aws

经典负载均衡器

Elastic Load Balancing

Elastic Load Balancing: 经典负载均衡器

Table of Contents

什么是经典负载均衡器？

> **Note**
>
> 经典负载均衡器是 Elastic Load Balancing 中的上一代负载均衡器。我们建议您迁移到最新一代的负载均衡器。有关更多信息，请参阅迁移您的 Classic Load Balancer。

Elastic Load Balancing 会自动将您的传入流量分配到一个或多个可用区域中的多个目标，例如 EC2 实例、容器和 IP 地址。它会监控已注册目标的运行状况，并仅将流量传输到运行状况良好的目标。弹性负载均衡 根据传入流量随时间的变化对负载均衡器进行扩展。它可以自动扩缩来处理绝大部分工作负载。

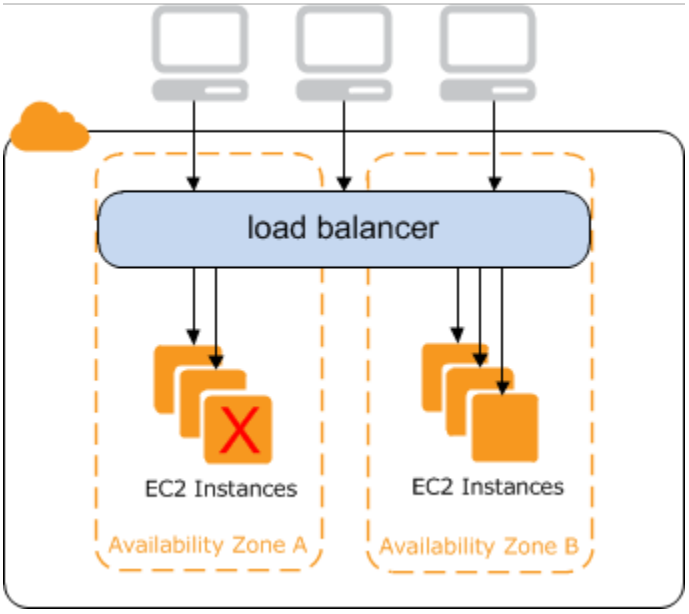
经典负载均衡器概述

负载均衡器将传入的应用程序流量分配到多个可用区的多个 EC2 实例上。这可提高应用程序的容错能力。弹性负载均衡会检测运行状况不佳的实例，并将流量仅路由到运行正常的实例。

您的负载均衡器将作为客户端的单一接触点。这将提高应用程序的可用性。您可以根据需求变化在 负载均衡器中添加和删除实例，而不会中断应用程序的整体请求流。弹性负载均衡 根据传输到应用程序的流量随时间的变化对负载均衡器进行扩展。弹性负载均衡 能够自动扩展来处理绝大部分工作负载。

侦听器 使用您配置的协议和端口来检查来自客户端的连接请求，并使用您配置的协议和端口号将请求转发到一个或多个注册实例。可以向您的负载均衡器添加一个或多个侦听器。

您可以配置运行状况检查，这些检查可用来监控已注册实例的运行状况，以便负载均衡器仅将请求发送到正常实例。



要确保您的注册实例能够处理每个可用区中的请求负载，每个可用区中向负载均衡器注册的实例的数量必须大致相同。例如，如果您在 us-west-2a 可用区中有十个实例，在 us-west-2b 可用区中有两个实例，则请求将在两个可用区之间平均分配。因此，us-west-2b 中的两个实例便会与 us-west-2a 中的十个实例承担相同的流量。应改为每个可用区中有六个实例。

默认情况下，负载均衡器在为您的负载均衡器启用的可用区之间均匀分配流量。要在所有启用的可用区中的所有注册实例间平均分配流量，请在您的负载均衡器上启用跨区域负载均衡。但我们仍然建议您在每个可用区中保持大致相等的实例数，以便实现更好的容错能力。

有关更多信息，请参阅 弹性负载均衡 用户指南中的 Elastic Load Balancing 工作原理

优势

使用经典负载均衡器而不是应用程序负载均衡器具有以下好处：

- 支持 TCP 和 SSL 侦听器
- 支持使用应用程序生成的 cookie 的粘性会话

要详细了解每种负载均衡器类型支持的功能，请参阅 弹性负载均衡 产品比较。

如何开始

- 要了解如何创建 Classic Load Balancer 并向其注册 EC2 实例，请参阅创建面向 Internet 的经典负载均衡器。

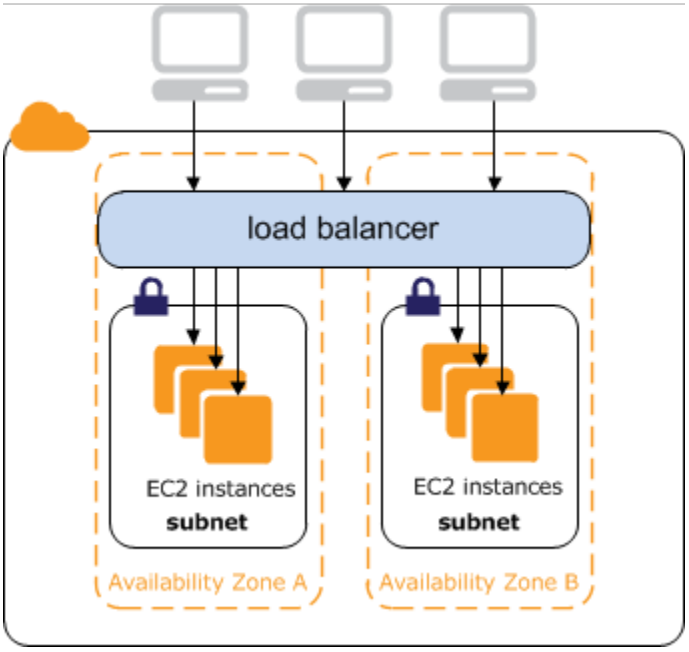
- 要了解如何创建 HTTPS 负载均衡器并向其注册 EC2 实例，请参阅创建带有 HTTPS 侦听器的经典负载均衡器。
- 要了解如何使用经典负载均衡器支持的各种特征，请参阅配置经典负载均衡器。

定价

利用负载均衡器，您可以按实际用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。

面向 Internet 的经典负载均衡器

创建经典负载均衡器时，您可以使其成为内部负载均衡器或面向 Internet 的负载均衡器。面向互联网的负载均衡器具有可公开解析的 DNS 名称，因此它可以通过互联网将来自客户端的请求路由到在负载均衡器中注册的 EC2 实例。



内部负载均衡器的 DNS 名称可公开解析为节点的私有 IP 地址。因此，内部负载均衡器可路由的请求只能来自对负载均衡器的 VPC 具有访问权限的客户端。有关更多信息，请参阅 内部负载均衡器。

内容

您的负载均衡器的公有 DNS 名称

创建负载均衡器后，它会收到一个公有 DNS 名称，客户端可使用该名称发送请求。DNS 服务器将您的负载均衡器的 DNS 名称解析为您负载均衡器的负载均衡器节点的公有 IP 地址。每个负载均衡器节点均使用私有 IP 地址连接到后端实例。

控制台显示具有以下格式的公有 DNS 名称：

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

创建面向 Internet 的经典负载均衡器

创建负载均衡器时，您配置侦听器、配置运行状况检查并注册后端实例。通过指定前端 (客户端到负载均衡器) 连接的协议和端口以及后端 (负载均衡器到后端实例) 连接的协议和端口来配置侦听器。可以为负载均衡器配置多个侦听器。

本教程通过基于 Web 的界面提供了经典负载均衡器的实际操作介绍。 AWS Management Console您将创建一个负载均衡器，用于接收公有 HTTP 流量并将其发送到您的 EC2 实例。

要使用 HTTPS 侦听器创建负载均衡器，请参阅创建带有 HTTPS 侦听器的经典负载均衡器。

任务

- 开始前的准备工作
- 使用创建 Classic Load Balancer AWS Management Console

开始前的准备工作

- 创建虚拟私有云（VPC）。有关更多信息，请参阅 关于 VPC 的建议。
- 启动您计划向负载均衡器注册的 EC2 实例。确保这些实例的安全组允许端口 80 上的 HTTP 访问。
- 在每个实例上安装一个 Web 服务器，例如，Apache 或 Internet Information Services (IIS)。在连接到 Internet 的 Web 浏览器的地址字段中输入其 DNS 名称，并确保浏览器显示该服务器的默认页面。

使用创建 Classic Load Balancer AWS Management Console

按照以下过程创建经典负载均衡器。提供负载均衡器的基本配置信息，例如名称和模式。然后提供有关网络以及要将流量路由到实例的侦听器的信息。

使用控制台创建经典负载均衡器

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航栏上，选择您的负载均衡器所在的区域。请务必选择与您为 EC2 实例选择的相同区域。
3. 在导航窗格上的 Load Balancing (负载均衡) 下，选择 Load Balancers (负载均衡器)。
4. 选择 Create Load Balancer (创建负载均衡器)。
5. 展开经典负载均衡器部分，然后选择创建。
6. 基本配置

a. 对于负载均衡器名称，键入负载均衡器的名称。

   在当前区域的经典负载均衡器集内，经典负载均衡器的名称必须唯一，最多可以有 32 个字符，只能包含字母数字字符和连字符，不能以连字符开头或结尾。

b. 对于模式，选择面向互联网。

7. 网络映射

   a. 对于 VPC，选择您为实例选择的 VPC。

   b. 对于映射，首先选择一个可用区，然后从其可用子网中选择一个公有子网。每个可用区只能选择一个子网。要提高负载均衡器的可用性，请选择多个可用区和子网。

8. 安全组

   - 对于安全组，选择一个配置为允许在端口 80 上传输所需 HTTP 流量的现有安全组。

9. 侦听器和路由

   a. 对于侦听器，确保协议为 HTTP，端口为 80。

   b. 对于实例，确保协议为 HTTP，端口为 80。

10. 运行状况检查

    a. 对于 Ping 协议，确保协议为 HTTP。

    b. 对于 Ping 端口，确保端口为 80。

    c. 对于 Ping 路径，确保路径为 /。

    d. 对于高级运行状况检查设置，请使用默认值。

11. 实例

    a. 选择添加实例，这时将显示实例选择页面。

    b. 在可用实例下，您可以根据当前的网络设置，从负载均衡器可用的当前实例中进行选择。

    c. 确认选择无误后，选择确认以将要注册的实例添加到负载均衡器。

12. Attributes

    - 对于启用跨可用区负载均衡、启用连接耗尽以及超时（耗尽间隔时间），请保留默认值。

13. 负载均衡器标签（可选）

    a. 键字段为必填项。

    b. 值字段为可选项。

c. 要添加其他标签，请选择添加新标签，然后输入键字段的值，以及可选的值字段的值。

d. 要移除现有标签，请选择要移除的标签旁的移除。

14. 摘要和创建

a. 如果需要更改任何设置，请选择需要更改的设置旁的编辑。

b. 确认摘要中显示的所有设置无误后，选择创建负载均衡器以开始创建负载均衡器。

c. 在最终创建页面上，选择查看负载均衡器以在 Amazon EC2 控制台中查看您的负载均衡器。

15. Verify

a. 选择新的负载均衡器。

b. 在目标实例选项卡中，选中运行状态列。在您的至少一个 EC2 实例处于服务状态后，您可以测试您的负载均衡器。

c. 在详细信息部分中，复制负载均衡器的 DNS 名称，这看起来类似于 `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`。

d. 将负载均衡器的 DNS 名称粘贴到已连接到公共互联网的 Web 浏览器地址栏中。如果负载均衡器运行正常，则会看到服务器的默认页面。

16. 删除（可选）

a. 如果您有一个指向负载均衡器的域的一个别名记录，请将它指向新的位置并等待 DNS 更改生效，然后再删除您的负载均衡器。

b. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

c. 选择负载均衡器。

d. 依次选择操作、删除负载均衡器。

e. 提示进行确认时，键入 `confirm`，然后选择删除。

f. 删除负载均衡器后，在该负载均衡器中注册的 EC2 实例将继续运行。您将按实例继续运行的部分或完整小时数付费。当您不再需要某个 EC2 实例时，可以停止或终止该实例，以免产生额外费用。

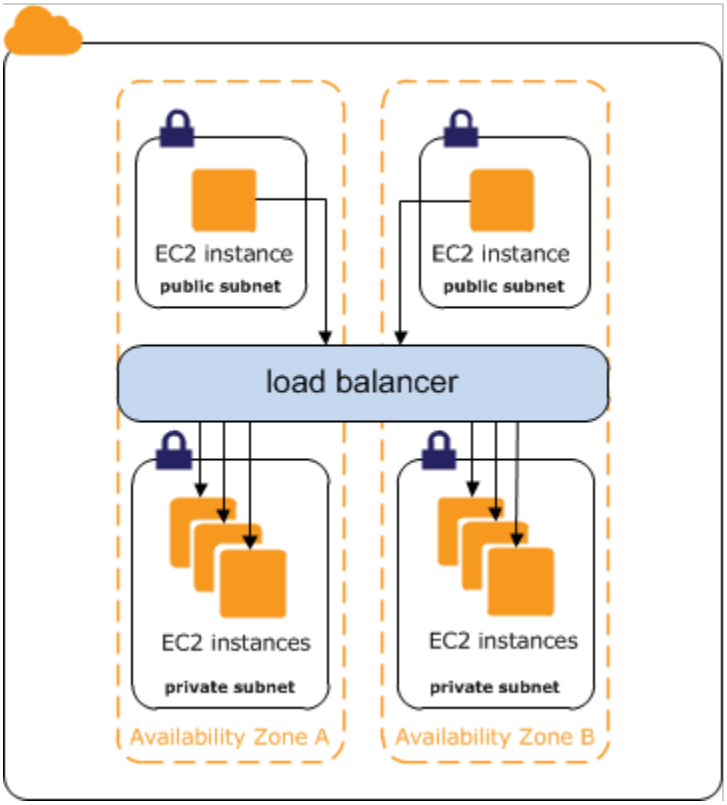
内部传统负载均衡器

在创建负载均衡器时，您必须选择使其成为内部负载均衡器还是面向 Internet 的负载均衡器。

面向 Internet 的负载均衡器的节点具有公共 IP 地址。面向 Internet 的负载均衡器的 DNS 名称可公开解析为节点的公共 IP 地址。因此，面向 Internet 的负载均衡器可以通过 Internet 路由来自客户端的请求。有关更多信息，请参阅 面向 Internet 的经典负载均衡器。

内部负载均衡器的节点只有私有 IP 地址。内部负载均衡器的 DNS 名称可公开解析为节点的私有 IP 地址。因此，内部负载均衡器可路由的请求只能来自对负载均衡器的 VPC 具有访问权限的客户端。

如果您的应用程序具有多个层（例如，必须连接到 Internet 的 Web 服务器和只连接到 Web 服务器的数据库服务器），则您可以设计一个同时使用内部负载均衡器和面向 Internet 的负载均衡器的架构。创建一个面向 Internet 的负载均衡器并向其注册 Web 服务器。创建一个内部负载均衡器并向它注册数据库服务器。Web 服务器接收来自面向 Internet 的负载均衡器的请求，并将数据库服务器的请求发送到内部负载均衡器。数据库服务器接收来自内部负载均衡器的请求。



内容

您的负载均衡器的公有 DNS 名称

在创建内部负载均衡器后，它将接收以下格式的公有 DNS 名称：

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

DNS 服务器将负载均衡器的 DNS 名称解析为内部负载均衡器的负载均衡器节点的私有 IP 地址。每个负载均衡器节点均通过弹性网络接口连接到后端实例的私有 IP 地址。如果启用了跨区域负载均衡，则每个节点都将连接到每个后端实例，而不考虑可用区。否则，每个节点仅连接到其可用区内的实例。

创建内部经典负载均衡器

您可以创建内部负载均衡器，将流量从有权访问负载均衡器的 VPC 的客户端分配到您的 EC2 实例。

内容

前提条件

- 如果您尚未为负载均衡器创建 VPC，则必须在开始操作前先创建它。有关更多信息，请参阅 关于 VPC 的建议。
- 启动您计划向内部负载均衡器注册的 EC2 实例。确保在打算用于负载均衡器的 VPC 中的私有子网中启动它们。

使用控制台创建内部负载均衡器

按照以下过程创建内部经典负载均衡器。提供负载均衡器的基本配置信息，例如名称和模式。然后提供有关网络以及要将流量路由到实例的侦听器的信息。

使用控制台创建内部经典负载均衡器

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航栏上，选择您的负载均衡器所在的区域。请务必选择与您为 EC2 实例选择的相同区域。
3. 在导航窗格上的 Load Balancing (负载均衡) 下，选择 Load Balancers (负载均衡器)。

4. 选择 Create Load Balancer (创建负载均衡器)。
5. 展开经典负载均衡器部分，然后选择创建。
6. 基本配置
   a. 对于负载均衡器名称，键入负载均衡器的名称。

      在当前区域的经典负载均衡器集内，经典负载均衡器的名称必须唯一，最多可以有 32 个字符，只能包含字母数字字符和连字符，不能以连字符开头或结尾。

   b. 对于模式，选择内部。
7. 网络映射
   a. 对于 VPC，选择您为实例选择的 VPC。
   b. 对于映射，首先选择一个可用区，然后从该可用区的可用子网中选择一个子网。每个可用区只能选择一个子网。要提高负载均衡器的可用性，请选择多个可用区和子网。
8. 对于安全组，选择一个配置为允许在端口 80 上传输所需 HTTP 流量的现有安全组。如果您的应用程序使用其他协议和端口，则也可以创建新的安全组。
9. 侦听器和路由
   a. 对于侦听器，确保协议为 HTTP，端口为 80。
   b. 对于实例，确保协议为 HTTP，端口为 80。
10. 运行状况检查
    a. 对于 Ping 协议，默认值为 HTTP。
    b. 对于 Ping 端口，默认值为 80。
    c. 对于 Ping 路径，默认值为 /。
    d. 对于高级运行状况检查设置，请使用默认值或输入应用程序特定的值。
11. 实例
    a. 选择添加实例，这时将显示实例选择页面。
    b. 在可用实例下，您可以根据之前选择的网络设置，从负载均衡器可用的当前实例中进行选择。
    c. 确认选择无误后，选择确认以将要注册的实例添加到负载均衡器。
12. Attributes
    - 对于启用跨可用区负载均衡、启用连接耗尽以及超时（耗尽间隔时间），请保留默认值。
13. 负载均衡器标签（可选）

a. 键字段为必填项。

b. 值字段为可选项。

c. 要添加其他标签，请选择添加新标签，然后输入键字段的值，以及可选的值字段的值。

d. 要移除现有标签，请选择要移除的标签旁的移除。

14. 摘要和创建

a. 如果需要更改任何设置，请选择需要更改的设置旁的编辑。

b. 确认摘要中显示的所有设置无误后，选择创建负载均衡器以开始创建负载均衡器。

c. 在最终创建页面上，选择查看负载均衡器以在 Amazon EC2 控制台中查看您的负载均衡器。

15. Verify

a. 选择新的负载均衡器。

b. 在目标实例选项卡中，选中运行状态列。在您的至少一个 EC2 实例处于服务状态后，您可以测试您的负载均衡器。

c. 在详细信息部分中，复制负载均衡器的 DNS 名称，这看起来类似于 `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`。

d. 将负载均衡器的 DNS 名称粘贴到已连接到公共互联网的 Web 浏览器地址栏中。如果负载均衡器运行正常，则会看到服务器的默认页面。

16. 删除（可选）

a. 如果您有一个指向负载均衡器的域的一个别名记录，请将它指向新的位置并等待 DNS 更改生效，然后再删除您的负载均衡器。

b. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

c. 选择负载均衡器。

d. 依次选择操作、删除负载均衡器。

e. 提示进行确认时，键入 `confirm`，然后选择删除。

f. 删除负载均衡器后，在该负载均衡器中注册的 EC2 实例将继续运行。您将按实例继续运行的部分或完整小时数付费。当您不再需要某个 EC2 实例时，可以停止或终止该实例，以免产生额外费用。

使用创建内部负载均衡器 AWS CLI

默认情况下，Elastic Load Balancing 会创建面向 Internet 的负载均衡器。使用以下过程创建内部负载均衡器，并将您的 EC2实例注册到新创建的内部负载均衡器。

创建内部负载均衡器

1. 使用将`--scheme`选项设置为的create-load-balancer命令`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
```

以下为响应示例。请注意，该名称表示这是一个内部负载均衡器。

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

2. 使用以下 register-instances-with-load-balancer 命令添加实例：

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

以下为响应示例：

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

3. （可选）使用以下describe-load-balancers命令验证内部负载均衡器：

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

响应包含 DNSName 和 Scheme 字段，表示这是一个内部负载均衡器。

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

配置经典负载均衡器

创建经典负载均衡器后，您可以更改其配置。例如，您可以更新负载均衡器的属性、子网和安全组。

负载均衡器属性

连接耗尽

如果启用，负载均衡器将允许在其从已取消注册或运行不正常的实例转移流量之前，完成现有请求。

跨可用区负载均衡

如果启用，则负载均衡器会在所有实例中均匀地路由请求流量，而不管可用区如何。

异步缓解模式

确定负载均衡器如何处理可能对您的应用程序构成安全风险的请求。可能的值为 `monitor`、`defensive` 和 `strictest`。默认为 `defensive`。

空闲超时

如果启用，则负载均衡器允许连接在指定的持续时间内保持空闲（不通过连接发送任何数据）。默认值为 60 秒。

粘性会话

经典负载均衡器支持基于持续时间和基于应用程序的会话粘性。

负载均衡器详细信息

安全组

负载均衡器的安全组必须允许侦听器端口和运行状况检查端口上的流量。

子网

您可将负载均衡器的能力扩展到其他子网。

代理协议

如果启用，我们会添加一个标头，其中包含发送到实例的连接信息。

标签

您可以添加标签以对负载均衡器进行分类。

配置经典负载均衡器的空闲连接超时

对于客户端通过经典负载均衡器发出的每个请求，负载均衡器将维护两个连接。前端连接位于客户端和负载均衡器之间。后端连接位于负载均衡器和注册 EC2 实例之间。负载均衡器具有应用于其连接的已配置空闲超时期限。超过空闲超时期限后，如果没有发送或接收任何数据，负载均衡器将关闭连接。为确保长时间运行的操作 (例如文件上传) 有足够时间来完成，请在到达每个空闲超时期限前发送至少 1 个字节的数据，并根据需要增大空闲超时期限的长度。

如果您使用 HTTP 和 HTTPS 侦听器，建议为实例启用 HTTP 保持活动选项。您可以在 实例的 Web 服务器设置中启用 保持活动选项。启用保持活动选项后，可使负载均衡器重复使用后端连接，直到保持活动超时过期。为确保由负载均衡器负责关闭与您的实例的连接，请确保设置的 HTTP 保持活动时间值大于为负载均衡器配置的空闲超时设置。

请注意，TCP 保持活动探测器不会阻止负载均衡器终止连接，因为它们不在有效负载中发送数据。

目录

使用控制台配置空闲超时

默认情况下，Elastic Load Balancing 将负载均衡器的空闲超时设置为 60 秒。使用以下过程为空闲超时设置不同的值。

使用控制台为负载均衡器配置空闲超时设置

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的流量配置部分中，键入空闲超时的值。空闲超时的范围为 1 到 4,000 秒。
6. 选择 Save changes（保存更改）。

使用 AWS CLI配置空闲超时

使用以下modify-load-balancer-attributes命令为您的负载均衡器设置空闲超时：

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

以下为响应示例：

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

配置经典负载均衡器的跨区域负载均衡

借助跨区域负载均衡，经典负载均衡器的每个负载均衡器节点会跨所有启用的可用区中的已注册实例平均分配请求。如果禁用了跨区域负载均衡，则每个负载均衡器节点会仅在其可用区中的已注册实例之间平均分配请求。有关更多信息，请参阅 Elastic Load Balancing 用户指南中的跨区域负载均衡。

跨区域负载均衡可降低在每个启用的可用区中保持相同数量实例的需求，并提高应用程序处理一个或多个实例丢失情况的能力。但我们仍然建议您在每个已启用的可用区中保持大致相等的实例数，以实现更高的容错能力。

对于客户端缓存 DNS 查找所在的环境，传入请求可能会优先选择一个可用区。通过使用跨区域负载均衡，请求负载中的这种不平衡将分散在此区域中的所有可用实例中，从而减小操作不良的客户端产生的影响。

在创建经典负载均衡器时，跨区域负载均衡的默认值取决于创建负载均衡器的方式。默认情况下，使用 API 或 CLI 时将禁用跨区域负载均衡。使用时 AWS Management Console，默认情况下会选择启用跨区域负载平衡的选项。创建经典负载均衡器后，您随时可以启用或禁用跨区域负载均衡。

目录

启用跨区域负载均衡

您随时可以对经典负载均衡器启用跨区域负载均衡。

使用控制台启用跨区域负载均衡

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的可用区路由配置部分中，启用跨可用区负载均衡。
6. 选择 Save changes（保存更改）。

要启用跨区域负载均衡，请使用 AWS CLI

1. 使用以下modify-load-balancer-attributes命令将您的负载均衡器的`CrossZoneLoadBalancing`属性设置为`true`：

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

以下为响应示例：

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

2. （可选）使用以下describe-load-balancer-attributes命令验证您的负载均衡器是否已启用跨区域负载均衡：

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

以下为响应示例：

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
```

