許暫時連接埠VPCCIDR上 的傳出流量

設定適用於您的 Classic Load Balancer 的自訂網域名稱

每個 Classic Load Balancer 都會收到預設網域名稱系統（DNS）名稱。此DNS名稱包含建立負載平衡器 AWS 的區域名稱。例如，如果您在美國西部（奧勒岡）區域中建立名為 `my-loadbalancer`的負載平衡器，您的負載平衡器會收到DNS名稱，例如 `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com`。若要存取執行個體上的網站，請將此DNS名稱貼到 Web 瀏覽器的地址欄位中。不過，此DNS名稱並不容易讓客戶記住和使用。

如果您想要為負載平衡器使用易記DNS的名稱，例如 `www.example.com`，而非預設DNS名稱，您可以建立自訂網域名稱，並將其與負載平衡器DNS的名稱建立關聯。當用戶端使用此自訂網域名稱提出請求時，DNS伺服器會將其解析為負載平衡器DNS的名稱。

目錄

將您的自訂網域名稱與您的負載平衡器名稱建立關聯

首先，如果您尚未這麼做，請註冊您的網域名稱。Internet Corporation for Assigned Names and Numbers（ICANN）會管理網際網路上的網域名稱。您可以使用網域名稱註冊商 註冊網域名稱，這是ICANN認可的組織，可管理網域名稱的登錄。您的網站註冊商網站將為註冊您的網域名稱提供詳細指示和定價資訊。如需詳細資訊，請參閱下列資源：

- 若要使用 Amazon Route 53 註冊網域名稱，請參閱 Amazon Route 53 開發人員指南中的使用 Route 53 註冊網域名稱。
- 如需這類註冊機構的清單，請參閱認可的註冊機構目錄。

接下來，使用您的 DNS服務，例如網域註冊商，建立CNAME記錄以將查詢路由至負載平衡器。如需詳細資訊，請參閱 DNS服務的文件。

或者，您可以使用 Route 53 作為DNS服務。您可以建立託管區域，其中包含如何在網際網路上路由傳送網域流量的相關資訊，以及別名資源記錄集，可將網域名稱的查詢路由傳送至負載平衡器。Route 53 不會針對別名記錄集的DNS查詢收費，而且您可以使用別名記錄集，將DNS查詢路由至網域區域頂點的負載平衡器（例如 `example.com`）。如需將現有網域DNS的服務轉移至 Route 53 的相關資訊，請參閱 Amazon Route 53 開發人員指南 中的將 Route 53 設定為您的DNS服務。

最後，使用 Route 53 為您的網域建立託管區域和別名記錄集。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的將流量路由到負載平衡器。

針對負載平衡器使用 Route 53 DNS 容錯移轉

如果您使用 Route 53 將DNS查詢路由至負載平衡器，也可以使用 Route 53 為負載平衡器設定DNS容錯移轉。在容錯移轉組態中，Route 53 會檢查負載平衡器已註冊EC2執行個體的運作狀態，以判斷是否可用。如果沒有向負載平衡器註冊的健全EC2執行個體，或者負載平衡器本身運作狀態不佳，Route 53 會將流量路由至其他可用資源，例如運作狀態良好的負載平衡器或 Amazon S3 中的靜態網站。

例如，假設您有一個 `www.example.com` Web 應用程式，而且您需要在後方執行兩個負載平衡器備援執行個體，位於不同的區域。您希望流量在一個區域主要路由到負載平衡器，而且您想要在其他區域使用負載平衡器，以供失敗時備份。如果您設定DNS容錯移轉，則可以指定主要和次要（備份）負載平衡器。Route 53 會引導流量到可用的主要負載平衡器，或是次要負載平衡器。

使用「評估目標運作狀態」

- 當「評估目標運作狀態」設定為 Classic Load Balancer 別名記錄上的 `Yes` 時，Route 53 會評估 `alias target` 值所指定資源的運作狀態。針對 Classic Load Balancer，Route 53 會使用與負載平衡器關聯的執行個體運作狀態檢查。
- 當 Classic Load Balancer 中至少有一個註冊的執行個體運作狀態良好時，Route 53 會將別名記錄標記為運作狀態良好。之後，Route 53 會根據您的路由政策傳回記錄。如果使用容錯移轉路由政策，則 Route 53 會傳回主要記錄。

- 當 Classic Load Balancer 中所有註冊的執行個體均運作狀態不佳時，Route 53 會將別名記錄標記為運作狀態不佳。之後，Route 53 會根據您的路由政策傳回記錄。如果使用容錯移轉路由政策，則 Route 53 會傳回次要記錄。

如需詳細資訊，請參閱 Amazon Route 53 開發人員指南 中的設定DNS容錯移轉。

將您的自訂網域名稱與您的負載平衡器名稱取消關聯

您可以從負載平衡器執行個體取消您的自訂網域名稱，方法是先在您的託管區域的資源紀錄集刪除，然後刪除託管區域。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的編輯記錄和刪除公有託管區域。

Classic Load Balancer 的接聽程式

開始使用 Elastic Load Balancing 之前，您必須為 Classic Load Balancer 設定一或多個接聽程式。接聽程式是檢查連線請求的程序。它是透過一個前端 (用戶端到負載平衡器) 連線的協定和連接埠，以及一個後端 (負載平衡器到後端執行個體) 連線的協定和連接埠進行設定。

Elastic Load Balancing 支援以下通訊協定：

- HTTP
- HTTPS（安全HTTP）
- TCP
- SSL（安全TCP）

該HTTPS協議使用該SSL協議在該HTTP層上建立安全連接。您也可以使用通SSL訊協定在TCP層上建立安全連線。

如果前端連線使用TCP或SSL，則後端連線可以使用TCP或SSL。如果前端連線使用HTTP或HTTPS，則後端連線可以使用HTTP或HTTPS。

後端執行個體可以在連接埠 1-65535 上監聽。

可以在以下連接埠上接聽負載平衡器：1-65535

目錄

通訊協定

一般 Web 應用程式的通訊都會通過硬體和軟體層。每一層提供特定的通訊功能。通訊功能的控制權會從一個 layer 依序傳遞到下一個。開放系統互連（OSI）定義了一個模型框架，用於實現通信的標準格式，稱為協議，在這些層。有關更多信息，請參閱維基百科中的OSI模型。

當使用 Elastic Load Balancing 時，您需要對 Layer 4 和 Layer 7 有基本了解。第 4 層是說明用戶端與後端執行個體之間透過負載平衡器之間的傳輸控制通訊協定 (TCP) 連線的傳輸層。第 4 層是負載平衡

器是可設定的最低層級。第 7 層是一個應用程式層，說明如何使用從用戶端到負載平HTTP衡器，以及從負載平衡器到後端執行個體的超文字傳輸通訊協定 HTTPS (HTTP) 和 (安全) 連線。

安全通訊端層 (SSL) 通訊協定主要用於透過不安全的網路 (例如網際網路) 加密機密資料。該SSL協議在客戶端和後端服務器之間建立安全連接，並確保客戶端和服務器之間傳遞的所有數據都是私有且整合的。

TCP/SSL協議

當您同時針對前端和後端連線使用 TCP (第 4 層) 時，負載平衡器會將要求轉送至後端執行個體，而不需修改標頭。負載平衡器收到要求之後，它會嘗試在接聽程式組態中指定的TCP連接埠上開啟後端執行個體的連線。

因為負載平衡器會攔截用戶端與後端執行個體的流量，所以後端執行個體存取日誌 (適用於包含負載平衡器的 IP 地址，而不包含來源用戶端的後端執行個體)。您可以啟用 Proxy Protocol，其新增含用戶端連線資訊的標題，例如來源 IP 地址、目的地 IP 地址和連接埠號碼。然後標頭會做為請求的一部分傳送到後端執行個體。您可以剖析請求中的第一行以擷取連線資訊。如需詳細資訊，請參閱設定 Classic Load Balancer 的代理通訊協定。

使用此組態時，您不會收到工作階段黏著性或 X-Forwarded 標頭的 Cookie。

HTTP/HTTPS協議

當您同時針對前端和後端連線使用 HTTP (第 7 層) 時，負載平衡器會先剖析要求中的標頭，再將要求傳送至後端執行個體。

對於HTTP/HTTPS負載平衡器後面的每個已註冊且運作良好的執行個體，Elastic Load Balancing 會開啟並維護一或多個TCP連線。這些連接確保始終有一個已建立的連接準備好接收HTTP/HTTPS請求。

HTTP請求和HTTP響應使用標題字段發送有關HTTP消息的信息。Elastic Load Balancing 支援 `X-Forwarded-For` 標頭。由於負載平衡器攔截用戶端和伺服器之間的流量，您的伺服器存取日誌僅包含負載平衡器的 IP 地址。若要查看用戶端的 IP 地址，請使用 `X-Forwarded-For` 請求標頭。如需詳細資訊，請參閱X-Forwarded-For。

當您使用HTTP/時HTTPS，您可以在負載平衡器上啟用黏性工作階段。黏性工作階段會將使用者工作階段繫結至特定的後端執行個體。這樣能確保該工作階段期間所有來自使用者的請求都能傳送到相同的後端執行個體。如需詳細資訊，請參閱為 Classic Load Balancer 設定黏性工作階段。

並非所有HTTP擴充功能都受到負載平衡器的支援。如果負載平衡器由於非預期的方法、回應代碼或其他非標準 HTTP 1.0/1.1 實作而無法終止要求，您可能需要使用TCP偵聽程式。

HTTPS/SSL聽眾

您可以使用以下安全功能建立負載平衡器。

SSL伺服器憑證

如果您SSL為前端連線使用HTTPS或，則必須在負載平衡器上部署 X.509 憑證 (SSL伺服器憑證)。負載平衡器會先將用戶端的要求解密，然後再將其傳送至後端執行個體 (稱為SSL終止)。如需詳細資訊，請參閱SSLClassic Load Balancer 的 /TLS 憑證。

如果您不希望負載平衡器處理SSL終止 (稱為SSL卸載)，您可以同時用TCP於前端和後端連線，並在處理要求的已註冊執行個體上部署憑證。

SSL談判

Elastic Load Balancing 提供預先定義的SSL交SSL涉組態，用於在用戶端與負載平衡器之間建立連線時進行交涉。SSL協商組態提供與廣泛用戶端的相容性，並使用稱為加密的高強度加密演算法。不過，一些使用案例可能需要網路上的所有資料進行加密，並且僅允許特定加密。某些安全性符合標準 (例如PCISOX、等) 可能需要用戶端提供一組特定的通訊協定和密碼，以確保符合安全性標準。在這種情況下，您可以根據您的特定需求建立自訂SSL交涉組態。您的加密和通訊協定應該會在 30 秒內生效。如需詳細資訊，請參閱SSL Classic Load Balancer 的交涉組態。

後端伺服器身分驗證

如果您使用HTTPS或SSL進行後端連線，則可以啟用已註冊執行個體的驗證。然後，您可以使用身分驗證程序來確保執行個體只接受加密的通訊，並確保每個註冊執行個體具有正確的公有金鑰。

如需詳細資訊，請參閱設定後端伺服器驗證。

Classic Load Balancer 的接聽程式組態

下表說明 Classic Load Balancer 的可能組態HTTP和HTTPS接聽程式。

使用案例	前端通訊協定	前端選項	後端通訊協定	後端選項	備註
基本HTTP負載平衡器	HTTP	NA	HTTP	NA	• 支援 X-Forwarded 標頭

使用案例	前端通訊協定	前端選項	後端通訊協定	後端選項	備註
使用 Elastic Load Balancing 來卸載SSL解密，保護網站或應用程式	HTTPS	SSL談判	HTTP	NA	• 支援 X-Forwarded 標頭 • 需要在負載平衡器上部署的SSL憑證
使用 end-to-end 加密保護網站或應用程式	HTTPS	SSL談判	HTTPS	後端身分驗證	• 支援 X-Forwarded 標頭 • 需要在負載平衡器和已註冊執行個體上部署的SSL憑證

下表說明 Classic Load Balancer 的可能組態TCP和SSL接聽程式。

使用案例	前端通訊協定	前端選項	後端通訊協定	後端選項	備註
基本TCP負載平衡器	TCP	NA	TCP	NA	• 支援 Proxy Protocol 標頭
使用 Elastic Load Balancing 來卸載SSL解密，保護網站或應用程式	SSL	SSL談判	TCP	NA	• 需要在負載平衡器上部署的SSL憑證 • 支援 Proxy Protocol 標頭

使用案例	前端通訊協定	前端選項	後端通訊協定	後端選項	備註
使用 Elastic Load Balancing end-to-end 加密來保護網站或應用程式	SSL	SSL談判	SSL	後端身分驗證	• 需要在負載平衡器和已註冊執行個體上部署的SSL憑證 • 不在後端SSL連線上插入SNI標頭 • 不支援 Proxy Protocol 標頭

HTTP標題和傳統負載平衡器

HTTP請求和HTTP響應使用標題字段發送有關HTTP消息的信息。標頭欄位是以冒號分隔的名稱值組，以歸位字元 (CR) 和換行 (LF) 分隔。標準的標HTTP頭欄位集在 RFC 2616「郵件標頭」中定義。還有非標準標HTTP頭可用（並自動添加），這些標題廣泛被應用程序使用。一些非標準標HTTP頭有一個`X-Forwarded`前綴。Classic Load Balancer 支援以下 `X-Forwarded` 標頭。

如需有關HTTP連線的詳細資訊，請參閱 E lastic Load Balancing 使用者指南中的要求路由。

必要條件

- 確認您的接聽程式設定支援 X-Forwarded 標頭。如需詳細資訊，請參閱Classic Load Balancer 的接聽程式組態。
- 設定您的 Web 伺服器至日誌用戶端 IP 地址。

X-Forwarded 標頭

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

X-Forwarded-For

X-Forwarded-For要求標頭會自動新增，並協助您在使用HTTP或HTTPS負載平衡器時識別用戶端的 IP 位址。由於負載平衡器攔截用戶端和伺服器之間的流量，您的伺服器存取日誌僅包含負載平衡器的 IP 地址。若要查看用戶端的 IP 地址，請使用 X-Forwarded-For 請求標頭。Elastic Load Balancing 會將用戶端的 IP 位址儲存在 X-Forwarded-For 請求標頭，並將標頭傳遞給您的伺服器。如果 X-Forwarded-For 請求標頭未包含在請求中，負載平衡器會以用戶端 IP 地址做為請求值建立請求標頭。否則，負載平衡器會將用戶端 IP 地址附加至現有標頭，並將標頭傳遞給您的伺服器。X-Forwarded-For 請求標頭可能包含以逗號分隔的多個 IP 地址。最左邊的地址是首先提出請求的用戶端 IP。後面則以鏈顯示所有接續的代理標識符。

X-Forwarded-For 請求標頭採用以下格式：

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

下列是具有 IP 地址 203.0.113.7 之用戶端的範例 X-Forwarded-For 請求標頭。

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

以下是IPv6地址為的客戶端的X-Forwarded-For請求標頭示例2001:DB8::21f:5bff:febf:ce22:8a2e。

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

X-Forwarded-Proto

X-Forwarded-Proto要求標頭可協助您識別用戶端用來連線到負載平衡器的通訊協定 (HTTP或HTTPS)。您的伺服器存取日誌僅包含在伺服器和負載平衡器之間使用的通訊協定，但不包含用戶端和負載平衡器之間使用的通訊協定相關資訊。若要判斷用戶端和負載平衡器之間使用的通訊協定，請使用 X-Forwarded-Proto 請求標頭。Elastic Load Balancing 會將用戶端和負載平衡器之間使用的通訊協定儲存在 X-Forwarded-Proto 請求標頭，並將標頭傳遞給您的伺服器。

您的應用程式或網站可以使用儲存在X-Forwarded-Proto要求標頭中的通訊協定來呈現重新導向至適當的回應URL。

X-Forwarded-Proto 請求標頭採用以下格式：

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

下列範例包含來自用戶端作為要求的要求的HTTPS要求標頭：`X-Forwarded-Proto`

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

X-Forwarded-Port

`X-Forwarded-Port` 請求標頭協助您識別用戶端用於連接到負載平衡器的目的地連接埠。

HTTPS Classic Load Balancer 的接聽程式

您可以建立使用 SSL/TLS 通訊協定進行加密連線的負載平衡器（也稱為SSL卸載）。此功能可啟用負載平衡器與啟動HTTPS工作階段的用戶端之間的流量加密，以及負載平衡器與EC2執行個體之間的連線。

Elastic Load Balancing 使用 Secure Sockets Layer（SSL）交涉組態，稱為安全政策，來交涉用戶端與負載平衡器之間的連線。當您針對前端連線使用 HTTPS/SSL 時，您可以使用預先定義的安全政策或自訂安全政策。您必須在負載平衡器上部署SSL憑證。負載平衡器使用此憑證終止連接，然後解密用戶端的請求，再將它們傳送到執行個體。負載平衡器將靜態加密套件用於後端連線。您可以選擇性地選擇在您的執行個體啟用身分驗證。

Classic Load Balancer 不支援伺服器名稱指示（SNI）。您可以改用下列其中一個替代選項：

- 在負載平衡器上部署一個憑證，並為每個額外的網站新增主體別名（SAN）。SANs 可讓您使用單一憑證來保護多個主機名稱。如需每個憑證SANs支援的數目以及如何新增和移除 的詳細資訊，請洽詢您的憑證提供者SANs。
- 使用連接埠 443 上的TCP接聽程式進行前端和後端連線。負載平衡器會照原樣傳遞請求，因此您可以處理EC2執行個體上的HTTPS終止。

Classic Load Balancer 不支援相互TLS身分驗證（m TLS）。對於 mTLS 支援，請建立TCP接聽程式。負載平衡器會照原樣傳遞請求，因此您可以在EC2執行個體上實作 mTLS。

目錄

SSLClassic Load Balancer 的 /TLS 憑證

如果您將 HTTPS（SSL 或 TLS）用於前端接聽程式，則必須在負載平衡器上部署 SSL/TLS 憑證。負載平衡器使用此憑證終止連接，然後解密用戶端的請求，再將它們傳送到執行個體。

SSL 和 TLS通訊協定使用 X.509 憑證（SSL/TLS 伺服器憑證）來驗證用戶端和後端應用程式。X.509 憑證是憑證授權機構 (CA) 發出的數位身分證，其中包含識別資訊、有效期間、公有金鑰、序號和發行機構的數位簽章。

