# 管理负载平衡

## StorageGRID 11.7

NetApp
April 12, 2024

# 目录

管理负载平衡 . . . . . 1
负载平衡注意事项 . . . . . 1
配置负载平衡器端点 . . . . . 4

# 管理负载平衡

## 负载平衡注意事项

您可以使用负载平衡处理来自S3和Swift客户端的载入和检索工作负载。

### 什么是负载平衡?

当客户端应用程序从StorageGRID 系统保存或检索数据时、StorageGRID 使用负载平衡器管理载入和检索工作负载。负载平衡通过在多个存储节点之间分布工作负载、最大限度地提高速度和连接容量。

StorageGRID 负载平衡器服务安装在所有管理节点和所有网关节点上，并提供第 7 层负载平衡。它会终止客户端请求，检查请求并与存储节点建立新的安全连接。

将客户端流量转发到存储节点时，每个节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。

> 虽然建议使用 StorageGRID 负载平衡器服务来平衡负载，但您可能希望集成第三方负载平衡器。有关信息，请联系您的 NetApp 客户代表或参阅 "TR-4626： StorageGRID 第三方和全局负载平衡器"。

### 我需要多少个负载平衡节点?

作为一般最佳实践， StorageGRID 系统中的每个站点都应包含两个或更多具有负载平衡器服务的节点。例如，一个站点可能包含两个网关节点，或者同时包含一个管理节点和一个网关节点。无论您使用的是 SG100 或 SG1000 服务设备，裸机节点还是基于虚拟机（ VM ）的节点，确保每个负载平衡节点都有足够的网络，硬件或虚拟化基础架构。

### 什么是负载平衡器端点?

负载平衡器端点定义了传入和传出客户端应用程序请求用来访问包含负载平衡器服务的节点的端口和网络协议(HTTPS或HTTP)。端点还可以定义客户端类型(S3或Swift)、绑定模式以及允许或阻止的租户列表(可选)。

要创建负载平衡器端点，请选择*配置*>*网络*>*负载平衡器端点*或完成FabricPool 和S3设置向导。有关说明：

- "配置负载平衡器端点"
- "使用S3设置向导"
- "使用FabricPool 设置向导"

#### 端口注意事项

对于您创建的第一个端点、负载平衡器端点的端口默认为10433、但您可以指定介于1到65535之间的任何未使用的外部端口。如果使用端口80或443、则端点将仅在网关节点上使用负载平衡器服务。这些端口在管理节点上预留。如果对多个端点使用同一端口、则必须为每个端点指定不同的绑定模式。

不允许其他网格服务使用的端口。请参见 "网络端口参考"。

网络协议注意事项

在大多数情况下、客户端应用程序和StorageGRID 之间的连接应使用传输层安全(Transport Layer Security、TLS)加密。支持在不使用TLS加密的情况下连接到StorageGRID 、但不建议这样做、尤其是在生产环境中。为StorageGRID 负载平衡器端点选择网络协议时，应选择*HTTPS*。

负载平衡器端点证书的注意事项

如果选择*HTTPS*作为负载平衡器端点的网络协议，则必须提供安全证书。在创建负载平衡器端点时、您可以使用以下三个选项中的任何一个：

- 上传签名证书**(**建议**)**。此证书可以由公共信任的证书颁发机构(CA)或私有证书颁发机构(CA)签名。最佳做法是、使用公共信任的CA服务器证书来保护连接安全。与生成的证书不同、由CA签名的证书可以无干扰地轮换、这有助于避免过期问题。

  在创建负载平衡器端点之前、您必须获取以下文件：

  - 自定义服务器证书文件。
  - 自定义服务器证书专用密钥文件。
  - (可选)来自每个中间颁发证书颁发机构的证书的CA包。
- 生成自签名证书。
- 使用全局**StorageGRID S3**和**Swift**证书。您必须先上传或生成此证书的自定义版本、然后才能为负载平衡器端点选择此证书。请参见 "配置 S3 和 Swift API 证书"。

我需要什么值?