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

禁用跨区域负载均衡

您随时可以对负载均衡器禁用跨区域负载均衡选项。

使用控制台禁用跨区域负载均衡

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的可用区路由配置部分中，禁用跨可用区负载均衡。
6. 选择 Save changes（保存更改）。

要禁用跨区域负载均衡，请将负载均衡器的 `CrossZoneLoadBalancing` 属性设置为 `false`。

要禁用跨区域负载均衡，请使用 AWS CLI

1. 使用以下 modify-load-balancer-attributes 命令：

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

以下为响应示例：

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

2. （可选）使用以下describe-load-balancer-attributes命令验证您的负载均衡器是否已禁用跨区域负载均衡：

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

以下为响应示例：

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

配置经典负载均衡器的 Connection Draining

要确保经典负载均衡器停止向正在取消注册或运行状况不佳的实例发送请求，并使现有连接保持打开状态，请使用 Connection Draining。这将使负载均衡器能够完成向正在取消注册或运行状况不佳的实例发出的进行中请求。

启用连接耗尽时，您可以指定在将实例报告为已取消注册之前，负载均衡器使连接保持活动状态的最大时间。最大超时值可设置为介于 1 和 3600 秒之间 (默认值为 300 秒)。当达到最大时间限制时，负载均衡器会强制关闭与正在取消注册的实例的连接。

在为进行中请求提供服务时，负载均衡器会将正在取消注册的实例的状态报告为 `InService: Instance deregistration currently in progress`。当正在取消注册的实例为所有进行中请求提供完服务时，或在达到最大超时限制时，负载均衡器会将实例状态报告为 `OutOfService: Instance is not currently registered with the LoadBalancer`。

如果实例运行状况不佳，则负载均衡器会将实例状态报告为 `OutOfService`。如果存在向运行状况不佳的实例发出的进行中请求，则会完成这些请求。最大超时限制不适用于与运行状况不佳的实例的连接。

如果您的实例属于 Auto Scaling 组，并且为负载均衡器启用了 Connection Draining，则 Auto Scaling 在由于扩展事件或运行状况检查替换而终止实例之前，将会等待进行中的请求完成或等待最大超时过期。

如果您希望负载均衡器立即关闭与正在取消注册的实例或运行状况不佳的实例的连接，则可以禁用连接耗尽。禁用连接耗尽后，不会完成向正在取消注册的实例或运行状况不佳的实例发出的任何进行中请求。

目录

启用 Connection Draining

您可以随时为负载均衡器启用连接耗尽。

使用控制台启用连接耗尽

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的流量配置部分中，选择启用连接耗尽。
6. （可选）对于超时（耗尽间隔时间），键入一个介于 1 到 3600 秒之间的值。如果您不做任何选择，则将使用 300 秒的默认值。

7. 选择 Save changes（保存更改）。

要启用连接耗尽，请使用 AWS CLI

使用以下 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}}"
```

以下为响应示例：

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

禁用 Connection Draining

您可以随时为负载均衡器禁用连接耗尽。

使用控制台禁用连接耗尽

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的流量配置部分中，取消选择启用连接耗尽。
6. 选择 Save changes（保存更改）。

要禁用连接耗尽，请使用 AWS CLI

使用以下 modify-load-balancer-attributes 命令：

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

以下为响应示例：

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

为经典负载均衡器配置粘性会话

默认情况下，经典负载均衡器会将每项请求单独路由到负载最小的已注册实例。但是，您可以使用粘性会话 功能 (也称为会话关联)，使负载均衡器能够将用户会话绑定到特定的实例。这可确保在会话期间将来自用户的所有请求发送到相同的实例中。

管理粘性会话的关键是确定负载均衡器一致地将用户请求路由到相同实例的时间长短。如果您的应用程序具有自己的会话 Cookie，则可以配置 Elastic Load Balancing，以便会话 Cookie 遵循应用程序会话 Cookie 指定的持续时间。如果您的应用程序没有自己的会话信息记录程序，您可以配置 Elastic Load Balancing，以通过指定您自己的粘性持续时间来创建会话信息记录程序。

Elastic Load Balancin AWSELB g 会创建一个名为的 cookie，用于将会话映射到实例。

要求

- HTTP/HTTPS 负载均衡器。
- 每个可用区内至少有一个运行状况良好的实例。

兼容性

- Cookie 路径属性的 RFC 允许使用下划线。不过，Elastic Load Balancing URI 将下划线字符编码为 %5F，因为某些浏览器（如 Internet Explorer 7）规定下划线的 URI 编码为 %5F。由于可能影响当前运行的浏览器，Elastic Load Balancing 继续对下划线字符进行 URI 编码。例如，如果 Cookie

具有属性 path=/my_path，则 Elastic Load Balancing 在转发请求中将此属性更改为 path=/my%5Fpath。

- 您不能对基于持续时间的会话粘性 Cookie 设置 secure 标志或 HttpOnly 标志。不过，这些 Cookie 不包含敏感数据。请注意，如果您在应用程序控制的会话粘性 Cookie 上设置secureHttpOnly标志或标志，则也会在 Cookie 上设置该标志或标志。 AWSELB
- 如果您在应用程序 cookie 的 Set-Cookie 域中有一个尾随分号，负载均衡器会忽略 cookie。

目录

基于持续时间的会话粘性

负载均衡器使用特殊的 Cookie 来跟踪向每个侦听器发出的每个请求的实例。 AWSELB在负载均衡器收到请求时，它首先会检查并查看请求中是否存在这个 Cookie。如果是这样的话，该请求会发送到 Cookie 中指定的实例。如果没有 Cookie，负载均衡器会根据现有的负载均衡算法选择一个实例。响应中会插入 Cookie，从而将同一用户发出的后续请求绑定到该实例中。粘性策略配置会定义 Cookie 的过期时间，从而确定每个 Cookie 的有效持续时间。负载均衡器不会刷新 Cookie 的过期时间，并且在使用 Cookie 前不会检查它是否已过期。Cookie 过期后，会话将不再具有粘性。一旦 Cookie 过期，客户端就会从其 Cookie 存储中删除 Cookie。

对于 CORS（跨源资源共享）请求，某些浏览器需要 SameSite=None; Secure 来启用粘性。在这种情况下，Elastic Load Balancing 会创建第二个粘性 cookie AWSELBCORS，其中包含与原始粘性 cookie 相同的信息以及此属性。SameSite客户端会同时收到这两个 Cookie。

如果实例失败或者实例运行状况不佳，负载均衡器会停止将请求路由到该实例，并根据现有负载均衡算法来选择新的运行状况良好的实例。此时会将请求路由到新实例，就像没有 Cookie 一样，会话不再具有粘性。

如果客户端切换到带其他后端端口的侦听器，粘性将丢失。

使用控制台为负载均衡器启用基于持续时间的粘性会话

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择管理侦听器。

5. 在管理侦听器页面上，找到要更新的侦听器，然后选择 Cookie 粘性下的编辑。
6. 在编辑 Cookie 粘性设置弹出窗口中，选择由负载均衡器生成。
7. （可选）对于有效期，键入 Cookie 有效期（以秒为单位）。如果不指定有效期，只要浏览器会话不中断，粘性会话就会持续。
8. 选择保存更改关闭弹出窗口。
9. 选择保存更改返回到负载均衡器详细信息页面。

使用 AWS CLI为负载均衡器启用基于持续时间的粘性会话

1. 使用以下 create-lb-cookie-stickiness- policy 命令创建由负载均衡器生成的 Cookie 粘性策略，Cookie 过期时间为 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. 使用以下 set-load-balancer-policiesof-listener 命令为指定的负载均衡器启用会话粘性：

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

> **Note**
>
> `set-load-balancer-policies-of-listener` 命令替换与指定负载均衡器端口关联的当前策略集。每次使用此命令时，请指定 `--policy-names` 选项以列出所有要启用的策略。

3. （可选）使用以下describe-load-balancers命令验证策略是否已启用：

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

响应包含以下信息，表明已在指定端口上为侦听器启用策略：

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

应用程序控制的会话粘性

负载均衡器使用一个特殊的 Cookie 将会话和处理初始请求的实例相关联，但会沿用策略配置中指定的应用程序 Cookie 的使用时间限制。负载均衡器只会在应用程序响应中包含新的应用程序信息记录程序时，才会插入新的粘性信息记录程序。负载均衡器粘性信息记录程序不会根据每项请求进行更新。如果应用程序信息记录程序被明确删除或过期，会话便会停止粘着，直至发布新的应用程序信息记录程序为止。

系统会将以下由后端实例设置的属性发送到 Cookie 中的客户端：path、port、domain、secure、httponly、discard、max-age、expires、version、comment、commenturl 和 samesite。

如果实例失败或者实例运行状况不佳，负载均衡器会停止将请求路由到该实例，并根据现有负载均衡算法来选择新的运行状况良好的实例。现在，负载均衡器将会话视为“附加”到新的正常运行实例，并继续将请求路由至该实例，即使之前失败的实例已恢复正常运行。

使用控制台启用应用程序控制的会话粘性

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择管理侦听器。
5. 在管理侦听器页面上，找到要更新的侦听器，然后选择 Cookie 粘性下的编辑。
6. 选择由应用程序生成。
7. 对于 Cookie Name，键入您的应用程序 Cookie 的名称。
8. 选择 Save changes（保存更改）。

要启用应用程序控制的会话粘性，请使用 AWS CLI

1. 使用以下 create-app-cookie-stickiness-policy 命令创建应用程序生成的 Cookie 粘性策略：

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

2. 使用以下 set-load-balancer-policiesof-listener 命令为负载均衡器启用会话粘性：

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

> **Note**
>
> set-load-balancer-policies-of-listener 命令替换与指定负载均衡器端口关联的当前策略集。每次使用此命令时，请指定 --policy-names 选项以列出所有要启用的策略。

3. （可选）使用以下describe-load-balancers命令验证粘性策略是否已启用：

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

4. 响应包含以下信息，表明已在指定端口上为侦听器启用策略：

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

为经典负载均衡器配置异步缓解模式

异步缓解模式可以保护您的应用程序不受由于 HTTP 异步造成的问题的影响。负载均衡器根据每个请求的威胁级别对请求进行分类，允许安全请求，然后根据您指定的缓解模式来减轻风险。异步缓解模式包括“监控”、“防御”和“最严格”。默认情况下采用“防御”模式，该模式可在保持应用程序可用性的同时，针对 HTTP 异步提供持久的缓解作用。您可以切换到最严格模式，确保应用程序只接收符合 RFC 7230 标准的请求。

http_desync_guardian 库会分析 HTTP 请求，防止发生 HTTP 异步攻击。有关更多信息，请参阅 github 上的 HTTP 异步监护。

目录

> **Tip**
>
> 此配置仅适用于经典负载均衡器。有关适用于 Application Load Balancer 的信息，请参阅取消 Application Load Balancers 的同步缓解模式。

分类

下面列出了这些分类。

- 合规 – 请求符合 RFC 7230 标准，不构成已知的安全威胁。

- 可接受 - 请求不符合 RFC 7230 标准，但不构成已知的安全威胁。
- 不明确 - 请求不符合 RFC 7230 标准，会带来风险，因为各个 Web 服务器和代理可能会以不同的方式处理该请求。
- 严重 - 请求会带来很高的安全风险。负载均衡器会阻止请求，向客户端提供 400 响应，并关闭客户端连接。

下面的列表描述了每个分类的问题。

可接受

- 标头包含非 ASCII 字符或控制字符。
- 请求版本包含错误的值。
- 对于 GET 或 HEAD 请求，有一个值为 0 的 Content-Length 标头。
- 请求 URI 包含一个未采用 URL 编码的空格。

不明确

- 请求 URI 包含控制字符。
- 请求同时包含 Transfer-Encoding 标头和 Content-Length 标头。
- 存在多个具有相同值的 Content-Length 标头。
- 标头是空的，或者有一行中只包含空格。
- 有一个标头可以使用常见的文本规范化技术标准化为 Transfer-Encoding 或 Content-Length。
- GET 或 HEAD 请求有 Content-Length 标头。
- GET 或 HEAD 请求有 Transfer-Encoding 标头。

严重

- 请求 URI 包含 Null 字符或回车符。
- Content-Length 标头包含一个无法解析或不是有效数字的值。
- 标头包含 Null 字符或回车符。
- Transfer-Encoding 标头包含错误的值。
- 请求方法格式不正确。
- 请求版本格式不正确。

- 存在多个具有不同值的 Content-Length 标头。
- 存在多个 Transfer-Encoding: chunked 标头。

如果请求不符合 RFC 7230 标准，负载均衡器将递增 `DesyncMitigationMode_NonCompliant_Request_Count` 指标。有关更多信息，请参阅 经典负载均衡器指标。

模式

下表描述 Classic Load Balancers 如何根据模式和分类来处理请求。

分类。	监控模式	防御模式	最严格模式
合规	已允许	已允许	已允许
可接受	已允许	已允许	阻止
不明确	已允许	已允许[1]	阻止
严重	已允许	阻止	阻止

[1] 系统将路由请求，但关闭客户端和目标连接。

修改异步缓解模式

使用控制台更新异步缓解模式

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的流量配置下，选择防御 – 推荐、最严格 或 监控。
6. 选择 Save changes（保存更改）。

要更新不同步缓解模式，请使用 AWS CLI

使用elb.http.desyncmitigationmode属性设置为monitordefensive、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
```

下面是 attribute.json 的内容。

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

为经典负载均衡器配置代理协议

代理协议是一种 Internet 协议，用于将连接信息从请求连接的源传递到请求连接到的目标。Elastic Load Balancing 使用代理协议版本 1，该版本使用人类可读的标头格式。

默认情况下，在对前端和后端连接使用传输控制协议 (TCP) 时，您的经典负载均衡器会将请求转发到实例，而不修改请求标头。如果您启用代理协议，则会向请求标头添加一个用户可读的标头，其中包含连接信息（如源 IP 地址、目标 IP 地址和端口号）。该标头随后作为请求的一部分发送到实例。

> **Note**
>
> AWS Management Console 不支持启用代理协议。

内容

代理协议标头

在您具有负载均衡器来使用 TCP 进行后端连接时，代理协议标头有助于识别客户端的 IP 地址。因为负载均衡器会拦截客户端与您的实例之间的流量，因此您实例的访问日志中将包含负载均衡器的 IP 地址而不是原始客户端的 IP 地址。您可以分析该请求的第一行，以检索该客户端的 IP 地址和端口号。

标头中的代理地址 IPv6 是您的负载均衡器的公共 IPv6 地址。此 IPv6 地址与从您的负载均衡器的 DNS 名称中解析的 IP 地址相匹配，该名称以`ipv6`或开头`dualstack`。如果客户端与连接 IPv4，则标头中的代理地址是负载均衡器的私有 IPv4 地址，无法通过 DNS 查询进行解析。

该代理协议行以回车符和换行符 (`"\r\n"`) 结束，并且具有以下形式：

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

例如： IPv4

以下是的代理协议行示例 IPv4。

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

启用代理协议的先决条件

开始之前，请执行以下操作：

- 确认您的负载均衡器不在启用了代理协议的代理服务器之后。如果在代理服务器和负载均衡器上同时启用了代理协议，则负载均衡器会向已具有来自代理服务器的标头的请求添加另一个标头。根据实例的配置方式，这种重复可能会导致错误。
- 确认您的实例可以处理代理协议信息。
- 确认您的侦听器设置支持代理协议。有关更多信息，请参阅 经典负载均衡器的侦听器配置。

使用 AWS CLI启用代理协议

要启用代理协议，您需要创建 `ProxyProtocolPolicyType` 类型的策略，然后在实例端口上启用该策略。

使用以下过程为您的负载均衡器创建 `ProxyProtocolPolicyType` 类型的新策略，将新创建的策略应用于端口 `80` 上的实例，然后确认已启用该策略。

为负载均衡器启用代理协议

1. （可选）使用以下 describe-load-balancer-policy-types 命令列出 Elastic Load Balancing 支持的策略：

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

响应包含支持的策略类型的名称和描述。下面显示了 ProxyProtocolPolicyType 类型的输出：

```
{
    "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. 使用以下create-load-balancer-policy命令创建启用代理协议的策略：

```
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. 使用以下 set-load-balancer-policies-for-backend-server 命令在指定端口上启用新创建的策略。请注意，此命令将替代当前已启用的策略组。因此，--policy-names 选项必须同时指定要添加到列表中的策略 (例如 my-ProxyProtocol-policy) 和所有当前已启用的策略 (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. （可选）使用以下describe-load-balancers命令验证代理协议是否已启用：