您可以使用 AWS Certificate Manager 或支援 SSL和 TLS通訊協定的工具來建立憑證，例如 Open SSL。當您為負載平衡器建立或更新HTTPS接聽程式時，您將指定此憑證。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。憑證上的網域名稱必須與自訂網域名稱記錄相符。如果不相符，將不會加密流量，因為無法驗證TLS連線。

您必須為憑證指定完整網域名稱（FQDN），例如 `www.example.com`或 apex 網域名稱，例如 `example.com`。您也可以使用星號 (*) 做為萬用字元，以保護相同網域中的多個網站名稱。請求萬用字元憑證時，星號 (*) 必須在網域名稱的最左方，而且僅能保護一個子網域層級。例如，`*.example.com` 保護 `corp.example.com` 和 `images.example.com`，但它無法保護 `test.login.example.com`。另請注意，`*.example.com` 只可以保護 `example.com` 的子網域，無法保護 bare 或 apex 網域 (`example.com`)。萬用字元名稱會顯示於 ACM 憑證的主體欄位和憑證的主體別名延伸。如需公有憑證的詳細資訊，請參閱 AWS Certificate Manager 使用者指南中的請求公有憑證。

使用 建立或匯入 SSL/TLS 憑證 AWS Certificate Manager

建議您使用 AWS Certificate Manager（ACM）來建立或匯入負載平衡器的憑證。ACM 與 Elastic Load Balancing 整合，讓您可以在負載平衡器上部署憑證。若要在負載平衡器上部署憑證，此憑證必須位於和負載平衡器同一個區域。如需詳細資訊，請參閱《AWS Certificate Manager 使用者指南》中的請求公有憑證或匯入憑證。

若要允許使用者使用 在負載平衡器上部署憑證 AWS Management Console，您必須允許存取 ACM`ListCertificates`API動作。如需詳細資訊，請參閱 AWS Certificate Manager 使用者指南中的列出憑證。

> **Important**
>
> 您無法透過與 的整合，在負載平衡器上安裝具有 4096 位元RSA金鑰或 EC 金鑰的憑證ACM。您必須將具有 4096 位元RSA金鑰或 EC 金鑰的憑證上傳至 IAM ，才能搭配負載平衡器使用。

使用 匯入 SSL/TLS 憑證 IAM

如果您不使用 ACM，則可以使用 SSL/TLS 工具，例如 Open SSL來建立憑證簽署請求 （CSR）、取得 CA CSR簽署來產生憑證，並將憑證上傳到 IAM。如需詳細資訊，請參閱 IAM 使用者指南 中的使用伺服器憑證。

SSL Classic Load Balancer 的交涉組態

Elastic Load Balancing 使用 Secure Socket Layer （SSL） 交涉組態，稱為安全政策 ，來交涉用戶端與負載平衡器之間的SSL連線。安全政策是SSL通訊協定、SSL密碼和 Server Order 偏好設定選項的組合。如需為負載平衡器設定SSL連線的詳細資訊，請參閱 Classic Load Balancer 的接聽程式。

目錄

安全政策

安全政策會決定用戶端與負載平衡器之間的SSL交涉期間支援哪些密碼和通訊協定。您可以設定 Classic Load Balancer 使用預先定義或自訂安全政策。

請注意， AWS Certificate Manager （ACM） 提供的憑證包含RSA公有金鑰。因此，如果您使用 提供的憑證，則必須在安全政策RSA中使用密碼套件ACM；否則，TLS連線會失敗。

預先定義的安全政策

最新的預先定義安全政策名稱包含根據年和月發佈的版本資訊。例如，預設的預先定義安全政策為 `ELBSecurityPolicy-2016-08`。每當發佈新的預先定義安全政策時，您可以更新設定以使用它。

如需為預先定義安全政策啟用通訊協定和加密的相關詳細資訊，請參閱Classic Load Balancer 的預先定義SSL安全政策。

自訂安全政策

您可以建立含所需的加密方式和通訊協定的自訂溝通組態。例如，某些安全合規標準（例如 PCI和 SOC）可能需要一組特定的通訊協定和密碼，以確保符合安全標準。在這種情況下，您可以建立自訂安全政策以符合這些標準。

如需建立自訂安全政策的詳細資訊，請參閱更新 Classic Load Balancer SSL 的交涉組態。

SSL 通訊協定

SSL 通訊協定會在用戶端和伺服器之間建立安全連線，並確保用戶端和負載平衡器之間傳遞的所有資料皆為私有。

Secure Sockets Layer（SSL）和 Transport Layer Security（TLS）是密碼編譯通訊協定，用於透過網際網路等不安全的網路加密機密資料。TLS 通訊協定是新版的SSL通訊協定。在 Elastic Load Balancing 文件中，我們將 SSL和 TLS通訊協定稱為SSL通訊協定。

建議的通訊協定

我們建議 TLS 1.2，用於 ELBSecurityPolicy-TLS-1-2-2017-01 預先定義的安全政策。您也可以在自訂安全政策中使用 TLS 1.2。預設安全政策同時支援 TLS 1.2 和舊版TLS，因此其安全性低於 ELBSecurityPolicy-TLS-1-2-2017-01。

已廢除的通訊協定

如果您先前已在自訂政策中啟用 SSL 2.0 通訊協定，建議您將安全政策更新為其中一個預先定義的安全政策。

伺服器優先順序

Elastic Load Balancing 支援適用於用戶端和負載平衡器之間溝通連線的伺服器優先順序選項。在SSL連線交涉過程中，用戶端和負載平衡器會依偏好列出他們各自支援的加密和通訊協定清單。根據預設，用戶端清單上符合任何一個負載平衡器密碼的第一個密碼會選取用於SSL連線。如果負載平衡器設定為支援伺服器優先順序，則該負載平衡器會在清單中 (亦即用戶端加密清單) 選擇第一個加密。這可確保負載平衡器決定用於SSL連線的密碼。如果您不啟用伺服器優先順序，用戶端顯示的加密順序是用於溝通用戶端和負載平衡器之間的連線。

SSL 密碼

SSL 密碼是一種加密演算法，使用加密金鑰來建立編碼訊息。SSL 通訊協定使用數個SSL密碼來加密網際網路上的資料。

請注意， AWS Certificate Manager （ACM） 提供的憑證包含RSA公有金鑰。因此，如果您使用 提供的憑證，則必須在安全政策RSA中使用密碼套件ACM；否則，TLS連線會失敗。

Elastic Load Balancing 支援下列可與 Classic Load Balancer 搭配使用的加密方式。這些密碼的子集會由預先定義的SSL政策使用。所有這些加密方式可用於自訂政策。我們建議您使用僅使用包含在預設安全政策 (加星號者) 的加密方式。許多其他加密方式並不安全，應自擔風險來使用。

加密方式

- 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 *
- DHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-GCM-SHA384 *
- ECDHE-RSA-AES256-GCM-SHA384 *
- ECDHE-ECDSA-AES256-SHA384 *
- ECDHE-RSA-AES256-SHA384 *
- ECDHE-RSA-AES256-SHA *
- ECDHE-ECDSA-AES256-SHA *
- AES128-GCM-SHA256 *
- AES128-SHA256 *
- AES128-SHA *
- AES256-GCM-SHA384 *
- AES256-SHA256 *
- AES256-SHA *
- DHE-DSS-AES128-SHA

- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- ECDHE-RSA-RC4-SHA
- RC4-SHA
- ECDHE-ECDSA-RC4-SHA
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-DSS-CAMELLIA256-SHA
- CAMELLIA256-SHA
- EDH-DSS-DES-CBC3-SHA
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DHE-RSA-CAMELLIA128-SHA
- DHE-DSS-CAMELLIA128-SHA
- ADH-AES128-GCM-SHA256
- ADH-AES128-SHA
- ADH-AES128-SHA256
- ADH-AES256-GCM-SHA384
- ADH-AES256-SHA
- ADH-AES256-SHA256
- ADH-CAMELLIA128-SHA
- ADH-CAMELLIA256-SHA

- ADH-DES-CBC3-SHA
- 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-AES256-CBC-SHA
- PSK-3DES-EDE-CBC-SHA
- KRB5-DES-CBC3-SHA
- KRB5-DES-CBC3-MD5
- PSK-AES128-CBC-SHA
- PSK-RC4-SHA
- KRB5-RC4-SHA
- 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-RC2-CBC-MD5

- EXP-KRB5-RC2-CBC-SHA
- EXP-KRB5-DES-CBC-SHA
- EXP-KRB5-RC2-CBC-MD5
- EXP-KRB5-DES-CBC-MD5
- EXP-ADH-RC4-MD5
- EXP-RC4-MD5
- EXP-KRB5-RC4-SHA
- EXP-KRB5-RC4-MD5

* 這些是預設安全政策 ELBSecurityPolicy-2016-08 中包含的密碼。

Classic Load Balancer 的預先定義SSL安全政策

您可以為 HTTPS/SSL 接聽程式選擇其中一個預先定義的安全政策。您可以使用其中一個`ELBSecurityPolicy-TLS`政策來符合需要停用特定TLS通訊協定版本的合規和安全標準。或者，您也可以建立自訂安全政策。如需詳細資訊，請參閱更新交SSL涉組態。

- RSA和 DSA型密碼是用來建立SSL憑證的簽署演算法特有的。請務必使用以安全政策啟用的密碼為基礎的簽署演算法來建立SSL憑證。

如果您選擇的政策已針對伺服器優先順序而啟用，負載平衡器會依此處指定的順序使用加密方式來溝通協調用戶端和負載平衡器之間的連線。否則，負載平衡器會依用戶端列出的順序使用加密。

下列各節說明 Classic Load Balancer 的最新預先定義安全政策，包括其已啟用的SSL通訊協定和SSL密碼。您也可以使用 describe-load-balancer-policies命令描述預先定義的政策。

> **Tip**
>
> 此資訊僅適用於 Classic Load Balancer。如需適用於其他負載平衡器的資訊，請參閱 Application Load Balancer 的安全政策，以及 Network Load Balancer 的安全政策。

目錄

依政策的通訊協定

下表說明每個安全政策支援的TLS通訊協定。

安全政策	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS-1-2-2017-01	是	否	否
ELBSecurityPolicy-TLS-1-1-2017-01	是	是	否
ELBSecurityPolicy-2016 年 8 月	是	是	是
ELBSecurityPolicy-2015 年 5 月	是	是	是
ELBSecurityPolicy-2015 年 3 月	是	是	是
ELBSecurityPolicy-2015 年 2 月	是	是	是

依政策的 Ciphers

下表說明每個安全政策支援的密碼。

安全政策	加密方式
ELBSecurityPolicy-TLS-1-2-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384

安全政策	加密方式
	• ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA
ELBSecurityPolicy-TLS-1-1-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全政策	加密方式
ELBSecurityPolicy-2016 年 8 月	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全政策	加密方式
ELBSecurityPolicy-2015 年 5 月	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DES-CBC3-SHA

安全政策	加密方式
ELBSecurityPolicy-2015 年 3 月	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DHE-RSA-AES128-SHA • DHE-DSS-AES128-SHA • DES-CBC3-SHA

安全政策	加密方式
ELBSecurityPolicy-2015 年 2 月	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DHE-RSA-AES128-SHA • DHE-DSS-AES128-SHA

依密碼顯示政策

下表說明支援每個密碼的安全政策。

密碼名稱	安全政策	密碼套件
開啟SSL – ECDHE-ECDSA-AES128-GCM-SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月	c02b

密碼名稱	安全政策	密碼套件
IANA – TLS_ECDHE_ECDSA_WITHAES__128_GCM_SHA256	• ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	
開啟SSL – ECDHE-RSA-AES128-GCM-SHA256 IANA – TLS_ECDHE_RSA_WITHAES__128_GCM_SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c02f
開啟SSL – ECDHE-ECDSA-AES128-SHA256 IANA – TLS_ECDHE_ECDSA_WITHAES__128_CBC_SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c023
開啟SSL – ECDHE-RSA-AES128-SHA256 IANA – TLS_ECDHE_RSA_WITHAES__128_CBC_SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c027
開啟SSL – ECDHE-ECDSA-AES128-SHA IANA – TLS_ECDHE_ECDSA_WITHAES__128_CBC_SHA	• ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c009

密碼名稱	安全政策	密碼套件
開啟SSL – ECDHE-RSA-AES128-SHA IANA – TLS_ECDHE_RSA_WITH AES__128_CBC_SHA	• ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c013
開啟SSL – ECDHE-ECDSA-AES256-GCM-SHA384 IANA – TLS_ECDHE_ECDSA_WI TH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c02c
開啟SSL – ECDHE-RSA-AES256-GCM-SHA384 IANA – TLS_ECDHE_RSA_WITH _AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c030
開啟SSL – ECDHE-ECDSA-AES256-SHA384 IANA – TLS_ECDHE_ECDSA_WI TH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c024

密碼名稱	安全政策	密碼套件
開啟SSL – ECDHE-RSA-AES256-SHA384 IANA – TLS_ECDHE_RSA_WITH AES__256_CBC_SHA384	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c028
開啟SSL – ECDHE-ECDSA-AES256-SHA IANA – TLS_ECDHE_RSA_WITH _AES_256_CBC_SHA	• ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c014
開啟SSL – ECDHE-RSA-AES256-SHA IANA – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	c00a
開啟SSL – AES128-GCM-SHA256 IANA – TLS_RSA_WITHAES_128_GCM_SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	9c

密碼名稱	安全政策	密碼套件
開啟SSL – AES128-SHA256 IANA – TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	3c
開啟SSL – AES128-SHA IANA – TLS_RSA_WITHAES__128_CBC_SHA	• ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	2f
開啟SSL – AES256-GCM-SHA384 IANA – TLS_RSA_WITHAES__256_GCM_SHA384	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	9 天
開啟SSL – AES256-SHA256 IANA – TLS_RSA_WITHAES_256_CBC_SHA256	• ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	3d

密碼名稱	安全政策	密碼套件
開啟SSL – AES256-SHA IANA – TLS_RSA_WITHAES_256_CBC_SHA	• ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016 年 8 月 • ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	35
開啟SSL – DHE-RSA-AES128-SHA IANA – TLS_DHE_RSA_WITHAES__128_CBC_SHA	• ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	33
開啟SSL – DHE-DSS-AES128-SHA IANA – TLS_DHE_DSS_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-2015 年 3 月 • ELBSecurityPolicy-2015 年 2 月	32
開啟SSL – DES-CBC3-SHA IANA – TLS_RSAWITH_3DES_EDE_CBC_SHA	• ELBSecurityPolicy-2015 年 5 月 • ELBSecurityPolicy-2015 年 3 月	0a

使用HTTPS接聽程式建立 Classic Load Balancer

負載平衡器會從用戶端接收請求，並將其分佈到向負載平衡器註冊的EC2執行個體。

您可以建立在 HTTP（80） 和 HTTPS（443） 連接埠上監聽的負載平衡器。如果您指定HTTPS接聽程式將請求傳送至連接埠 80 上的執行個體，負載平衡器會終止請求，而且不會加密從負載平衡器到執行個體的通訊。如果HTTPS接聽程式將請求傳送至連接埠 443 上的執行個體，則會加密從負載平衡器到執行個體的通訊。

如果您的負載平衡器使用已加密的連線來與執行個體通訊，您就可以選擇性啟用執行個體的身分驗證。這可確保負載平衡器僅與執行個體通訊，若其公有金鑰符合您為此目的而指定到負載平衡器的金鑰的話。

如需將HTTPS接聽程式新增至現有負載平衡器的資訊，請參閱 設定 Classic Load Balancer 的HTTPS接聽程式。

目錄

必要條件

在開始使用之前，請確認您已符合以下必要條件：

- 完成「為您的建議 VPC」中的步驟。
- 啟動您計劃向負載平衡器註冊的EC2執行個體。這些執行個體的安全群組必須允許負載平衡器的流量。
- EC2 執行個體必須以HTTP狀態碼 200 回應運作狀態檢查的目標。如需詳細資訊，請參閱Classic Load Balancer 執行個體的 Health 狀態檢查。
- 如果您計劃在EC2執行個體上啟用保持連線選項，建議您將保持連線設定設為負載平衡器的至少閒置逾時設定。若您想要確保負載平衡器負責關閉您的執行個體連線，請確保持續連線時間適用之執行個體上的值集大於您的負載平衡器上的閒置逾時設定。如需詳細資訊，請參閱為 Classic Load Balancer 設定閒置連線逾時。
- 如果您建立安全接聽程式，則必須在負載平衡器上部署SSL伺服器憑證。負載平衡器使用此憑證以終止然後解密請求，再將它們傳送到執行個體。如果您沒有SSL憑證，您可以建立憑證。如需詳細資訊，請參閱SSLClassic Load Balancer 的 /TLS 憑證。

使用主控台建立HTTPS負載平衡器

在此範例中，您為負載平衡器設定兩個接聽程式。第一個接聽程式接受連接埠 80 上的HTTP請求，並使用 將其傳送至連接埠 80 上的執行個體HTTP。第二個接聽程式接受連接埠 443 上的HTTPS請求，並使用HTTP連接埠 80 （如果您想要設定後端執行個體身分驗證，也可以HTTPS在連接埠 443 上使用）將請求傳送至執行個體。

接聽程式是檢查連線請求的程序。它是透過一個前端 (用戶端到負載平衡器) 連線的協定和連接埠，以及一個後端 (負載平衡器到執行個體) 連線的協定和連接埠進行設定。如需有關 Elastic Load Balancing 支援的連接埠、通訊協定和接聽程式組態的詳細資訊，請參閱 Classic Load Balancer 的接聽程式。

使用主控台建立安全的 Classic Load Balancer

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

2. 於導覽列上，為負載平衡器選擇一個區域。請務必選取您為EC2執行個體選取的相同區域。
3. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
4. 選擇 Create Load Balancer (建立負載平衡器)。
5. 展開 Classic Load Balancer 區段，然後選擇建立。
6. 基本組態

   a. 針對負載平衡器名稱，輸入負載平衡器的名稱。

      在區域的 Classic Load Balancer 組合中，您的 Classic Load Balancer 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，但開頭或結尾都不可為連字號。

   b. 針對結構描述，選取面向網際網路。
7. 網路映射

   a. 針對 VPC，選取VPC您為執行個體選取的相同項目。

   b. 針對映射，先選取可用區域，然後從可用子網路中選擇公有子網路。一個可用區域只能選取一個子網路。為了提高您的負載平衡器可用性，可選取一個以上的可用區域和子網路。
8. 安全群組