要创建证书、您必须知道S3或Swift客户端应用程序将用于访问端点的所有域名和IP地址。

证书的*Subject DN*(可分辨名称)条目必须包含客户端应用程序将用于StorageGRID 的完全限定域名。例如：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

根据需要、此证书可以使用通配符来表示运行负载平衡器服务的所有管理节点和网关节点的完全限定域名。例如：`*.storagegrid.example.com` 使用*通配符表示 `adm1.storagegrid.example.com` 和 `gn1.storagegrid.example.com`。

如果您计划使用S3虚拟托管模式请求，则证书还必须为每个包含一个*备用名称*条目 "S3端点域名" 您已配置、包括任何通配符名称。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> 如果域名使用通配符、请查看 "服务器证书的强化准则"。

您还必须为安全证书中的每个名称定义一个DNS条目。

如何管理即将到期的证书?

> 如果用于保护S3应用程序和StorageGRID 之间连接的证书到期、则该应用程序可能会暂时无法访问StorageGRID。

要避免证书到期问题、请遵循以下最佳实践：

- 请仔细监控任何警告证书到期日期即将到来的警报，例如S3和Swift API*警报的*负载平衡器端点证书到期*和*全局服务器证书到期。
- 请始终保持StorageGRID 和S3应用程序的证书版本同步。如果要替换或续订用于负载平衡器端点的证书、则必须替换或续订S3应用程序使用的等效证书。
- 使用公共签名的CA证书。如果使用由CA签名的证书、则可以无系统地替换即将到期的证书。
- 如果您已生成自签名StorageGRID 证书、并且该证书即将过期、则必须在现有证书过期之前手动替换StorageGRID 和S3应用程序中的证书。

绑定模式的注意事项

通过绑定模式、您可以控制可用于访问负载平衡器端点的IP地址。如果端点使用绑定模式、则客户端应用程序仅在使用允许的IP地址或其对应的完全限定域名(FQDN)时才能访问该端点。使用任何其他IP地址或FQDN的客户端应用程序无法访问此端点。

您可以指定以下任意绑定模式：

- 全局(默认)：客户端应用程序可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。除非需要限制端点的可访问性、否则请使用此设置。
- * HA组的虚拟IP *。客户端应用程序必须使用HA组的虚拟IP地址(或相应的FQDN)。
- 节点接口。客户端必须使用选定节点接口的IP地址(或相应FQDN)。
- 节点类型。根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)。

租户访问注意事项

租户访问是一项可选的安全功能、可用于控制哪些StorageGRID 租户帐户可以使用负载平衡器端点来访问其分段。您可以允许所有租户访问某个端点(默认)、也可以为每个端点指定允许或阻止的租户列表。

您可以使用此功能在租户及其端点之间提供更好的安全隔离。例如、您可以使用此功能来确保一个租户所拥有的绝密或高度机密材料始终不会被其他租户完全访问。

> 出于访问控制的目的、租户是根据客户端请求中使用的访问密钥来确定的、如果在请求中未提供访问密钥(例如匿名访问)、则使用存储分段所有者来确定租户。

租户访问示例

要了解此安全功能的工作原理、请考虑以下示例：

1. 您已创建两个负载平衡器端点、如下所示：
    - *公共*端点：使用端口10443并允许所有租户访问。

- *top密钥*端点：使用端口10444并仅允许访问*top密钥*租户。系统将阻止所有其他租户访问此端点。

2. 。 `top-secret.pdf` 位于*top密钥*租户拥有的存储分段中。

以访问 `top-secret.pdf`，“Top SECRELE*”租户中的用户可以向其发送问题描述 GET请求 `https://w.x.y.z:10444/top-secret.pdf`。由于允许此租户使用10444端点、因此用户可以访问此对象。但是、如果属于任何其他租户的用户向同一URL发出相同请求、他们将收到"立即拒绝访问"消息。即使凭据和签名有效、访问也会被拒绝。

### CPU 可用性

在向存储节点转发 S3 或 Swift 流量时，每个管理节点和网关节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。节点 CPU 负载信息每隔几分钟更新一次，但权重可能会更频繁地更新。即使节点报告利用率为 100% 或未能报告利用率，也会为所有存储节点分配最小基本权重值。