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

响应包含以下信息，该信息表明 my-ProxyProtocol-policy 策略与端口 80 关联。

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

使用 AWS CLI禁用代理协议

您可以禁用与您的实例关联的策略，然后在将来启用它们。

禁用代理协议策略

1. 使用以下 set-load-balancer-policies-for-backend-server 命令禁用代理协议策略，方法是将其从--policy-names选项中省略，但包括应保持启用状态的其他策略（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-existing-policy
```

如果没有其他要启用的策略，请使用 --policy-names 选项指定空字符串，如下所示：

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

2. （可选）使用以下describe-load-balancers命令验证策略是否已禁用：

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

响应包含以下信息，表明没有与策略关联的端口。

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

为经典负载均衡器添加标签

使用标签可帮助您按各种标准对负载均衡器进行分类，例如按用途、所有者或环境。

您最多可以为每个经典负载均衡器添加多个标签。每个负载均衡器的标签键必须唯一。如果您添加的标签中的键已经与负载均衡器关联，它将更新该标签的值。

当您用完标签时，可以从负载均衡器中将其删除。

目录

标签限制

下面是适用于标签的基本限制：

- 每个资源的标签数上限 – 50
- 最大密钥长度 - 127 个 Unicode 字符
- 最大值长度 - 255 个 Unicode 字符
- 标签键和值区分大小写。允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符： + - = 。 _ : / @。请不要使用前导空格或尾随空格。
- 请勿在标签名称或值中使用aws:前缀，因为它已保留供 AWS 使用。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。

添加标签

您可以随时向负载均衡器添加标签。

使用控制台添加标签

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在标签选项卡上，选择管理标签。
5. 在管理标签页面上，对于每个标签，选择添加新标签，然后指定键和值。
6. 完成添加标签后，选择保存更改。

要添加标签，请使用 AWS CLI

使用以下 add-tags 命令可添加指定标签：

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

删除标签

无论何时用完标签，您都可以从负载均衡器中将其删除。

使用控制台删除标签

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。

3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在标签选项卡上，选择管理标签。
5. 在管理标签页面上，选择要移除的每个标签旁的移除。
6. 完成移除标签后，选择保存更改。

要移除标签，请使用 AWS CLI

使用以下 remove-tags 命令可删除带指定键的标记：

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

为经典负载均衡器配置子网

如果将一个子网添加到您的负载均衡器，Elastic Load Balancing 会在该可用区中创建一个负载均衡器节点。负载均衡器节点接受来自客户端的流量并将请求转发到一个或多个可用区中的正常注册实例。建议您至少为两个可用区分别添加一个子网。这可以提高您的负载均衡器的可用性。请注意，您可随时修改负载均衡器的子网。

从实例所在的可用区选择子网。如果您的负载均衡器是面向 Internet 的负载均衡器，您必须选择公有子网，以便您的后端实例从负载均衡器接收流量（即使后端实例位于私有子网）。如果您的负载均衡器是内部负载均衡器，我们建议您选择私有子网。有关负载均衡器子网的更多信息，请参阅关于 VPC 的建议。

要添加子网，请将可用区中的实例注册到负载均衡器，然后将该可用区中的子网附加到负载均衡器。有关更多信息，请参阅 向经典负载均衡器注册实例。

添加子网后，负载均衡器开始将请求路由至对应可用区中的注册实例。默认情况下，负载均衡器在其子网的可用区间均衡地路由请求。要在其子网的可用区中的注册实例间均衡地路由请求，请启用跨区域负载均衡。有关更多信息，请参阅 配置经典负载均衡器的跨区域负载均衡。

如果子网的可用区中没有运行状况良好的注册实例，或者您希望对注册实例进行故障排除或更新，那么可能需要暂时从负载均衡器删除子网。删除子网后，负载均衡器停止将请求路由至其可用区中的注册实例，但继续将请求路由至剩余子网的可用区中的注册实例。请注意，删除一个子网后，该子网中的实例将保持已注册到负载均衡器的状态，但您也可以选择取消注册。有关更多信息，请参阅 向经典负载均衡器注册实例。

内容

要求

更新负载均衡器的子网时，必须满足以下要求：

- 负载均衡器必须始终至少有一个子网。
- 每个可用区最多可以添加一个子网。
- 您无法添加本地区域子网。

由于在负载均衡器中添加和删除子网是分开 APIs 的，因此为了满足这些要求，在将当前子网交换为新子网时，必须仔细考虑操作顺序。如果需要为负载均衡器切换所有子网，您还必须临时从另一个可用区添加子网。例如，如果负载均衡器有单个可用区，并且您需要将其子网切换为另一个子网，则必须首先从第二个可用区添加子网。随后可以从原可用区删除子网 (子网不少于一个)，从原可用区添加新子网 (每个可用区不超过一个子网)，然后从第二个可用区删除子网 (如果只需要执行切换)。

使用控制台配置子网

使用控制台按以下过程添加或删除子网。

使用控制台配置子网

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在网络映射选项卡上，选择编辑子网。
5. 在编辑子网页面的网络映射部分，根据需要添加或移除子网。
6. 在完成后，选择保存更改。

使用 CLI 配置子网

使用 AWS CLI根据以下示例添加或移除子网。

使用 CLI 将子网添加到负载均衡器

使用以下 attach-load-balancer-to-subnets 命令向您的负载均衡器添加两个子网：

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

响应将列出负载均衡器的所有子网。例如：

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

要移除子网，请使用 AWS CLI

使用以下 detach-load-balancer-from-subnets 命令从指定的负载均衡器中删除指定的子网：

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

响应将列出负载均衡器的剩余子网。例如：

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

为经典负载均衡器配置安全组

使用创建负载均衡器时，您可以选择现有安全组或创建新安全组。 AWS Management Console 如果您选择现有安全组，则它必须允许侦听器端口和运行状况检查端口上针对负载均衡器的双向流量。如果您选择创建安全组，则控制台将自动添加规则以允许这两个端口上的所有流量。

[非默认 VPC] 如果您使用 AWS CLI 或 API 在非默认 VPC 中创建负载均衡器，但未指定安全组，则您的负载均衡器会自动与 VPC 的默认安全组关联。

[默认 VPC] 如果您使用 AWS CLI 或 API 在默认 VPC 中创建负载均衡器，则无法为负载均衡器选择现有安全组。相反，Elastic Load Balancing 将为安全组提供规则，以允许指定端口上针对负载均衡器的所有流量。Elastic Load Balancing 为每个 AWS 账户只创建一个这样的安全组，其名称格式为 default_elb_*id*（例如）。`default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`您在默认 VPC 中创建的后续负载均衡器也使用此安全组。务必查看安全组规则以确保它们允许侦听器端口和运行状况检查端口上针对新负载均衡器的流量。删除负载均衡器时，不会自动删除此安全组。

如果您向现有负载均衡器添加侦听器，则必须检查安全组以确保它们允许新侦听器端口上的双向流量。

目录

负载均衡器安全组的推荐规则

负载均衡器的安全组必须允许它们与您的实例进行通信。推荐规则取决于负载均衡器的类型（面向 Internet 或内部）。

面向 Internet 的负载均衡器

下表显示了面向 Internet 的负载均衡器的推荐入站规则。

来源	协议	端口范围	评论
0.0.0.0/0	TCP	*listener*	在负载均衡器侦听器端口上允许所有入站流量

下表显示了面向 Internet 的负载均衡器的推荐出站规则。

目标	协议	端口范围	注释
instance security group	TCP	*instance listener*	在实例侦听器端口上允许流向实例的出站流量

目标	协议	端口范围	注释
instance security group	TCP	*health check*	在运行状况检查端口上允许流向实例的出站流量

内部负载均衡器

下表显示了内部负载均衡器的推荐入站规则。

来源	协议	端口范围	注释
VPC CIDR	TCP	*listener*	在负载均衡器侦听器端口上允许来自 VPC CIDR 的入站流量

下表显示了内部负载均衡器的推荐出站规则。

目标	协议	端口范围	注释
instance security group	TCP	*instance listener*	在实例侦听器端口上允许流向实例的出站流量
instance security group	TCP	*health check*	在运行状况检查端口上允许流向实例的出站流量

使用控制台分配安全组

使用以下过程可更改与负载均衡器关联的安全组。

使用控制台更新分配给负载均衡器的安全组

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。

4. 在安全性选项卡上，选择编辑。
5. 在编辑安全组页面的安全组下，根据需要添加或移除安全组。

   您最多可以添加 5 个安全组。
6. 在完成后，选择保存更改。

使用分配安全组 AWS CLI

使用以下 apply-security-groups-to-load-balancer 命令将安全组与负载均衡器相关联。指定的安全组会覆盖之前关联的安全组。

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

以下为响应示例：

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

ACLs 为您的 Classic Load Balancer 配置网络

VPC 的默认网络访问控制列表 (ACL) 允许所有入站和出站流量。如果您创建自定义网络 ACLs，则必须添加允许负载均衡器和实例通信的规则。

负载均衡器子网的推荐规则取决于负载均衡器类型（面向 Internet 或内部）。

面向 Internet 的负载均衡器

下面显示了面向 Internet 的负载均衡器的推荐入站规则。

来源	协议	端口范围	评论
0.0.0.0/0	TCP	*listener*	在负载均衡器侦听器端口上允许所有入站流量

来源	协议	端口范围	评论
VPC CIDR	TCP	1024-65535	在临时端口上允许来自 VPC CIDR 的入站流量

下面显示了面向 Internet 的负载均衡器的推荐出站规则。

目标	协议	端口范围	注释
VPC CIDR	TCP	*instance listener*	在实例侦听器端口上允许所有出站流量
VPC CIDR	TCP	*health check*	在运行状况检查端口上允许所有出站流量
0.0.0.0/0	TCP	1024-65535	在临时端口上允许所有出站流量

内部负载均衡器

下面显示了内部负载均衡器的推荐入站规则。

来源	协议	端口范围	注释
VPC CIDR	TCP	*listener*	在负载均衡器侦听器端口上允许来自 VPC CIDR 的入站流量
VPC CIDR	TCP	1024-65535	在临时端口上允许来自 VPC CIDR 的入站流量

下面显示了内部负载均衡器的推荐出站规则。

目标	协议	端口范围	注释
VPC CIDR	TCP	*instance listener*	在实例侦听器端口上允许流向 VPC CIDR 的出站流量

目标	协议	端口范围	注释
VPC CIDR	TCP	*health check*	在运行状况检查端口上允许流向 VPC CIDR 的出站流量
VPC CIDR	TCP	1024-65535	在临时端口上允许流向 VPC CIDR 的出站流量

为您的经典负载均衡器配置自定义域名

每个经典负载均衡器都会收到一个默认的域名系统 (DNS) 名称。此 DNS 名称包括创建负载均衡器的 AWS 区域的名称。例如，如果您在美国西部（俄勒冈）区域中创建名为 `my-loadbalancer` 的负载均衡器，则您的负载均衡器会收到一个 DNS 名称，例如 `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com`。要在实例上访问网站，请将此 DNS 名称粘贴到 Web 浏览器的地址栏中。不过，您的客户要记住和使用此 DNS 名称可并不容易。

如果您希望对负载均衡器使用友好的 DNS 名称 (如 `www.example.com`) 而非默认 DNS 名称，您可以创建自定义域名并将其与负载均衡器的 DNS 名称相关联。在客户端使用此自定义域名进行请求时，DNS 服务器将它解析为负载均衡器的 DNS 名称。

目录

将您的自定义域名与负载均衡器名称相关联

首先，如果您尚未注册域名，请注册您的域名。Internet 上的域名由 Internet 名称和数字地址分配机构 (ICANN) 管理。您需要通过域名注册商 (ICANN 认可的管理域名注册的组织) 注册域名。您的注册商的网站上会提供关于注册域名的详细说明和定价信息。有关更多信息，请参阅以下资源：

- 要使用 Amazon Route 53 注册域名，请参阅 Amazon Route 53 开发人员指南中的使用 Route 53 注册域名。
- 有关经认证的注册商名单，请参阅经认证的注册商名单。

下一步，通过您的 DNS 服务 (如您的域注册商) 创建一条别名记录将查询路由到您的负载均衡器。有关更多信息，请参阅您的 DNS 服务的文档。

或者，您可以使用 Route 53 作为您的 DNS 服务。创建托管区域，其中包含有关如何在 Internet 上为域路由流量的信息，以及将域名查询路由到负载均衡器的别名资源记录集。Route 53 对别名记录集的 DNS 查询不收费，您可以使用别名记录集为您的域（例如 `example.com`）的顶级域名将 DNS 查询路由到您的负载均衡器。有关将现有域的 DNS 服务转移到 Route 53 的信息，请参阅 Amazon Route 53 开发人员指南中的将 Route 53 配置为您的 DNS 服务。

最后，使用 Route 53 为域创建托管区域和别名记录集。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的将流量路由到负载均衡器。

为负载均衡器使用 Route 53 DNS 故障转移

如果使用 Route 53 将 DNS 查询路由到您的负载均衡器，您也可以使用 Route 53 为您的负载均衡器配置 DNS 故障转移。在故障转移配置中，Route 53 会检查负载均衡器的注册 EC2 实例的运行状况，以确定它们是否可用。如果没有向负载均衡器注册的正常 EC2实例，或者负载均衡器本身运行状况不佳，则 Route 53 会将流量路由到其他可用资源，例如运行良好的负载均衡器或 Amazon S3 中的静态网站。

例如，假设您有一个用于 `www.example.com` 的 Web 应用程序，并且您希望使用在不同区域内的两个负载均衡器之后运行的冗余实例。您希望流量主要路由到一个区域中的负载均衡器，并且您希望在发生故障期间将另一个区域中的负载均衡器用作备份。如果配置 DNS 故障转移，则可以指定您的主和辅助 (备份) 负载均衡器。如果主负载均衡器可用，则 Route 53 会将流量定向到主负载均衡器，否则会将流量定向到辅助负载均衡器。

使用评估目标运行状况功能

- 当经典负载均衡器别名记录上的“评估目标运行状况”设置为 `Yes` 时，Route 53 将评估 `alias target` 值指定的资源的运行状况。对于经典负载均衡器，Route 53 使用与负载均衡器关联的实例运行状况检查。
- 当经典负载均衡器中至少有一个注册的实例运行状况良好时，Route 53 会将该别名记录运行状况标记为良好。然后，Route 53 会根据您的路由策略返回记录。如果使用失效转移路由策略，则 Route 53 返回主记录。
- 当经典负载均衡器中至少有一个注册的实例运行状况不佳时，Route 53 会将该别名记录运行状况标记为不佳。然后，Route 53 会根据您的路由策略返回记录。如果使用失效转移路由策略，则 Route 53 返回辅助记录。

有关更多信息，请参阅 Amazon Route 53 开发人员指南中的配置 DNS 故障转移。

将您的自定义域名与负载均衡器取消关联

您可以首先删除托管区域内的资源记录集，并随后删除托管区域，从而将您的自定义域名与负载均衡器实例分离。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的编辑记录和删除公有托管区域。

经典负载均衡器的侦听器

在开始使用 Elastic Load Balancing 之前，您必须为经典负载均衡器配置一个或多个侦听器。侦听器是用于检查连接请求的进程。使用前端（客户端到负载均衡器）连接的协议和端口和后端（负载均衡器到后端实例）连接的协议和端口配置侦听器。

Elastic Load Balancing 支持以下协议：

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

HTTPS 协议使用 SSL 协议在 HTTP 层上建立安全连接。您也可以使用 SSL 协议在 TCP 层上建立安全连接。

如果前端连接使用 TCP 或 SSL，则您的后端连接可以使用 TCP 或 SSL。如果前端连接使用 HTTP 或 HTTPS，则您的后端连接可以使用 HTTP 或 HTTPS。

后端实例可以侦听端口 1-65535。

负载均衡器可以侦听以下端口：1–65535

内容

协议

典型 Web 应用程序的通信可以穿过硬件和软件的各个分层。每层都会提供特定的通信功能。对通信功能的控制可依次由一层传递至下一层。开放系统互连 (OSI) 会定义模型框架，以在这些分层中实施标准通信格式，这个框架被称为协议。有关更多信息，请参阅 Wikipedia 中的 OSI 模型。

使用 Elastic Load Balancing 时，您需要对分层 4 和分层 7 有基本的了解。分层 4 是传输层，描述了客户端到您的后端实例之间通过负载均衡器的传输控制协议 (TCP) 连接。分层 4 是可为您的负载均衡器

配置的最低分层。分层 7 是应用程序层，描述了客户端到负载均衡器、以及负载均衡器到您的后端实例之间的超文本传送协议 (HTTP) 和 HTTPS (安全 HTTP) 连接。

安全套接字层 (SSL) 协议主要用于对通过不安全网络（如 Internet）传输的机密数据进行加密。SSL 协议在客户端与后端服务器之间建立安全连接，确保在您的客户端和服务器之间传递的所有数据都是私有且完整的。

TCP/SSL 协议

如果您在前端和后端连接中均使用 TCP (分层 4)，您的负载均衡器会将请求转发到后端实例，而不修改标头。负载均衡器收到请求之后，会尝试在侦听器配置中指定的端口上打开与后端实例的 TCP 连接。

由于负载均衡器会拦截客户端与您的后端实例之间的流量，因此您的后端实例的访问日志中将包含负载均衡器的 IP 地址而不是原始客户端的 IP 地址。您可以启用代理协议，它会添加一个包含客户端的连接信息（如源 IP 地址、目标 IP 地址和端口号）的标头。该标头随后作为请求的一部分发送到后端实例。您可以解析请求的第一行来检索连接信息。有关更多信息，请参阅 为经典负载均衡器配置代理协议。

通过使用此配置，您将不会收到会话粘性或 X-Forwarded 标头的 Cookie。

HTTP/HTTPS 协议

如果前端和后端连接均使用 HTTP（分层 7），负载均衡器会解析请求中的标头，然后将请求发送到后端实例。

对于HTTP/HTTPS load balancer, Elastic Load Balancing opens and maintains one or more TCP connections. These connections ensure that there is always an established connection ready to receive HTTP/HTTPS请求背后的每个已注册且运行良好的实例。

HTTP 请求和 HTTP 响应使用标头字段发送有关 HTTP 消息的信息。Elastic Load Balancing 支持 `X-Forwarded-For` 标头。因为负载均衡器会拦截客户端和服务器之间的流量，因此您的服务器访问日志中将仅含有负载均衡器的 IP 地址。要查看客户端的 IP 地址，请使用 `X-Forwarded-For` 请求标头。有关更多信息，请参阅 X-Forwarded-For。

使用 HTTP/HTTPS 时，您可在负载均衡器上启用粘性会话。粘性会话将用户的会话绑定到特定后端实例。这样可以确保在会话期间，来自同一用户的所有请求均将被发送到相同的后端实例中。有关更多信息，请参阅 为经典负载均衡器配置粘性会话。

负载均衡器并不支持所有 HTTP 扩展名。如果负载均衡器因为意外的方法、响应码或其他非标准 HTTP 1.0/1.1 实施而无法终止请求，则需要使用 TCP 侦听器。

HTTPS/SSL 侦听器

您可以使用以下安全功能创建负载均衡器。

SSL 服务器证书

如果前端连接使用 HTTPS 或 SSL，则必须在负载均衡器上部署 X.509 证书 (SSL 服务器证书)。负载均衡器先解密来自客户端的请求，然后再将请求发送到后端实例 (称为 SSL 终端)。有关更多信息，请参阅 经典负载均衡器的 SSL/TLS 证书。

如果您不希望负载均衡器处理 SSL 终止 (称为 SSL 卸载)，可在前端和后端连接均使用 TCP，并为处理请求的已注册实例部署证书。

SSL 协商

Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用名为密码的高强度加密算法。然而，某些使用案例可能需要对网络中的所有数据进行加密且只允许使用特定密码。某些安全合规性标准 (如 PCI、SOX 等) 可能要求客户端提供一组特定协议和密码，以确保符合安全标准。在此类情况下，您可以根据您的特定要求创建自定义 SSL 协商配置。您的密码和协议应在 30 秒内生效。有关更多信息，请参阅 经典负载均衡器的 SSL 协商配置。

后端服务器身份验证

如果后端连接使用 HTTPS 或 SSL，您可以启用已注册实例的身份验证。之后您即可使用身份验证过程来确保实例仅接受加密的通信，并确保每个已注册实例具有正确的公有密钥。

有关更多信息，请参阅配置后端服务器身份验证。

经典负载均衡器的侦听器配置

下表描述了经典负载均衡器的 HTTP 和 HTTPS 侦听器的可能配置。

应用场景	前端协议	前端选项	后端协议	后端选项	备注
基本 HTTP 负载均衡器	HTTP	NA	HTTP	NA	• 支持 X-Forwarded 标头

应用场景	前端协议	前端选项	后端协议	后端选项	备注
保护使用 Elastic Load Balancing 的网站或应用程序以卸载 SSL 解密	HTTPS	SSL 协商	HTTP	NA	• 支持 X-Forwarded 标头 • 需要在负载均衡器上部署 SSL 证书
使用 end-to-end加密保护网站或应用程序	HTTPS	SSL 协商	HTTPS	后端身份验证	• 支持 X-Forwarded 标头 • 需要在负载均衡器和注册实例上部署 SSL 证书

下表描述了经典负载均衡器的 TCP 和 SSL 侦听器的可能配置。

应用场景	前端协议	前端选项	后端协议	后端选项	备注
基本 TCP 负载均衡器	TCP	NA	TCP	NA	• 支持代理协议标头
保护使用 Elastic Load Balancing 的网站或应用程序以卸载 SSL 解密	SSL	SSL 协商	TCP	NA	• 需要在负载均衡器上部署 SSL 证书 • 支持代理协议标头
使用 Elastic Load Balancing	SSL	SSL 协商	SSL	后端身份验证	• 需要在负载均衡器和注册实例上部

应用场景	前端协议	前端选项	后端协议	后端选项	备注
end-to-end 加密保护网站或应用程序					署 SSL 证书 • 不在后端 SSL 连接中插入 SNI 标头 • 不支持代理协议标头

HTTP 标头和经典负载均衡器

HTTP 请求和 HTTP 响应使用标头字段发送有关 HTTP 消息的信息。标头字段为冒号分隔的名称值对，各个值对之间由回车符 (CR) 和换行符 (LF) 进行分隔。RFC 2616 信息标头中定义了标准 HTTP 标头字段集。此外还有应用程序广泛使用（和自动添加）的非标准 HTTP 标头。某些非标准 HTTP 标头具有 `X-Forwarded` 前缀。经典负载均衡器支持以下 `X-Forwarded` 标头。

有关 HTTP 连接的更多信息，请参阅 Elastic Load Balancing 用户指南中的请求路由。

先决条件

- 确认您的侦听器设置支持 X-Forwarded 标头。有关更多信息，请参阅 经典负载均衡器的侦听器配置。
- 配置您的 Web 服务器以记录客户端 IP 地址。

X-Forwarded 标头

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

X-Forwarded-For

在您使用 HTTP 或 HTTPS 负载均衡器时，`X-Forwarded-For` 请求标头可自动添加并帮助您识别客户端的 IP 地址。因为负载均衡器会拦截客户端和服务器之间的流量，因此您的服务器访问日志中将仅

含有负载均衡器的 IP 地址。要查看客户端的 IP 地址，请使用 X-Forwarded-For 请求标头。Elastic Load Balancing 会在 X-Forwarded-For 请求标头中存储客户端的 IP 地址，并将标头传递到您的服务器。如果 X-Forwarded-For 请求标头未包含在请求中，则负载均衡器会创建一个以客户端 IP 地址作为请求值的标头。否则，负载均衡器会将客户端 IP 地址附加到现有标头，并将该标头传递到您的服务器。X-Forwarded-For 请求标头可能包含多个以逗号分隔的 IP 地址。最左边的地址是首次发出请求的客户端 IP。在链中，会有任何后续代理标识符跟随。

X-Forwarded-For 请求标头采用以下形式：

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

下面是 IP 地址为 203.0.113.7 的客户端的 X-Forwarded-For 请求标头的示例。

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

以下是 IPv6 地址为的客户端的X-Forwarded-For请求标头示例2001:DB8::21f:5bff:febf:ce22:8a2e。

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

X-Forwarded-Proto

X-Forwarded-Proto 请求标头可帮助您识别客户端与您的负载均衡器连接时所用的协议 (HTTP 或 HTTPS)。您的服务器访问日志仅包含在服务器和负载均衡器之间使用的协议；不含任何关于在客户端和负载均衡器之间使用的协议之信息。如需判断在客户端和负载均衡器之间使用的协议，使用 X-Forwarded-Proto 请求标题。Elastic Load Balancing 会在 X-Forwarded-Proto 请求标头中存储客户端和负载均衡器之间使用的协议，并将标头传递到您的服务器。

您的应用程序或网站可以使用存储在 X-Forwarded-Proto 请求标头中的协议来呈现重新定向至适用 URL 的响应。

X-Forwarded-Proto 请求标头采用以下形式：

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

以下示例包含以 HTTPS 请求形式源自客户端的请求的 X-Forwarded-Proto 请求标头：

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

X-Forwarded-Port

`X-Forwarded-Port` 请求标头可帮助您识别客户端与您的负载均衡器连接时所用的目标端口。

经典负载均衡器的 HTTPS 侦听器

您可创建对加密连接使用 SSL/TLS 协议 (也称为 SSL 卸载) 的负载均衡器。此功能可对您的负载均衡器与启动 HTTPS 会话的客户端之间以及您的负载均衡器与您的 EC2 实例之间的连接进行流量加密。

Elastic Load Balancing 使用安全套接字层 (SSL) 协商配置（称为安全策略），以便在客户端与负载均衡器之间协商连接。在对前端连接使用 HTTPS/SSL 时，可使用预定义安全策略或自定义安全策略。您必须在负载均衡器上部署 SSL 证书。负载均衡器先使用此证书终止连接，解密来自客户端的请求，然后再将请求发送到实例。负载均衡器使用静态密码套件建立后端连接。您可选择性地在您的实例上启用身份验证。

经典负载均衡器不支持服务器名称指示（SNI）。您可以改为使用以下备选项之一：

- 在负载均衡器上部署一个证书，并为每个其他网站添加主题备用名称 (SAN)。 SANs 使您能够使用单个证书保护多个主机名。有关每个证书支持的数量以及如何添加和删除的更多信息 SANs ，请咨询您的证书提供商 SANs。
- 对于前端和后端连接，在端口 443 上使用 TCP 侦听器。负载均衡器按原样传递请求，因此您可以处理 EC2 实例上的 HTTPS 终止。

经典负载均衡器不支持双向 TLS 身份验证（mTLS）。要获得 mTLS 支持，请创建一个 TCP 侦听器。负载均衡器按原样传递请求，因此您可以在 EC2 实例上实现 mTLS。

内容

经典负载均衡器的 SSL/TLS 证书

如果前端侦听器使用 HTTPS (SSL 或 TLS)，则必须在负载均衡器上部署 SSL/TLS 证书。负载均衡器先使用此证书终止连接，解密来自客户端的请求，然后再将请求发送到实例。

SSL 和 TLS 协议使用 X.509 证书 (SSL/TLS 服务器证书) 对客户端和后端应用程序进行身份验证。X.509 证书是证书颁发机构 (CA) 颁发的数字形式的标识，包含标识信息、有效期限、公钥、序列号以及颁发者的数字签名。

您可以使用 AWS Certificate Manager 或支持 SSL 和 TLS 协议的工具（例如 OpenSSL）来创建证书。在创建或更新负载均衡器的 HTTPS 侦听器时，您需要指定该证书。在创建用于负载均衡器的证书时，您必须指定域名。

在创建用于负载均衡器的证书时，您必须指定域名。证书上的域名必须与自定义域名记录匹配。如果不匹配，则不会对流量进行加密，因为无法验证 TLS 连接。

必须为证书指定一个完全限定域名 (FQDN)（例如 `www.example.com`）或顶点域名（例如 `example.com`）。您还可以使用星号 (*) 作为通配符来保护同一域中的多个站点名称。请求通配符证书时，星号 (*) 必须位于域名的最左侧位置，而且只能保护一个子域级别。例如，`*.example.com` 保护 `corp.example.com` 和 `images.example.com`，但无法保护 `test.login.example.com`。另请注意，`*.example.com` 仅保护 `example.com` 的子域，而不保护裸域或顶点域 (`example.com`)。通配符名称将显示在证书的 Subject（主题）字段和 Subject Alternative Name（主题替代名称）扩展中。有关公共证书的更多信息，请参阅 AWS Certificate Manager 用户指南中的请求公共证书。

使用创建或导入 SSL/TLS 证书 AWS Certificate Manager

我们建议您使用 AWS Certificate Manager (ACM) 为负载均衡器创建或导入证书。ACM 与 Elastic Load Balancing 集成，以便您可以在负载均衡器上部署证书。要在负载均衡器上部署证书，证书与负载均衡器必须在同一区域中。有关更多信息，请参阅 AWS Certificate Manager 用户用户指南中的请求公有证书或导入证书。

要允许用户使用 AWS Management Console在您的负载均衡器上部署证书，您必须向其授予对 ACM `ListCertificates` API 操作的访问权限。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的列出证书。

> **Important**
>
> 您无法通过与 ACM 集成在负载均衡器上安装带有 4096 位 RSA 密钥或 EC 密钥的证书。您必须将带有 4096 位 RSA 密钥或 EC 密钥的证书上传到 IAM，以便将它们与负载均衡器结合使用。

使用 IAM 导入 SSL/TLS 证书

如果您未使用 ACM，则可以使用 SSL/TLS 工具（如 OpenSSL）创建证书签名请求 (CSR)、获取 CA 签署的 CSR 以生成证书，并将证书上传到 IAM。有关更多信息，请参阅 IAM 用户指南中的使用服务器证书。

经典负载均衡器的 SSL 协商配置

Elastic Load Balancing 使用一个安全套接字层 (SSL) 协商配置（称为安全策略）在客户端与负载均衡器之间协商 SSL 连接。安全策略是 SSL 协议、SSL 密码和服务器顺序首选项选项的组合。有关为负载均衡器配置 SSL 连接的更多信息，请参阅经典负载均衡器的侦听器。

目录

安全策略

安全策略确定在客户端与负载均衡器之间进行 SSL 协商期间受支持的密码和协议。您可以配置自己的经典负载均衡器以使用预定义或自定义的安全策略。

请注意，由 AWS Certificate Manager (ACM) 提供的证书包含 RSA 公钥。因此，如果您使用 ACM 提供的证书，则安全策略必须包括一个使用 RSA 的密码包；否则，TLS 连接会失败。

预定义安全策略

最新预定义安全策略的名称包括发布预定义安全策略的年份和月份的版本信息。例如，默认预定义安全策略为 `ELBSecurityPolicy-2016-08`。只要发布新的预定义安全策略，您就能更新配置以使用它。

有关为预定义安全策略启用的协议和密码的信息，请参阅 经典负载均衡器的预定义 SSL 安全策略。

自定义安全策略

您可使用所需的密码和协议创建自定义协商配置。例如，某些安全合规性标准 (如 PCI 和 SOC) 可能需要一组特定协议和密码，以确保符合安全标准。在这种情况下，可创建自定义安全策略来符合这些标准。

有关创建自定义安全策略的信息，请参阅 更新经典负载均衡器的 SSL 协商配置。

SSL 协议

SSL 协议 在客户端与服务器之间建立安全连接，确保在客户端与负载均衡器之间传递的所有数据都是私密的。

安全套接字层 (SSL) 和传输层安全性 (TLS) 是用于对通过不安全网络（如 Internet）传输的机密数据进行加密的加密协议。TLS 协议是更新版本的 SSL 协议。在 Elastic Load Balancing 文档中，我们将 SSL 和 TLS 协议都称为 SSL 协议。

推荐的协议

我们推荐 TLS 1.2，它用于策略 T ELBSecurity LS-1-2-2017-01 预定义的安全策略。您也可以在自定义安全策略中使用 TLS 1.2。默认安全策略同时支持 TLS 1.2 和更早版本的 TLS，因此其安全性不如ELBSecurity策略-TLS-1-2-2017-01。

已弃用的协议

如果之前在自定义策略中启用了 SSL 2.0 协议，我们推荐您将安全策略更新到预定义安全策略之一。

服务器顺序首选项

Elastic Load Balancing 支持服务器顺序首选项选项，该选项用于协商客户端与负载均衡器之间的连接。在 SSL 连接协商过程中，客户端和负载均衡器会按首选项顺序提供各自支持的密码和协议的列表。默认情况下，会为 SSL 连接选择客户端列表中与任何一个负载均衡器的密码匹配的第一个密码。如果负载均衡器配置为支持服务器顺序首选项，则负载均衡器会在其列表中选择位于客户端的密码列表中的第一个密码。这可确保由负载均衡器确定用于 SSL 连接的密码。如果您未启用服务器顺序首选项，则使用客户端提供的密码顺序来协商客户端与负载均衡器之间的连接。

SSL 密码

SSL 密码 是一种加密算法，它使用加密密钥创建编码的消息。SSL 协议使用多种 SSL 密码对 Internet 上的数据进行加密。

请注意，由 AWS Certificate Manager (ACM) 提供的证书包含 RSA 公钥。因此，如果您使用 ACM 提供的证书，则安全策略必须包括一个使用 RSA 的密码包；否则，TLS 连接会失败。

Elastic Load Balancing 支持以下密码以用于经典负载均衡器。预定义的 SSL 策略使用这些密码的子集。所有这些密码可用于自定义策略中。我们建议您仅使用默认安全策略 (带有星号) 中包括的密码。其他许多密码并不安全，需要自行承担使用风险。

密码

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

- DHE-DSS--AES256 SHA256
- DHE-RSA--SHA AES256
- DHE-DSS-SHA AES256
- DHE-RSA--SHA CAMELLIA256
- DHE-DSS-SHA CAMELLIA256
- CAMELLIA256-SHA
- EDH-DSS-DES-SHA CBC3
- DHE-DSS--GCM-AES128 SHA256
- DHE-RSA--GCM-AES128 SHA256
- DHE-RSA--AES128 SHA256
- DHE-DSS--AES128 SHA256
- DHE-RSA--SHA CAMELLIA128
- DHE-DSS-SHA CAMELLIA128
- 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--SHA CBC3
- ADH-DES-CBC-SHA
- ADH-RC4-MD5
- ADH-SEED-SHA
- DES-CBC-SHA
- DHE-DSS-SEED-SHA
- DHE-RSA-SEED-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA

- IDEA-CBC-SHA
- RC4-MD5
- SEED-SHA
- DES-CBC3-MD5
- DES-CBC-MD5
- RC2-加拿大广播公司-MD5
- PSK--CBC-SH AES256 A
- PSK-3DES-EDE-CBC-SHA
- KRB5-DES--SH CBC3 A
- KRB5-DES--CBC3 MD5
- PSK--CBC-SH AES128 A
- PSK--SH RC4 A
- 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--CBC-SHA RC2
- EXP--DES-CBC-SHA KRB5
- EXP-KRB5-RC2-CBC-MD5
- EXP--DES KRB5-CBC-MD5
- EXP-ADH--RC4 MD5
- EXP--RC4 MD5
- EXP-KRB5--SHA RC4
- EXP-KRB5--RC4 MD5

* 这些是默认安全策略 Policy-2016-08 中包含的密码。 ELBSecurity

经典负载均衡器的预定义 SSL 安全策略

您可以为 HTTPS/SSL 侦听器选择预定义的安全策略之一。您可以使用 ELBSecurityPolicy-TLS 策略之一来满足要求禁用某些 TLS 协议版本的合规性和安全标准。或者，您也可以创建自定义安全策略。有关更多信息，请参阅 更新 SSL 协商配置。

基于 RSA 和 DSA 的密码特定于用于创建 SSL 证书的签名算法。请确保使用基于为安全策略启用的密码的签名算法来创建 SSL 证书。

如果选择为“服务器顺序首选项”启用的策略，则负载均衡器会按密码在这里的指定顺序使用密码，以协商客户端与负载均衡器之间的连接。否则，负载均衡器会按客户端提供的密码的顺序使用密码。

以下章节介绍了经典负载均衡器的最新预定义安全策略，包括其启用的 SSL 协议和 SSL 密码。您也可以使用describe-load-balancer-policies命令描述预定义的策略。

> **Tip**
>
> 这些信息仅适用于经典负载均衡器。有关适用于其他负载均衡器的信息，请参阅适用于应用程序负载均衡器的安全策略和适用于网络负载均衡器的安全策略。

内容

按策略划分的协议

下表描述了每个安全策略支持的 TLS 协议。

安全策略	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-tls-1-2-2017-01	是	没有	没有
ELBSecurity政策-tls-1-1-2017-01	是	是	没有

安全策略	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurity政策-2016-08	是	是	是
ELBSecurity政策-2015-05	是	是	是
ELBSecurity政策-2015-03	是	是	是
ELBSecurity政策-2015-02	是	是	是

按策略划分的密码

下表描述了每个安全策略支持的密码。

安全策略	密码
ELBSecurityPolicy-tls-1-2-2017-01	• ECDHE-ECDSA--GCM-AES128 SHA256 • ECDHE-RSA--GCM-AES128 SHA256 • ECDHE-ECDSA--AES128 SHA256 • ECDHE-RSA--AES128 SHA256 • ECDHE-ECDSA--GCM-AES256 SHA384 • ECDHE-RSA--GCM-AES256 SHA384 • ECDHE-ECDSA--AES256 SHA384 • ECDHE-RSA--AES256 SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256
ELBSecurity政策-tls-1-1-2017-01	• ECDHE-ECDSA--GCM-AES128 SHA256 • ECDHE-RSA--GCM-AES128 SHA256

安全策略	密码
	• ECDHE-ECDSA--AES128 SHA256 • ECDHE-RSA--AES128 SHA256 • ECDHE-ECDSA--SHA AES128 • ECDHE-RSA--SHA AES128 • ECDHE-ECDSA--GCM-AES256 SHA384 • ECDHE-RSA--GCM-AES256 SHA384 • ECDHE-ECDSA--AES256 SHA384 • ECDHE-RSA--AES256 SHA384 • ECDHE-ECDSA--SHA AES256 • ECDHE-RSA--SHA AES256 • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurity政策-2016-08	• ECDHE-ECDSA--GCM-AES128 SHA256 • ECDHE-RSA--GCM-AES128 SHA256 • ECDHE-ECDSA--AES128 SHA256 • ECDHE-RSA--AES128 SHA256 • ECDHE-ECDSA--SHA AES128 • ECDHE-RSA--SHA AES128 • ECDHE-ECDSA--GCM-AES256 SHA384 • ECDHE-RSA--GCM-AES256 SHA384 • ECDHE-ECDSA--AES256 SHA384 • ECDHE-RSA--AES256 SHA384 • ECDHE-ECDSA--SHA AES256 • ECDHE-RSA--SHA AES256 • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurity政策-2015-05	• ECDHE-ECDSA--GCM-AES128 SHA256 • ECDHE-RSA--GCM-AES128 SHA256 • ECDHE-ECDSA--AES128 SHA256 • ECDHE-RSA--AES128 SHA256 • ECDHE-ECDSA--SHA AES128 • ECDHE-RSA--SHA AES128 • ECDHE-ECDSA--GCM-AES256 SHA384 • ECDHE-RSA--GCM-AES256 SHA384 • ECDHE-ECDSA--AES256 SHA384 • ECDHE-RSA--AES256 SHA384 • ECDHE-ECDSA--SHA AES256 • ECDHE-RSA--SHA AES256 • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DES CBC3--SHA

安全策略	密码
ELBSecurity政策-2015-03	• ECDHE-ECDSA--GCM-AES128 SHA256 • ECDHE-RSA--GCM-AES128 SHA256 • ECDHE-ECDSA--AES128 SHA256 • ECDHE-RSA--AES128 SHA256 • ECDHE-ECDSA--SHA AES128 • ECDHE-RSA--SHA AES128 • ECDHE-ECDSA--GCM-AES256 SHA384 • ECDHE-RSA--GCM-AES256 SHA384 • ECDHE-ECDSA--AES256 SHA384 • ECDHE-RSA--AES256 SHA384 • ECDHE-ECDSA--SHA AES256 • ECDHE-RSA--SHA AES256 • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DHE-RSA--SHA AES128 • DHE-DSS-SHA AES128 • DES CBC3--SHA

安全策略	密码
ELBSecurity政策-2015-02	• ECDHE-ECDSA--GCM-AES128 SHA256 • ECDHE-RSA--GCM-AES128 SHA256 • ECDHE-ECDSA--AES128 SHA256 • ECDHE-RSA--AES128 SHA256 • ECDHE-ECDSA--SHA AES128 • ECDHE-RSA--SHA AES128 • ECDHE-ECDSA--GCM-AES256 SHA384 • ECDHE-RSA--GCM-AES256 SHA384 • ECDHE-ECDSA--AES256 SHA384 • ECDHE-RSA--AES256 SHA384 • ECDHE-ECDSA--SHA AES256 • ECDHE-RSA--SHA AES256 • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DHE-RSA--SHA AES128 • DHE-DSS-SHA AES128

按密码划分的策略

下表描述了支持每个密码的安全策略。

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES 128-GCM-SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08	c02b

密码名称	安全策略	密码套件
IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	
OpenSSL — ECDHE-RSA-AES 128-GCM-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c02f
OpenSSL — 12 8- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c023
OpenSSL — 12 8- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c027
OpenSSL — 128-SHA ECDHE-ECDSA-AES IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c009

密码名称	安全策略	密码套件
OpenSSL — 128-SHA ECDHE-RSA-AES IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c013
OpenSSL — ECDHE-ECDSA-AES 256-GCM-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c02c
OpenSSL — ECDHE-RSA-AES 256-GCM-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c030
OpenSSL — 25 6- ECDHE-ECDSA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c024

密码名称	安全策略	密码套件
OpenSSL — 25 6- ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_ SHA384	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c028
OpenSSL — 256-SHA ECDHE-ECDSA-AES IANA：TLS_ECDHE_RSA_WIT H_AES_256_CBC_SHA	• ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c014
OpenSSL — 256-SHA ECDHE-RSA-AES IANA：TLS_ECDHE_ECDSA_W ITH_AES_256_CBC_SHA	• ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	c00a
OpenSSL —- AES128 G CM-SHA256 IANA — TLS_RSA_WITH_AES_1 28_GCM_ SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	9c

密码名称	安全策略	密码套件
OpenSSL —- AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	3c
OpenSSL —-SHA AES128 IANA：TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	2f
OpenSSL —- AES256 G CM-SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	9d
OpenSSL —- AES256 SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityPolicy-tls-1-2-2017-01 • ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	3d

密码名称	安全策略	密码套件
OpenSSL —-SHA AES256 IANA：TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurity政策-tls-1-1-2017-01 • ELBSecurity政策-2016-08 • ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	35
OpenSSL — 128-SHA DHE-RSA-AES IANA：TLS_DHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	33
OpenSSL — 128-SHA DHE-DSS-AES IANA：TLS_DHE_DSS_WITH_AES_128_CBC_SHA	• ELBSecurity政策-2015-03 • ELBSecurity政策-2015-02	32
OpenSSL — DES-SHA CBC3 IANA：TLS_RSA_WITH_3DES_EDE_CBC_SHA	• ELBSecurity政策-2015-05 • ELBSecurity政策-2015-03	0a

创建带有 HTTPS 侦听器的经典负载均衡器

负载均衡器接受来自客户端的请求，并将请求分发到向负载均衡器注册的 EC2实例中。

您可以创建一个同时侦听 HTTP (80) 和 HTTPS (443) 端口的负载均衡器。如果指定 HTTPS 侦听器将请求发送到端口 80 上的实例，则负载均衡器将终止请求，并且不加密从负载均衡器到实例的通信。如果 HTTPS 侦听器将请求发送到端口 443 上的实例，则对从负载均衡器到实例的通信进行加密。

如果负载均衡器使用加密连接与实例通信，您可以选择启用实例身份验证。这可确保只有在实例的公钥与您出于通信目的为负载均衡器指定的密钥匹配时，负载均衡器才与实例通信。

有关如何向现有负载均衡器添加 HTTPS 侦听器的信息，请参阅为您的经典负载均衡器配置 HTTPS 侦听器。

内容

前提条件

在您开始之前，请确保您已符合以下先决条件：

- 完成 关于 VPC 的建议 中的步骤。
- 启动您计划向负载均衡器注册的 EC2 实例。这些实例的安全组必须允许来自负载均衡器的流量。
- EC2 实例必须使用 HTTP 状态代码 200 响应运行状况检查的目标。有关更多信息，请参阅 对经典负载均衡器中的实例执行运行状况检查。
- 如果您计划在 EC2 实例上启用 keep-alive 选项，我们建议您将保持活动设置至少设置为负载均衡器的空闲超时设置。如果要确保由负载均衡器负责关闭与实例的连接，请确保在实例上设置的保持活动时间值要大于在负载均衡器上设置的空闲超时设置。有关更多信息，请参阅 配置经典负载均衡器的空闲连接超时。
- 如果您创建安全侦听器，必须在负载均衡器上部署 SSL 服务器证书。负载均衡器会在将请求发送到实例之前，使用证书终止并解密请求。如果您没有 SSL 证书，您可以创建一个。有关更多信息，请参阅 经典负载均衡器的 SSL/TLS 证书。

使用控制台创建 HTTPS 负载均衡器

在此示例中，您为负载均衡器配置了两个侦听器。第一个侦听器接收端口 80 上的 HTTP 请求，并使用 HTTP 在端口 80 上向实例发送这些请求。第二个侦听器接受端口 443 上的 HTTPS 请求，并使用端口 80 上的 HTTP (如果您希望配置后端实例身份验证，请使用端口 443 上的 HTTPS) 向实例发送这些请求。

侦听器是用于检查连接请求的进程。使用前端 (客户端到负载均衡器) 连接的协议和端口与后端 (负载均衡器到实例) 连接的协议和端口配置侦听器。有关 Elastic Load Balancing 支持的端口、协议和侦听器配置的信息，请参阅经典负载均衡器的侦听器。

使用控制台创建安全的经典负载均衡器

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航栏上，选择您的负载均衡器所在的区域。请务必选择与您为 EC2 实例选择的相同区域。
3. 在导航窗格上的 Load Balancing (负载均衡) 下，选择 Load Balancers (负载均衡器)。

4. 选择 Create Load Balancer (创建负载均衡器)。
5. 展开经典负载均衡器部分，然后选择创建。
6. 基本配置

   a. 对于负载均衡器名称，键入负载均衡器的名称。

      在当前区域的经典负载均衡器集内，经典负载均衡器的名称必须唯一，最多可以有 32 个字符，只能包含字母数字字符和连字符，不能以连字符开头或结尾。

   b. 对于模式，选择面向互联网。
7. 网络映射

   a. 对于 VPC，选择您为实例选择的 VPC。

   b. 对于映射，首先选择一个可用区，然后从其可用子网中选择一个公有子网。每个可用区只能选择一个子网。要提高负载均衡器的可用性，请选择多个可用区和子网。
8. 安全组

   - 对于安全组，选择一个配置为允许在端口 80 上传输所需 HTTP 流量以及在端口 443 上传输所需 HTTPS 流量的现有安全组。

     如果安全组不存在，则可以创建一个具有必要规则的新安全组。
9. 侦听器和路由

   a. 保留默认侦听器的默认设置，然后选择添加侦听器。

   b. 对于新侦听器的侦听器部分，选择 HTTPS，因为协议和端口将更新为 443。默认情况下，实例将使用 HTTP 协议和端口 80。

   c. 如果需要进行后端身份验证，请将实例协议更改为 HTTPS。此操作还会将实例端口更改为 443。
10. 安全侦听器设置

    当您对前端侦听器使用 HTTPS 或 SSL 时，必须在负载均衡器上部署 SSL 证书。负载均衡器先使用此证书终止连接，解密来自客户端的请求，然后再将请求发送到实例。您还必须指定安全策略。Elastic Load Balancing 提供了已预定义 SSL 协商配置的安全策略，您也可以创建自己的自定义安全策略。如果您在后端连接中配置 HTTPS/SSL，可选择启用实例身份验证。

    a. 对于安全策略，建议您始终使用最新的预定义安全策略，您也可创建自定义的策略。请参阅更新 SSL 协商配置。

    b. 对于默认 SSL/TLS 证书，可使用以下选项：

- 如果您使用创建或导入了证书 AWS Certificate Manager，请选择来自 ACM，然后从 “选择证书” 中选择证书。
- 如果使用 IAM 导入了证书，请选择从 IAM，然后在选择证书中选择该证书。
- 如果您有要导入的证书，但您所在的区域不提供 ACM，请选择导入，然后选择到 IAM。在证书名称字段中输入证书的名称。在证书私有密钥中，复制并粘贴私有密钥文件（PEM 编码的文件）的内容。在证书正文中，复制并粘贴公有密钥证书文件（PEM 编码的文件）的内容。在 Certificate Chain 中，复制并粘贴证书链文件（PEM 编码的文件）的内容，除非您使用的是自签名证书并且浏览器是否隐式接受证书并不重要。

c. （可选）如果您将 HTTPS 侦听器配置为使用加密连接与实例通信，则可以选择在后端身份验证证书中设置实例身份验证。

> **Note**
>
> 如果看不到后端身份验证证书部分，请返回侦听器和路由部分，然后对于实例的协议选择 HTTPS。

i. 对于 Certificate name，键入公钥证书的名称。

ii. 对于证书正文（PEM 编码），复制并粘贴该证书的内容。只有在实例的公钥与此密钥匹配时，负载均衡器才会与该实例通信。

iii. 要添加其他证书，请选择添加新后端证书。最多可以添加五个。

11. 运行状况检查

a. 在 Ping 目标部分中，选择一个 Ping 协议和 Ping 端口。您的 EC2 实例必须接受指定 ping 端口上的流量。

b. 对于 Ping 端口，确保端口为 80。

c. 对于 Ping 路径，请将默认值替换为单正斜线（/）。这会指示 Elastic Load Balancing 将运行状况检查请求发送到您的 Web 服务器的默认主页，如 index.html。

d. 对于高级运行状况检查设置，请使用默认值。

12. 实例

a. 选择添加实例，这时将显示实例选择页面。

b. 在可用实例下，您可以根据之前选择的网络设置，从负载均衡器可用的当前实例中进行选择。

c. 确认选择无误后，选择确认以将要注册的实例添加到负载均衡器。

13. Attributes

    - 对于启用跨可用区负载均衡、启用连接耗尽以及超时（耗尽间隔时间），请保留默认值。

14. 负载均衡器标签（可选）

    a. 键字段为必填项。

    b. 值字段为可选项。

    c. 要添加其他标签，请选择添加新标签，然后输入键字段的值，以及可选的值字段的值。

    d. 要移除现有标签，请选择要移除的标签旁的移除。

15. 摘要和创建

    a. 如果需要更改任何设置，请选择需要更改的设置旁的编辑。

    b. 确认摘要中显示的所有设置无误后，选择创建负载均衡器以开始创建负载均衡器。

    c. 在最终创建页面上，选择查看负载均衡器以在 Amazon EC2 控制台中查看您的负载均衡器。

16. Verify

    a. 选择新的负载均衡器。

    b. 在目标实例选项卡中，选中运行状态列。在您的至少一个 EC2 实例处于服务状态后，您可以测试您的负载均衡器。

    c. 在详细信息部分中，复制负载均衡器的 DNS 名称，这看起来类似于 `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`。

    d. 将负载均衡器的 DNS 名称粘贴到已连接到公共互联网的 Web 浏览器地址栏中。如果负载均衡器运行正常，则会看到服务器的默认页面。

17. 删除（可选）

    a. 如果您有一个指向负载均衡器的域的一个别名记录，请将它指向新的位置并等待 DNS 更改生效，然后再删除您的负载均衡器。

    b. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

    c. 选择负载均衡器。

    d. 依次选择操作、删除负载均衡器。

    e. 提示进行确认时，键入 `confirm`，然后选择删除。

    f. 删除负载均衡器后，在该负载均衡器中注册的 EC2 实例将继续运行。您将按实例继续运行的部分或完整小时数付费。当您不再需要某个 EC2 实例时，可以停止或终止该实例，以免产生额外费用。

使用创建 HTTPS 负载均衡器 AWS CLI

按照以下说明使用 AWS CLI创建 HTTPS/SSL 负载均衡器。

任务

步骤 1：配置侦听器

侦听器是用于检查连接请求的进程。使用前端 (客户端到负载均衡器) 连接的协议和端口与后端 (负载均衡器到实例) 连接的协议和端口配置侦听器。有关 Elastic Load Balancing 支持的端口、协议和侦听器配置的信息，请参阅经典负载均衡器的侦听器。

在此示例中，通过指定要用于前端和后端连接的端口和协议为您的负载均衡器配置两个侦听器。第一个侦听器接收端口 80 上的 HTTP 请求，并使用 HTTP 在端口 80 上向实例发送这些请求。第二个侦听器接受端口 443 上的 HTTPS 请求，并使用端口 80 上的 HTTP 向实例发送这些请求。

因为第二个侦听器在前端连接中使用 HTTPS，所以您必须在负载均衡器上部署 SSL 服务器证书。负载均衡器会在将请求发送到实例之前，使用证书终止并解密请求。

为您的负载均衡器配置侦听器

1. 获取 SSL 证书的 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. 使用以下create-load-balancer命令为负载均衡器配置两个侦听器：