   - 針對安全群組 ，選取已設定為允許連接埠 80 上所需HTTP流量和連接埠 443 上所需HTTPS流量的現有安全群組。

     如果沒有安全群組符合條件，您可以建立擁有必要規則的新安全群組。
9. 接聽程式和路由

   a. 保留預設接聽程式的預設設定，然後選取新增接聽程式。

   b. 針對新接聽程式上的接聽程式，請選取 HTTPS 做為通訊協定，然後連接埠會更新為 443。根據預設，執行個體會在連接埠 80 上使用 HTTP 通訊協定。

   c. 如果需要執行後端身分驗證，請將執行個體通訊協定變更為 HTTPS。這也會將執行個體連接埠更新為 443
10. 安全接聽程式設定

    當您SSL為前端接聽程式使用 HTTPS或 時，您必須在負載平衡器上部署SSL憑證。負載平衡器使用此憑證終止連接，然後解密用戶端的請求，再將它們傳送到執行個體。您也必須指定安全政策。Elastic Load Balancing SSL 提供具有預先定義交涉組態的安全政策，或者您可以建立自己的自訂安全政策。如果您在後端連線上設定 HTTPS/SSL，您可以啟用執行個體的身分驗證。

a. 對於安全政策 ，我們建議您一律使用最新的預先定義安全政策，或建立自訂政策。請參閱更新SSL協商組態。

b. 對於預設 SSL/TLS 憑證 ，可使用下列選項：

- 如果您使用 建立或匯入憑證 AWS Certificate Manager，請選取從 ACM，然後從選取憑證中選取憑證。
- 如果您使用 匯入憑證IAM，請選取從 IAM，然後從選取憑證 選取您的憑證。
- 如果您有要匯入的憑證，但您的區域ACM無法使用，請選取匯入 ，然後選取至 IAM。在憑證名稱欄位輸入憑證名稱。在憑證私有金鑰 中，複製並貼上私有金鑰檔案 （PEM編碼） 的內容。在憑證內文 中，複製並貼上公有金鑰憑證檔案 （PEM編碼） 的內容。在憑證鏈 中，複製並貼上憑證鏈檔案的內容 （PEM編碼），除非您使用自我簽署憑證，而且瀏覽器不一定要隱含接受憑證。

c. （選用） 如果您將HTTPS接聽程式設定為使用加密連線與執行個體通訊，則可以選擇性地在後端身分驗證憑證 中設定執行個體的身分驗證。

> **Note**
>
> 如果您沒有看到後端身分驗證憑證區段，請返回接聽程式和路由，然後選取 HTTPS 做為執行個體的通訊協定。

i. 針對 Certificate name (憑證名稱)，輸入公有金鑰憑證的名稱。

ii. 對於憑證內文 （PEM 編碼），請複製並貼上憑證的內容。如果公有金鑰符合此金鑰，負載平衡器只會與執行個體通訊。

iii. 若要新增另一個憑證，請選擇新增後端憑證。最多五個憑證。

11. 運作狀態檢查

a. 在 Ping 目標區段中，選取 Ping 通訊協定和 Ping 連接埠。您的EC2執行個體必須接受指定 ping 連接埠上的流量。

b. 針對 Ping 連接埠，請確定連接埠為 80。

c. 針對 Ping 路徑，請將預設值取代為單一政協線 (/)。這會告知 Elastic Load Balancing 將運作狀態檢查請求傳送給您 Web 伺服器的預設首頁，例如 `index.html`。

d. 針對進階運作狀態檢查設定，請使用預設值。

12. 執行個體

a. 選取新增執行個體以開啟執行個體選取畫面。

b. 在可用執行個體下方，您可以根據先前選取的網路設定，選取目前可用於負載平衡器的執行個體。

c. 當您對您的選項感到滿意時，請選取確認，將要註冊的執行個體新增至負載平衡器。

13. Attributes

- 針對啟用跨區域負載平衡、啟用連接耗盡和逾時 (耗盡間隔)，請保留預設值。

14. 負載平衡器標籤 (選用)

a. 索引鍵欄位為必填。

b. 值欄位為選填。

c. 若要新增另一個標籤，請選取新增標籤，然後輸入索引鍵欄位值，並選擇性地填寫值欄位。

d. 若要移除現有的標籤，請在要移除的標籤旁選取移除。

15. 摘要和建立

a. 如果您需要變更任何設定，請在需要變更的設定旁選取編輯。

b. 如果您對摘要中顯示的所有設定感到滿意，請選取建立負載平衡器，開始建立您的負載平衡器。

c. 在最終建立頁面上，選取檢視負載平衡器，以在 Amazon EC2主控台中檢視負載平衡器。

16. 確認

a. 選取新的負載平衡器。

b. 在目標執行個體索引標籤中，檢查運作狀態欄位。在至少一個EC2執行個體處於使用中狀態之後，您可以測試負載平衡器。

c. 在詳細資訊區段中，複製負載平衡器DNS名稱 ，其看起來會類似於 `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`。

d. 將您的負載平衡器DNS名稱貼到公有網際網路連線 Web 瀏覽器的地址欄位中。如果負載平衡器運作正常，您會看到伺服器的預設頁面。

17. 刪除 (選用)

a. 如果您的網域有指向負載平衡器CNAME的記錄，請將其指向新的位置，並等待DNS變更生效，然後再刪除負載平衡器。

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

c. 選取負載平衡器。

d. 選擇動作、刪除負載平衡器。

e. 出現確認提示時，請輸入 `confirm`，然後選取刪除。

f. 刪除負載平衡器後，向負載平衡器註冊的EC2執行個體會繼續執行。系統將根據執行個體繼續執行的時間，按每小時或不足一小時的時數計費。當您不再需要EC2執行個體時，您可以停止或終止執行個體，以避免產生額外費用。

使用 建立HTTPS負載平衡器 AWS CLI

使用以下指示，使用 建立 HTTPS/SSL 負載平衡器 AWS CLI。

任務

- 步驟 1：設定接聽程式
- 步驟 2：設定SSL安全政策
- 步驟 3：設定後端執行個體身分驗證 (選用)
- 步驟 4：設定運作狀態檢查(選用)
- 步驟 5：註冊EC2執行個體
- 步驟 6：驗證執行個體
- 步驟 7：刪除負載平衡器 (選用)

步驟 1：設定接聽程式

接聽程式是檢查連線請求的程序。它是透過一個前端 (用戶端到負載平衡器) 連線的協定和連接埠，以及一個後端 (負載平衡器到執行個體) 連線的協定和連接埠進行設定。如需有關 Elastic Load Balancing 支援的連接埠、通訊協定和接聽程式組態的詳細資訊，請參閱 Classic Load Balancer 的接聽程式。

在這個範例中，您為負載平衡器設定兩個接聽程式，做法是指定連接埠和通訊協定以用於前端和後端連線。第一個接聽程式接受連接埠 80 上的HTTP請求，並使用 將請求傳送至連接埠 80 上的執行個體HTTP。第二個接聽程式接受連接埠 443 上的HTTPS請求，並將請求傳送到連接埠 80 HTTP上的執行個體。

由於第二個接聽程式HTTPS用於前端連線，因此您必須在負載平衡器上部署SSL伺服器憑證。負載平衡器使用此憑證以終止然後解密請求，再將它們傳送到執行個體。

設定負載平衡器的接聽程式。

1. 取得SSL憑證的 Amazon Resource Name（ARN）。例如：

ACM

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

IAM

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

2. 使用下列create-load-balancer命令，使用兩個接聽程式來設定負載平衡器：

```
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
```

以下是回應範例：

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

3. （選用）使用下列describe-load-balancers命令來檢視負載平衡器的詳細資訊：

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

步驟 2：設定SSL安全政策

您可以選擇一個預先定義的安全政策，或可建立自己的自訂安全政策。否則，Elastic Load Balancing 會使用預設的預先定義安全政策 `ELBSecurityPolicy-2016-08` 來設定您的負載平衡器。如需詳細資訊，請參閱SSL Classic Load Balancer 的交涉組態。

確認您的負載平衡器與預設安全政策相關聯

使用下列 describe-load-balancers 命令：

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

以下是回應範例。請注意，`ELBSecurityPolicy-2016-08` 與連接埠 443 的負載平衡器相關聯。

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

如果您願意，您可以設定負載平衡器SSL的安全政策，而不是使用預設的安全政策。

（選用）使用預先定義的SSL安全政策

1. 使用以下describe-load-balancer-policies命令列出預先定義安全政策的名稱：

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

   如需有關為預先定義安全政策的組態的詳細資訊，請參閱Classic Load Balancer 的預先定義SSL安全政策。

2. 使用下列create-load-balancer-policy命令，使用您在上一個步驟中描述的其中一個預先定義安全政策來建立SSL交涉政策：

```
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. （選用）使用下列describe-load-balancer-policies命令來驗證政策是否已建立：

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

回應包含政策的描述。

4. 使用下列 set-load-balancer-policies-of-listener 命令，在負載平衡器連接埠 443 上啟用政策：

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

> **Note**
>
> 此 `set-load-balancer-policies-of-listener` 命令會將指定的負載平衡器連接埠的目前政策集合取代為指定的政策。`--policy-names` 清單必須包含所有要啟用的 政策。如果您省略的政策目前已啟用，它會被停用。

5. （選用）使用下列describe-load-balancers命令來驗證政策是否已啟用：

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

以下是範例回應，其顯示政策在連接埠 443 上啟用。

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

當您建立自訂安全政策，您必須至少啟用一個通訊協定，和一個加密方式。DSA 和 RSA 密碼專屬於簽署演算法，並用於建立SSL憑證。如果您已有SSL憑證，請務必啟用用來建立憑證的密碼。您的自訂政策名稱不得以 `ELBSample-` 或 `ELBSecurityPolicy-` 開頭，因為這些字首是預留給預先定義安全政策的名稱使用。

（選用）使用自訂SSL安全政策

1. 使用 SSL create-load-balancer-policy命令來使用自訂安全政策建立交涉政策。例如：

```
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. （選用）使用下列describe-load-balancer-policies命令來驗證政策是否已建立：

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

回應包含政策的描述。

3. 使用下列 set-load-balancer-policies-of-listener 命令在負載平衡器連接埠 443 上啟用政策：

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

> **Note**
>
> 此 `set-load-balancer-policies-of-listener` 命令會將指定的負載平衡器連接埠的目前政策集合取代為指定的政策。`--policy-names` 清單必須包含所有要啟用的 政策。如果您省略的政策目前已啟用，它會被停用。

4. （選用）使用下列describe-load-balancers命令來驗證政策是否已啟用：

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

以下是範例回應，其顯示政策在連接埠 443 上啟用。

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

步驟 3：設定後端執行個體身分驗證 (選用)

如果您在後端連線上設定 HTTPS/SSL，您可以選擇設定執行個體的身分驗證。

當您設定後端執行個體身分驗證時，會建立公有金鑰政策。接著，您會使用這個公有金鑰政策來建立後端執行個體身分驗證政策。最後，您可以使用HTTPS通訊協定的執行個體連接埠設定後端執行個體身分驗證政策。

只有在執行個體提供給負載平衡器的公有金鑰符合您的負載平衡器身分驗證政策的公有金鑰時，負載平衡器才會與執行個體通訊。

設定後端執行個體身分驗證

1. 使用下列命令來擷取公有金鑰：

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

2. 使用下列create-load-balancer-policy命令來建立公有金鑰政策：

```
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**
>
> 若要指定 `--policy-attributes` 的公有金鑰值，請移除第一個和最後一行公有金鑰 (該行各包含`-----BEGIN PUBLIC KEY-----` 和 `-----END PUBLIC KEY-----`)。AWS CLI 不接受 中的空格字元`--policy-attributes`。

3. 使用以下create-load-balancer-policy命令，使用 建立後端執行個體身分驗證政策`my-PublicKey-policy`。

```
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
```

   您可以選擇性使用多個公有金鑰政策。負載平衡器嘗試所有金鑰，一次一個。如果執行個體提供的公有金鑰符合這些公有金鑰的其中一個，該執行個體會被驗證。

4. 使用下列 set-load-balancer-policies- for-backend-server命令`my-authentication-policy`，將 設定為 的執行個體連接埠HTTPS。在此範例中，執行個體連接埠為 443。

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

5. （選用）使用以下describe-load-balancer-policies命令列出負載平衡器的所有政策：

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

6. （選用）使用下列describe-load-balancer-policies命令來檢視政策的詳細資訊：

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

步驟 4：設定運作狀態檢查(選用)

Elastic Load Balancing 會根據您設定的運作狀態檢查，定期檢查每個已註冊EC2執行個體的運作狀態。如果 Elastic Load Balancing 找到運作狀態不佳的執行個體，則會停止將流量傳送至執行個體，並將流量路由至運作狀態良好的執行個體。如需詳細資訊，請參閱Classic Load Balancer 執行個體的 Health 狀態檢查。

當您建立您的負載平衡器，Elastic Load Balancing 會使用預設的運作狀態檢查設定。如果您願意，您可以為您的負載平衡器變更運作狀態檢查組態，而不是使用預設的設定。

設定執行個體的運作狀態檢查

使用下列 configure-health-check 命令：

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

以下是回應範例：

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

步驟 5：註冊EC2執行個體

建立負載平衡器之後，您必須向負載平衡器註冊EC2執行個體。您可以從與負載平衡器位於相同區域內的單一可用區域或多個可用區域選取EC2執行個體。如需詳細資訊，請參閱Classic Load Balancer 的註冊執行個體。

使用 register-instances-with-load-balancer 命令，如下所示：

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

以下是回應範例：

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

步驟 6：驗證執行個體

只要任何一個已註冊執行個體在 `InService` 狀態，您的負載平衡器便可使用。

若要檢查新註冊EC2執行個體的狀態，請使用下列describe-instance-health命令：

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

以下是回應範例：

```
{
    "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"
        }
    ]
```

```
}
```

如果執行個體的 `State` 欄位是 `OutOfService`，原因可能是您的執行個體仍在註冊中。如需詳細資訊，請參閱故障診斷 Classic Load Balancer：執行個體註冊。

當至少有一個執行個體處於 `InService` 狀態後，您即可測試負載平衡器。若要測試負載平衡器，請複製負載平衡器DNS的名稱，並將其貼到網際網路連線 Web 瀏覽器的地址欄位中。如果您的負載平衡器正常運作，您會看到HTTP伺服器的預設頁面。

步驟 7：刪除負載平衡器 (選用)

刪除負載平衡器會自動取消註冊其相關聯的EC2執行個體。負載平衡器刪除後，即無需再支付該負載平衡器的費用。不過，EC2執行個體會繼續執行，而且您會持續產生費用。

若要刪除負載平衡器，請使用下列delete-load-balancer命令：

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

若要停止EC2執行個體，請使用 stop-instances 命令。若要終止EC2執行個體，請使用 terminate-instances 命令。

設定 Classic Load Balancer 的HTTPS接聽程式

接聽程式是檢查連線請求的程序。它是透過一個前端 (用戶端到負載平衡器) 連線的協定和連接埠，以及一個後端 (負載平衡器到執行個體) 連線的協定和連接埠進行設定。如需有關 Elastic Load Balancing 支援的連接埠、通訊協定和接聽程式組態的詳細資訊，請參閱 Classic Load Balancer 的接聽程式。

如果您有負載平衡器，其接聽程式接受連接埠 80 上的HTTP請求，您可以新增接聽程式，接受連接埠 443 上的HTTPS請求。如果您指定HTTPS接聽程式將請求傳送至連接埠 80 上的執行個體，負載平衡器會終止SSL請求，而且不會加密從負載平衡器到執行個體的通訊。如果HTTPS接聽程式將請求傳送至連接埠 443 上的執行個體，則會加密從負載平衡器到執行個體的通訊。

如果您的負載平衡器使用已加密的連線來與執行個體通訊，您就可以選擇性啟用執行個體的身分驗證。這可確保負載平衡器僅與執行個體通訊，若其公有金鑰符合您為此目的而指定到負載平衡器的金鑰的話。

如需建立新的HTTPS接聽程式的資訊，請參閱 使用HTTPS接聽程式建立 Classic Load Balancer 。

目錄

- 使用主控台新增HTTPS接聽程式
- 使用 新增HTTPS接聽程式 AWS CLI

必要條件

若要啟用HTTPS接聽程式的HTTPS支援，您必須在負載平衡器上部署SSL伺服器憑證。負載平衡器使用此憑證以終止然後解密請求，再將它們傳送到執行個體。如果您沒有SSL憑證，您可以建立憑證。如需詳細資訊，請參閱SSLClassic Load Balancer 的 /TLS 憑證。

使用主控台新增HTTPS接聽程式

您可以將HTTPS接聽程式新增至現有的負載平衡器。

使用主控台將HTTPS接聽程式新增至負載平衡器

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在接聽程式索引標籤中，選擇管理接聽程式。
5. 在管理接聽程式頁面的接聽程式區段中，選擇新增接聽程式。
6. 針對接聽程式通訊協定 ，選取 HTTPS 。

> **Important**
>
> 根據預設，執行個體通訊協定為 HTTP。如果您想要設定後端執行個體身分驗證，請將執行個體通訊協定變更為 HTTPS 。

7. 對於安全政策 ，我們建議您使用最新的預先定義安全政策。如果您需要使用不同的預先定義安全政策或建立自訂政策，請參閱更新SSL協商組態。
8. 對於預設SSL憑證 ，選擇編輯 ，然後執行下列其中一項操作：
   - 如果您使用 建立或匯入憑證 AWS Certificate Manager，請選擇從 ACM，從清單中選擇憑證，然後選擇儲存變更。

     > **Note**
     >
     > 此選項僅適用於支援 AWS Certificate Manager的區域。

- 如果您使用 匯入憑證IAM，請選擇從 IAM，從清單中選擇憑證，然後選擇儲存變更 。
- 如果您有要匯入 的SSL憑證ACM，請選取匯入 和 至 ACM。在憑證私有金鑰 中，複製並貼上 PEM編碼的私有金鑰檔案的內容。在憑證內文 中，複製並貼上 PEM編碼的公有金鑰憑證檔案的內容。在憑證鏈 - 選用 中，複製並貼上 PEM編碼憑證鏈檔案的內容，除非您使用自我簽署憑證，而且瀏覽器不一定要隱含接受憑證。
- 如果您有要匯入的SSL憑證，但此區域ACM不支援，請選取匯入 和 至 IAM。在憑證名稱中輸入憑證名稱。在憑證私有金鑰 中，複製並貼上 PEM編碼的私有金鑰檔案的內容。在憑證內文 中，複製並貼上 PEM編碼的公有金鑰憑證檔案的內容。在憑證鏈 - 選用 中，複製並貼上 PEM編碼憑證鏈檔案的內容，除非您使用自我簽署憑證，而且瀏覽器不一定要隱含接受憑證。
- 選擇 Save changes (儲存變更)。

9. Cookie 黏性預設為停用。若要變更此設定，請選擇編輯。若選擇由負載平衡器產生，則必須指定過期期間。若選擇由應用程式產生，則必須指定 Cookie 名稱。做出這些選擇後，請選擇儲存變更。
10. (選用) 選擇新增接聽程式以新增額外的接聽程式。
11. 選擇儲存變更以新增您剛設定的接聽程式。
12. （選用）若要設定現有負載平衡器的後端執行個體身分驗證，您必須使用 AWS CLI 或 API，因為此任務不支援使用主控台執行。如需詳細資訊，請參閱設定後端執行個體。

使用 新增HTTPS接聽程式 AWS CLI

您可以將HTTPS接聽程式新增至現有的負載平衡器。

若要使用 將HTTPS接聽程式新增至負載平衡器 AWS CLI

1. 取得SSL憑證的 Amazon Resource Name（ARN）。例如：

   ACM

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

   IAM

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

2. 使用下列create-load-balancer-listeners命令，將接聽程式新增至接受連接埠 443 上HTTPS請求的負載平衡器，並使用 將請求傳送至連接埠 80 上的執行個體HTTP：

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

如果您想要設定後端執行個體身分驗證，請使用下列命令來新增接聽程式，以接受連接埠 443 上的HTTPS請求，並使用 將請求傳送至連接埠 443 上的執行個體HTTPS：

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

3. （選用）您可以使用下列describe-load-balancers命令來檢視負載平衡器的更新詳細資訊：

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

以下是回應範例：