在某些情况下，有关 CPU 可用性的信息仅限于负载平衡器服务所在的站点。

# 配置负载平衡器端点

负载平衡器端点决定了 S3 和 Swift 客户端在连接到网关和管理节点上的 StorageGRID 负载平衡器时可以使用的端口和网络协议。

> 对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。
- 您已查看 "负载平衡注意事项"。
- 如果您先前已重新映射要用于负载平衡器端点的端口，则表示您已重新映射 "已删除端口重新映射"。
- 您已创建计划使用的任何高可用性（ HA ）组。建议使用 HA 组，但不要求使用 HA 组。请参见 "管理高可用性组"。
- 负载平衡器端点是否将由使用 "S3 Select 的 S3 租户"，不能使用任何裸机节点的 IP 地址或 FQDN 。用于 S3 Select 的负载平衡器端点仅允许使用 SG100 或 SG1000 设备以及基于 VMware 的软件节点。
- 您已配置计划使用的任何 VLAN 接口。请参见 "配置 VLAN 接口"。
- 如果要创建 HTTPS 端点（建议），则您具有服务器证书的信息。

  > 对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

  - 要上传证书，您需要服务器证书，证书专用密钥以及 CA 捆绑包（可选）。
  - 要生成证书，您需要 S3 或 Swift 客户端用于访问此端点的所有域名和 IP 地址。您还必须知道主题（可分辨名称）。
  - 如果要使用 StorageGRID S3 和 Swift API 证书（也可用于直接连接到存储节点），则已将默认证书替换为由外部证书颁发机构签名的自定义证书。请参见"配置 S3 和 Swift API 证书"。

## 创建负载平衡器端点

每个负载平衡器端点都指定一个端口，一个客户端类型（ S3 或 Swift ）和一个网络协议（ HTTP 或 HTTPS ）。

### 访问向导

步骤

1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。
2. 选择 * 创建 * 。

### 输入端点详细信息

步骤

1. 输入端点的详细信息。

| 字段 | **Description** |
| --- | --- |
| Name | 端点的描述性名称，将显示在负载平衡器端点页面的表中。 |
| Port | 要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入介于1到65535之间的任何未使用的外部端口。<br><br>如果输入 * 。 80* 或 * 。 443* ，则仅在网关节点上配置端点。这些端口在管理节点上预留。 |
| 客户端类型 | 要使用此端点的客户端应用程序类型，可以是 * S3 或 * Swift* 。 |
| 网络协议 | 客户端在连接到此端点时将使用的网络协议。<br><br>• 选择 * HTTPS * 可进行安全的 TLS 加密通信（建议）。您必须附加安全证书，然后才能保存此端点。<br>• 选择 * HTTP * 可实现不太安全的未加密通信。对于非生产网格，请仅使用 HTTP 。 |

2. 选择 * 继续 * 。

### 选择绑定模式

步骤

1. 为端点选择绑定模式、以控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

| 选项 | Description |
| --- | --- |
| 全局（默认） | 客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。<br><br>除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。 |
| HA 组的虚拟 IP | 客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。<br><br>具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。 |
| 节点接口 | 客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。 |
| 节点类型 | 根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。 |

> 如果多个端点使用同一端口，StorageGRID 将使用此优先级顺序来确定要使用的端点：**HA**组的虚拟**IP *>*Node interfaces**>*Node type*>*Global"。

2. 如果选择了 * HA 组的虚拟 IP * ，请选择一个或多个 HA 组。
3. 如果选择了 * 节点接口 * ，请为要与此端点关联的每个管理节点或网关节点选择一个或多个节点接口。
4. 如果选择了*Node type*，请选择管理节点(包括主管理节点和任何非主管理节点)或网关节点。

控制租户访问

步骤

1. 对于*租户访问*步骤，请选择以下选项之一：

| 字段 | Description |
| --- | --- |
| 允许所有租户(默认) | 所有租户帐户都可以使用此端点来访问其分段。<br><br>如果尚未创建任何租户帐户、则必须选择此选项。添加租户帐户后、您可以编辑负载平衡器端点以允许或阻止特定帐户。 |
| 允许选定租户 | 只有选定租户帐户才能使用此端点访问其分段。 |
| 阻止选定租户 | 选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。 |