```
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
```

以下为响应示例：

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

3. （可选）使用以下describe-load-balancers命令查看您的负载均衡器的详细信息：

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

步骤 2：配置 SSL 安全策略

您可选择预定义安全策略之一，或者可创建自己的自定义安全策略。否则，Elastic Load Balancing 使用默认预定义安全策略 ELBSecurityPolicy-2016-08 配置您的负载均衡器。有关更多信息，请参阅 经典负载均衡器的 SSL 协商配置。

验证您的负载均衡器是否与默认安全策略关联

使用以下 describe-load-balancers 命令：

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

以下为响应示例。请注意，ELBSecurityPolicy-2016-08 已在端口 443 上与负载均衡器关联。

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

如果您愿意，可以为您的负载均衡器配置 SSL 安全策略，而不是使用默认安全策略。

（可选）使用预定义 SSL 安全策略

1. 使用以下describe-load-balancer-policies命令列出预定义安全策略的名称：

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

   有关预定义安全策略的配置的信息，请参阅经典负载均衡器的预定义 SSL 安全策略。

2. 使用以下create-load-balancer-policy命令使用您在上一步中描述的预定义安全策略之一创建 SSL 协商策略：

   ```
   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. （可选）使用以下describe-load-balancer-policies命令验证策略是否已创建：