```
{
    "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. （選用）您的HTTPS接聽程式是使用預設安全政策建立的。如果您想要指定不同的預先定義安全政策或自訂安全政策，請使用 create-load-balancer-policy和 set-load-balancer-policies接聽程式命令。如需詳細資訊，請參閱使用 SSL 更新交涉組態 AWS CLI。
5. （選用）若要設定後端執行個體身分驗證，請使用 set-load-balancer-policies-for-backend-server命令。如需詳細資訊，請參閱設定後端執行個體。

取代 Classic Load Balancer 的SSL憑證

如果您有HTTPS接聽程式，當您建立接聽程式時，會在負載平衡器上部署SSL伺服器憑證。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，續約或更換憑證。

您可以在負載平衡器上自動續約由 提供 AWS Certificate Manager 和部署的憑證。ACM 會嘗試在憑證過期之前續約憑證。如需詳細資訊，請參閱 AWS Certificate Manager 使用者指南中的受管續約。如果您將憑證匯入 ACM，則必須監控憑證的過期日期，並在憑證過期之前將其續約。如需詳細資訊，請參閱 AWS Certificate Manager 使用者指南中的匯入憑證。當部署在負載平衡器上的憑證被更新後，新的請求會使用更新的憑證。

若要替換憑證，您必須先遵循建立目前的憑證時所使用的相同步驟來建立新憑證。然後，您可以替換憑證。當部署在負載平衡器上的憑證被取代後，新的請求會使用新的憑證。

請注意，更新或更換憑證並不會影響負載平衡器節點已接收，並且等待路由到運作狀態良好目標的請求。

目錄

使用主控台取代SSL憑證

您可以將部署在負載平衡器上的憑證取代為 提供的憑證ACM或上傳至 的憑證IAM。

使用主控台取代HTTPS負載平衡器的SSL憑證

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在接聽程式索引標籤中，選擇管理接聽程式。
5. 在管理接聽程式頁面上，找到要更新的接聽程式，選擇預設SSL憑證下的編輯，然後執行下列其中一項操作：

   - 如果您使用 建立或匯入憑證 AWS Certificate Manager，請選擇從 ACM，從清單中選擇憑證，然後選擇儲存變更。

     > **Note**
     > 此選項僅適用於支援 AWS Certificate Manager的區域。

   - 如果您使用 匯入憑證IAM，請選擇從 IAM，從清單中選擇憑證，然後選擇儲存變更 。
   - 如果您有要匯入 的SSL憑證ACM，請選取匯入 和 至 ACM。在憑證私有金鑰 中，複製並貼上 PEM編碼的私有金鑰檔案的內容。在憑證內文 中，複製並貼上 PEM編碼的公有金鑰憑證檔案的內容。在憑證鏈 - 選用 中，複製並貼上 PEM編碼憑證鏈檔案的內容，除非您使用自我簽署憑證，而且瀏覽器不一定要隱含接受憑證。
   - 如果您有要匯入的SSL憑證，但此區域ACM不支援，請選取匯入 和 至 IAM。在憑證名稱中輸入憑證名稱。在憑證私有金鑰 中，複製並貼上 PEM編碼的私有金鑰檔案的內容。在憑證內文 中，複製並貼上 PEM編碼的公有金鑰憑證檔案的內容。在憑證鏈 - 選用 中，複製並貼上 PEM編碼憑證鏈檔案的內容，除非您使用自我簽署憑證，而且瀏覽器不一定要隱含接受憑證。
   - 選擇 Save changes (儲存變更)。

使用 取代SSL憑證 AWS CLI

您可以將部署在負載平衡器上的憑證取代為 提供的憑證ACM或上傳至 的憑證IAM。

使用 提供的SSL憑證取代憑證 ACM

1. 使用下列的 request-certificate 命令申請新憑證：

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

2. 使用下列 set-load-balancer-listener-ssl-certificate 命令來設定憑證：

```
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
```

若要將SSL憑證取代為上傳至 的憑證 IAM

1. 如果您有SSL憑證但尚未上傳，請參閱 IAM 使用者指南 中的上傳伺服器憑證。
2. 使用下列get-server-certificate命令取得憑證ARN的 ：

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

3. 使用下列 set-load-balancer-listener-ssl-certificate 命令來設定憑證：

```
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
```

更新 Classic Load Balancer SSL 的交涉組態

Elastic Load Balancing SSL 提供具有預先定義交涉組態的安全政策，可用於交涉用戶端和負載平衡器之間的SSL連線。如果您為接聽程式使用 HTTPS/SSL 通訊協定，則可以使用其中一個預先定義的安全政策，或使用您自己的自訂安全政策。

如需關於安全政策的詳細資訊，請參閱SSL Classic Load Balancer 的交涉組態。如需有關 Elastic Load Balancing 提供之安全政策的組態的詳細資訊，請參閱 Classic Load Balancer 的預先定義SSL安全政策。

如果您建立 HTTPS/SSL 接聽程式而不將安全政策建立關聯，Elastic Load Balancing 會將預設預先定義的安全政策 `ELBSecurityPolicy-2016-08`與負載平衡器建立關聯。

如果您願意的話，您可以建立自訂組態。強烈建議您在升級負載平衡器組態之前先測試您的安全政策。

下列範例示範如何更新 SSL HTTPS/SSL 接聽程式的交涉組態。請注意，變更不影響負載平衡器節點所接收的請求，而這些請求都在等待路由到運作狀態良好的執行個體，但更新的組態將會與新的請求一起使用。

目錄

- 使用主控台更新交SSL涉組態
- 使用 SSL 更新交涉組態 AWS CLI

使用主控台更新交SSL涉組態

在預設情況下，Elastic Load Balancing 會建立最新預先定義政策與您的負載平衡器之間的關聯。新增新的預先定義政策時，建議您更新負載平衡器，以使用新的預先定義政策。或者，您可以選擇不同的預先定義安全政策或建立自訂政策。

使用主控台更新 HTTPS/SSL 負載平衡器的SSL交涉組態

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在接聽程式索引標籤中，選擇管理接聽程式。
5. 在管理接聽程式頁面上找到要更新的接聽程式，在安全政策下方選擇編輯，然後使用下列其中一個選項選取安全政策：
   - 保留預設政策 ELBSecurityPolicy-2016-08，然後選擇儲存變更 。
   - 選取預設政策以外的預先定義政策，然後選擇儲存變更。
   - 選取自訂並至少啟用一個通訊協定和一個加密方式，如下所示：
     a. 對於SSL通訊協定 ，選取要啟用的一或多個通訊協定。
     b. 對於SSL選項 ，選取伺服器順序偏好設定，以使用 中列出的順序Classic Load Balancer的預先定義SSL安全政策進行SSL交涉。
     c. 針對 SSLCiphers ，選取要啟用的一或多個密碼。如果您已有SSL憑證，則必須啟用用來建立憑證的密碼，因為 DSA和 RSA 密碼是簽署演算法特有的。
     d. 選擇 Save changes (儲存變更)。

使用 SSL 更新交涉組態 AWS CLI

您可以使用預設的預先定義安全政策、`ELBSecurityPolicy-2016-08`、不同的預先定義安全政策，或自訂安全政策。

使用預先定義的SSL安全政策

1. 使用以下describe-load-balancer-policies命令列出 Elastic Load Balancing 提供的預先定義安全政策。您使用的語法取決於您所使用的作業系統和 Shell。

   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
   ```

   下列為範例輸出：

   ```
   ----------------------------------------
   |      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  |
   +----------------------------------------+
   ```

   若要判斷哪些加密已針對來政策啟用，請使用下列命令：

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

如需有關為預先定義安全政策的組態的詳細資訊，請參閱Classic Load Balancer 的預先定義SSL安全政策。

2. 使用 SSL create-load-balancer-policy命令，使用您在上一個步驟中描述的其中一個預先定義安全政策來建立交涉政策。例如，以下命令會使用預設的預先定義安全政策：

```
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
```

如果您超過負載平衡器政策數量的限制，請使用 delete-load-balancer-policy命令刪除任何未使用的政策。

3. （選用）使用下列describe-load-balancer-policies命令來驗證政策是否已建立：

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

回應包含政策的描述。

4. 使用下列 set-load-balancer-policies-of-listener 命令，在負載平衡器連接埠 443 上啟用政策：

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

> **Note**
>
> 此 `set-load-balancer-policies-of-listener` 命令會將指定的負載平衡器連接埠的目前政策集合取代為指定的政策。`--policy-names` 清單必須包含所有要啟用的 政策。如果您省略的政策目前已啟用，它會被停用。

5. （選用）使用下列describe-load-balancers命令來驗證是否已針對負載平衡器連接埠啟用新政策：

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

該回應會顯示政策已在連接埠 443 上啟用。

```
...
  {
```

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

當您建立自訂安全政策，您必須至少啟用一個通訊協定，和一個加密方式。DSA 和 RSA 密碼專屬於簽署演算法，並用於建立SSL憑證。如果您已有SSL憑證，請務必啟用用來建立憑證的密碼。您的自訂政策名稱不得以 `ELBSample-` 或 `ELBSecurityPolicy-` 開頭，因為這些字首是預留給預先定義安全政策的名稱使用。

使用自訂SSL安全政策

1. 使用 SSL create-load-balancer-policy命令來使用自訂安全政策建立交涉政策。例如：

```
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
```

   如果您超過負載平衡器政策數量的限制，請使用 delete-load-balancer-policy命令刪除任何未使用的政策。

2. （選用）使用下列describe-load-balancer-policies命令來驗證政策是否已建立：

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

   回應包含政策的描述。

3. 使用下列 set-load-balancer-policies-of-listener 命令，在負載平衡器連接埠 443 上啟用政策：

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

> **Note**
>
> 此 `set-load-balancer-policies-of-listener` 命令會將指定的負載平衡器連接埠的目前政策集合取代為指定的政策。`--policy-names` 清單必須包含所有要啟用的 政策。如果您省略的政策目前已啟用，它會被停用。

4. （選用）使用下列describe-load-balancers命令來驗證負載平衡器連接埠是否已啟用新政策：

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

該回應會顯示政策已在連接埠 443 上啟用。

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

Classic Load Balancer 的註冊執行個體

建立 Classic Load Balancer 之後，您必須向負載平衡器註冊EC2執行個體。您可以從與負載平衡器相同區域內的單一可用區域或多個可用區域中選取EC2執行個體。Elastic Load Balancer 會定期對已註冊的執行EC2個體執行健康狀態檢查，並自動將傳入的要求分配到已註冊且運作良EC2好的執行個體之間的負載平衡器DNS名稱。

目錄

執行個體最佳實務

- 您必須確保負載平衡器可以同時在接聽程式連接埠和運作狀態檢查連接埠上，與您的執行個體通訊。如需詳細資訊，請參閱設定您的 Classic Load Balancer 的安全群組。您的執行個體的安全群組必須允許在負載平衡器的每個子網路的兩個連接埠雙向流量。
- 在您打算向負載平衡器註冊的所有執行個體上安裝 Web 伺服器，例如 Apache 或網際網路資訊服務 (IIS)。
- 對於HTTP和接HTTPS聽程式，我們建議您在EC2執行個體中啟用 keep-alive 選項，這樣可讓負載平衡器針對多個用戶端要求重複使用與執行個體的連線。這可減少 Web 伺服器的負載，進而提升負載平衡器的輸送量。持續作用逾時應至少為 60 秒，以確保負載平衡器負責關閉連接到您的執行個體。
- Elastic Load Balancing 支援路徑最大傳輸單元 (MTU) 探索。為了確保路徑MTU探索可以正常運作，您必須確定執行個體的安全性群組允許所需的ICMP片段 (類型 3，程式碼 4) 訊息。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的路徑MTU探索。

為您的建議 VPC

虛擬私有雲 (VPC)

除非您VPC在 2014 年 AWS 帳戶 之前建立了，否則每個區域都有預設值。您可以為負載平衡器使VPC用預設值 (如果有的話)，也可以建立新的負載平衡器VPC。如需詳細資訊，請參閱 Amazon VPC 使用者指南。

負載平衡器的子網路

為確保負載平衡器可以正確擴展，請確認負載平衡器的每個子網路都具有至少包含/27位元遮罩的CIDR區塊 (例如，10.0.0.0/27)，且至少有 8 個可用 IP 位址。負載平衡器會使用這些 IP 地址與執行個體建立連線，並在必要時橫向擴展。如果 IP 地址不足，負載平衡器可能無法擴展，並且由於容量不足而導致 503 錯誤。

在每個您想要啟動執行個體的可用區域建立子網路。根據您的應用程式，您可以在公有子網路、私有子網路、公有和私有子網路的組合啟動您的執行個體。公有子網路包含到網際網路閘道的路由。請注意，依預設，每VPCs個可用區域都有一個公用子網路。

當您建立負載平衡器，您必須新增一或多個公有子網路到負載平衡器。如果您的執行個體位於私有子網路，請在相同的可用區域中建立公有子網路，如同您的執行個體的子網路；您會新增這些公有子網路到負載平衡器。

網絡 ACLs

您的網路ACLsVPC必須允許接聽程式連接埠和健全狀況檢查連接埠上兩個方向的流量。如需詳細資訊，請參閱Classic Load Balancer 執行個體的網路 ACLs。

使用 Classic Load Balancer 註冊執行個體

註冊EC2執行個體會將其新增至您的負載平衡器。負載平衡器在啟用的可用區域持續監控註冊的執行個體的運作狀態，並將請求路由到運作狀態良好的執行個體。如果執行個體的需求增加，您可以向負載平衡器註冊額外的執行個體來處理需求。

取消註冊EC2執行個體會將其從負載平衡器中移除。執行個體取消註冊後，負載平衡器即停止路由請求到該執行個體。如果需求減少或您需要為執行個體提供服務，則可從負載平衡器取消註冊執行個體。取消註冊的執行個體仍會執行，但是不會再從負載平衡器接收流量，當您需要時可以再向負載平衡器註冊。

當您取消註冊執行個體時，如果啟用連接耗盡，Elastic Load Balancing 會等到處理中的請求完成。如需詳細資訊，請參閱為 Classic Load Balancer 設定連接耗盡。

如果您連接執行個體到 Auto Scaling 群組，群組中的執行個體已自動註冊了負載平衡器。如果分離負載平衡器與您的 Auto Scaling 群組的連結，會自動從該目標群組中取消執行個體的註冊。

Elastic Load Balancing 會使用其 IP 位址向負載平衡器註冊您的EC2執行個體。

[EC2-VPC] 當您註冊連接了 elastic network interface (ENI) 的執行個體時，負載平衡器會將要求路由至執行個體主要介面 (eth0) 的主要 IP 位址。

目錄

註冊執行個體

當您準備好，以您的負載平衡器註冊您的執行個體。如果在可用區域內的執行個體是在已啟用負載平衡器，執行個體準備好接受流量時便立即通過所需的負載平衡器的運作狀態檢查。

使用主控台註冊您的執行個體

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在目標執行個體索引標籤中，選取管理執行個體。
5. 在管理執行個體頁面的可用執行個體表中，選取要向負載平衡器註冊的執行個體。
6. 確認檢閱所選執行個體表中出現需要註冊的執行個體。
7. 選擇 Save changes (儲存變更)。

使用註冊執行個體 AWS CLI

使用以下 register-instances-with-load-平衡器命令：

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

以下是範例回應執行個體註冊列出的負載平衡器：

```
{
    "Instances": [
```

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

檢視使用負載平衡器註冊的執行個體。

使用下列describe-load-balancers命令列出在指定負載平衡器註冊的執行個體：

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

下列為範例輸出：

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

判斷已註冊執行個體的負載平衡器

使用下列describe-load-balancers命令取得指定執行個體所註冊之負載平衡器的名稱：

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

下列為範例輸出：

```
my-load-balancer
```

取消註冊執行個體

您可以從您的負載平衡器取消註冊執行個體，如果您不再需要的容量，或如果您需要服務的執行個體。

如果負載平衡器連接到 Auto Scaling 群組，從群組分離執行個體，則執行個體會從負載平衡器取消註冊。如需詳細資訊，請參閱 Amazon Auto Scaling 使用者指南中的將EC2執行個體從您的 EC2 Auto Scaling 群組分離。

使用主控台取消註冊您的執行個體

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在目標執行個體索引標籤中，選取管理執行個體。
5. 在管理執行個體頁面的可用執行個體表中，取消選取要從負載平衡器取消註冊的執行個體。
6. 確認檢閱所選執行個體表中沒有需要取消註冊的執行個體。
7. 選擇 Save changes (儲存變更)。

若要取消註冊執行個體，請使用 AWS CLI

使用以下 deregister-instances-from-load-平衡器命令：

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

以下是範例回應剩餘執行個體註冊列出的負載平衡器：

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

Classic Load Balancer 執行個體的 Health 狀態檢查

您的 Classic Load Balancer 會定期將請求傳送到已註冊的執行個體來測試其狀態。這些測試稱為運作狀況檢查。在進行運作狀態檢查時，運作狀態良好的執行個體的狀態為 `InService`。在進行運作狀態檢查時，運作狀態不佳的執行個體狀態為 `OutOfService`。無論執行個體運作狀態良好或不佳，負載平衡器都會在所有註冊的執行個體上執行運作狀態檢查。

負載平衡器只會將請求路由到運作狀態良好的執行個體。當負載平衡器判斷某個執行個體的運作狀態不佳時，會停止將請求路由到該執行個體。在執行個體還原到運作良好的狀態後，負載平衡器就會重新恢復路由請求到該執行個體。

負載平衡器會檢查其已註冊執行個體的運作狀態，使用方式是透過 Elastic Load Balancing 所提供預設的運作狀態檢查組態，或是您指定的自訂運作狀態檢查組態。

如果您的 Auto Scaling 群組與 Classic Load Balancer 相關聯，您可以使用負載平衡器的運作狀態檢查，以確定您的 Auto Scaling 群組中的執行個體的運作狀態。根據預設，每個執行個體的 Auto Scaling 群組定期決定運作狀態。如需詳細資訊，請參閱 Amazon Auto Scaling 使用者指南中的將 Elastic Load Balancing 運作狀態檢查新增至您的 EC2 Auto Scaling 群組。

目錄

運作狀態檢查組態

設定運作狀態，包含負載平衡器用於決定註冊執行個體的運作狀態的資訊。下表說明組態欄位的運作狀態檢查。

欄位	描述
通訊協定	使用通訊協定連線到執行個體。 有效值：TCP、HTTP、HTTPS 和 SSL 主控台預設：HTTP CLI/API預設值：TCP
連線埠	使用連接埠連線到執行個體,，像是 `protocol:port` 對。如果該負載平衡器無法與執行個體在設定的回應逾時時間在指定的連接埠連線，執行個體就視為運作狀態不佳。 通訊協定：TCP、HTTP、HTTPS 和 SSL 連接埠範圍：1 到 65535

欄位	描述
	主控台預設：`HTTP:80` CLI/API預設值：`TCP:80`
路徑	HTTP或HTTPS要求的目的地。 HTTP或HTTPSGET要求會發出給連接埠和路徑上的執行個體。如果運作狀態檢查在回應的逾時時段內收到「200 OK」以外的任何回應，執行個體會被視為狀況不良。如果回應包含內文，您的應用程式必須將 Content-Length 標頭設為大於或等於零的值，或指定 Transfer-Encoding 值設為「區塊」。 預設：`/index.html`
回應逾時	等待收到運作狀態檢查回應的時間，(以秒為單位)。 有效值：2 到 60 預設：5
HealthCheck 間隔	個別執行個體的運作狀態檢查之間的時間，(以秒為單位)。 有效值：5 到 300 預設：30
狀態不良閾值	宣告EC2執行個體運作狀態不良之前，必須進行的連續失敗運作狀態檢查次數。 有效值：2 到 10 預設：2

欄位	描述
運作良好閾值	宣告EC2執行個體健康狀態良好之前，必須進行的連續成功運作狀態檢查次數。 有效值：2 到 10 預設：10

負載平衡器每隔 `Interval` 秒會使用指定的連接埠、通訊協定和路徑，向每個已註冊執行個體傳送運作狀態檢查請求。每個運作狀態檢查請求是各自獨立，且在整個間隔內持續進行。執行個體回應所花的時間不影響下次運作狀態檢查請求的間隔。如果健全狀況檢查超過UnhealthyThresholdCount連續的失敗，負載平衡器會將執行個體停止服務。當健康狀態檢查超過HealthyThresholdCount連續成功時，負載平衡器會將執行個體重新啟用。

如果執行個體在HTTPS健康狀態檢查間隔內傳回 200 個回應碼，就會成功執行HTTP/健康狀態檢查。如果TCP連線成功，TCP健康狀態檢查就會成功。如果SSL交握成功，SSL健全狀況檢查就會成功。

更新運作狀態檢查組態

您可以在任何時間更新您的負載平衡器的運作狀態檢查的組態。

使用主控台更新您的負載平衡器的運作狀態檢查的組態。

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在 Health checks (運作狀態檢查) 標籤上，選擇 Edit (編輯)。
5. 在編輯運作狀態檢查設定頁面的運作狀態檢查下方，視需要更新組態。
6. 對您的選項感到滿意後，請選擇儲存變更。

使用更新負載平衡器的健康狀態檢查組態 AWS CLI

使用下列 configure-health-check 命令：

```
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
```

檢查您的執行個體的運作狀態

您可以查看您已註冊執行個體的運作狀態。

使用主控台檢查執行個體的運作狀態

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在詳細資訊區段中，狀態表示在服務中的執行個體數量。
5. 在目標執行個體索引標籤的目標執行個體表中，運作狀態欄位表示每個註冊執行個體的具體狀態。

使用檢查執行個體的健全狀態 AWS CLI

使用下列 describe-instance-health 命令：

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

故障診斷運作狀態檢查

您的已註冊執行個體未能通過負載平衡器的運作狀態檢查的原因有若干個。執行健康狀態檢查失敗的最常見原因是EC2執行個體關閉與負載平衡器的連線，或EC2執行個體的回應逾時。如需有關可能原因和步驟，以及您需要採取哪些步驟解決運作狀態檢查問題的詳細資訊，請參閱故障診斷 Classic Load Balancer：運作狀態檢查。

Classic Load Balancer 執行個體的安全性群組

security group (安全群組) 扮演防火牆的角色，可控制允許進出一或多個執行個體的流量。啟動EC2執行個體時，您可以將一或多個安全群組與執行個體建立關聯。針對每個安全群組，您可新增一或多個規則來允許流量。您可以隨時修改安全群組的規則；系統會自動將新規則套用至與安全群組相關聯的所有執行個體。如需詳細資訊，請參閱 Amazon EC2使用者指南中的 Amazon EC2 安全群組。

您的執行個體的安全群組，必須允許它們與負載平衡器進行通訊。下表顯示建議的輸入規則。

來源	通訊協定	連接埠範圍	註解
load balancer security group	TCP	*instance listener*	允許來自負載平衡器在執行個體接聽程式連接埠上的流量
load balancer security group	TCP	*health check*	允許負載平衡器透過運作狀態檢查連接埠傳送的流量

我們也建議您允許輸入ICMP流量以支援路徑MTU探索。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的路徑MTU探索。

Classic Load Balancer 執行個體的網路 ACLs

網路存取控制清單 (ACL) 允許或拒絕子網路層級的特定輸入或輸出流量。您可以ACL為您的使用預設網路VPC，或者您可以使用VPC與安全性群組規則類似的規則建立自訂網ACL路，以便為您的安全性增加一層額外的安全性VPC。

VPC允許所有輸入和輸出流量的預設網路存取控制清單 (ACL)。如果您建立自訂網路ACLs，則必須新增允許負載平衡器和執行個體進行通訊的規則。

您的執行個體的子網路建議規則，取決於子網路是私有或公有。以下規則用於一個私有子網路。如果您的執行個體位於公有子網路中，請將來源和目的地從CIDR的變更VPC為`0.0.0.0/0`。

以下是建議的入站規則。

來源	通訊協定	連接埠範圍	註解
VPC CIDR	TCP	*instance listener*	允許執行處理監聽程式連接埠VPCCIDR上的輸入流量
VPC CIDR	TCP	*health check*	允許來自健全狀況檢查連接埠VPCCIDR上的輸入流量

以下是建議的輸出規則。

目的地	通訊協定	連接埠範圍	註解
VPC CIDR	TCP	1024-65535	允許對暫時連接埠VPCCIDR上的輸出流量

監控 Classic Load Balancer

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後端執行個體相關的問題進行疑難排解。

CloudWatch 指標

Elastic Load Balancing 會將負載平衡器和後端執行個體 CloudWatch 的資料點發佈至 Amazon。CloudWatch 可讓您擷取這些資料點的統計資料，作為一組有序的時間序列資料，稱為指標 。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 Classic Load Balancer 的指標。

Elastic Load Balancing 存取日誌

Elastic Load Balancing 的存取日誌會擷取您的負載平衡器所提出之請求的詳細資訊，並將它們以日誌檔形式存放在您指定的 Amazon S3 儲存貯體中。每個日誌包含接收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等的詳細資訊。您可以使用這些存取日誌來分析流量模式，並排除後端應用程式的問題。如需詳細資訊，請參閱Classic Load Balancer 存取日誌。

CloudTrail 日誌

AWS CloudTrail 可讓您追蹤API由 帳戶或代表 AWS 您的帳戶對 Elastic Load Balancing 進行的呼叫。 會將資訊 CloudTrail 儲存在您指定的 Amazon S3 儲存貯體中的日誌檔案中。您可以使用這些日誌檔來監控負載平衡器的活動，以判斷請求的類型、請求來自哪個來源 IP 地址、是誰提出請求的及何時產生要求等等。如需詳細資訊，請參閱使用 記錄 Elastic Load Balancing 的API呼叫 CloudTrail。

CloudWatch Classic Load Balancer 的指標

Elastic Load Balancing CloudWatch 會將負載平衡器和後端執行個體的資料點發佈至 Amazon。CloudWatch 可讓您擷取這些資料點的統計資料，做為一組有序的時間序列資料，稱為指標 。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，您可以監控指定期間內負載平衡器運作狀態良好的EC2執行個體總數。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，您可以建立 CloudWatch 警示來監控指定的指標，並在指標超出您認為可接受的範圍時啟動動作 （例如將通知傳送至電子郵件地址）。

Elastic Load Balancing CloudWatch 只會在請求流經負載平衡器時，將指標報告為 。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 Amazon 的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南 。

目錄

Classic Load Balancer 指標

AWS/ELB 命名空間包含下列指標。

指標	描述
BackendConnectionErrors	負載平衡器與註冊執行個體之間未成功建立的連線數目。由於發生錯誤時，負載平衡器會重試連線，此計數可能會超過請求率。請注意，此計數亦包含與運作狀態檢查有關的任何連線錯誤。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。請注意，每個負載平衡器節點都會回報 Average、Minimum 及 Maximum，但通常不太有用。但是，最小值與最大值 (或峰值與平均值，或平均值與傳輸量) 之間的差異，對於判斷負載平衡器節點是否為異常值是有用的。 範例：假設您的負載平衡器在 us-west-2a 有 2 個執行個體，在 us-west-2b 有 2 個執行個體，而嘗試連線至 us-west-2a 的 1 個執行個體發生後端連線錯誤。us-west-2a 的總和包括這些連線錯誤，而 us-west-2b 的總和則不包含。因此，負載平衡器的總和等於 us-west-2a 的總和。
DesyncMitigationMode_NonCompliant_Request_Count	【HTTP接聽程式】 不符合 7230 RFC 的請求數目。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。

指標	描述
HealthyHostCount	已向您的負載平衡器註冊的正常狀態執行個體的數量。通過第一次運作狀態檢查之後，新註冊的執行個體將被視為狀態正常。如果已啟用跨區域負載平衡，LoadBalancerName 維度的正常狀態執行個體的數量將以所有可用區域計算。否則將以每個可用區域計算。 報告條件：有已註冊的執行個體 統計資訊：最實用的統計資訊是 Average 與 Maximum。這些統計資訊由負載平衡器節點決定。請注意，有些負載平衡器節點可能會短暫判斷某執行個體狀態不良，同時其他節點則判斷該執行個體為狀態正常。 範例：假設您的負載平衡器在 us-west-2a 有 2 個執行個體，在 us-west-2b 有 2 個執行個體，us-west-2a 有 1 個執行個體狀態不良，而 us-west-2b 沒有狀態不良的執行個體。使用 AvailabilityZone 維度時，us-west-2a 平均有 1 個狀態正常與 1 個狀態不良的執行個體，us-west-2b 平均有 2 個狀態正常與 0 個狀態不良的執行個體。
HTTPCode_Backend_2XX，HTTPCode_Backend_3XX，HTTPCode_Backend_4XX，HTTPCode_Backend_5XX	【HTTP接聽程式】 已註冊執行個體產生的HTTP回應碼數目。此計數不包含負載平衡器產生的任何回應碼。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。請注意，Minimum、Maximum 及 Average 皆為 1。 範例 ：假設您的負載平衡器在 us-west-2a 中有 2 個執行個體，在 us-west-2b 中有 2 個執行個體，且傳送至 us-west-2a 中的 1 個執行個體的請求會產生 HTTP 500 個回應。us-west-2a 的總和包括這些錯誤回應，而 us-west-2b 的總和則不包含。因此，負載平衡器的總和等於 us-west-2a 的總和。

指標	描述
HTTPCode_ELB_4XX	【HTTP接聽程式】 負載平衡器產生的 HTTP 4XX 用戶端錯誤碼數目。請求的格式不正確或不完整時，會產生用戶端錯誤。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。請注意，Minimum、Maximum 及 Average 皆為 1。 範例 ：假設您的負載平衡器已啟用 us-west-2a 和 us-west-2b，且用戶端請求包含格式錯誤的請求 URL。因此，所有可用區域中的用戶端錯誤可能會增加。負載平衡器的總和為可用區域的值的總和。
HTTPCode_ELB_5XX	【HTTP接聽程式】 負載平衡器產生的 HTTP 5XX 伺服器錯誤碼數目。此計數不包含註冊執行個體產生的任何回應碼。如果沒有狀態正常的執行個體向負載平衡器註冊，或如果請求率超過執行個體 (溢出) 或負載平衡器的容量，將會回報此指標。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。請注意，Minimum、Maximum 及 Average 皆為 1。 範例：假設您的負載平衡器已啟用 us-west-2a 與 us-west-2b，而 us-west-2a 中的執行個體出現高延遲，對請求的回應過慢。結果，us-west-2a 中的負載平衡器節點的突增佇列將會填入，用戶端將收到 503 錯誤。如果 us-west-2b 繼續正常回應，負載平衡器的總和等於 us-west-2a 的總和。

指標	描述
Latency	【HTTP接聽程式】 從負載平衡器將請求傳送至已註冊執行個體到執行個體開始傳送回應標頭所經過的總時間，以秒為單位。 【TCP接聽程式】 負載平衡器成功建立與已註冊執行個體連線所經過的總時間，以秒為單位。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Average。使用 Maximum 判斷是否有些請求花費的時間大幅長於平均時間。請注意，Minimum 通常不太有用。 範例：假設您的負載平衡器在 us-west-2a 有 2 個執行個體，在 us-west-2b 有 2 個執行個體，而傳送請求至 us-west-2a 的 1 個執行個體時，有較高的延遲。us-west-2a 的平均值高於 us-west-2b 的平均值。

指標	描述
RequestCount	已完成的請求數量或在指定時間間隔 (1 或 5 分鐘) 內建立的連線數量。 【HTTP接聽程式】 接收和路由的請求數量，包括來自已註冊執行個體的HTTP錯誤回應。 【TCP接聽程式】 對已註冊執行個體的連線數。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。請注意，Minimum、Maximum 與 Average 都會傳回 1。 範例：假設您的負載平衡器在 us-west-2a 有 2 個執行個體，在 us-west-2b 有 2 個執行個體，並且有 100 個請求傳送至負載平衡器。有 60 個請求傳送至 us-west-2a，每個執行個體接收 30 個請求，有 40 個請求傳送至 us-west-2b，每個執行個體接收 20 個請求。使用 AvailabilityZone 維度，us-west-2a 總計有 60 個請求，us-west-2b 總計有 40 個請求。使用 LoadBalancerName 維度，總計有 100 個請求。

指標	描述
SpilloverCount	由於突增佇列已滿，導致請求遭拒的總數。 【HTTP接聽程式】 負載平衡器傳回 HTTP 503 錯誤碼。 【TCP接聽程式】 負載平衡器會關閉連線。 報告條件：有非零值 統計資訊：最實用的統計資訊是 Sum。請注意，每個負載平衡器節點都會回報 Average、Minimum 及 Maximum，但通常不太有用。 範例：假設您的負載平衡器已啟用 us-west-2a 與 us-west-2b，而 us-west-2a 中的執行個體出現高延遲，對請求的回應過慢。結果，us-west-2a 中的負載平衡器節點的突增佇列將會填入，導致溢出。如果 us-west-2b 繼續正常回應，負載平衡器的總和將與 us-west-2a 的總和相同。
SurgeQueueLength	正在等待路由至運作狀態良好的執行個體的請求 （HTTP接聽程式） 或連線 （TCP接聽程式） 總數。佇列的大小上限為 1,024。當佇列已滿，其他要求或連線將遭拒。如需詳細資訊，請參閱SpilloverCount 。 報告條件：有非零值。 統計資訊：最有用的統計資訊為 Maximum，因為它表示已排入佇列的請求峰值。Average 統計資訊與 Minimum 及 Maximum 組合時比較有用，可供判斷已排入佇列的請求範圍。請注意，Sum 不太有用。 範例：假設您的負載平衡器已啟用 us-west-2a 與 us-west-2b，而 us-west-2a 中的執行個體出現高延遲，對請求的回應過慢。結果，us-west-2a 中的負載平衡器節點的突增佇列將會填入，用戶端可能會遇到回應時間拉長的情況。如果此情況持續發生，負載平衡器可能會溢出 (請參閱 SpilloverCount 指標)。如果 us-west-2b 繼續正常回應，負載平衡器的 max 將與 us-west-2a 的 max 相同。

指標	描述
UnHealthyHostCount	已向您的負載平衡器註冊的不良狀態執行個體的數量。在執行個體超過運作狀態檢查中所設定的不良閾值之後，執行個體將被視為狀態不良。在執行個體符合運作狀態檢查中所設定的正常閾值之後，狀態不良的執行個體將再次被視為狀態正常。 報告條件：有已註冊的執行個體 統計資訊：最實用的統計資訊是 Average 與 Minimum。這些統計資訊由負載平衡器節點決定。請注意，有些負載平衡器節點可能會短暫判斷某執行個體狀態不良，同時其他節點則判斷該執行個體為狀態正常。 範例：請參閱 HealthyHostCount 。

如果您將 Classic Load Balancer 移轉至 Application Load Balancer，以下指標可讓您估計成本。這些指標僅供參考，不適用於 CloudWatch 警示。請注意，如果您的 Classic Load Balancer 有多個接聽程式，這些指標將會彙整各個接聽程式。

這些估算依據負載平衡器而定，它有一個預設規則及 2K 大小的憑證。如果使用 4K 或更大的憑證，建議您以下列方式進行估算：使用遷移工具，以您的 Classic Load Balancer 為基礎建立 Application Load Balancer，並監控 Application Load Balancer 的 ConsumedLCUs 指標。如需詳細資訊，請參閱 Elastic Load Balancing 使用指南中的從 Classic Load Balancer 移轉至 Application Load Balancer。

指標	描述
EstimatedALBActiveConnectionCount	從用戶端到負載平衡器以及從負載平衡器到目標的預估並行TCP連線數。
EstimatedALBConsumedLCUs	Application Load Balancer 使用的負載平衡器容量單位預估數量（LCU）。您為每小時LCUs使用的 數量付費。如需詳細資訊，請參閱「Elastic Load Balancing 定價」。
EstimatedALBNewConnectionCount	

指標	描述
	從用戶端到負載平衡器，以及從負載平衡器到目標建立的新TCP連線預估數量。
EstimatedProcessedBytes	Application Load Balancer 處理的位元組估計數量。

Classic Load Balancer 的指標維度

若要篩選 Classic Load Balancer 的指標，請使用下列維度。

維度	描述
AvailabilityZone	依指定的可用區域篩選指標資料。
LoadBalancerName	依指定的負載平衡器篩選指標資料。

Classic Load Balancer 指標的統計資料

CloudWatch 根據 Elastic Load Balancing 發佈的指標資料點提供統計資料。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，您可以為在特定可用區域中啟動的負載平衡器之後的所有運作狀態良好的EC2執行個體請求統計資料。

Minimum 與 Maximum 統計資料會反應由個別負載平衡器節點回報的最低與最高值。例如，假設有 2 個負載平衡器節點。一個節點有內含 Minimum 2、Maximum 10、Average 6 的 HealthyHostCount，而其他節點有內含 Minimum 1、Maximum 5、以及 Average 3 的 HealthyHostCount。因此，負載平衡器有 Minimum 1、Maximum 10、以及因為約為 4 的 Average。

Sum 統計資料為來自所有負載平衡器節點的彙總值。因為指標包含各期間的多個報告，Sum 僅適用於彙總跨所有負載平衡器節點的指標，例如 RequestCount、HTTPCode_ELB_XXX、HTTPCode_Backend_XXX、BackendConnectionErrors 和 SpilloverCount。

`SampleCount` 統計資料為測量而得的範本數量。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，使用 `HealthyHostCount`，`SampleCount` 是根據每個負載平衡器節點回報的範本數量，而非運作狀態良好的主機數量。

百分位數指出資料集之某個值的相對位置。您可以指定任何百分位數，最多使用兩位小數 (例如，p95.45)。例如，第 95 個百分位數表示 95% 的資料低於這個值，而 5% 高於這個值。百分位數通常用於隔離異常。例如，假設應用程式以 1-2 毫秒處理快取中的大部分請求，但如果快取是空的，則是 100-200 毫秒。上限會反映最慢的情況，大約 200 毫秒。平均數不表示資料的分佈。百分位數以更有意義的觀點表達應用程式的效能。透過使用第 99 百分位數作為 Auto Scaling 觸發條件或 CloudWatch 警示，您可以鎖定不超過 1% 的請求需要超過 2 毫秒來處理的目標。

檢視負載平衡器的 CloudWatch 指標

您可以使用 Amazon EC2主控台檢視負載平衡器的 CloudWatch 指標。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 主控台檢視負載平衡器的指標。

使用 主控台檢視指標

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選擇負載平衡器的名稱來開啟其詳細資訊頁面。
4. 選擇 Monitoring (監控) 索引標籤。
5. 若要取得單一指標的詳細資訊，請將滑鼠游標暫留在其圖形上，然後選擇 `Maximize` 圖示。下列指標可供使用：

   - 運作狀況良好主機 — `HealthyHostCount`
   - 運作狀況不良主機 — `UnHealthyHostCount`
   - 平均延遲 — `Latency`
   - 請求 — `RequestCount`
   - 後端連接錯誤 — `BackendConnectionErrors`
   - 突增佇列長度 — `SurgeQueueLength`
   - Spillover 計數 — `SpilloverCount`
   - HTTP 2XXs — `HTTPCode_Backend_2XX`
   - HTTP 3XXs — `HTTPCode_Backend_3XX`

- HTTP 4XXs — `HTTPCode_Backend_4XX`
- HTTP 5XXs — `HTTPCode_Backend_5XX`
- ELB HTTP 4XXs — `HTTPCode_ELB_4XX`
- ELB HTTP 5XXs — `HTTPCode_ELB_5XX`
- 預估處理的位元組 — `EstimatedProcessedBytes`
- 預估ALB已耗用 LCUs — `EstimatedALBConsumedLCUs`
- 預估ALB作用中連線計數 — `EstimatedALBActiveConnectionCount`
- 預估ALB新連線計數 — `EstimatedALBNewConnectionCount`

使用 CloudWatch 主控台檢視指標

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇 指標。
3. 选择 ELB 命名空间。
4. 執行以下任意一項：
   - 選取指標維度以透過負載平衡器、可用區域或跨所有負載平衡器檢視指標。
   - 若要檢視所有維度的指標，請在搜尋欄位中鍵入其名稱。
   - 若要檢視單一負載平衡器的指標，請在搜尋欄位中輸入其名稱。
   - 若要檢視單一可用區域的指標，請在搜尋欄位中輸入其名稱。

Classic Load Balancer 存取日誌

Elastic Load Balancing 提供存取日誌，可針對傳送到負載平衡器的請求，擷取其詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。您可以使用這些存取日誌來分析流量模式和排除問題。

存取日誌是 Elastic Load Balancing 的選用功能，預設為停用。對負載平衡器啟動存取日誌之後，Elastic Load Balancing 會擷取日誌並存放在您指定的 Amazon S3 儲存貯體中。您可以隨時停用存取記錄。

每個存取日誌檔案在儲存在 SSSE-S3S3 自動加密，並在您存取時解密。您不需要採取任何動作；加密和解密都是透明地執行。每個日誌檔案都會使用唯一金鑰加密，該金鑰本身會定期輪換的KMS金鑰加密。如需詳細資訊，請參閱Amazon Simple Storage Service 使用者指南中的使用伺服器端加密與Amazon S3-managed加密金鑰（SSE-S3）保護資料。

存取日誌無需額外收費。您將需支付 Amazon S3, 的儲存成本，但 Elastic Load Balancing 將日誌檔傳送到 Amazon S3, 所使用的頻寬不需要付費。如需儲存成本的詳細資訊，請參閱 Amazon S3 定價。

目錄

存取日誌檔

Elastic Load Balancing 在您指定的間隔發佈每個負載平衡器節點的日誌檔。當您啟用負載平衡器的存取日誌，您可以指定 5 分鐘或 60 分鐘的發佈間隔。在預設情況下，Elastic Load Balancing 在每 60 分鐘間隔發佈日誌。如果間隔設為 5 分鐘，會在 1:05、1:10、1:15 等間隔時間發佈日誌，以此類推。若間隔設為 5 分鐘，日誌交付的開始時間最多延遲 5 分鐘，若間隔設為 60 分鐘，則最多延遲 15 分鐘。您可以隨時修改發佈間隔。

負載平衡器可能在相同期間傳遞多個日誌。這通常發生於網站有高流量、多個負載平衡器節點和短日誌發佈間隔。

存取日誌的檔案名稱使用以下格式：