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

响应包括策略的描述。

4. 使用以下 set-load-balancer-policiesof-listener 命令在负载均衡器端口 443 上启用该策略：

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

> **Note**
>
> set-load-balancer-policies-of-listener 命令将指定负载均衡器端口的当前策略集替换为指定的策略集。--policy-names 列表必须包括要启用的所有策略。如果您省略当前已启用的策略，则禁用此策略。

5. （可选）使用以下describe-load-balancers命令验证策略是否已启用：

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

以下是指明已在端口 443 上启用策略的响应示例。

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

当您创建自定义安全策略时，必须至少启用一项协议和一个密码。DSA 和 RSA 密码特定于签名算法，用于创建 SSL 证书。如果您已有 SSL 证书，请确保启用用于创建证书的密码。您的自定义策略的名称不得以 ELBSecurityPolicy- 或 ELBSample- 开头，因为这些前缀是为预定义安全策略的名称保留的。

（可选）使用自定义 SSL 安全策略

1. 使用create-load-balancer-policy命令使用自定义安全策略创建 SSL 协商策略。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. （可选）使用以下describe-load-balancer-policies命令验证策略是否已创建：

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

   响应包括策略的描述。

3. 使用以下 set-load-balancer-policiesof-listener 命令在负载均衡器端口 443 上启用该策略：

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

> **Note**
>
> set-load-balancer-policies-of-listener 命令将指定负载均衡器端口的当前策略集替换为指定的策略集。--policy-names 列表必须包括要启用的所有策略。如果您省略当前已启用的策略，则禁用此策略。

4. （可选）使用以下describe-load-balancers命令验证策略是否已启用：

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

以下是指明已在端口 443 上启用策略的响应示例。

```
{
    "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": []
```

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

步骤 3：配置后端实例身份验证（可选）

如果您在后端连接上设置 HTTPS/SSL，则可以选择设置实例身份验证。

在设置后端实例身份验证时，您将创建一个公钥策略。接下来，您可使用此公钥策略创建后端实例身份验证策略。最后，使用 HTTPS 协议的实例端口设置后端实例身份验证策略。

只有在实例提供给负载均衡器的公钥与负载均衡器的身份验证策略中的公钥匹配时，负载均衡器才会与实例通信。

配置后端实例身份验证

1. 使用以下命令检索公钥：

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

2. 使用以下create-load-balancer-policy命令创建公钥策略：

```
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**
>
> 要指定 --policy-attributes 的公钥值，请删除公钥的第一行和最后一行内容 (包含“-----BEGIN PUBLIC KEY-----”和“-----END PUBLIC KEY-----”的两行)。AWS CLI 不接受中的空格字符--policy-attributes。

3. 使用以下create-load-balancer-policy命令使用创建后端实例身份验证my-PublicKey-policy策略。

```
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
```

您可以选择使用多个公钥策略。负载均衡器会尝试所有密钥，一次尝试一个。如果实例提供的公钥与其中一个公钥匹配，则表示此实例已经过身份验证。

4. 使用以下 set-load-balancer-policies-for-backend-server 命令设置my-authentication-policy为 HTTPS 的实例端口。在此示例中，实例端口为端口 443。

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

5. （可选）使用以下describe-load-balancer-policies命令列出您的负载均衡器的所有策略：

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

6. （可选）使用以下describe-load-balancer-policies命令查看策略的详细信息：

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

步骤 4：配置运行状况检查（可选）

Elastic Load Balancing 会根据您配置的运行状况检查定期检查每个注册 EC2 实例的运行状况。如果 Elastic Load Balancing 发现某一运行不正常的实例，它会停止向这个实例发送流量，并将流量路由到运行正常的实例。有关更多信息，请参阅 对经典负载均衡器中的实例执行运行状况检查。

当您创建负载均衡器时，Elastic Load Balancing 会使用运行状况检查的默认设置。如果您愿意，您可更改负载均衡器的运行状况检查配置，而不是使用默认设置。

为您的实例配置运行状况检查

使用以下 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
```

以下为响应示例：

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

步骤 5：注册 EC2 实例

创建负载均衡器后，您必须向负载均衡器注册您的 EC2 实例。您可以从与负载均衡器位于同一区域内的单个可用区或多个可用区中选择 EC2 实例。有关更多信息，请参阅 经典负载均衡器的已注册实例。

按如下方式使用 register-instances-with-load-balancer 命令：

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

以下为响应示例：

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

```
    ]
}
```

步骤 6：验证实例

当您的任何一个已注册实例处于 InService 状态后，您的负载均衡器即可使用。

要检查您新注册的 EC2 实例的状态，请使用以下describe-instance-health命令：

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

以下为响应示例：

```
{
    "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"
        }
    ]
}
```

如果实例的 State 字段为 OutOfService，则可能是因为您的实例仍在注册中。有关更多信息，请参阅 对经典负载均衡器进行故障排除：实例注册。

在您的至少一个实例的状态为 InService 后，便可测试负载均衡器。要测试您的负载均衡器，请复制负载均衡器的 DNS 名称，然后将其粘贴到已连接 Internet 的 Web 浏览器的地址栏中。如果您的负载均衡器正在运行，您会看到 HTTP 服务器的默认页面。

步骤 7：删除您的负载均衡器（可选）

删除负载均衡器会自动注销其关联 EC2实例。当负载均衡器被删除之后，您便不再需要支付负载均衡器费用。但是，这些 EC2 实例会继续运行，并且您会继续产生费用。

要删除您的负载均衡器，请使用以下delete-load-balancer命令：

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

要停止您的 EC2 实例，请使用停止实例命令。要终止您的 EC2 实例，请使用终止实例命令。

为您的经典负载均衡器配置 HTTPS 侦听器

侦听器是用于检查连接请求的进程。使用前端 (客户端到负载均衡器) 连接的协议和端口与后端 (负载均衡器到实例) 连接的协议和端口配置侦听器。有关 Elastic Load Balancing 支持的端口、协议和侦听器配置的信息，请参阅经典负载均衡器的侦听器。

如果您的负载均衡器具有接受端口 80 上的 HTTP 请求的侦听器，则可以添加接受端口 443 上的 HTTPS 请求的侦听器。如果指定 HTTPS 侦听器将请求发送到端口 80 上的实例，则负载均衡器将终止 SSL 请求，并且不加密从负载均衡器到实例的通信。如果 HTTPS 侦听器将请求发送到端口 443 上的实例，则对从负载均衡器到实例的通信进行加密。

如果负载均衡器使用加密连接与实例通信，您可以选择启用实例身份验证。这可确保只有在实例的公钥与您出于通信目的为负载均衡器指定的密钥匹配时，负载均衡器才与实例通信。

有关创建新的 HTTPS 侦听器的信息，请参阅创建带有 HTTPS 侦听器的经典负载均衡器。

内容

前提条件

若要为 HTTPS 侦听器启用 HTTPS 支持，您必须在负载均衡器上部署 SSL 服务器证书。负载均衡器会在将请求发送到实例之前，使用证书终止并解密请求。如果您没有 SSL 证书，您可以创建一个。有关更多信息，请参阅 经典负载均衡器的 SSL/TLS 证书。

使用控制台添加 HTTPS 侦听器

您可以将 HTTPS 监听器添加到现有负载均衡器。

使用控制台向负载均衡器添加 HTTPS 侦听器

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择管理侦听器。
5. 在管理侦听器页面的侦听器部分中，选择添加侦听器。
6. 对于侦听器协议，选择 HTTPS。

> **Important**
>
> 默认情况下，实例协议为 HTTP。如果要设置后端实例身份验证，请将实例协议更改为 HTTPS。

7. 对于安全策略，建议您使用最新的预定义安全策略。如果您需要使用其他预定义安全策略或创建自定义策略，请参阅更新 SSL 协商配置。
8. 对于默认 SSL 证书，请选择编辑，然后执行以下操作之一：

   - 如果您使用创建或导入了证书 AWS Certificate Manager，请选择 F rom ACM，从列表中选择证书，然后选择保存更改。

     > **Note**
     >
     > 此选项只在支持 的区域中可用 AWS Certificate Manager

   - 如果使用 IAM 导入了证书，请选择从 IAM 并从列表中选择该证书，然后选择保存更改。
   - 如果您有 SSL 证书要导入到 ACM，请选择导入和到 ACM。在证书私有密钥中，复制并粘贴 PEM 编码的私有密钥文件的内容。在证书正文中，复制并粘贴 PEM 编码的公有密钥证书文件的内容。在证书链 – 可选中，复制并粘贴 PEM 编码的证书链文件的内容，除非您使用的是自行签名的证书并且浏览器是否隐式接受证书并不重要。
   - 如果您有要导入的 SSL 证书，但该区域不支持 ACM，请选择导入和到 IAM。在证书名称字段中输入证书的名称。在证书私有密钥中，复制并粘贴 PEM 编码的私有密钥文件的内容。在证书正文中，复制并粘贴 PEM 编码的公有密钥证书文件的内容。在证书链 – 可选中，复制并粘贴 PEM 编码的证书链文件的内容，除非您使用的是自行签名的证书并且浏览器是否隐式接受证书并不重要。
   - 选择 Save changes（保存更改）。

9. 对于 Cookie 粘性，默认设置为已禁用。要更改此设置，请选择编辑。如果选择由负载均衡器生成，则必须指定一个有效期。如果选择由应用程序生成，则必须指定一个 Cookie 名称。完成选择后，选择保存更改。
10. （可选）选择添加侦听器以添加其他侦听器。
11. 选择保存更改以添加您刚才配置的侦听器。
12. （可选）要为现有负载均衡器设置后端实例身份验证，必须使用 AWS CLI 或 API，因为控制台不支持此任务。有关更多信息，请参阅配置后端实例身份验证。

使用添加 HTTPS 监听器 AWS CLI

您可以将 HTTPS 监听器添加到现有负载均衡器。

要向您的负载均衡器添加 HTTPS 侦听器，请使用 AWS CLI

1. 获取 SSL 证书的 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. 使用以下create-load-balancer-listeners命令向您的负载均衡器添加侦听器，该侦听器在端口 443 上接受 HTTPS 请求，并使用 HTTP 将请求发送到端口 80 上的实例：

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

   如果要设置后端实例身份验证，请使用以下命令添加一个侦听器，此侦听器接受端口 443 上的 HTTPS 请求并使用 HTTPS 将请求发送到端口 443 上的实例：

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

3. （可选）您可以使用以下describe-load-balancers命令查看负载均衡器的更新详细信息：

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

以下为响应示例：

```
{
    "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. (可选) 您的 HTTPS 侦听器是使用默认安全策略创建的。如果要指定不同的预定义安全策略或自定义安全策略，请使用create-load-balancer-policy和 set-load-balancer-policiesof-listener 命令。有关更多信息，请参阅 使用更新 SSL 协商配置 AWS CLI。

5. （可选）要设置后端实例身份验证，请使用 set-load-balancer-policies-for-backend-server 命令。有关更多信息，请参阅配置后端实例身份验证。

替换经典负载均衡器的 SSL 证书

如果您有 HTTPS 侦听器，在创建侦听器时已在负载均衡器上部署了 SSL 服务器证书。每个证书都有有效期限。您必须确保在其有效期限结束前续订或替换证书。

由您的负载均衡器提供 AWS Certificate Manager 并部署在您的负载均衡器上的证书可以自动续订。ACM 会尝试在到期之前续订证书。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的托管续订。如果您将证书导入 ACM，则必须监视证书的到期日期并在到期前续订。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的导入证书。续订部署在负载均衡器上的证书之后，新请求使用续订的证书。

要替换证书，您必须先按照在首次创建当前证书时使用的相同步骤操作来创建新证书。然后，您可以替换该证书。替换部署在负载均衡器上的证书之后，新请求使用新的证书。

请注意，续订或替换证书不影响负载均衡器节点已收到的请求，并暂停指向正常运行的目标的路由。

目录

使用控制台替换 SSL 证书

您可以使用 ACM 提供的证书或上传到 IAM 的证书替换负载均衡器上部署的证书。

使用控制台替换 HTTPS 负载均衡器的 SSL 证书

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择管理侦听器。
5. 在管理侦听器页面上，找到要更新的侦听器，再选择默认 SSL 证书下的编辑，然后执行以下操作之一：

- 如果您使用创建或导入了证书 AWS Certificate Manager，请选择 F rom ACM，从列表中选择证书，然后选择保存更改。

> **Note**
>
> 此选项只在支持 的区域中可用 AWS Certificate Manager

- 如果使用 IAM 导入了证书，请选择从 IAM 并从列表中选择该证书，然后选择保存更改。
- 如果您有 SSL 证书要导入到 ACM，请选择导入和到 ACM。在证书私有密钥中，复制并粘贴 PEM 编码的私有密钥文件的内容。在证书正文中，复制并粘贴 PEM 编码的公有密钥证书文件的内容。在证书链 – 可选中，复制并粘贴 PEM 编码的证书链文件的内容，除非您使用的是自行签名的证书并且浏览器是否隐式接受证书并不重要。
- 如果您有要导入的 SSL 证书，但该区域不支持 ACM，请选择导入和到 IAM。在证书名称字段中输入证书的名称。在证书私有密钥中，复制并粘贴 PEM 编码的私有密钥文件的内容。在证书正文中，复制并粘贴 PEM 编码的公有密钥证书文件的内容。在证书链 – 可选中，复制并粘贴 PEM 编码的证书链文件的内容，除非您使用的是自行签名的证书并且浏览器是否隐式接受证书并不重要。
- 选择 Save changes（保存更改）。

使用 AWS CLI替换 SSL 证书

您可以使用 ACM 提供的证书或上传到 IAM 的证书替换负载均衡器上部署的证书。

使用 ACM 提供的证书替换 SSL 证书

1. 使用以下 request-certificate 命令请求新的证书：

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

2. 使用以下 set-load-balancer-listener-ssl-certificate 命令设置证书：

```
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
```

使用已上传到 IAM 的证书替换 SSL 证书

1. 如果您有未上传的 SSL 证书，请参阅 IAM 用户指南中的上传服务器证书。
2. 使用以下get-server-certificate命令获取证书的 ARN：

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

3. 使用以下 set-load-balancer-listener-ssl-certificate 命令设置证书：

```
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
```

更新经典负载均衡器的 SSL 协商配置

Elastic Load Balancing 提供了具有预定义 SSL 协商配置的安全策略，可使用这些配置协商客户端与负载均衡器之间的 SSL 连接。如果您对侦听器使用 HTTPS/SSL 协议，则可使用其中一个预定义安全策略，或者使用您自己的自定义安全策略。

有关安全策略的更多信息，请参阅经典负载均衡器的 SSL 协商配置。如需了解 Elastic Load Balancing 提供的安全策略的配置，请参阅经典负载均衡器的预定义 SSL 安全策略。

如果在没有关联安全策略的情况下创建 HTTPS/SSL 侦听器，Elastic Load Balancing 会将默认预定义安全策略 ELBSecurityPolicy-2016-08 与您的负载均衡器关联。

如果您愿意，可创建一个自定义配置。强烈建议您先测试安全策略，然后再升级负载均衡器配置。

以下示例说明如何为 HTTPS/SSL 侦听器更新 SSL 协商配置。请注意，更改不影响由负载均衡器节点接收并等待路由到运行正常的实例的请求，但是更新的配置将用于接收的新请求。

目录

使用控制台更新 SSL 协商配置

默认情况下，Elastic Load Balancing 将最新的预定义策略与您的负载均衡器关联。添加新的预定义策略后，建议您将负载均衡器更新为使用新的预定义策略。或者，您也可以选择其他预定义安全策略或创建自定义策略。

使用控制台更新 HTTPS/SSL 负载均衡器的 SSL 协商配置

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择管理侦听器。
5. 在管理侦听器页面上，找到要更新的侦听器，选择安全策略下的编辑，然后使用下面的任意一种选项选择安全策略：
   - 保留默认策略 P ELBSecurityolicy-2016-08，然后选择保存更改。
   - 选择除默认策略以外的预定义策略，然后选择保存更改。
   - 选择自定义，然后至少启用一项协议和一个密码，如下所示：
     a. 对于 SSL Protocols，选择要启用的一个或多个协议。
     b. 对于 SSL 选项，选择服务器顺序首选项，以便对 SSL 协商使用经典负载均衡器的预定义 SSL 安全策略中列出的顺序。
     c. 对于 SSL Ciphers，选择要启用的一个或多个密码。如果您已有一个 SSL 证书，则必须启用用于创建该证书的密码，因为 DSA 和 RSA 密码特定于签名算法。
     d. 选择 Save changes（保存更改）。

使用更新 SSL 协商配置 AWS CLI

您可使用默认预定义安全策略 `ELBSecurityPolicy-2016-08`、其他预定义安全策略或自定义安全策略。

使用预定义 SSL 安全策略

1. 使用以下describe-load-balancer-policies命令列出 Elastic Load Balancing 提供的预定义安全策略。您可以使用的语法取决于您使用的操作系统和 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
```

下面是示例输出：

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

若要确定为策略启用的密码，请使用以下命令：

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

有关预定义安全策略的配置的信息，请参阅经典负载均衡器的预定义 SSL 安全策略。

2. 使用create-load-balancer-policy命令使用您在上一步中描述的预定义安全策略之一创建 SSL 协商策略。例如，以下命令使用默认预定义安全策略：

```
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
```

如果您超出了负载均衡器策略数量的限制，请使用delete-load-balancer-policy命令删除所有未使用的策略。

3. （可选）使用以下describe-load-balancer-policies命令验证策略是否已创建：

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

响应包括策略的描述。

4. 使用以下 set-load-balancer-policiesof-listener 命令在负载均衡器端口 443 上启用该策略：

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

> **Note**
>
> set-load-balancer-policies-of-listener 命令将指定负载均衡器端口的当前策略集替换为指定的策略集。--policy-names 列表必须包括要启用的所有策略。如果您省略当前已启用的策略，则禁用此策略。

5. （可选）使用以下describe-load-balancers命令验证是否已为负载平衡器端口启用新策略：

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

响应表明已在端口 443 上启用该策略。

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

```
      ]
  }
...
```

当您创建自定义安全策略时，必须至少启用一项协议和一个密码。DSA 和 RSA 密码特定于签名算法，用于创建 SSL 证书。如果您已有一个 SSL 证书，请确保启用用于创建该证书的密码。您的自定义策略的名称不得以 ELBSecurityPolicy- 或 ELBSample- 开头，因为这些前缀是为预定义安全策略的名称保留的。

使用自定义 SSL 安全策略

1. 使用create-load-balancer-policy命令使用自定义安全策略创建 SSL 协商策略。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
```

   如果您超出了负载均衡器策略数量的限制，请使用delete-load-balancer-policy命令删除所有未使用的策略。

2. （可选）使用以下describe-load-balancer-policies命令验证策略是否已创建：

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

   响应包括策略的描述。

3. 使用以下 set-load-balancer-policiesof-listener 命令在负载均衡器端口 443 上启用该策略：

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

> **Note**
>
> set-load-balancer-policies-of-listener 命令将指定负载均衡器端口的当前策略集替换为指定的策略集。--policy-names 列表必须包括要启用的所有策略。如果您省略当前已启用的策略，则禁用此策略。

4. （可选）使用以下describe-load-balancers命令验证是否已为负载平衡器端口启用新策略：

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

响应表明已在端口 443 上启用该策略。

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

经典负载均衡器的已注册实例

创建 Classic Load Balancer 后，您必须向负载均衡器注册您的 EC2 实例。您可以从与负载均衡器位于同一区域内的单个可用区或多个可用区中选择 EC2 实例。Elastic Load Balancing 会定期对注册的 EC2 实例执行运行状况检查，并自动将传入请求分配到已注册的运行状况良好的 EC2 实例中的负载均衡器的 DNS 名称。

内容

实例的最佳实践

- 您必须确保负载均衡器可同时在侦听器端口和运行状况检查端口上与实例进行通信。有关更多信息，请参阅 为经典负载均衡器配置安全组。您实例的安全组必须为负载均衡器的每个子网允许两个端口上的双向流量。
- 在计划向负载均衡器注册的所有实例上安装 Web 服务器 (如 Apache 或 Internet Information Services (IIS))。
- 对于 HTTP 和 HTTPS 侦听器，我们建议您在 EC2 实例中启用 keep-alive 选项，这样负载均衡器就可以将与您的实例的连接重复用于多个客户端请求。这样可减少 Web 服务器上的负载并提高负载均衡器吞吐量。保持活动超时应至少为 60 秒，以确保由负载均衡器负责关闭实例连接。
- Elastic Load Balancing 支持路径最大传输单元 (MTU) 发现。要确保路径 MTU 发现可以正常运行，您必须确保实例的安全组允许使用需要 ICMP 分片 (类型 3，代码 4) 的消息。有关更多信息，请参阅《亚马逊 EC2 用户指南》中的 MTU 发现路径。

关于 VPC 的建议

Virtual Private Cloud (VPC) [虚拟私有云（ VPC ）]

除非您在 2014 年 AWS 账户 之前创建的，否则每个区域都有一个默认 VPC。可以使用负载均衡器的默认 VPC（如有），也可以创建新的 VPC。有关更多信息，请参阅 Amazon VPC 用户指南。

您的负载均衡器的子网

要确保您的负载均衡器可以正确扩展，请验证您的负载均衡器的每个子网都具有一个带有至少一个 /27 位掩码 (例如 10.0.0.0/27) 的 CIDR 块和至少 8 个空闲 IP 地址。您的负载均衡器将使用这些 IP 地址与实例建立连接，并在需要时横向扩展。如果 IP 地址不足，则负载均衡器可能无法扩展，导致因容量不足而出现 503 错误。

在要启动实例的每个可用区中创建子网。根据您的应用程序，您可以在公有子网、私有子网或这两者的组合中启动实例。公有子网有一条指向互联网网关的路由。请注意，默认情况下，每个可用区 VPCs 都有一个公有子网。

当您创建负载均衡器时，必须将一个或多个公有子网添加到负载均衡器。如果实例在私有子网中，请在包含实例的子网所在的可用区中创建公有子网；您会将这些公有子网添加到负载均衡器。

网络 ACLs

您 ACLs 的 VPC 的网络必须允许侦听器端口和运行状况检查端口上的双向流量。有关更多信息，请参阅 ACLs Classic Load Balancer 实例的网络。

向经典负载均衡器注册实例

注册 EC2 实例会将其添加到您的负载均衡器中。负载均衡器连续监控其已启用的可用区中注册实例的运行状况，并将请求路由至运行正常的注册实例。如果对实例的需求上升，您可以向负载均衡器注册其他实例以处理需求。

注销 EC2 实例会将其从您的负载均衡器中移除。某个实例注销之后，负载均衡器立即停止将请求路由到该实例。如果需求降低，或者您需要维护实例，可以从负载均衡器注销实例。注销的实例仍保持运行，但不再从负载均衡器接收流量，您可以在准备好时再次向负载均衡器注册它。

注销实例时，Elastic Load Balancing 会等到进行中的请求完成（如果启用了 Connection Draining）。有关更多信息，请参阅 配置经典负载均衡器的 Connection Draining。

如果负载均衡器连接到某个 Auto Scaling 组，则该组中的实例会自动向负载均衡器注册。如果您从 Auto Scaling 组分离负载均衡器，则该组中的实例会注销。

Elastic Load Balancing 使用负载均衡器的 IP 地址将您的 EC2 实例注册到您的负载均衡器。

[EC2-VPC] 当您注册连接了弹性网络接口 (ENI) 的实例时，负载均衡器会将请求路由到该实例的主接口 (eth0) 的主要 IP 地址。

内容

注册实例

准备就绪时，向负载均衡器注册实例。如果实例位于为负载均衡器启用的可用区中，那么实例只要通过所需数量的运行状况检查，即可从负载均衡器接收流量。

使用控制台注册您的实例

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在目标实例选项卡上，选择管理实例。
5. 在管理实例页面的可用实例表中，选择要注册到负载均衡器的实例。
6. 确保需要注册的实例已填充到查看选定实例表中。
7. 选择 Save changes（保存更改）。

要使用注册您的实例 AWS CLI

使用以下 register-instances-with-load-balancer 命令：

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

以下示例响应列出了已向负载均衡器注册的实例：

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