```
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

S3 儲存貯體的名稱。

prefix

(選用) 儲存貯體的字首 (邏輯階層)。您指定的字首不得包含字串 `AWSLogs`。如需詳細資訊，請參閱使用字首組織物件。

`AWSLogs`

我們在您指定的儲存貯體名稱和可選字首之後，增加了以 `AWSLogs` 開頭的檔案名稱部分。

aws-account-id

擁有者的帳戶 AWS ID。

region

負載平衡器和 S3 儲存貯體的區域。

yyyy/mm/dd

傳遞日誌的日期。

load-balancer-name

負載平衡器名稱。

end-time

記錄間隔結束的日期和時間。例如，如果發佈間隔為 5 分鐘，則 20140215T2340Z 的結束時間包含 23:40 和 23:35 項目之間的請求項目。

ip-address

處理請求之負載平衡器節點的 IP 地址。對於內部負載平衡器，這是私有 IP 地址。

random-string

系統產生的隨機字串。

以下是字首為 " 的日誌檔案名稱範例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
```

以下是不含字首的日誌檔案名稱範例：

```
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
```

日誌檔案可存放於儲存貯體任意長時間，但您也可以定義 Amazon S3 生命週期規則，自動封存或刪除日誌檔案。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的物件生命週期管理。

存取日誌項目

Elastic Load Balancing 會記錄傳送到負載平衡器的請求，包括從未送達後端執行個體的請求。例如，如果用戶端傳送格式不正確的請求，或沒有運作狀態良好的執行個體可回應請求，則仍然會記錄請求。

> **Important**
>
> Elastic Load Balancing 會盡可能記錄請求。建議您使用存取日誌來了解請求的性質，而不是為了全面解釋所有請求。

語法

每個日誌項目包含對負載平衡器所做的單一請求的詳細資訊。以空格分隔的日誌項目的所有欄位。日誌檔中的每個項目的格式如下：

```
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
```

下表說明存取日誌項目的欄位。

欄位	描述
time	負載平衡器收到用戶端請求的時間，格式ISO為 8601。
elb	負載平衡器名稱
client:port	提出請求之用戶端的 IP 地址和連接埠。
backend:port	處理此請求之已註冊執行個體的 IP 地址和連接埠。 如果該負載平衡器無法傳送請求到已註冊執行個體，或是執行個體在傳送回應之前關閉連線，則此值設定為 -。 如果已註冊的執行個體在閒置逾時之前沒有回應，這個值也可能設為 -。
request_processing_time	【HTTP接聽程式】 從負載平衡器收到請求到將請求傳送至已註冊執行個體所經過的總時間，以秒為單位。

欄位	描述
	【TCP接聽程式】 從負載平衡器接受來自用戶端的 TCP/SSL 連線到負載平衡器將第一個位元組資料傳送至已註冊執行個體所經過的總時間，以秒為單位。 如果負載平衡器無法將請求分派到已註冊執行個體，這個值會設為 -1。如果已註冊執行個體的在閒置逾時之前關閉連線，或用戶端傳送格式不正確的請求，就可能發生此情況。此外，對於TCP接聽者，如果用戶端與負載平衡器建立連線，但未傳送任何資料，則可能會發生這種情況。 如果已註冊的執行個體在閒置逾時之前沒有回應，這個值也可能設為 -1。
backend_processing_time	【HTTP接聽程式】 從負載平衡器將請求傳送至已註冊執行個體到執行個體開始傳送回應標頭所經過的總時間，以秒為單位。 【TCP接聽程式】 負載平衡器成功建立與已註冊執行個體連線所經過的總時間，以秒為單位。 如果負載平衡器無法將請求分派到已註冊執行個體，這個值會設為 -1。如果已註冊執行個體的在閒置逾時之前關閉連線，或用戶端傳送格式不正確的請求，就可能發生此情況。 如果已註冊的執行個體在閒置逾時之前沒有回應，這個值也可能設為 -1。
response_processing_time	【HTTP接聽程式】 從負載平衡器從已註冊執行個體收到回應標頭到開始將回應傳送至用戶端為止所經過的總時間（以秒為單位）。這包括負載平衡器上的佇列時間，以及從負載平衡器到用戶端的連線取得時間。 【TCP接聽程式】 從負載平衡器從已註冊執行個體收到第一個位元組到開始將回應傳送至用戶端所經過的總時間，以秒為單位。 如果負載平衡器無法將請求分派到已註冊執行個體，這個值會設為 -1。如果已註冊執行個體的在閒置逾時之前關閉連線，或用戶端傳送格式不正確的請求，就可能發生此情況。 如果已註冊的執行個體在閒置逾時之前沒有回應，這個值也可能設為 -1。

欄位	描述
elb_status_code	【HTTP接聽程式】 負載平衡器回應的狀態碼。
backend_status_code	【HTTP接聽程式】 來自已註冊執行個體之回應的狀態碼。
received_bytes	從用戶端 (請求者) 收到的請求大小 (以位元組為單位)。 【HTTP接聽程式】 值包含請求內文，但不包含標頭。 【TCP接聽程式】 值包含請求內文和標頭。
sent_bytes	傳回到用戶端 (請求者) 的回應大小 (以位元組為單位)。 【HTTP接聽程式】 值包含回應內文，但不包含標頭。 【TCP接聽程式】 值包含請求內文和標頭。
請求	以雙引號括住且以下列格式記錄的用戶端請求行：HTTPMethod + Protocol：//Host header：port + Path + HTTP version。記錄請求 時，負載平衡器會保留用戶端URL傳送的 。 URI它不會為存取日誌檔案設定內容類型。當您處理此欄位時，請考慮用戶端如何傳送 URL。 【TCP接聽程式】 URL有三個破折號，每個破折號以空格分隔，並以空格（"- - - "）結尾。
user_agent	【HTTP/HTTPS listener】 使用者代理字串，用於識別發起請求的用戶端。此字串包含一或多個產品識別符，product[/version]。如果字串超過 8 KB，則會截斷。
ssl_cipher	【HTTPS/SSL listener】 SSL 密碼。只有在成功交涉後建立傳入 SSL/TLS 連線時，才會記錄此值。否則，值設定為 -。
ssl_protocol	【HTTPS/SSL 接聽程式】 SSL通訊協定。只有在成功交涉後建立傳入 SSL/TLS 連線時，才會記錄此值。否則，值設定為 -。

範例

範例HTTP項目

以下是HTTP接聽程式（連接埠 80 到連接埠 80）的日誌項目範例：

```
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"
 - -
```

範例HTTPS項目

以下是HTTPS接聽程式（連接埠 443 到連接埠 80）的日誌項目範例：

```
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
```

範例TCP項目

以下是TCP接聽程式（連接埠 8080 到連接埠 80）的日誌項目範例：

```
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 "- - - " "-" - -
```

範例SSL項目

以下是SSL接聽程式（連接埠 8443 到連接埠 80）的日誌項目範例：

```
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
```

處理存取日誌

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。您可能無法使用 line-by-line處理處理來處理如此大量的資料。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 是一種互動式查詢服務，可讓您使用標準 輕鬆分析 Amazon S3 中的資料SQL。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的查詢 Classic Load Balancer 日誌。
- Loggly
- Splunk
- Sumo Logic

啟用 Classic Load Balancer 的存取日誌

若要啟用負載平衡器的日誌記錄，您必須指定 Amazon S3 儲存貯體的名稱，供負載平衡器存放日誌。您也必須連接儲存貯體政策到此儲存貯體，其授權 Elastic Load Balancing 寫入儲存貯體。

任務

- 步驟 1：建立 S3 儲存貯體
- 步驟 2：連接政策到您的 S3 儲存貯體
- 步驟 3：設定存取日誌
- 步驟 4：確認儲存貯體許可
- 故障診斷

步驟 1：建立 S3 儲存貯體

當您啟用存取日誌時，您必須為存取日誌檔案指定 S3 儲存貯體。儲存貯體必須符合下列需求。

要求

- 儲存貯體與負載平衡器必須位於相同的 Region (區域)。儲存貯體和負載平衡器可以由不同的帳戶擁有。
- 支援的唯一伺服器端加密選項是 Amazon S3-managed金鑰（SSE-S3）。如需詳細資訊，請參閱 Amazon S3-managed加密金鑰（SSE-S3）。

使用 Amazon S3 主控台建立 S3 儲存貯體

1. 在 開啟 Amazon S3 主控台https://console.aws.amazon.com/s3/。
2. 選擇建立儲存貯體。
3. 在 Create bucket (建立儲存貯體) 頁面上，執行下列操作：
   a. 針對 Bucket name (儲存貯體名稱)，輸入儲存貯體的名稱。該名稱在 Amazon S3 中所有現有的儲存貯體名稱之間，不得重複。在某些區域，可能會對儲存貯體的名稱進行其他限制。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的儲存貯體限制與局限。
   b. 針對 AWS 區域，選取您建立負載平衡器時所在的區域。
   c. 對於預設加密 ，選擇 Amazon S3-managed金鑰（SSE-S3）。
   d. 選擇建立儲存貯體。

步驟 2：連接政策到您的 S3 儲存貯體

您的 S3 儲存貯體必須擁有儲存貯體政策，以授權 Elastic Load Balancing 將存取日誌寫入到儲存貯體。儲存貯體政策是以存取政策語言編寫的JSON陳述式集合，用於定義儲存貯體的存取許可。每個陳述式包含單一許可的相關資訊，且包含一系列的元素。

如果您目前使用的儲存貯體有已連接的政策，您可以將 Elastic Load Balancing 存取日誌的陳述式加入至政策中。若您這麼做，建議您評估所產生的一組許可，以確保它們適用於需要存取儲存貯體以取得存取日誌的使用者。

可用的儲存貯體政策

您將使用的儲存貯體政策取決於儲存貯體 AWS 區域 的 。

2022 年 8 月或之後可用的區域

此政策會將許可授予指定的日誌交付服務。針對下列「區域」內的「可用區域」和「本地區域」中的負載平衡器使用此政策：

- 亞太區域 (海德拉巴)
- 亞太區域 （馬來西亞）
- 亞太區域 (墨爾本)
- 加拿大西部 (卡加利)
- 歐洲 (西班牙)
- 歐洲 (蘇黎世)
- 以色列 (特拉維夫)
- 中東 （UAE）

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-loadbalancer-logs/logging-prefix/
AWSLogs/012345678912/*"
```

```
    }
  ]
}
```