```
        }
    ]
}
```

查看向负载均衡器注册的实例

使用以下describe-load-balancers命令列出在指定负载均衡器中注册的实例：

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

下面是示例输出：

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

确定已注册实例的负载均衡器

使用以下describe-load-balancers命令获取注册指定实例的负载均衡器的名称：

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

下面是示例输出：

```
my-load-balancer
```

注销实例

如果您不再需要容量，或者如果需要维护实例，可以从负载均衡器注销实例。

如果负载均衡器连接到某个 Auto Scaling 组，则从该组分离实例也会从负载均衡器将其注销。有关更多信息，请参阅 Amazon Auto Scaling 用户指南中的将 EC2 实例从 Aut EC2 o Sc aling 组中分离出来。

使用控制台注销您的实例

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。

3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在目标实例选项卡上，选择管理实例。
5. 在管理实例页面的可用实例表中，取消选择该实例，以将其从负载均衡器取消注册。
6. 确保需要取消注册的实例未填充到查看选定实例表中。
7. 选择 Save changes（保存更改）。

要取消注册您的实例，请使用 AWS CLI

使用以下 deregister-instances-from-load-balancer 命令：

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

以下示例响应列出了向负载均衡器注册的其他实例：

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

对经典负载均衡器中的实例执行运行状况检查

您的经典负载均衡器会定期向其注册实例发送请求以测试其状态。这些测试称为运行状况检查。在执行运行状况检查时，运行状况良好的实例的状态为 InService。在执行运行状况检查时，运行状况不佳的任何实例的状态为 OutOfService。负载均衡器会对所有已注册实例执行运行状况检查，无论实例处于运行状况良好状态还是不佳状态。

负载均衡器仅将请求路由到正常的实例。当负载均衡器确定某个实例不正常时，会停止将请求路由到该实例。当实例恢复正常状态时，负载均衡器将恢复向该实例路由请求。

负载均衡器使用 Elastic Load Balancing 提供的默认运行状况检查配置，或使用您配置的运行状况检查配置检查已注册实例的运行状况。

如果您已将 Auto Scaling 组与经典负载均衡器关联，则可以使用负载均衡器运行状况检查确定 Auto Scaling 组中的实例的运行状况。默认情况下，Auto Scaling 组会定期确定每个实例的运行状况。有关

更多信息，请参阅 Amazon Auto Scaling 用户指南中的将 Elastic Load Balancing 运行状况检查添加到您的 A EC2 uto Scaling 群组。

内容

运行状况检查配置

运行状况配置包含负载均衡器用于确定已注册实例的运行状况的信息。下表介绍了运行状况检查配置字段。

字段	描述
协议	连接到实例所使用的协议。 有效值：TCP、HTTP、HTTPS 和 SSL 控制台默认值：HTTP CLI/API 默认值：TCP
端口	用于以 `protocol:port` 对的形式连接实例的端口。如果负载均衡器在配置的响应超时期内未能在指定端口上与实例连接，则将实例视为运行状况不佳。 协议：TCP、HTTP、HTTPS 和 SSL 端口范围：1 至 65535 控制台默认值：`HTTP:80` CLI/API 默认值：`TCP:80`
路径	HTTP 或 HTTPS 请求的目标。

字段	描述
	在端口和路径上向实例发出 HTTP 或 HTTPS GET 请求。如果负载均衡器在响应超时期内收到“200 OK”之外的任何响应，则会将实例视为运行状况不佳。如果响应包括正文，则应用程序必须将 Content-Length 标头设置为大于等于零的值，或者指定其值设置为“chunked”的 Transfer-Encoding。 默认值：`/index.html`
响应超时	接收来自运行状况检查的响应时要等待的时间 (秒)。 有效值：2 至 60 默认值：5
HealthCheck 间隔	单个实例的运行状况检查之间的时间量 (秒)。 有效值：5 至 300 默认值：30
不正常阈值	在宣布EC2 实例运行状况不佳之前必须连续失败的运行状况检查次数。 有效值：2 至 10 默认值：2
正常阈值	在宣布EC2 实例运行正常之前必须连续成功进行运行状况检查的次数。 有效值：2 至 10 默认值：10

负载均衡器使用指定的端口、协议和路径，每 `Interval` 秒向每个已注册的实例发送一次运行状况检查请求。每个运行状况检查请求都是独立的，并且在整个时间间隔内持续。等待实例响应所花费的时间不会影响下次运行状况检查的时间间隔。如果运行状况检查超过UnhealthyThresholdCount连续失败次数，则负载均衡器会使该实例停止服务。当运行状况检查超过HealthyThresholdCount连续成功率时，负载均衡器会将实例重新投入使用。

如果实例在运行状况检查的时间间隔内返回 200 响应代码，则 HTTP/HTTPS 运行状况检查成功。如果 TCP 连接成功，则 TCP 运行状况检查成功。如果 SSL 握手成功，则 SSL 运行状况检查成功。

更新运行状况检查配置

您可随时更新负载均衡器的运行状况检查配置。

使用控制台更新负载均衡器的运行状况检查配置

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Health checks 选项卡上，选择 Edit。
5. 在编辑运行状况检查设置页面的运行状况检查下，根据需要更新配置。
6. 确定选择无误之后，选择保存更改。

要更新负载均衡器的运行状况检查配置，请使用 AWS CLI

使用以下 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
```

检查实例的运行状况

您可检查已注册实例的运行状况。

使用控制台检查实例的运行状况

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。

3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在详细信息部分中，状态将指示使用中的实例数量。
5. 在目标实例选项卡的目标实例表内，运行状态列将指示每个已注册实例的具体状态。

要使用检查您的实例的运行状况 AWS CLI

使用以下 describe-instance-health 命令：

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

根据运行状况检查进行故障排除

已注册的实例可能因多种原因无法通过负载均衡器运行状况检查。运行状况检查失败的最常见原因是 EC2 实例关闭了与您的负载均衡器的连接，或者 EC2 实例的响应超时。有关失败的运行状况检查问题的可能原因以及您可以采取的解决问题的措施的信息，请参阅 对经典负载均衡器进行故障排除：运行状况检查。

经典负载均衡器的实例的安全组

安全组 起到防火墙的作用，可控制允许往返于一个或多个实例的流量。启动 EC2 实例时，您可以将一个或多个安全组与该实例关联起来。对于每个安全组，添加一个或多个规则以允许流量。您可以随时修改某个安全组的规则；新规则会自动应用于与该安全组关联的所有实例。有关更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 安全组。

您的实例的安全组必须允许它们与负载均衡器进行通信。下表显示了推荐的入站规则。

来源	协议	端口范围	注释
load balancer security group	TCP	*instance listener*	在实例侦听器端口上允许来自负载均衡器的流量
load balancer security group	TCP	*health check*	在运行状况检查端口上允许来自负载均衡器的流量

我们还建议您允许入站 ICMP 流量以支持路径 MTU 发现。有关更多信息，请参阅《亚马逊 EC2 用户指南》中的 MTU 发现路径。

ACLs Classic Load Balancer 实例的网络

网络访问控制列表 (ACL) 在子网级别允许或拒绝特定的入站或出站流量。您可以使用 VPC 的默认网络 ACL，也可以为 VPC 创建自定义网络 ACL，使其规则与您安全组的规则相似，以便为您的 VPC 添加额外安全层。

VPC 的默认网络访问控制列表 (ACL) 允许所有入站和出站流量。如果您创建自定义网络 ACLs，则必须添加允许负载均衡器和实例通信的规则。

实例子网的推荐规则取决于子网是私有还是公有子网。以下规则适用于私有子网。如果您的实例在公有子网中，请将源和目标从 VPC 的 CIDR 更改为 `0.0.0.0/0`。

以下是推荐的入站规则。

来源	协议	端口范围	注释
VPC CIDR	TCP	*instance listener*	在实例侦听器端口上允许来自 VPC CIDR 的入站流量
VPC CIDR	TCP	*health check*	在运行状况检查端口上允许来自 VPC CIDR 的入站流量

以下是推荐的出站规则。

目标	协议	端口范围	注释
VPC CIDR	TCP	1024-65535	在临时端口上允许流向 VPC CIDR 的出站流量

监控经典负载均衡器

您可使用以下功能监控负载均衡器，分析流量模式及解决与负载均衡器和后端实例相关的问题。

CloudWatch 指标

Elastic Load Balancing 向亚马逊发布 CloudWatch 有关您的负载均衡器和后端实例的数据点。CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。您可使用这些指标来验证您的系统是否按预期运行。有关更多信息，请参阅 CloudWatch 您的 Classic Load Balancer 的指标。

Elastic Load Balancing 访问日志

Elastic Load Balancing 访问日志可捕获向负载均衡器发出的请求的详细信息，并将这些信息作为日志文件存储在您指定的 Amazon S3 存储桶中。每个日志都包含详细信息（如收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应）。您可以使用这些访问日志分析流量模式并对后端应用程序进行故障排除。有关更多信息，请参阅 经典负载均衡器的访问日志。

CloudTrail 日志

AWS CloudTrail 使您能够跟踪您的账户或代表您的 AWS 账户向 Elastic Load Balancing API 发出的调用。 CloudTrail 将信息存储在您指定的 Amazon S3 存储桶中的日志文件中。可利用这些日志文件，通过确定已发出的请求、请求的源 IP 地址、请求的发出方、请求的发出时间等来监控负载均衡器的活动。有关更多信息，请参阅使用记录 Elastic Load Balancing 的 API 调用 CloudTrail。

CloudWatch 您的 Classic Load Balancer 的指标

Elastic Load Balancing 将您的 CloudWatch 负载均衡器和后端实例的数据点发布到亚马逊。CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。例如，您可以监控负载均衡器在指定时间段内 EC2 运行正常的实例总数。每个数据点都有相关联的时间戳和可选测量单位。

您可使用指标来验证系统是否正常运行。例如，您可以创建 CloudWatch 警报来监控指定的指标，并在该指标超出您认为可接受的范围时启动操作（例如向电子邮件地址发送通知）。

CloudWatch 仅当请求流经负载均衡器时，Elastic Load Balancing 才会向其报告指标。如果有请求流经负载均衡器，则 Elastic Load Balancing 进行测量并以 60 秒的间隔发送其指标。如果没有请求流经负载均衡器或指标无数据，则不报告指标。

有关亚马逊的更多信息 CloudWatch，请参阅亚马逊 CloudWatch 用户指南。

内容

经典负载均衡器指标

AWS/ELB 命名空间包括以下指标。

指标	描述
BackendConnectionErrors	负载均衡器和注册实例之间连接建立不成功的次数。因为负载均衡器在发生错误时会重试连接，所以此计数会超过请求速率。请注意，此计数还包含与运行状况检查有关的所有连接错误。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。请注意，Average、Minimum 和 Maximum 针对每个负载均衡器节点报告，一般并无用处。然而，最小值与最大值（或者峰值到平均值、平均值到谷底）之间的差异可用于确定负载均衡器节点是否存在异常。 示例：假设您的负载均衡器在 us-west-2a 和 us-west-2b 各有 2 个实例，并且向 us-west-2a 中 1 个实例的连接尝试导致出现后端连接错误。us-west-2a 的 sum 值包含这些连接错误，而 us-west-2b 的 sum 值不包含。因此，负载均衡器的 sum 值等于 us-west-2a 的 sum 值。
DesyncMitigationMode_NonCompliant_Request_Count	[HTTP 侦听器] 不符合 RFC 7230 标准的请求数。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。
HealthyHostCount	

指标	描述
	向负载均衡器注册的运行状况良好的实例的数量。新注册的实例在通过第一次运行状况检查后被视为运行状况良好。如果启用跨可用区负载均衡，则会跨所有可用区为 LoadBalancerName 维度计算运行状况良好的实例的数量。否则，将为每个可用区域计算该数量。 报告标准：有注册的实例 Statistics：最有用的统计工具为 Average 和 Maximum。这些统计数据由负载均衡器节点决定。请注意，某些负载均衡器节点可能在短时间内认为某实例运行状况不佳，而其他节点将该实例视为运行状况良好。 示例：假设您的负载均衡器在 us-west-2a 和 us-west-2b 各有 2 个实例，并且 us-west-2a 的 1 个实例运行状况不佳，而 us-west-2b 没有运行状况不佳的实例。对于 AvailabilityZone 维度，us-west-2a 平均有 1 个运行状况良好和 1 个运行状况不佳的实例，us-west-2b 平均有 2 个运行状况良好和 0 个运行状况不佳的实例。
HTTPCode_Backend_2XX，HTTPCode_Backend_3XX，HTTPCode_Backend_4XX，HTTPCode_Backend_5XX	[HTTP 侦听器] 注册实例生成的 HTTP 响应代码的数量。该计数不包含负载均衡器生成的任何响应代码。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均为 1。 示例：假设您的负载均衡器在 us-west-2a 和 us-west-2b 各有 2 个实例，并且发送到 us-west-2a 中的 1 个实例的请求导致了 HTTP 500 响应。us-west-2a 的 sum 值包含这些错误响应，而 us-west-2b 的 sum 值不包含。因此，负载均衡器的 sum 值等于 us-west-2a 的 sum 值。

指标	描述
HTTPCode_ELB_4XX	[HTTP 侦听器] 负载均衡器生成的 HTTP 4XX 客户端错误代码的数量。如果请求格式错误或不完整，则会生成客户端错误。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均为 1。 示例：假设您的负载均衡器启用了 us-west-2a 和 us-west-2b，并且客户端请求包含格式错误的请求 URL。结果可能导致所有可用区中客户端错误增加。负载均衡器的 sum 值为各可用区的值的总和。
HTTPCode_ELB_5XX	[HTTP 侦听器] 负载均衡器生成的 HTTP 5XX 服务器错误代码的数量。此计数不包括注册实例生成的任何响应代码。如果没有运行状况良好的实例注册到负载均衡器，或者请求速率超过实例或负载均衡器的容量（溢出），则会报告该指标。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均为 1。 示例：假设您的负载均衡器启用了 us-west-2a 和 us-west-2b，并且 us-west-2a 中的实例具有较高的延迟，对请求的响应较慢。结果，us-west-2a 中的负载均衡器节点波动队列填满，客户端收到 503 错误。如果 us-west-2b 继续正常响应，则负载均衡器的 sum 值将等于 us-west-2a 的 sum 值。

指标	描述
Latency	[HTTP 侦听器] 从负载均衡器将请求发送到已注册实例到该实例开始发送响应标头所用的总时间 (以秒为单位)。 [TCP 侦听器] 负载均衡器成功与注册实例建立连接所用的总时间 (以秒为单位)。 报告标准：有非零值 Statistics：最有用的统计工具是 Average。Maximum 可用于确定某些请求的耗时是否大大超过平均时间。请注意，Minimum 一般没什么用处。 示例：假设您的负载均衡器在 us-west-2a 和 us-west-2b 各有 2 个实例，并且发送到 us-west-2a 中的 1 个实例的请求具有较高的延迟。us-west-2a 的 average 值将高于 us-west-2b 的 average 值。
RequestCount	在指定的时间段（1 或 5 分钟）完成的请求或者发出的连接的数量。 [HTTP 侦听器] 收到和路由的请求数，包括来自注册实例的 HTTP 错误响应。 [TCP 侦听器] 向注册实例发出的连接的数量。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。请注意，Minimum、Maximum 和 Average 均返回 1。 示例：假设您的负载均衡器在 us-west-2a 和 us-west-2b 各有 2 个实例，并有 100 个请求发送至该负载均衡器。有 60 个请求发送至 us-west-2a，每个实例接收 30 个请求，有 40 个请求发送至 us-west-2b，每个实例接收 20 个请求。对于 AvailabilityZone 维度，us-west-2a 总计有 60 个请求，us-west-2b 总计有 40 个请求。对于 LoadBalancerName 维度，总计有 100 个请求。

指标	描述
SpilloverCount	因波动队列填满而拒绝的请求的总数。 [HTTP 侦听器] 负载均衡器返回 HTTP 503 错误代码。 [TCP 侦听器] 负载均衡器关闭连接。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。请注意，Average、Minimum 和 Maximum 针对每个负载均衡器节点报告，一般并无用处。 示例：假设您的负载均衡器启用了 us-west-2a 和 us-west-2b，并且 us-west-2a 中的实例具有较高的延迟，对请求的响应较慢。结果是 us-west-2a 中的负载均衡器节点波动队列填满，导致溢出。如果 us-west-2b 继续正常响应，则负载均衡器的 sum 值将与 us-west-2a 的 sum 值相同。
SurgeQueueLength	正在等待路由到正常实例的请求（HTTP 侦听器）或连接（TCP 侦听器）总数。队列的最大大小为 1024。队列填满后，额外的请求或连接将被拒绝。有关更多信息，请参阅 SpilloverCount 。 报告标准：有非零值。 统计数据：最有价值的统计数据是 Maximum，因为它代表排队请求的峰值。结合使用 Average 统计数据与 Minimum 和 Maximum 可以确定排队请求的范围。请注意，Sum 并无用处。 示例：假设您的负载均衡器启用了 us-west-2a 和 us-west-2b，并且 us-west-2a 中的实例具有较高的延迟，对请求的响应较慢。结果是 us-west-2a 中的负载均衡器节点波动队列填满，很可能导致客户端的响应时间增加。如果这种情况继续存在，负载均衡器可能溢出（参阅 SpilloverCount 指标）。如果 us-west-2b 继续正常响应，则负载均衡器的 max 将与 us-west-2a 的 max 相同。

指标	描述
UnHealthyHostCount	向负载均衡器注册的运行状况不良的实例的数量。如果实例超过运行状况检查所配置的不佳阈值，则认为实例运行状况不佳。不佳实例在符合运行状况检查所配置的良好阈值之后，被重新视为运行状况良好。 报告标准：有注册的实例 Statistics：最有用的统计工具为 Average 和 Minimum。这些统计数据由负载均衡器节点决定。请注意，某些负载均衡器节点可能在短时间内认为某实例运行状况不佳，而其他节点将该实例视为运行状况良好。 示例：请参阅HealthyHostCount 。

以下指标使您能够估算将经典负载均衡器迁移到 Application Load Balancer 的成本。这些指标仅供参考，不用于 CloudWatch 警报。注意，如果您的经典负载均衡器有多个侦听器，则这些指标在所有侦听器上进行聚合。

估算值基于包含一条默认规则和一个大小为 2K 的证书的负载均衡器。如果您使用的是大小为 4K 或以上的证书，我们建议您按如下方式估算成本：使用迁移工具基于您的经典负载均衡器创建一个 Application Load Balancer，然后监控该 Application Load Balancer 的 ConsumedLCUs 指标。有关更多信息，请参阅《Elastic Load Balancing 用户指南》中的 迁移经典负载均衡器。

指标	描述
EstimatedALBActiveConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标的并发活动 TCP 连接的估计数。
EstimatedALBConsumedLCUs	Application Load Balancer 使用的负载均衡器容量单位 (LCU) 的估计数。您需要为每小时 LCUs 的使用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。
EstimatedALBNewConnectionCount	

指标	描述
	从客户端到负载均衡器以及从负载均衡器到目标建立的新 TCP 连接的估计数。
EstimatedProcessedBytes	Application Load Balancer 处理的估计字节数。

经典负载均衡器的指标维度

要筛选经典负载均衡器的指标，请使用以下维度。

维度	描述
AvailabilityZone	按指定的可用区筛选指标数据。
LoadBalancerName	按指定的负载均衡器筛选指标数据。

经典负载均衡器指标的统计数据

CloudWatch 根据 Elastic Load Balancing 发布的指标数据点提供统计数据。统计数据是在指定的时间段内汇总的指标数据。当请求统计数据时，返回的数据流按指标名称和维度进行识别。维度是用于唯一标识指标的名称/值对。例如，您可以请求在特定可用区启动的负载均衡器后面的所有运行正常的 EC2 实例的统计数据。

Minimum 和 Maximum 统计数据反映各个负载均衡器节点报告的最小值和最大值。例如，假定有两个负载均衡器节点。一个节点的 HealthyHostCount 的 Minimum 为 2，Maximum 为 10，Average 为 6，另一个节点的 HealthyHostCount 的 Minimum 为 1，Maximum 为 5，Average 为 3。因此，负载均衡器的 Minimum 为 1，Maximum 为 10，Average 大约为 4。

Sum 统计数据是所有负载均衡器节点的汇总值。由于这些指标在每个周期均包含多个报告，因此 Sum 仅适用于对所有负载均衡器节点进行汇总的指标，如 RequestCount、HTTPCode_ELB_XXX、HTTPCode_Backend_XXX、BackendConnectionErrors 和 SpilloverCount。

SampleCount 统计数据是测量的样本数。由于这些指标是基于采样间隔和事件进行收集的，因此此统计信息一般没有用。例如，对于 HealthyHostCount，SampleCount 基于每个负载均衡器节点报告的样本数，而不是运行状况正常的主机数。

百分位数指示某个值在数据集中的相对位置。您可以指定任何百分位数，最多使用两位小数 (例如 p95.45)。例如，第 95 个百分位数表示 95% 的数据低于此值，5% 的数据高于此值。百分位数通常用于隔离异常值。例如，假设某个应用程序从缓存服务大多数请求的时间是 1-2 毫秒，但如果缓存是空的，则时间需要 100-200 毫秒。最大值反映了最慢的情况，也就是大约 200 毫秒。平均值不表示数据的分布。百分位提供了一个更有意义的应用程序性能视图。通过使用第 99 个百分位数作为 Auto Scaling 触发器或 CloudWatch 警报，您可以将处理时间超过 2 毫秒的请求设定为不超过 1%。

查看您的负载均衡器的 CloudWatch 指标

您可以使用 Amazon EC2 控制台查看您的负载均衡器的 CloudWatch 指标。这些指标显示为监控图表。如果负载均衡器处于活动状态并且正在接收请求，则监控图表会显示数据点。

或者，您可以使用 CloudWatch 控制台查看负载均衡器的指标。

使用控制台查看指标

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 选择监控选项卡。
5. 要查看单个指标的大图，请将鼠标悬停在其图表上，然后选择 Maximize 图标。可供使用的指标如下：

   - 正常主机 - HealthyHostCount
   - 不正常的主机 - UnHealthyHostCount
   - 平均延迟 - Latency
   - 请求 – RequestCount
   - 后端连接错误 - BackendConnectionErrors
   - 波动队列长度 - SurgeQueueLength
   - 溢出计数 - SpilloverCount
   - HTTP 2 XXs — HTTPCode_Backend_2XX
   - HTTP 3 XXs — HTTPCode_Backend_3XX

- HTTP 4 XXs — HTTPCode_Backend_4XX
- HTTP 5 XXs — HTTPCode_Backend_5XX
- ELB HTTP 4 — XXs HTTPCode_ELB_4XX
- ELB HTTP 5 — XXs HTTPCode_ELB_5XX
- 估计已处理字节数 – EstimatedProcessedBytes
- 预计消耗的 ALB — LCUs EstimatedALBConsumedLCUs
- 估计 ALB 活动连接数 – EstimatedALBActiveConnectionCount
- 估计 ALB 新连接数 – EstimatedALBNewConnectionCount