2022 年 8 月前可用的區域

此政策會將許可授予指定的 Elastic Load Balancing 帳戶 ID。針對下列清單中 「區域」內的「可用區域」或「本地區域」中的負載平衡器使用此政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "s3-bucket-arn"
    }
  ]
}
```

Replace (取代) *elb-account-id* 搭配您 區域的 Elastic Load Balancing AWS 帳戶 ID：

- 美國東部 (維吉尼亞北部) – 127311923021
- 美國東部 (俄亥俄) – 033677994240
- 美國西部 (加利佛尼亞北部) – 027434742980
- 美國西部 (奧勒岡) – 797873946194
- 非洲 (開普敦) – 098369216593
- 亞太區域 (香港) – 754344448648
- 亞太區域 (雅加達) – 589379963580
- 亞太區域 (孟買) – 718504428378
- 亞太區域 (大阪) – 383597477331
- 亞太區域 (首爾) – 600734575887
- 亞太區域 (新加坡) – 114774131450
- 亞太區域 (雪梨) – 783225319266
- 亞太區域 (東京) – 582318560864

- 加拿大 (中部) – 985666609251
- 歐洲 (法蘭克福) – 054676820928
- 歐洲 (愛爾蘭) – 156460612806
- 歐洲 (倫敦) – 652711504416
- 歐洲 (米蘭) – 635631232127
- 歐洲 (巴黎) – 009996457667
- 歐洲 (斯德哥爾摩) – 897822967062
- 中東 (巴林) – 076674570225
- 南美洲 (聖保羅) – 507241528517

Replace (取代) *s3-bucket-arn* 存取日誌位置ARN的 。ARN 您指定的 取決於您在步驟 3 中啟用存取日誌時是否計劃指定字首。

- ARN 具有字首的範例

```
arn:aws:s3:::amzn-s3-demo-loadbalancer-logs/logging-prefix/AWSLogs/012345678912/*
```

- ARN 沒有字首的範例

```
arn:aws:s3:::amzn-s3-demo-loadbalancer-logs/AWSLogs/012345678912/*
```

AWS GovCloud (US) Regions

此政策會將許可授予指定的 Elastic Load Balancing 帳戶 ID。在下列清單中的可用區域或 AWS GovCloud (US) 區域中的負載平衡器使用此政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "s3-bucket-arn"
    }
```

```
  ]
}
```

Replace (取代) *elb-account-id* 搭配您 AWS 帳戶 區域的 AWS 帳戶 Elastic Load Balancing 的 ID：

- AWS GovCloud （美國西部） – 048591011584
- AWS GovCloud （美國東部） – 190560391635

Replace (取代) *s3-bucket-arn* 存取日誌位置ARN的 。ARN 您指定的 取決於您在步驟 3 中啟用存取日誌時是否計劃指定字首。

- ARN 具有字首的範例

```
arn:aws-us-gov:s3:::amzn-s3-demo-loadbalancer-logs/logging-prefix/
AWSLogs/012345678912/*
```

- ARN 沒有字首的範例

```
arn:aws-us-gov:s3:::amzn-s3-demo-loadbalancer-logs/AWSLogs/012345678912/*
```

使用 Amazon S3 主控台，將存取日誌的儲存貯體政策連接到儲存貯體

1. 在 開啟 Amazon S3 主控台https://console.aws.amazon.com/s3/。
2. 選取儲存貯體的名稱，開啟其詳細資訊頁面。
3. 選擇 Permissions (許可)，然後選擇 Bucket policy (儲存貯體政策)、Edit (編輯)。
4. 更新儲存貯體政策，授予所需許可。
5. 選擇 Save changes (儲存變更)。

步驟 3：設定存取日誌

使用下列程序來設定存取日誌，以擷取請求資訊並將日誌檔案交付至 S3 儲存貯體。

要求

儲存貯體必須符合步驟 1 中所述的要求，且您必須按照步驟 2 所述連接儲存貯體政策。如果您指定字首，則不得包含字串 "AWSLogs"。

使用主控台為您的負載平衡器設定存取日誌

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選取您負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的監控區段中，執行下列操作：
   a. 啟用存取日誌。
   b. 針對 S3 URI，輸入日誌檔案URI的 S3。URI 您指定的 取決於您是否使用字首。
      - URI 加上字首： `s3://amzn-s3-demo-loadbalancer-logs/logging-prefix`
      - URI 沒有字首： `s3://amzn-s3-demo-loadbalancer-logs`
   c. 將日誌間隔保留為 `60 minutes - default`。
   d. 選擇 Save changes (儲存變更)。

使用 設定負載平衡器的存取日誌 AWS CLI

首先，建立 .json 檔案，以讓 Elastic Load Balancing 每個 60 分鐘擷取和交付日誌檔到您為日誌建立的 S3 儲存貯體：

```
{
  "AccessLog": {
    "Enabled": true,
    "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
    "EmitInterval": 60,
    "S3BucketPrefix": "my-app"
  }
}
```

接下來，在modify-load-balancer-attributes命令中指定 .json 檔案，如下所示：

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

以下是回應範例。

```
{
```

```
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
            "EmitInterval": 60,
            "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
            "S3BucketPrefix": "my-app"
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

管理存取日誌的 S3 儲存貯體

在刪除您為存取日誌設定的儲存貯體之前，請務必停用存取日誌。否則，如果在 中建立的新儲存貯體名稱相同，且 AWS 帳戶 具有您未擁有的必要儲存貯體政策，則 Elastic Load Balancing 可以將負載平衡器的存取日誌寫入此新儲存貯體。

步驟 4：確認儲存貯體許可

為負載平衡器啟用存取日誌之後，Load Balancing 會驗證 S3 儲存貯體，並建立測試檔案，以確保儲存貯體政策指定所需的許可。您可以使用 S3 主控台來確認是否已建立測試檔案。測試檔案不是實際的存取日誌檔案；它不包含範例記錄。

驗證 Elastic Load Balancing 已在 S3 儲存貯體中建立測試檔案

1. 在 開啟 Amazon S3 主控台https://console.aws.amazon.com/s3/。
2. 選取您為存取日誌指定的 S3 儲存貯體名稱。
3. 導覽到測試檔案，`ELBAccessLogTestFile`。位置取決於您是否使用字首。
   - 具有字首的位置：*amzn-s3-demo-loadbalancer-logs*/*logging-prefix*/AWSLogs/*123456789012*/ELBAccessLogTestFile
   - 沒有字首的位置：*amzn-s3-demo-loadbalancer-logs*/AWSLogs/*123456789012*/ELBAccessLogTestFile

故障診斷

儲存貯體的存取遭拒：***bucket-name***。 請檢查 S3bucket許可

如果您收到此錯誤，則以下是可能的原因：

- 儲存貯體政策不會授權 Elastic Load Balancing 將存取日誌寫入儲存貯體。確認您正在使用適合該區域的正確儲存貯體政策。驗證資源ARN是否使用您在啟用存取日誌時指定的相同儲存貯體名稱。如果您在啟用存取日誌時未指定字首，請確認資源ARN不包含字首。
- 儲存貯體使用不支援的伺服器端加密選項。儲存貯體必須使用 Amazon S3-managed金鑰（SSE-S3）。

停用 Classic Load Balancer 的存取日誌

您可以隨時對負載平衡器停用存取日誌。在您停用存取日誌之後，存取日誌會保留在 Amazon S3 中，直到將它們刪除為止。如需詳細資訊，請參閱Amazon Simple Storage Service 使用者指南中的使用 S3 儲存貯體。

使用主控台為您的負載平衡器停用存取日誌

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格的 Load Balancing (負載平衡器)，選擇 Load Balancer (負載平衡器)。
3. 選取您負載平衡器的名稱來開啟其詳細資訊頁面。
4. 在屬性索引標籤中，選擇編輯。
5. 在編輯負載平衡器屬性頁面的監控區段中，停用存取日誌。

使用 停用存取日誌 AWS CLI

使用下列modify-load-balancer-attributes命令來停用存取日誌：

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

以下是回應範例：

```
{
    "LoadBalancerName": "my-loadbalancer",
    "LoadBalancerAttributes": {
        "AccessLog": {
            "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
            "EmitInterval": 60,
            "Enabled": false,
            "S3BucketPrefix": "my-app"
        }
```

```
    }
}
```

故障診斷 Classic Load Balancer

下表列出故障診斷資源，有助您尋找使用 Classic Load Balancer 的實用資訊。

API錯誤

錯誤
CertificateNotFound：未定義
OutofService：發生暫時性錯誤

HTTP錯誤

錯誤
HTTPBADREQUEST
HTTPMETHODNOTALLOWED
HTTP408: 請求逾時
HTTP502: 網關錯誤
HTTP503: 無法使用此服務
HTTP504：閘道逾時

回應代碼指標

回應代碼指標
HTTPCodeELB_
HTTPCodeELB_
HTTPCode_ 回端
HTTPCode_ 回端

回應代碼指標
HTTPCode_ 回程
HTTPCode_ 回端

運作狀態檢查問題

問題
運作狀態檢查目標頁面錯誤
與執行個體的連線已經逾時。
公有金鑰身分驗證失敗
執行個體不會接收負載平衡器的流量
執行個體上未開啟連接埠
Auto Scaling 群組中的執行個體未通過ELB健康狀態檢查

連線問題

問題
用戶端無法連接到面向網際網路的負載平衡器
負載平衡器不會收到傳送至自訂域的請求
HTTPS傳送至負載平衡器的要求會傳回「NET:: ERR CERT _ _ COMMON _ NAME _ _INVALID」

執行個體註冊問題

問題
註冊EC2執行個體花費太長時間
無法註冊從付費啟動的執行個體 AMI

疑難排解 Classic Load Balancer：API錯誤

以下是 Elastic Load Balancing 傳回的錯誤訊息API、可能的原因，以及您可以採取解決問題的步驟。

錯誤訊息

- CertificateNotFound：未定義
- OutofService：發生暫時性錯誤

CertificateNotFound：未定義

原因 1：當使用 AWS Management Console建立憑證時，傳播憑證到所有區域發生延遲。當發生此延遲，建立負載平衡器的程序的最後一個步驟出現錯誤訊息。

解決方案 1：等待約 15 分鐘，然後再試一次。如果問題仍存在，請前往 AWS Support Center 尋求協助。

原因 2：如果您API直接使用 AWS CLI 或，如果您為不存在的憑證提供 Amazon 資源名稱 (ARN)，則可能會收到此錯誤。

解決方案 2：使用 AWS Identity and Access Management (IAM) 動作GetServerCertificate取得憑證，ARN並確認您為ARN.

OutofService：發生暫時性錯誤

原因：在 Elastic Load Balancing 服務或基本網路內發生暫時性內部問題。當 Elastic Load Balancing 查詢負載平衡器及其已註冊的執行個體的運作狀態時，這也可能發生暫時性問題。

解決方案：重試API呼叫。如果問題仍存在，請前往 AWS Support Center 尋求協助。

疑難排解 Classic Load Balancer：HTTP錯誤

該HTTP方法（也稱為動詞）指定要在接收HTTP請求的資源上執行的動作。HTTP請求的標準方法在 RFC 2616「方法定義」中定義。標準方法包括GETPOST、PUT、HEAD、和OPTIONS。一些 Web 應用程序需要（有時也會引入）方法，這些方法是 HTTP /1.1 方法的擴展。HTTP擴充方法的常見範例包括PATCHREPORTMKCOLPROPFIND、MOVE、、和LOCK。Elastic Load Balancing 接受所有標準和非標準HTTP方法。

HTTP請求和響應使用標題字段發送有關HTTP消息的信息。標頭欄位是以冒號分隔的名稱值組，以歸位字元 (CR) 和換行 (LF) 分隔。一組標準的標HTTP題欄位是在 RFC 2616「訊息標頭」中定義的。如需詳細資訊，請參閱HTTP標題和傳統負載平衡器。

當負載平衡器收到請HTTP求時，它會檢查格式錯誤的請求以及方法的長度。向負載平衡器發出HTTP要求的總方法長度不得超過 127 個字元。如果HTTP要求通過這兩項檢查，負載平衡器會將要求傳送至EC2執行個體。如果請求中的方法欄位格式不正確，負載平衡器會回應HTTPBADREQUEST錯誤。如果請求中的方法長度超過 127 個字元，負載平衡器會回應HTTPMETHODNOTALLOWED錯誤。

該實EC2例通過在請求中實現該方法並將響應發送回客戶端來處理有效的請求。必須設定您的執行個體，以處理這兩種支援和不支援的方法。

以下是您的負載平衡器傳回的錯誤訊息、可能原因，以及解決問題所需採取的步驟。

錯誤訊息

- HTTPBADREQUEST
- HTTPMETHODNOTALLOWED
- HTTP408: 請求逾時
- HTTP502: 網關錯誤
- HTTP503: 無法使用此服務
- HTTP504：閘道逾時

HTTPBADREQUEST

Description：表示用戶端傳送錯誤的請求。

原因 1：用戶端傳送格式錯誤的要求，不符合HTTP規格。例如，請求中不能包含空格URL。

原因 2：客戶端使HTTPCONNECT用了 Elastic Load Balancing 不支持的方法。

解決方案：直接連接到您的執行個體，並擷取用戶端請求的詳細資訊。檢閱標頭和格式錯誤URL的要求。確認要求符合HTTP規格。請確認HTTPCONNECT未使用。

HTTPMETHODNOTALLOWED

描述：表示方法長度無效。

原因：請求標頭中的方法長度超過 127 個字元。

解決方案：檢查方法的長度。

HTTP408: 請求逾時

描述：表示用戶端取消請求，或無法傳送完整的請求。

原因 1：網路中斷或錯誤的請求建構，例如部分的格式標頭；指定的內容大小不符實際傳輸的內容大小，以此類推。

解決方案 1：檢查提出請求的程式碼，並嘗試直接傳送到您註冊的執行個體 (或開發/測試環境)，其讓您更能掌控檢查實際的請求。

原因 2：與用戶端連線已關閉 (負載平衡器無法傳送回應)

解決方案 2：利用發出請求的機器上的封包偵測程式來確認用戶端未在傳送回應之前關閉連線。

HTTP502: 網關錯誤

描述：指出負載平衡器無法剖析從已註冊之執行個體傳送的回應。

原因：來自執行個體的錯誤回應，或可能的負載平衡器問題。

解決方案：確認從執行個體傳送的回應是否符合HTTP規格。前往 AWS Support Center 尋求協助。

HTTP503: 無法使用此服務

描述：指出執行個體或已註冊的負載平衡器造成錯誤。

原因 1：負載平衡器中的容量不足，無法處理請求。

解決方案 1：這應該是暫時性問題，不應持續超過幾分鐘時間。如果問題仍存在，請前往 AWS Support Center 尋求協助。

原因 2：沒有已註冊的執行個體。

解決方案 2：在您的負載平衡器設定為回應的每個可用區域中，至少註冊一個執行個體。通過查看中的`HealthyHostCount`指標來驗證這一點 CloudWatch。如果您無法確保在每個可用區域註冊執行個體，我們建議啟用跨區域的負載平衡。如需詳細資訊，請參閱為 Classic Load Balancer 設定跨區域負載平衡。。

原因 3：沒有正常運作的執行個體。

解決方案 3：請確定在您的負載平衡器設定為回應的每個可用區域中，都有運作狀況良好的執行個體。請透過查看 `HealthyHostCount` 指標來確認。

原因 4：突增佇列已滿。

解決方案 4：確認您的執行個體有足夠的容量能處理請求速率。請透過查看 `SpilloverCount` 指標來確認。

HTTP504：閘道逾時

描述：指出負載平衡器已關閉連線，因為請求未在閒置逾時期間內完成。

原因 1：應用程式需要比設定的閒置逾時更長時間來回應。

解決方案 1：監控 `HTTPCode_ELB_5XX` 和 `Latency` 指標。如果這些指標有提高，原因可能是由於應用程式內沒有在閒置逾時時間內回應。如需有關即將逾時的請求的詳細資訊，請在負載平衡器上啟用存取日誌，並檢閱 Elastic Load Balancing 所產生的日誌中的 504 回應碼。如有需要，您可以增加容量或增加設定的閒置逾時，讓冗長的操作 (例如，上傳大型檔案) 可以完成。如需詳細資訊，請參閱為 Classic Load Balancer 設定閒置連線逾時及如何排除 Elastic Load Balancing 高延遲問題。

原因 2：註冊的執行個體關閉與 Elastic Load Balancing 的連線。

解決方案 2：在EC2執行個體上啟用持續作用設定，並確定保持連線逾時大於負載平衡器的閒置逾時設定。

故障診斷 Classic Load Balancer：回應代碼指標

您的負載平衡器會將傳送給 CloudWatch 用戶端的HTTP回應代碼指標傳送給 Amazon，將錯誤來源識別為負載平衡器或已註冊的執行個體。您可以使用負載平衡器傳回 CloudWatch 的指標來疑難排解問題。如需詳細資訊，請參閱CloudWatch Classic Load Balancer 的指標。

以下是負載平衡器傳回 CloudWatch 的回應程式碼測量結果、可能原因，以及解決問題時可採取的步驟。

回應代碼指標

- HTTPCodeELB_
- HTTPCodeELB_
- HTTPCode_ 回端
- HTTPCode_ 回端
- HTTPCode_ 回程
- HTTPCode_ 回端

HTTPCodeELB_

原因：來自用戶端的格式錯誤或已取消的請求。

解決方案

- 請參閱 HTTPBADREQUEST。
- 請參閱 HTTPMETHODNOTALLOWED。
- 請參閱 HTTP408: 請求逾時。

HTTPCodeELB_

原因：負載平衡器或已註冊的執行個體造成錯誤，或負載平衡器無法剖析回應。

解決方案

- 請參閱 HTTP502: 網關錯誤。
- 請參閱 HTTP503: 無法使用此服務。
- 請參閱 HTTP504：閘道逾時。

HTTPCode_ 回端

原因：來自註冊的執行個體的正常且成功的回應。

解決方案：無。

HTTPCode_ 回端

原因：從已註冊的執行個體傳送的重新導向回應。

解決方案：檢視您執行個體上的存取日誌或錯誤日誌，以判定原因。直接傳送請求到執行個體 (繞過負載平衡器)，以檢視回應。

HTTPCode_ 回程

原因：從已註冊的執行個體傳送的用戶端錯誤回應。

解決方案：檢視您執行個體上的存取日誌或錯誤日誌，以判定原因。直接傳送請求到執行個體 (繞過負載平衡器)，以檢視回應。

> **Note**
>
> 如果用戶端取消了使用`Transfer-Encoding: chunked`標頭起始的HTTP要求，則負載平衡器會將要求轉送至執行個體，即使用戶端取消了要求，也會發生已知問題。這可能導致後端錯誤。

HTTPCode_ 回端

原因：從已註冊的執行個體傳送的伺服器錯誤回應。

解決方案：檢視您執行個體上的存取日誌或錯誤日誌，以判定原因。直接傳送請求到執行個體 (繞過負載平衡器)，以檢視回應。

> **Note**
>
> 如果用戶端取消了使用`Transfer-Encoding: chunked`標頭起始的HTTP要求，則負載平衡器會將要求轉送至執行個體，即使用戶端取消了要求，也會發生已知問題。這可能導致後端錯誤。

故障診斷 Classic Load Balancer：運作狀態檢查

您的負載平衡器會檢查其已註冊執行個體的運作狀態，使用方式是透過 Elastic Load Balancing 所提供預設的運作狀態檢查組態，或是您指定的自訂運作狀態檢查組態。運作狀態檢查組態包含資訊，例如通訊協定、ping 連接埠、ping 路徑、回應逾時及運作狀態檢查間隔。如果在運作狀態檢查間隔內傳回 200 個回應代碼，執行個體會被視為運作狀態良好。如需詳細資訊，請參閱Classic Load Balancer 執行個體的 Health 狀態檢查。

如果部分或所有執行個體目前狀態是 `OutOfService`，且描述欄位顯示訊息`Instance has failed at least the Unhealthy Threshold number of health checks consecutively`，則表示執行個體的負載平衡器運作狀態檢查失敗。以下是要尋找的問題、可能原因，以及解決問題所需採取的步驟。

問題

- 運作狀態檢查目標頁面錯誤
- 與執行個體的連線已經逾時。
- 公有金鑰身分驗證失敗

- 執行個體不會接收負載平衡器的流量
- 執行個體上未開啟連接埠
- Auto Scaling 群組中的執行個體未通過ELB健康狀態檢查

運作狀態檢查目標頁面錯誤

問題：在指定的偵測連接埠和偵測路徑上發出給執行個體的HTTPGET要求 (例如，: 80/index.htmlHTTP) 會收到非 200 回應碼。

原因 1：未在執行個體上設定目標頁面。

解決方案 1：在每個註冊執行個體建立目標頁面 (例如， `index.html`)，並指定其路徑做為 ping 路徑。

原因 2：在回應中未設定 Content-Length 標頭的值。

解決方案 2：如果回應包含內文，然後將 Content-Length 標頭設為大於或等於零的值，或設定 Transfer-Encoding 值為「區塊」。

原因 3：應用程式未設定為從負載平衡器接收請求，或傳回 200 回應代碼。

解決方案 3：檢查您執行個體上的應用程式以調查原因。

與執行個體的連線已經逾時。

問題：負載平衡器向EC2執行個體發出的 Health 狀態檢查要求逾時或間歇性失敗。

首先，直接連接執行個體以驗證該問題。我們建議您使用執行個體的私有 IP 地址，從網路內連接到您的執行個體。

對TCP連接使用以下命令：