使用 CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 选择 ELB 命名空间。
4. 请执行下列操作之一：
   - 选择一种指标维度，按负载均衡器、可用区或跨所有负载均衡器查看指标。
   - 要跨所有维度查看某个指标，请在搜索字段中键入其名称。
   - 要查看单个负载均衡器的指标，请在搜索字段中键入其名称。
   - 要查看单个可用区的指标，请在搜索字段中键入其名称。

经典负载均衡器的访问日志

Elastic Load Balancing 提供了访问日志，该访问日志可捕获有关发送到负载均衡器的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。您可以使用这些访问日志分析流量模式并解决问题。

访问日志是 Elastic Load Balancing 的一项可选功能，默认情况下已禁用此功能。为负载均衡器启用访问日志之后，Elastic Load Balancing 捕获日志并将其存储在您指定的 Amazon S3 存储桶中。您可以随时禁用访问日志记录。

每个访问日志文件在存储到 S3 存储桶中之前将自动使用 SSE-S3 加密，并在您访问它时进行解密。您不需要执行任何操作；加密和解密以透明方式执行。每个日志文件都使用一个唯一密钥进行加密，此密钥本身将使用定期轮换的 KMS 密钥进行加密。有关更多信息，请参阅 Amazon S3 用户指南中的使用 Amazon S3 托管加密密钥使用服务器端加密保护数据 (SSE-S3)。

使用访问日志无需额外付费。您需要支付 Amazon S3 的存储成本，但 Elastic Load Balancing 用以将日志文件发送到 Amazon S3 的带宽是免费的。有关存储成本的更多信息，请参阅 Amazon S3 定价。

目录

访问日志文件

Elastic Load Balancing 以指定间隔从每个负载均衡器节点发布日志文件。为负载均衡器启用访问日志时，可以指定 5 分钟或 60 分钟的发布间隔。在默认情况下，Elastic Load Balancing 以 60 分钟间隔发布日志。如果将间隔设置为 5 分钟，则日志的发布时间为 1:05、1:10、1:15，以此类推。如果将间隔设置为 5 分钟，则日志传输最多延迟 5 分钟；如果将间隔设置为 60 分钟，则最多延迟 15 分钟。您可以随时修改发布间隔。

负载均衡器可以传输相同时间段的多个日志。如果站点具有高流量、多个负载均衡器节点和较短日志发布间隔，则通常会发生这种情况。

访问日志的文件名采用以下格式：

```
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 存储桶的名称。

prefix

（可选）存储桶的前缀（逻辑层级结构）。您指定的前缀不得包含字符串 AWSLogs。要获取更多信息，请参阅使用前缀整理对象。

AWSLogs

我们会在您指定的存储桶名称和可选前缀后添加以 AWSLogs 开头的文件名部分。

aws-account-id

所有者的 AWS 账户 ID。

region

负载均衡器和 S3 存储桶所在的区域。

yyyy/mm/dd

传输日志的日期。

load-balancer-name

负载均衡器的名称。

end-time

日志记录间隔结束的日期和时间。例如，如果发布间隔是 5 分钟，则结束时间 20140215T2340Z 中将包含在 23:35 与 23:40 之间发出的请求的条目。

ip-address

处理请求的负载均衡器节点的 IP 地址。对于内部负载均衡器，这是私有 IP 地址。

random-string

系统生成的随机字符串。

以下是前缀为” 的日志文件名示例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
```

以下是一个不带前缀的日志文件名示例：

```
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
```

日志文件可以在存储桶中存储任意长时间，不过您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。有关更多信息，请参阅 Amazon S3 用户指南中的对象生命周期管理。

访问日志条目

Elastic Load Balancing 记录发送给负载均衡器的请求，包括从未到达后端实例的请求。例如，如果客户端发送格式错误的请求或是没有运行状况良好的实例进行响应，仍会记录请求。

> **Important**
>
> Elastic Load Balancing 将尽力记录请求。我们建议您使用访问日志来了解请求性质，而不是作为所有请求的完整描述。

语法

每个日志条目都包含向负载均衡器进行的单个请求的详细信息。日志条目中的所有字段用空格分隔。日志文件中的每个条目都遵循以下格式：

```
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
```

下表描述了访问日志条目的字段。

字段	描述
time	负载均衡器从客户端收到请求的时间 (采用 ISO 8601 格式)。
elb	负载均衡器的名称
client:port	请求客户端的 IP 地址和端口。
backend:port	处理此请求的已注册实例的 IP 地址和端口。 如果负载均衡器无法将请求发送到已注册实例，或者如果在发送响应之前实例关闭了连接，则将此值设置为 -。 如果注册的实例在空闲超时之前未响应，也可将此值设置为 -。
request_processing_time	[HTTP 侦听器] 从负载均衡器收到请求一直到将请求发送到注册实例所用的总时间 (以秒为单位)。

字段	描述
	[TCP 侦听器] 从负载均衡器接受来自客户端的 TCP/SSL 连接到负载均衡器发送数据的第一个字节到注册实例所用的总时间 (以秒为单位)。 如果负载均衡器无法将请求分派到已注册实例，则此值设置为 -1。如果已注册实例在空闲超时前关闭连接，或客户端发送了格式错误的请求，则会发生这种情况。此外，对于 TCP 侦听器来说，如果客户端与负载均衡器建立连接，但是不发送任何数据，则会发生这种情况。 如果注册的实例在空闲超时之前未响应，也可将此值设置为 -1。
backend_processing_time	[HTTP 侦听器] 从负载均衡器将请求发送到已注册实例到该实例开始发送响应标头所用的总时间 (以秒为单位)。 [TCP 侦听器] 负载均衡器成功与注册实例建立连接所用的总时间 (以秒为单位)。 如果负载均衡器无法将请求分派到已注册实例，则此值设置为 -1。如果已注册实例在空闲超时前关闭连接，或客户端发送了格式错误的请求，则会发生这种情况。 如果注册的实例在空闲超时之前未响应，也可将此值设置为 -1。
response_processing_time	[HTTP 侦听器] 从负载均衡器收到来自已注册实例的响应标头到开始向客户端发送响应所用的总时间 (以秒为单位)。此时间包括在负载均衡器上的排队时间以及从负载均衡器到客户端的连接获取时间。 [TCP 侦听器] 从负载均衡器收到来自已注册实例的第一个字节到开始向客户端发送响应所用的总时间 (以秒为单位)。 如果负载均衡器无法将请求分派到已注册实例，则此值设置为 -1。如果已注册实例在空闲超时前关闭连接，或客户端发送了格式错误的请求，则会发生这种情况。 如果注册的实例在空闲超时之前未响应，也可将此值设置为 -1。
elb_status_code	[HTTP 侦听器] 来自负载均衡器的响应的状态代码。
backend_status_code	[HTTP 侦听器] 来自已注册实例的响应的状态代码。

字段	描述
received_bytes	从客户端 (申请方) 接收的请求大小 (以字节为单位)。 [HTTP 侦听器] 值包括请求正文，但不包括标头。 [TCP 侦听器] 值包括请求正文和标头。
sent_bytes	发送到客户端 (申请方) 的响应的大小 (以字节为单位)。 [HTTP 侦听器] 值包括响应正文，但不包括标头。 [TCP 侦听器] 值包括请求正文和标头。
请求	来自客户端的请求行，包含在双引号内并采用以下格式进行记录：HTTP 方法 + 协议://主机标头:端口 + 路径 + HTTP 版本。负载均衡器将保留客户端记录请求 URI 时发送的 URL。它不设置访问日志文件的内容类型。当您处理此字段时，请考虑客户端发送 URL 的方式。 [TCP 侦听器] URL 是三个短划线，相互之间用空格分隔并以空格结尾 ("- - - ")。
user_agent	[HTTP/HTTPS listener] A User-Agent string that identifies the client that originated the request. The string consists of one or more product identifiers, product[/version]。 如果字符串长度超过 8 KB，则会将其截断。
ssl_cipher	[HTTPS/SSL listener] The SSL cipher. This value is recorded only if the incoming SSL/TLS连接是在成功协商后建立的。否则，该值将设置为 -。
ssl_protocol	[HTTPS/SSL listener] The SSL protocol. This value is recorded only if the incoming SSL/TLS连接是在成功协商后建立的。否则，该值将设置为 -。

示例

示例 HTTP 条目

以下是 HTTP 侦听器 (端口 80 到端口 80) 的示例日志条目：

```
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"
 - -
```

示例 HTTPS 条目

以下是 HTTPS 侦听器 (端口 443 到端口 80) 的示例日志条目：

```
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
```

示例 TCP 条目

以下是 TCP 侦听器 (端口 8080 到端口 80) 的示例日志条目：

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

示例 SSL 条目

以下是 SSL 侦听器 (端口 8443 到端口 80) 的示例日志条目：

```
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
```

处理访问日志

如果您的网站上有大量需求，则负载均衡器可以生成包含大量数据的日志文件 (以 GB 为单位)。您可能无法使用处理来 line-by-line处理如此大量的数据。因此，您可能必须使用提供并行处理解决方案的分析工具。例如，您可以使用以下分析工具分析和处理访问日志：

- Amazon Athena 是一种交互式查询服务，让您能够轻松使用标准 SQL 分析 Amazon S3 中的数据。有关更多信息，请参阅 Amazon Athena 用户指南中的查询经典负载均衡器日志。
- Loggly
- Splunk
- Sumo Logic

为经典负载均衡器启用访问日志

要为负载均衡器启用访问日志，您必须指定负载均衡器将在其中存储日志的 Amazon S3 存储桶的名称。您还必须将一个存储桶策略附加到此存储桶，该策略向 Elastic Load Balancing 授予写入存储桶的权限。

任务

步骤 1：创建 S3 存储桶

在启用访问日志时，您必须为访问日志指定 S3 存储桶。存储桶必须满足以下要求。

要求

- 存储桶必须位于与负载均衡器相同的区域中。该存储桶和负载均衡器可由不同的账户拥有。
- 唯一支持的服务器端加密选项是 Amazon S3 托管密钥 (SSE-S3) 有关更多信息，请参阅 Amazon S3 托管的加密密钥 (SSE-S3)。

使用 Amazon S3 控制台创建 S3 存储桶。

1. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 选择 Create bucket (创建存储桶)。
3. 在 Create a bucket (创建存储桶) 页上，执行以下操作：
   a. 对于存储桶名称，请输入存储桶的名称。此名称在 Amazon S3 内所有现有存储桶名称中必须唯一。在某些区域，可能对存储桶名称有其他限制。有关更多信息，请参阅 Amazon S3 用户指南中的存储桶配额、限制和限制。
   b. 对于 AWS 区域，选择在其中创建负载均衡器的区域。
   c. 对于默认加密，选择 Amazon S3 托管式密钥（SSE-S3）。
   d. 选择 创建存储桶 。

步骤 2：将策略附加到 S3 存储桶

S3 存储桶必须具有为 Elastic Load Balancing 授予将访问日志写入存储桶的权限的存储桶策略。存储桶策略是 JSON 语句的集合，这些语句以访问策略语言编写，用于为存储桶定义访问权限。每个语句都包括有关单个权限的信息并包含一系列元素。

如果您正在使用具有附加策略的现有存储桶，则可以将 Elastic Load Balancing 访问日志的语句添加到该策略。如果您这样做，则建议您评估生成的权限集，以确保它们适用于需要具有对访问日志的存储桶的访问权的用户。

可用的存储桶策略

您将使用的存储桶策略取决于存储桶 AWS 区域 的策略。

⚠ 使用精确的 S3 存储桶增强安全性 ARNs。

- 使用完整的资源路径，而不仅仅是 S3 存储桶 ARN。
- 包括 S3 存储桶 ARN 的账户 ID 部分。
- 请勿在 S3 存储桶 ARN 的账户 ID 部分使用通配符 (*)。

截至 2022 年 8 月或之后可用的区域

该策略向指定的日志传送服务授予权限。此策略适用于以下区域的负载均衡器：

- 亚太地区（海得拉巴）
- 亚太地区（马来西亚）
- 亚太地区（墨尔本）
- 亚太地区（泰国）
- 加拿大西部（卡尔加里）
- 欧洲（西班牙）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 中东（阿联酋）
- 墨西哥（中部）

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
    }
  ]
}
```

对于Resource，使用示例策略中显示的格式，输入访问日志所在位置的 ARN。请务必在 S3 存储桶 ARN 的资源路径中包含负载均衡器账户的账户 ID。这样可以确保只有来自指定账户的负载均衡器才能将访问日志写入 S3 存储桶。

您指定的 S3 存储桶 ARN 取决于您在步骤 3 中启用访问日志时是否计划包含前缀。

带前缀的 S3 存储桶 ARN 示例

S3 存储桶名称是 amzn-s3-demo-logging-bucket 前缀是 logging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

不带前缀的 S3 存储桶 ARN 示例

S3 存储桶名称是 amzn-s3-demo-logging-bucket。 S3 存储桶 ARN 中没有前缀部分。

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

2022 年 8 月之前可用的区域

此策略向指定的 Elastic Load Balancing 账户授予权限。对下面列出的区域中的负载均衡器使用此政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
    }
  ]
}
```

对于Principal，请*elb-account-id*替换为负载均衡器所在区域的 Elastic Load Balancing 账户的 ID：

- 美国东部（弗吉尼亚州北部）– 127311923021
- 美国东部（俄亥俄州）– 033677994240
- 美国西部（北加利福尼亚）– 027434742980
- 美国西部（俄勒冈州）– 797873946194
- 非洲（开普敦）– 098369216593
- 亚太地区（香港）– 754344448648
- 亚太地区（雅加达）– 589379963580
- 亚太地区（孟买）– 718504428378
- 亚太地区（大阪）– 383597477331
- 亚太地区（首尔）– 600734575887
- 亚太地区（新加坡）– 114774131450
- 亚太地区（悉尼）– 783225319266
- 亚太地区（东京）– 582318560864
- 加拿大（中部）– 985666609251
- 欧洲（法兰克福）– 054676820928
- 欧洲（爱尔兰）– 156460612806
- 欧洲（伦敦）– 652711504416
- 欧洲（米兰）– 635631232127
- 欧洲（巴黎）– 009996457667
- 欧洲（斯德哥尔摩）– 897822967062
- 中东（巴林）– 076674570225
- 南美洲（圣保罗）– 507241528517

对于Resource，使用示例策略中显示的格式，输入访问日志所在位置的 ARN。请务必在 S3 存储桶 ARN 的资源路径中包含负载均衡器账户的账户 ID。这样可以确保只有来自指定账户的负载均衡器才能将访问日志写入 S3 存储桶。

您指定的 S3 存储桶 ARN 取决于您在步骤 3 中启用访问日志时是否计划包含前缀。

带前缀的 S3 存储桶 ARN 示例

S3 存储桶名称是 amzn-s3-demo-logging-bucket 前缀是 logging-prefix.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

不带前缀的 S3 存储桶 ARN 示例

S3 存储桶的名称是amzn-s3-demo-logging-bucket。

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regions

该策略向指定的 Elastic Load Balancing 账户 ID 授予权限。对 AWS GovCloud (US) 区域中的负载均衡器使用此策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

对于Principal，请*elb-account-id*替换为负载均衡器所在区域的 Elastic Load Balancing 账户的 ID：

- AWS GovCloud （美国西部）— 048591011584

- AWS GovCloud （美国东部）— 190560391635

对于Resource，输入访问日志所在位置的 ARN。请务必在 S3 存储桶 ARN 的资源路径中包含负载均衡器账户的账户 ID。这样可以确保只有来自指定账户的负载均衡器才能将访问日志写入 S3 存储桶。

您指定的 S3 存储桶 ARN 取决于您在步骤 3 中启用访问日志时是否计划包含前缀。

带前缀的 S3 存储桶 ARN 示例

S3 存储桶名称是 amzn-s3-demo-logging-bucket 前缀是 logging-prefix.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

不带前缀的 S3 存储桶 ARN 示例

S3 存储桶的名称是amzn-s3-demo-logging-bucket。S3 存储桶 ARN 中没有前缀部分。

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

使用 Amazon S3 控制台将访问日志的存储桶策略附加到您的存储桶

1. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 选择存储桶的名称以打开其详细信息页面。
3. 选择 Permissions（权限），然后选择 Bucket policy（存储桶策略)、Edit（编辑）。
4. 更新存储桶策略以授予所需权限。
5. 选择保存更改。

步骤 3：配置访问日志

使用以下过程配置访问日志，以捕获请求信息并将日志文件传输到 S3 存储桶。

要求

存储桶必须满足第 1 步中所描述的要求，并且必须附加第 2 步中所描述的存储桶策略。如果指定前缀，则前缀不得包含字符串 “AWSLogs”。

使用控制台为负载均衡器配置访问日志

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择您的负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的监控部分中，执行以下操作：

   a. 启用访问日志。
   b. 对于 S3 URI，输入日志文件的 S3 URI。您指定的 URI 取决于您是否使用前缀。

      - 带有前缀的 URI：`s3://amzn-s3-demo-logging-bucket/logging-prefix`
      - 不带前缀的 URI：`s3://amzn-s3-demo-logging-bucket`

   c. 将日志记录间隔时间保留为 `60 minutes - default`。
   d. 选择保存更改。

要为负载均衡器配置访问日志，请使用 AWS CLI

首先，创建一个 .json 文件，该文件使 Elastic Load Balancing 能够捕获日志并每 60 分钟将这些日志传输到您为日志创建的 S3 存储桶一次：

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

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

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

以下为响应示例。

```
{
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
```

```
            "EmitInterval": 60,
            "S3BucketName": "amzn-s3-demo-logging-bucket",
            "S3BucketPrefix": "my-app"
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

管理保存访问日志的 S3 存储桶

要删除您配置用于访问日志的存储桶，请确保首先禁用访问日志。否则，如果有一个名称相同的新存储桶，并且在您不拥有的存储桶中创建了所需的存储桶策略 AWS 账户 ，Elastic Load Balancing 可能会将您的负载均衡器的访问日志写入这个新存储桶。

步骤 4：确认存储桶权限

在为负载均衡器启用访问日志后，Elastic Load Balancing 将验证 S3 存储桶，并创建测试文件以确保存储桶策略指定所需权限。您可以使用 S3 控制台验证是否已创建测试文件。测试文件不是实际的访问日志文件；它不包含示例记录。

验证 Elastic Load Balancing 是否在 S3 存储桶中创建了测试文件

1. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 选择您指定用于访问日志的 S3 存储桶的名称。
3. 导航到测试文件 `ELBAccessLogTestFile`。位置取决于您是否使用前缀。

   - 带有前缀的位置：*amzn-s3-demo-loadbalancer-logslogging-prefix*/AWSLogs/*123456789012*/ELBAccessLogTestFile
   - 不带前缀的位置：*amzn-s3-demo-loadbalancer-logs*/AWSLogs/*123456789012*/ELBAccessLogTestFile

故障排除

存储桶的访问被拒绝：***bucket-name***。请检查 S3bucket 权限

如果您收到此错误，则以下是可能的原因：

- 存储桶策略没有为 Elastic Load Balancing 授予将访问日志写入存储桶的权限。确认您使用的是该区域正确的存储桶策略。确认资源 ARN 使用的存储桶名称与您在启用访问日志时指定的存储桶名称相同。如果您在启用访问日志时未指定前缀，请确认资源 ARN 不包含前缀。

- 存储桶使用不支持的服务器端加密选项。该存储段必须使用 Amazon S3 托管密钥（SSE-S3）。

为经典负载均衡器禁用访问日志

您随时可为您的负载均衡器禁用访问日志。在禁用访问日志后，您的访问日志将在 Amazon S3 中保留，直至您将其删除。有关更多信息，请参阅 Amazon S3 用户指南中的使用 S3 存储桶。

使用控制台为负载均衡器禁用访问日志

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择您的负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面的监控部分中，禁用访问日志。

要禁用访问日志，请使用 AWS CLI

使用以下modify-load-balancer-attributes命令禁用访问日志：

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

以下为响应示例：

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

对经典负载均衡器进行故障排除

下表列出了在您使用经典负载均衡器时可为您提供帮助的故障排除资源。

API 错误

错误
CertificateNotFound: 未定义
OutofService: 发生了暂时性错误

HTTP 错误

错误
HTTP 400：BAD_REQUEST
HTTP 405：METHOD_NOT_ALLOWED
HTTP 408：请求超时
HTTP 502：无效网关
HTTP 503：服务不可用
HTTP 504：网关超时

响应代码指标

响应代码指标
HTTPCode_ELB_4XX
HTTPCode_ELB_5XX
HTTPCode_backend_2xx
HTTPCode_backend_3xx

响应代码指标
HTTPCode_backend_4xx
HTTPCode_backend_5xx

运行状况检查问题

问题
运行状况检查目标页面错误
与实例的连接超时
公钥身份验证失败
实例未从负载均衡器接收流量
实例上的端口未打开
Auto Scaling 组中的实例未通过 ELB 运行状况检查

连接问题

事务
客户端无法连接到面向 Internet 的负载均衡器
负载均衡器无法接收发送到自定义域的请求
发送到负载均衡器的 HTTPS 请求返回“NET:: ERR_CERT_COMMON_NAME_INVALID”

实例注册问题

问题
注册 EC2 实例花费的时间太长
无法注册从已付 AMI 启动的实例

对经典负载均衡器进行故障排除：API 错误

下面是 Elastic Load Balancing API 返回的错误消息、潜在原因以及可以用于解决问题的步骤。

错误消息

- CertificateNotFound: 未定义
- OutofService: 发生了暂时性错误

CertificateNotFound: 未定义

原因 1：在将使用 AWS Management Console创建的证书传播到所有区域时出现延迟。在出现此延迟时，创建负载均衡器过程的最后一步中将显示错误消息。

解决方案 1：等待大约 15 分钟，然后重试一次。如果问题仍然存在，请转到 AWS 支持 Center 寻求帮助。

原因 2：如果您直接使用 AWS CLI 或 API，则如果您为不存在的证书提供了 Amazon 资源名称 (ARN)，则可能会收到此错误。

解决方案 2：使用 AWS Identity and Access Management (IAM) 操作GetServerCertificate获取证书 ARN 并验证您为 ARN 提供的值是否正确。

OutofService: 发生了暂时性错误

原因：Elastic Load Balancing 服务或基础网络中出现暂时性内部问题。在 Elastic Load Balancing 查询负载均衡器及其注册实例的运行状况时，也可能发生这种临时问题。

解决方案：重新尝试 API 请求。如果问题仍然存在，请转到 AWS 支持 Center 寻求帮助。

对经典负载均衡器进行故障排除：HTTP 错误

HTTP 方法 (也称为动词) 指定要对接收 HTTP 请求的资源执行的操作。RFC 2616 方法定义中定义了 HTTP 请求的标准方法。标准方法包括 GET、POST、PUT、HEAD 和 OPTIONS。某些 Web 应用程序需要 (有时会引入) 作为 HTTP/1.1 方法的扩展的方法。HTTP 扩展方法的常见示例包括 PATCH、REPORT、MKCOL、PROPFIND、MOVE 和 LOCK。Elastic Load Balancing 接受所有标准和非标准 HTTP 方法。

HTTP 请求和 HTTP 响应使用标头字段发送有关 HTTP 消息的信息。标头字段为冒号分隔的名称值对，各个值对之间由回车符 (CR) 和换行符 (LF) 进行分隔。RFC 2616 信息标头中定义了标准 HTTP 标头字段集。有关更多信息，请参阅 HTTP 标头和经典负载均衡器。

当负载均衡器接收 HTTP 请求时，它会对格式不正确的请求或方法长度进行检查。向负载均衡器发出的 HTTP 请求中的方法总长度不得超过 127 个字符。如果 HTTP 请求通过两项检查，则负载均衡器会将请求发送到 EC2 实例。如果该请求中的方法字段格式不正确，则负载均衡器会以 HTTP 400：BAD_REQUEST 错误做出响应。如果请求中方法的长度超过 127 个字符，则负载均衡器会以 HTTP 405：METHOD_NOT_ALLOWED 错误做出响应。

该 EC2 实例通过在请求中实现方法并将响应发送回客户端来处理有效请求。实例必须进行配置才能处理支持和不支持的方法。

下面是负载均衡器返回的错误消息、潜在原因以及可以用于解决问题的步骤。

错误消息

- HTTP 400：BAD_REQUEST
- HTTP 405：METHOD_NOT_ALLOWED
- HTTP 408：请求超时
- HTTP 502：无效网关
- HTTP 503：服务不可用
- HTTP 504：网关超时

HTTP 400：BAD_REQUEST

描述：表明客户端发送了错误请求。

原因 1：客户端发送的请求格式错误，不符合 HTTP 规范。例如，请求的 URL 中不能包含空格。

原因 2：客户端使用了 Elastic Load Balancing 不支持的 HTTP CONNECT 方法。

解决方案：直接连接到您的实例并获取客户端请求的详细信息。检查标头和 URL 以了解请求格式是否有误。验证请求是否符合 HTTP 规范。确认未使用 HTTP CONNECT。

HTTP 405：METHOD_NOT_ALLOWED

描述：表示方法长度无效。

原因：请求标头中方法的长度超过了 127 个字符。

解决方案：检查方法的长度。

HTTP 408：请求超时

描述：表明客户端取消了请求或未能发送完整请求。

原因 1：网络连接中断或错误请求结构，例如，部分成形的标头、指定内容大小与实际传播内容大小不匹配等。

解决方案 1：检查提出请求的代码，并尝试将其直接发送至您对检测实际请求拥有更多控制权限的已注册实例 (或开发/测试环境)。

原因 2：与客户端的连接关闭 (负载均衡器无法发送响应)

解决方案 2：通过在发出请求的计算机上使用数据包嗅探器，在发送响应之前验证客户端是否未关闭连接。

HTTP 502：无效网关

描述：表明负载均衡器未能解析来自已注册实例的请求。

原因：实例返回格式错误的响应，或负载均衡器可能出现问题。

解决方案：验证从实例中发出的响应是否符合 HTTP 规范。转到 AWS 支持 Center 寻求帮助。

HTTP 503：服务不可用

描述：表明负载均衡器或已注册实例导致了错误。

原因 1：负载均衡器处理请求的容量不足。

解决方案 1：这应是一种暂时性问题，持续时间不会超过几分钟。如果问题仍然存在，请转到 AWS 支持 Center 寻求帮助。

原因 2：无已注册实例。

解决方案 2：在您的负载均衡器被配置响应的每个可用区内注册至少一个实例。通过查看中的`HealthyHostCount`指标来验证这一点 CloudWatch。如果无法确保在每个可用区中都注册了实例，我们建议启用跨区域负载均衡。有关更多信息，请参阅 配置经典负载均衡器的跨区域负载均衡。

原因 3：无运行正常的实例。

解决方案 3：确保您的负载均衡器被配置响应的每个可用区内均有运行正常的实例。查看 `HealthyHostCount` 指标来核实此项。

原因 4：波动队列已满。

解决方案 4：确保您的实例具有足够的容量来处理请求速率。查看 `SpilloverCount` 指标来核实此项。

HTTP 504：网关超时

描述：表明负载均衡器已关闭连接，因为请求未在空闲超时期限内完成。

原因 1：应用程序的响应时间超出了配置的空闲超时。

解决方案 1：监控 `HTTPCode_ELB_5XX` 和 `Latency` 指标。如果这些指标有所上升，可能是因为应用程序未在空闲超时期限内做出响应。有关超时的请求的详细信息，请在负载均衡器上启用访问日志并在 Elastic Load Balancing 所生成的日志中查看 504 响应代码。如有必要，您可以扩大容量或增加配置的空闲超时，以便完成时间较长的操作 (例如，上传大型文件)。有关更多信息，请参阅 配置经典负载均衡器的空闲连接超时 和 如何对 Elastic Load Balancing 高延迟进行故障排除。

原因 2：已注册实例关闭了到 Elastic Load Balancing 的连接。

解决方案 2：在您的 EC2实例上启用保持活动状态设置，并确保保持活动超时时间大于负载均衡器的空闲超时设置。

对经典负载均衡器进行故障排除：响应代码指标

您的负载均衡器将发送给客户端 CloudWatch 的 HTTP 响应代码的指标发送给 Amazon，将错误源标识为负载均衡器或注册实例。您可以使用为负载均衡器返回 CloudWatch 的指标来解决问题。有关更多信息，请参阅 CloudWatch 您的 Classic Load Balancer 的指标。

以下是您的负载均衡器返回 CloudWatch 的响应代码指标、潜在原因以及您可以采取的解决问题的步骤。

响应代码指标

- HTTPCode_ELB_4XX
- HTTPCode_ELB_5XX

- HTTPCode_backend_2xx
- HTTPCode_backend_3xx
- HTTPCode_backend_4xx
- HTTPCode_backend_5xx

HTTPCode_ELB_4XX

原因：来自客户端的格式错误的或已取消的请求。

解决方案

- 请参阅 HTTP 400：BAD_REQUEST。
- 请参阅 HTTP 405：METHOD_NOT_ALLOWED。
- 请参阅 HTTP 408：请求超时。

HTTPCode_ELB_5XX

原因：负载均衡器或已注册实例导致了错误或负载均衡器无法解析响应。

解决方案

- 请参阅 HTTP 502：无效网关。
- 请参阅 HTTP 503：服务不可用。
- 请参阅 HTTP 504：网关超时。

HTTPCode_backend_2xx

原因：来自已注册实例的正常成功响应。

解决方案：无。

HTTPCode_backend_3xx

原因：由已注册实例发送的重定向响应。

解决方案：查看您的实例中的访问日志或错误日志以确定原因。将请求直接发送到实例 (绕过负载均衡器) 以查看响应。

HTTPCode_backend_4xx

原因：从已注册实例发送的客户端错误响应。

解决方案：查看您的实例中的访问或错误日志以确定原因。将请求直接发送到实例 (绕过负载均衡器) 以查看响应。

> **Note**
>
> 如果客户端取消了以 `Transfer-Encoding: chunked` 标头开头的 HTTP 请求，则会出现一个已知问题，即负载均衡器会将此请求转发到实例，即使客户端取消了此请求也是如此。这可能会导致后端错误。

HTTPCode_backend_5xx

原因：从已注册实例发送的服务器错误响应。

解决方案：查看您的实例中的访问日志或错误日志以确定原因。将请求直接发送到实例 (绕过负载均衡器) 以查看响应。

> **Note**
>
> 如果客户端取消了以 `Transfer-Encoding: chunked` 标头开头的 HTTP 请求，则会出现一个已知问题，即负载均衡器会将此请求转发到实例，即使客户端取消了此请求也是如此。这可能会导致后端错误。

对经典负载均衡器进行故障排除：运行状况检查

负载均衡器使用 Elastic Load Balancing 提供的默认运行状况检查配置，或使用您指定的自定义运行状况检查配置来检查已注册实例的运行状况。运行状况检查配置包含协议、ping 端口、ping 路径、响应超时和运行状况检查间隔等信息。如果在运行状况检查间隔内返回 200 响应代码，则会将该实例视为运行状况良好。有关更多信息，请参阅 对经典负载均衡器中的实例执行运行状况检查。

如果您的部分或所有实例的当前状态为 `OutOfService`，并且描述字段显示消息 `Instance has failed at least the Unhealthy Threshold number of health checks consecutively`，则表示实例未通过负载均衡器运行状况检查。下面是要查找的问题、潜在原因以及可以用于解决问题的步骤。

问题

运行状况检查目标页面错误

问题：在指定的 ping 端口和 ping 路径 (例如 HTTP:80/index.html) 上向实例发出的 HTTP GET 请求收到非 200 的响应代码。

原因 1：未在该实例上配置目标页面。

解决方案 1：在每个注册的实例上创建目标页面 (例如 `index.html`)，并指定其路径作为 ping 路径。

原因 2：响应中的 Content-Length 标头值未设置。

解决方案 2：如果响应包含正文，请将 Content-Length 标头设置为大于等于零的值，或将 Transfer-Encoding 值设置为“chunked”。

原因 3：应用程序未配置为从负载均衡器接收请求或返回 200 响应代码。

解决方案 3：检查实例上的应用程序以调查原因。

与实例的连接超时

问题：从您的负载均衡器向您的 EC2 实例发出的运行状况检查请求已超时或间歇性失败。

首先，通过直接连接到实例验证问题。我们建议使用实例的私有 IP 地址从网络内连接到实例。

对 TCP 连接使用以下命令：

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

对 HTTP 或 HTTPS 连接使用以下命令：

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

如果使用 HTTP/HTTPS 连接并收到非 200 的响应，请参阅运行状况检查目标页面错误。如果能够直接连接到实例，请检查以下各项：

原因 1：实例未能在配置的响应超时期内响应。

解决方案 1：调整负载均衡器运行状况检查配置中的响应超时设置。

原因 2：实例承担大量负载，从而导致响应时间超出配置的响应超时期。

解决方案 2：

- 检查监控图表了解 CPU 是否使用过度。有关信息，请参阅 Amazon EC2 用户指南中的获取特定 EC2 实例的统计数据。
- 通过连接到您的 EC2 实例，检查其他应用程序资源的利用率，例如内存或限制。
- 如果需要，请添加更多实例或启用 Auto Scaling。有关更多信息，请参阅 Amazon A EC2 uto Scaling 用户指南。

原因 3：如果您使用的是 HTTP 或 HTTPS 连接，并且对 ping 路径字段中指定的目标页面 (例如 `HTTP:80/index.html`) 执行运行状况检查，则目标页面的响应时间可能会超过配置的超时时间。

解决方案 3：使用更简单的运行状况检查目标页面或调整运行状况检查间隔设置。

公钥身份验证失败

问题：配置为使用 HTTPS 或 SSL 协议并且启用了后端身份验证的负载均衡器进行公钥身份验证时失败。

原因：SSL 证书上的公钥与负载均衡器上配置的公钥不匹配。请使用 `s_client` 命令查看证书链中的服务器证书的列表。有关更多信息，请参阅 OpenSSL 文档中的 s_client。

解决方案：您可能需要更新 SSL 证书。如果您的 SSL 证书是最新版本，请尝试在负载均衡器上重新安装它。有关更多信息，请参阅 替换经典负载均衡器的 SSL 证书。

实例未从负载均衡器接收流量

问题：实例的安全组阻止来自负载均衡器的流量。

对实例执行数据包捕获以验证问题。使用以下 命令：

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

原因 1：与实例关联的安全组不允许来自负载均衡器的流量。

解决方案 1：编辑实例安全组以允许来自负载均衡器的流量。添加规则以允许来自负载均衡器安全组的所有流量。

原因 2：您的负载均衡器的安全组不允许流量进入 EC2 实例。

解决方案 2：编辑负载均衡器的安全组以允许流量进入子网和 EC2 实例。

有关管理安全组的信息，请参阅 为经典负载均衡器配置安全组。

实例上的端口未打开

问题：负载均衡器发送到 EC2 实例的运行状况检查被端口或防火墙阻止。

请使用以下命令验证问题：

```
netstat –ant
```

原因：指定的运行状况端口或侦听器端口 (如果配置方式不同) 未打开。为运行状况检查指定的端口和侦听器端口必须都打开并正在进行侦听。

解决方案：在实例上打开侦听器端口和运行状况检查配置中指定的端口 (如果配置为不同端口) 以接收负载均衡器流量。

Auto Scaling 组中的实例未通过 ELB 运行状况检查

问题：Auto Scaling 组中的实例通过了默认Auto Scaling 运行状况检查，但未通过 ELB 运行状况检查。

原因：Auto Scaling 使用 EC2 状态检查来检测实例的硬件和软件问题，但负载均衡器通过向实例发送请求并等待 200 响应码或与实例建立 TCP 连接（用于基于 TCP 的运行状况检查）来执行运行状况检查。

实例未能通过 ELB 运行状况检查，可能是因为实例中运行的应用程序发生问题，导致负载均衡器将实例视为停止服务。此实例可能通过 Auto Scaling 运行状况检查；它不会被 Auto Scaling 策略所取代，因为根据 EC2 状态检查，它被视为运行状况良好。

解决方案：对 Auto Scaling 组使用 ELB 运行状况检查。使用 ELB 运行状况检查时，Auto Scaling 通过检查实例状态检查和 ELB 运行状况检查的结果来确定实例的运行状况。有关更多信息，请参阅

Amazon Auto Scaling 用户指南中的将 Elastic Load Balancing 运行状况检查添加到您的 A EC2 uto Scaling 群组。

对经典负载均衡器进行故障排除：客户端连接

客户端无法连接到面向 Internet 的负载均衡器

如果负载均衡器未响应请求，请检查以下问题：

您的面向 Internet 的负载均衡器已连接到私有子网

您必须为负载均衡器指定公有子网。公有子网有一个指向 Virtual Private Cloud (VPC) 的互联网网关的路由。

安全组或网络 ACL 不允许流量

负载均衡器的安全组和负载均衡器子网的任何网络 ACLs 都必须允许来自客户端的入站流量以及通过侦听器端口流向客户端的出站流量。有关更多信息，请参阅 为经典负载均衡器配置安全组。

负载均衡器无法接收发送到自定义域的请求

如果负载均衡器无法接收发送到自定义域的请求，请检查以下问题：

自定义域名无法解析为负载均衡器 IP 地址

- 使用命令行界面确认自定义域名解析为哪个 IP 地址。
  - Linux、macOS 或 Unix – 您可以在终端中使用 `dig` 命令。Ex.`dig example.com`
  - Windows – 您可以在命令提示符中使用 `nslookup` 命令。Ex.`nslookup example.com`
- 使用命令行界面确认负载均衡器 DNS 解析为哪个 IP 地址。
- 比较两个输出的结果。这两个 IP 地址应相匹配。

发送到负载均衡器的 HTTPS 请求返回“NET::ERR_CERT_COMMON_NAME_INVALID”

如果 HTTPS 请求收到来自负载均衡器的 `NET::ERR_CERT_COMMON_NAME_INVALID`，请查看以下可能的原因：

- HTTPS 请求中使用的域名与 ACM 证书所关联的侦听器中指定的备用名称不匹配。

- 正在使用负载均衡器的默认 DNS 名称。无法使用默认 DNS 名称发出 HTTPS 请求，因为无法为 `*.amazonaws.com` 域请求公有证书。

对经典负载均衡器进行故障排除：实例注册

当您使用负载均衡器注册一个实例时，在负载均衡器可以开始向您的实例发送请求之前，您仍需要完成多项步骤。

以下是您的负载均衡器在注册 EC2 实例时可能遇到的问题、潜在原因以及您可以采取的解决这些问题的步骤。

事务

- 注册 EC2 实例花费的时间太长
- 无法注册从已付 AMI 启动的实例

注册 EC2 实例花费的时间太长

问题：注册 EC2 实例处于该`InService`状态所需的时间比预期的要长。

原因：实例可能未通过运行状况检查。在完成最初的实例注册步骤之后 (可能需要约 30 秒)，负载均衡器开始发送运行状况检查请求。在成功通过一次运行状况检查之前，实例不会处于 `InService` 状态。

解决方案：请参阅 与实例的连接超时。

无法注册从已付 AMI 启动的实例

问题：Elastic Load Balancing 未注册使用付费 AMI 启动的实例。

原因：您的实例可能是使用亚马逊的付费 AMI 启动的 DevPay。

解决方案：Elastic Load Balancing 不支持注册使用亚马逊付费启动 AMIs 的实例 DevPay。请注意，您可以使用来 AMIs 自 AWS Marketplace 的付款。如果您已经在使用来自的付费 AMI AWS Marketplace ，但无法注册从该付费 AMI 启动的实例，请前往AWS 支持 中心寻求帮助。

经典负载均衡器的配额

您的 AWS 账户对每项 AWS 服务都有默认配额（以前称为限制）。除非另有说明，否则，每个配额是区域特定的。

要查看经典负载均衡器的配额，请打开服务配额控制台。在导航窗格中，选择 AWS services，然后选择 Elastic Load Balancing。您也可以使用 describe-account-limits(AWS CLI) 命令进行 Elastic Load Balancing。

要请求提高配额，请参阅《服务配额用户指南》中的请求提高配额。

您的 AWS 账户具有以下与经典负载均衡器相关的配额。

名称	默认值	可调整
每个区域的 Application Load Balancer 数	20	是
每个经典负载均衡器的侦听器数	100	是
每个经典负载均衡器的已注册实例数	1000	是

经典负载均衡器的文档历史记录

下表介绍了经典负载均衡器的版本。

变更	说明	日期
异步缓解模式	增加了对异步缓解模式的支持。有关更多信息，请参阅为经典负载均衡器配置异步缓解模式。	2020 年 8 月 17 日
经典负载均衡器	随着 Application Load Balancer 和 Network Load Balancer 的推出，使用 2016-06-01 API 创建的负载均衡器现在被称为 Classic Load Balancers。有关这些负载均衡器类型之间差异的更多信息，请参阅 Elastic Load Balancing 特征。	2016 年 8 月 11 日
Support fo AWS Certificate Manager r (ACM)	您可以从 ACM 请求一个 SSL/TLS 证书，然后将它部署到您的负载均衡器上。有关更多信息，请参阅为经典负载均衡器创建 SSL/TLS 证书。	2016 年 1 月 21 日
对其他端口的支持	负载均衡器可以侦听 1-65535 范围中的任何端口。有关更多信息，请参阅经典负载均衡器的侦听器。	2015 年 9 月 15 日
用于访问日志条目的其他字段	添加了 `user_agent` 、`ssl_cipher` 和 `ssl_protocol` 字段。有关更多信息，请参阅访问日志文件。	2015 年 5 月 18 日

支持为负载均衡器添加标签	从本版本开始，Elastic Load Balancing CLI (ELB CLI) 已被 AWS Command Line Interface (AWS CLI) 所取代，后者是一个用于管理多项 AWS 服务的统一工具。ELB CLI 版本 1.0.35.0（发布日期为 2014 年 7 月 24 日）之后发布的新功能仅在 AWS CLI 中提供。如果您当前正在使用 ELB CLI，我们建议您改为使用 AWS CLI。有关更多信息，请参阅 用户指南。AWS Command Line Interface	2014 年 8 月 11 日
空闲连接超时	您可以为负载均衡器配置空闲连接超时。	2014 年 7 月 24 日
支持授权用户和组访问特定负载均衡器或 API 操作	您可以创建策略来授权用户和组访问特定负载均衡器或 API 操作。	2014 年 5 月 12 日
Support AWS CloudTrail	您可以使用 CloudTrail ELB API、、ELB CLI 或， AWS 账户 来捕获由您或代表您发出的 API 调用。 AWS Management Console AWS CLI	2014 年 4 月 4 日
连接耗尽	添加有关连接耗尽的信息。借助此支持，您可以使负载均衡器在实例正在取消注册时或者实例运行状况不佳时停止向已注册实例发送新请求，同时保持现有连接处于打开状态。有关更多信息，请参阅为经典负载均衡器配置连接耗尽。	2014 年 3 月 20 日

访问日志	您可以启用负载均衡器以捕获有关发送到负载均衡器的请求的详细信息，并将此详细信息存储在 Amazon S3 存储桶中。有关更多信息，请参阅经典负载均衡器的访问日志。	2014 年 3 月 6 日
对 TLSv1 .1-1.2 的 Support	添加了有关配置有 HTTPS/SSL 侦听器的负载均衡器的 TLSv1 .1-1.2 协议支持的信息。借助该支持，Elastic Load Balancing 还更新了预定义 SSL 协商配置。有关更新的预定义 SSL 协商配置的信息，请参阅经典负载均衡器的 SSL 协商配置。有关更新当前 SSL 协商配置的信息，请参阅更新经典负载均衡器的 SSL 协商配置。	2014 年 2 月 19 日
跨可用区负载均衡	增加了有关如何为您的负载均衡器启用跨区域负载均衡的信息。有关更多信息，请参阅为经典负载均衡器配置跨区域负载均衡。	2013 年 11 月 6 日
其他 CloudWatch 指标	添加了有关由 Elastic Load Balancing 报告的其他 Cloudwatch 指标的信息。有关更多信息，请参阅 C lassic Load Balancer 的CloudWatch 指标。	2013 年 10 月 28 日
代理协议支持	添加了有关为 TCP/SSL 连接配置的负载均衡器的代理协议支持的信息。有关更多信息，请参阅代理协议标头。	2013 年 7 月 30 日

支持 DNS 故障转移	添加了有关为负载均衡器配置 Amazon Route 53 DNS 故障转移的信息。有关更多信息，请参阅对负载均衡器使用 Amazon Route 53 DNS 故障转移。	2013 年 6 月 3 日
控制台支持查看 CloudWatch 指标和创建警报	添加了有关使用控制台查看 CloudWatch 指标和为指定负载均衡器创建警报的信息。有关更多信息，请参阅 C lassic Load Balancer 的CloudWatch 指标。	2013 年 3 月 28 日
支持在默认 VPC 中注册 EC2 实例	增加了对在默认 VPC 中启动的 EC2 实例的支持。	2013 年 3 月 11 日
内部负载均衡器	借助此版本，Virtual Private Cloud (VPC) 中的负载均衡器可同时在内部或面向 Internet 使用。内部负载均衡器有可公开解析的 DNS 名称，解析到私有 IP 地址。面向 Internet 的负载均衡器有可公开解析的 DNS 名称，解析到公有 IP 地址。有关更多信息，请参阅创建内部经典负载均衡器。	2012 年 6 月 10 日
控制台支持管理侦听器、密码设置和 SSL 证书	有关信息，请参阅为经典负载均衡器配置 HTTPS 侦听器和替换经典负载均衡器的 SSL 证书。	2012 年 5 月 18 日
支持 Amazon VPC 中的 Elastic Load Balancing	添加了对在 Virtual Private Cloud (VPC) 中创建负载均衡器的支持。	2011 年 11 月 21 日

Amazon CloudWatch	您可以使用监控您的负载均衡器 CloudWatch。有关更多信息，请参阅 C lassic Load Balancer 的CloudWatch 指标。	2011 年 10 月 17 日
其他安全特征	您可以配置 SSL 密码、后端 SSL 和后端服务器身份验证。有关更多信息，请参阅创建带有 HTTPS 侦听器的经典负载均衡器。	2011 年 8 月 30 日
Zone Apex（机构根网域）域名	有关更多信息，请参阅为经典负载均衡器配置自定义域名。	2011 年 5 月 24 日
Support 对 X-Forwarded-Proto 和 X-Forwarded-Port标题的支持	标 X-Forwarded-Proto头表示原始请求的协议，标 X-Forwarded-Port头表示原始请求的端口。通过为请求添加这些标头，客户可以确定传入其负载均衡器的请求是否已加密，以及负载均衡器上收到请求的特定端口。有关更多信息，请参阅 HTTP 标头和经典负载均衡器。	2010 年 10 月 27 日
支持 HTTPS	借助此版本，您可以利用 SSL/TLS 协议加密流量，并卸载从应用程序实例到负载均衡器的 SSL 处理。此功能还提供负载均衡器的 SSL 服务器证书的集中管理，而不是管理各个应用程序实例上的证书。	2010 年 10 月 14 日
Support fo AWS Identity and Access Management r (IAM)	增加了对 IAM 的支持。	2010 年 9 月 2 日

粘性会话	有关更多信息，请参阅为经典负载均衡器配置粘性会话。	2010 年 4 月 7 日
适用于 Java 的 AWS SDK	支持对适用于 Java 的开发工具包的支持	2010 年 3 月 22 日
适用于 .NET 的 AWS SDK	增加了对... 的支持 适用于 .NET 的 SDK。	2009 年 11 月 11 日
新增服务	Elastic Load Balancing 最初的公共测试版。	2009 年 5 月 18 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。