```
telnet private-IP-address-of-the-instance port
```

對HTTP或HTTPS連接使用以下命令：

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

如果您正在使用HTTP/HTTPS連接並獲得非 200 響應，請參閱運作狀態檢查目標頁面錯誤。如果您能夠直接連接到執行個體，請檢查下列各項：

原因 1：執行個體在設定的回應逾時時間內沒有回應。

解決方案 1：在負載平衡器的運作狀態檢查的組態中調整回應逾時設定。

原因 2：執行個體承受極大的負載，並使用超過您設定的回應逾時時間來回應。

解決方案 2：

- 檢查監視圖表是否過度使用。CPU如需詳細資訊，請參閱 Amazon EC2 使用者指南中的取得特定EC2執行個體的統計資料。
- 透過連線至您的執行個體，檢查其他應用程式資源的使用率，例如記憶EC2體或限制。
- 如有必要，新增更多執行個體或啟用 Auto Scaling。如需詳細資訊，請參閱 Amazon EC2 Auto Scaling 使用者指南。

原因 3：如果您使用HTTP或HTTPS連線，而且正在 ping 路徑欄位中指定的目標頁面上執行健全狀況檢查 (例如，`HTTP:80/index.html`)，則目標頁面的回應時間可能會比您設定的逾時更長。

解決方案 3：使用較簡單的運作狀態檢查目標頁面，或調整運作狀態檢查間隔設定。

公有金鑰身分驗證失敗

問題：設定為在啟用後端驗證的情況下使用HTTPS或SSL通訊協定的負載平衡器會失敗公開金鑰驗證。

原因：SSL證書上的公鑰與負載平衡器上配置的公鑰不匹配。使用 `s_client` 命令查看憑證鏈中的伺服器憑證清單。如需詳細資訊，請參閱開啟SSL文件中的 s_client。

解決方案：您可能需要更新SSL憑證。如果您的SSL憑證是最新的，請嘗試在負載平衡器上重新安裝憑證。如需詳細資訊，請參閱取代 Classic Load Balancer 的SSL憑證。

執行個體不會接收負載平衡器的流量

問題：執行個體的安全群組封鎖來自負載平衡器的流量。

在執行個體上擷取封包以確認問題。使用下列命令：

```
# tcpdump port health-check-port
```

原因 1：與執行個體關聯的安全群組不允許負載平衡器的流量。

解決方案 1：編輯執行個體安全群組，以允許來自負載平衡器的流量。新增規則以允許來自負載平衡器安全群組的所有流量。

原因 2：負載平衡器的安全性群組不允許流量傳送至EC2執行個體。

解決方案 2：編輯負載平衡器的安全性群組，以允許子網路和EC2執行個體的流量。

如需管理安全群組的資訊，請參閱 設定您的 Classic Load Balancer 的安全群組。

執行個體上未開啟連接埠

問題：負載平衡器傳送至EC2執行個體的健康狀態檢查已遭連接埠或防火牆封鎖。

使用下列命令以確認問題：

```
netstat -ant
```

原因：指定的運作狀態連接埠或接聽程式連接埠 (如果設定不同) 未開啟。兩個指定的連接埠的運作狀態檢查和接聽程式連接埠，必須開啟和接聽。

解決方案：在您的執行個體上開啟接聽程式連接埠，和您的運作狀態檢查組態中指定的連接埠 (如果設定不同)，以接收負載平衡器流量。

Auto Scaling 群組中的執行個體未通過ELB健康狀態檢查

問題：Auto Scaling 群組中的執行個體通過預設的 Auto Scaling 健康狀態檢查，但未通過ELB健康狀態檢查

原因：Auto Scaling 使用EC2狀態檢查來偵測執行個體的硬體和軟體問題，但負載平衡器會傳送要求至執行個體並等待 200 個回應碼，或是建立與執行個體的TCP連線 (針對TCP基於健康狀態檢查)，來執行健康狀態檢查。

執行個體可能會失敗ELB健康狀態檢查，因為執行個體上執行的應用程式存在問題，導致負載平衡器將執行個體視為停止服務。此執行個體可能會通過 Auto Scaling 健康狀態檢查；它不會被 Auto Scaling 政策取代，因為根據EC2狀態檢查將其視為健康狀態。

解決方案：使用「Auto Scaling」群組的ELB健康狀態檢查。使用ELB健康狀態檢查時，Auto Scaling 會同時檢查執行個體狀態檢查和健康狀態檢查的結果，以判斷執行個體的ELB健康狀態。如需詳細資訊，請參閱 Amazon Auto Scaling 使用者指南中的將運作狀態檢查新增至您的 EC2 Auto Scaling 群組。

故障診斷 Classic Load Balancer：用戶端連線能力

用戶端無法連接到面向網際網路的負載平衡器

如果負載平衡器未回應請求，則請檢查下列問題：

您的面向網際網路的負載平衡器已連接到私有子網路

您必須為負載平衡器指定公有子網路。公用子網路具有前往您虛擬私有雲之網際網路閘道的路由 (VPC)。

安全性群組或網路ACL不允許流量

負載平衡器的安全性群組和負載平衡器子網路ACLs的任何網路都必須允許來自用戶端的輸入流量以及接聽程式連接埠上的用戶端的輸出流量。如需詳細資訊，請參閱設定您的 Classic Load Balancer 的安全群組。

負載平衡器不會收到傳送至自訂域的請求

如果負載平衡器未收到傳送至自訂域的請求，則請檢查下列問題：

自訂域名稱未解析為負載平衡器 IP 地址

- 使用命令列介面確認自訂域名稱解析的目標 IP 地址。
  - Linux、macOS 或 Unix – 您可以在終端內使用 `dig` 命令。例如 `dig example.com`
  - Windows – 您可以在命令提示內使用 `nslookup` 命令。例如 `nslookup example.com`
- 使用命令列介面確認負載平衡器DNS名稱解析為何 IP 位址。
- 比較兩種輸出的結果。IP 地址必須相符。

HTTPS傳送至負載平衡器的要求會傳回「NET:: ERR CERT _ _ COMMON _ NAME _ _INVALID」

如果HTTPS要求是`NET::ERR_CERT_COMMON_NAME_INVALID`從負載平衡器接收，請檢查下列可能原因：

- HTTPS要求中使用的網域名稱與接聽程式相關聯ACM憑證中指定的替代名稱不符。
- 正在使用負載平衡器預設DNS名稱。預設DNS名稱無法用來提出要HTTPS求，因為無法針對`*.amazonaws.com`網域要求公用憑證。

故障診斷 Classic Load Balancer：執行個體註冊

當您向負載平衡器註冊的執行個體，需要採取好幾個步驟後，負載平衡器才能開始傳送請求到您的執行個體。

以下是您的負載平衡器在註冊EC2執行個體時可能遇到的問題、潛在原因，以及解決問題時可能採取的步驟。

問題

- 註冊EC2執行個體花費太長時間
- 無法註冊從付費啟動的執行個體 AMI

註冊EC2執行個體花費太長時間

問題：已註冊的EC2執行個體所花費的時間超過預期的`InService`狀態。

原因：您的執行個體可能無法通過執行運作狀態檢查。在初次完成執行個體註冊步驟後 (最多約 30 秒)，負載平衡器會開始傳送運作狀態檢查請求。您的執行個體不是 `InService`，直到一個運作狀態檢查成功。

解決方案：請參閱與執行個體的連線已經逾時。。

無法註冊從付費啟動的執行個體 AMI

問題：Elastic Load Balancing 未註冊使用付費啟動的執行個體AMI。

原因：您的執行個體可能是使用 Amazon 付費AMI啟動的 DevPay。

解決方案：Elastic Load Balancing 不支援註冊使用 Amazon 付費啟動AMIs的執行個體 DevPay。請注意，您可以AMIs從 AWS Marketplace 使用付費功能。如果您已經使用付費AMI來源 AWS Marketplace ，但無法註冊從該付費啟動的執行個體AMI，請前往中AWS Support 心尋求協助。

Classic Load Balancer 的配額

您的 AWS 帳戶有每項 AWS 服務的預設配額 (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。

若要檢視 Classic Load Balancer 的配額，請開啟 Service Quotas console (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。您也可以使用 describe-account-limits(AWS CLI) 命令進行 Elastic Load Balancing。

若要請求提高配額，請參閱《Service Quotas 使用者指南》中的請求提高配額。

您的 AWS 帳戶具有下列與傳統負載平衡器相關的配額。

名稱	預設	可調整
每個區域的 Classic Load Balancer	20	是
每個 Classic Load Balancer 的接聽程式	100	是
每個 Classic Load Balancer 已註冊的執行個體	1,000	是

傳統負載平衡器的文件歷史記錄

下表說明 Classic Load Balancer 各版本。

變更	描述	日期
去同步緩解模式	新增對非同步緩和模式的支援。如需詳細資訊，請參閱設定 Classic Load Balancer 的不同步緩和模式。	2020 年 8 月 17 日
傳統負載平衡器	隨著應用程式負載平衡器和網路負載平衡器的推出，使用 2016-06-01 API 建立的負載平衡器現在稱為傳統負載平衡器。如需這些負載平衡器類型之間差異的詳細資訊，請參閱 E lastic Load Balancing 功能。	2016 年 8 月 11 日
Support AWS Certificate Manager（ACM）	您可以向負載平衡器要求SSL/TLS憑證，ACM並將其部署到負載平衡器。如需詳細資訊，請參閱 SSL/傳統負載平衡器的TLS憑證。	2016 年 1 月 21 日
Support 其他連接埠	負載平衡器可以監聽範圍 1-65535 的任何連接埠。如需詳細資訊，請參閱 C lassic Load Balancer 的接聽程式。	2015 年 9 月 15 日
存取日誌項目的其他欄位	新增 `user_agent` 、`ssl_cipher` 和 `ssl_protocol` 欄位。如需詳細資訊，請參閱存取記錄檔。	2015 年 5 月 18 日
Support 標記負載平衡器	從此發行版本開始，Elastic Load Balancing CLI (ELBCLI)	2014 年 8 月 11 日

	已由 AWS Command Line Interface (AWS CLI) 取代，這是用來管理多個 AWS 服務的統一工具。ELBCLI版本 1.0.35.0（日期為 14 年 7 月 24 日）之後發布的新功能將包含在唯一的。 AWS CLI 如果您目前正在使用 ELBCLI，建議您 AWS CLI 改用。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》。	
閒置連線逾時	您可以設定負載平衡器的閒置連接逾時。	2014 年 7 月 24 日
Support 授與使用者和群組存取特定負載平衡器或API動作	您可以建立原則來授與使用者和群組存取特定負載平衡器或API動作。	2014 年 5 月 12 日
Support AWS CloudTrail	您可 CloudTrail 以使用擷取您 AWS 帳戶 使用ELBAPI、、或代表您API撥打的呼叫 AWS CLI。 AWS Management Console ELB CLI如需詳細資訊，請 API Classic Load Balancer 用 AWS CloudTrail.	2014 年 4 月 4 日
連接排水	新增連接耗盡的相關資訊。有了這項支援，您可以在執行個體取消註冊，或執行個體在讓現有的連線保持開啟狀態時卻使運作狀態變得不好，此時您可讓負載平衡器停止傳送新請求到已註冊的執行個體。如需詳細資訊，請參閱設定 Classic Load Balancer 的連線排除。	2014 年 3 月 20 日

訪問日誌	您可以讓負載平衡器擷取有關傳送至負載平衡器的請求的詳細資訊，並將其存放在 Amazon S3 儲存貯體中。如需詳細資訊，請參閱 Classic Load Balancer 的存取記錄。	2014 年 3 月 6 日
對於 .1-1.2 的 TLSv1 Support	已新增有HTTPS關使用/接聽程式設定之負載平衡器之 TLSv1 .1-1.2 通訊協定支援的資訊。SSL有了這項支援，「Elastic Load Balancing」也會更新預先定義的SSL交涉組態。如需更新之預先定義SSL交涉組態的相關資訊，請參閱傳統負載平衡器的SSL交涉組態。如需更新目前SSL交涉組態的相關資訊，請參閱更新 Classic Load Balancer 的SSL交涉組態。	2014 年 2 月 19 日
跨區域負載平衡	已新增有關啟用跨區域負載平衡器的負載平衡的資訊。如需詳細資訊，請參閱為 C lassic Load Balancer 設定跨區域負載平衡。	2013 年 11 月 6 日
其他 CloudWatch 量度	已新增有關 Elastic Load Balancing 報告之額外 Cloudwatch 指標關資訊。如需詳細資訊，請參閱 C lassic Load Balancer 的CloudWatch 指標。	2013 年 10 月 28 日

Support 代理協議	已新增有關為TCP/SSL連線設定之負載平衡器的 Proxy 通訊協定支援的資訊。如需詳細資訊，請參閱 Proxy 通訊協定標頭。	2013 年 7 月 30 日
Support DNS 容錯移轉	新增有關為負載平衡器設定 Amazon Route 53 DNS 容錯移轉的相關資訊。如需詳細資訊，請參閱為負載平衡器使用 Amazon Route 53 DNS 容錯移轉。	二○一三年六月三日
主控台支援檢視 CloudWatch 指標和建立警示	已新增有關使用主控台檢視 CloudWatch 指定負載平衡器的指標和建立警示的資訊。如需詳細資訊，請參閱 C lassic Load Balancer 的CloudWatch 指標。	2013 年 3 月 28 日
Support 在預設值中註冊EC2執行個體 VPC	已新增預設啟動EC2執行個體的支援VPC。	2013 年 3 月 11 日
內部負載平衡器	透過此版本，虛擬私有雲 (VPC) 中的負載平衡器可設為內部或網際網路對向。內部負載平衡器具有可公開解析的DNS名稱，可解析為私有 IP 位址。面向網際網路的負載平衡器具有可公開解析的DNS名稱，可解析為公用 IP 位址。如需詳細資訊，請參閱建立內部 Classic Load Balancer。	2012 年 6 月 10 日

主控台支援管理接聽器、密碼設定和憑證 SSL	如需詳細資訊，請參閱設定 Classic Load Balancer 的HTTPS接聽程式和取代 Classic Load Balancer 的SSL憑證。	2012 年 5 月 18 日
Support Amazon 中的 Elastic Load Balancing VPC	已新增在虛擬私有雲 (VPC) 中建立負載平衡器的支援。	2011 年 11 月 21 日
Amazon CloudWatch	您可以使用 CloudWatch. 如需詳細資訊，請參閱 C lassic Load Balancer 的CloudWatch 指標。	2011 年 10 月 17 日
其他安全功能	您可以設定SSL加密、後端和後端SSL伺服器驗證。如需詳細資訊，請參閱使用HTTPS接聽程式建立 Classic Load Balancer。	2011 年 8 月 30 日
區域頂點域名	如需詳細資訊，請參閱設定 Classic Load Balancer 的自訂網域名稱。	2011 年 5 月 24 日
Support X 轉送原型和 X 轉送連接埠排針座	X-Forwarded-Proto 標頭表示原始請求的通訊協定，而 X-Forwarded-Port 標頭表示原始請求的連接埠。加入請求的這些標頭可讓客戶判斷傳入負載平衡器的請求是否已加密，以及收到請求的負載平衡器上的特定連接埠。如需詳細資訊，請參閱HTTP標頭和傳統負載平衡器。	2010 年 10 月 27 日

Support HTTPS	在此版本中，您可以利用SSL/通TLS訊協定加密流量，並將應用程式執行個體的SSL處理卸載到負載平衡器。此功能也可在負載平衡器上集中管理SSL伺服器憑證，而不是管理個別應用程式執行個體上的憑證。	2010 年 10 月 14 日
Support AWS Identity and Access Management（IAM）	增加了對IAM.	2010 年 9 月 2 日
黏性工作階段	如需詳細資訊，請參閱為 Classic Load Balancer 設定黏滯工作階段。	二○一○年四月七日
AWS SDK for Java	已新增對 Java SDK 的支援。	2010 年 3 月 22日
AWS SDK for .NET	增加了對 AWS SDK for .NET.	2009 年 11 月 11 日
新的服務	推出 Elastic Load Balancing 初始公用 Beta 版。	2009 年 5 月 18 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。