2. 如果要创建*HTTP*端点，则不需要附加证书。选择 * 创建 * 以添加新的负载平衡器端点。然后，转到 完成后。否则，请选择 * 继续 * 以附加证书。

附加证书

步骤

1. 如果要创建 * HTTPS * 端点，请选择要附加到该端点的安全证书类型。

   此证书可保护 S3 和 Swift 客户端之间的连接以及管理节点或网关节点上的负载平衡器服务。

   - * 上传证书 * 。如果您要上传自定义证书，请选择此选项。
   - * 生成证书 * 。如果您具有生成自定义证书所需的值，请选择此选项。
   - * 使用 StorageGRID S3 和 Swift 证书 * 。如果要使用全局 S3 和 Swift API 证书，则选择此选项，此证书也可用于直接连接到存储节点。

     除非将默认的S3和Swift API证书(由网格CA签名)替换为由外部证书颁发机构签名的自定义证书、否则无法选择此选项。请参见"配置 S3 和 Swift API 证书"。

2. 如果您未使用StorageGRID S3和Swift证书、请上传或生成此证书。

上传证书

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

- * 服务器证书 * ： PEM 编码的自定义服务器证书文件。
- 证书专用密钥:自定义服务器证书专用密钥文件（`.key`）。

> EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

- * CA bundle* ：一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

- 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 创建 * 。+ 已创建负载平衡器端点。自定义证书用于 S3 和 Swift 客户端与端点之间的所有后续新连接。

生成证书

a. 选择 * 生成证书 * 。

b. 指定证书信息：

| 字段 | **Description** |
| --- | --- |
| 域名 | 要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。 |
| IP | 要包含在证书中的一个或多个IP地址。 |
| 主题(可选) | 证书所有者的X.509主题或可分辨名称(DN)。<br><br>如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。 |
| 有效天数 | 创建后证书过期的天数。 |

| 字段 | Description |
| --- | --- |
| 添加密钥用法扩展 | 如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。<br><br>这些扩展定义了证书中所含密钥的用途。<br><br>注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。 |

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 创建 * 。

   此时将创建负载平衡器端点。自定义证书用于 S3 和 Swift 客户端与此端点之间的所有后续新连接。

完成后

步骤

1. 如果使用DNS、请确保DNS包含一条记录、用于将StorageGRID 完全限定域名(FQDN)与客户端用于建立连接的每个IP地址相关联。

   在 DNS 记录中输入的 IP 地址取决于您是否使用的是由负载平衡节点组成的 HA 组：

   - 如果已配置HA组、则客户端将连接到该HA组的虚拟IP地址。
   - 如果不使用HA组、则客户端将使用网关节点或管理节点的IP地址连接到StorageGRID 负载平衡器服务。

     此外，还必须确保 DNS 记录引用所有必需的端点域名，包括任何通配符名称。

2. 为 S3 和 Swift 客户端提供连接到端点所需的信息：
   - 端口号
   - 完全限定域名或 IP 地址
   - 任何必需的证书详细信息

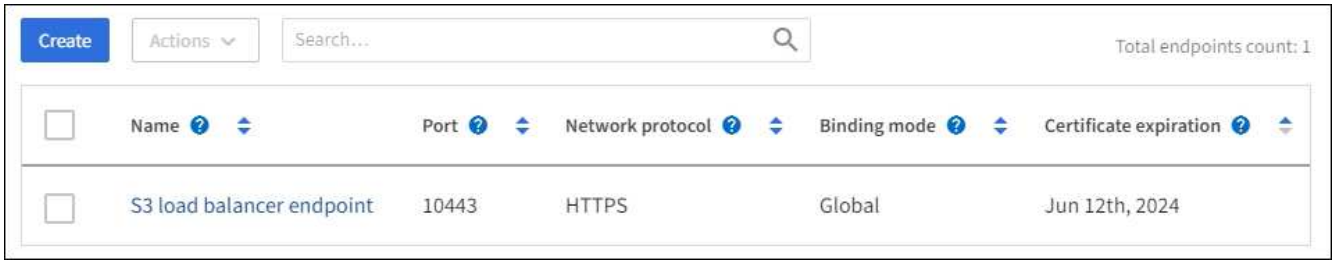
## 查看和编辑负载平衡器端点

您可以查看现有负载平衡器端点的详细信息，包括安全端点的证书元数据。您还可以更改端点的名称或绑定模式

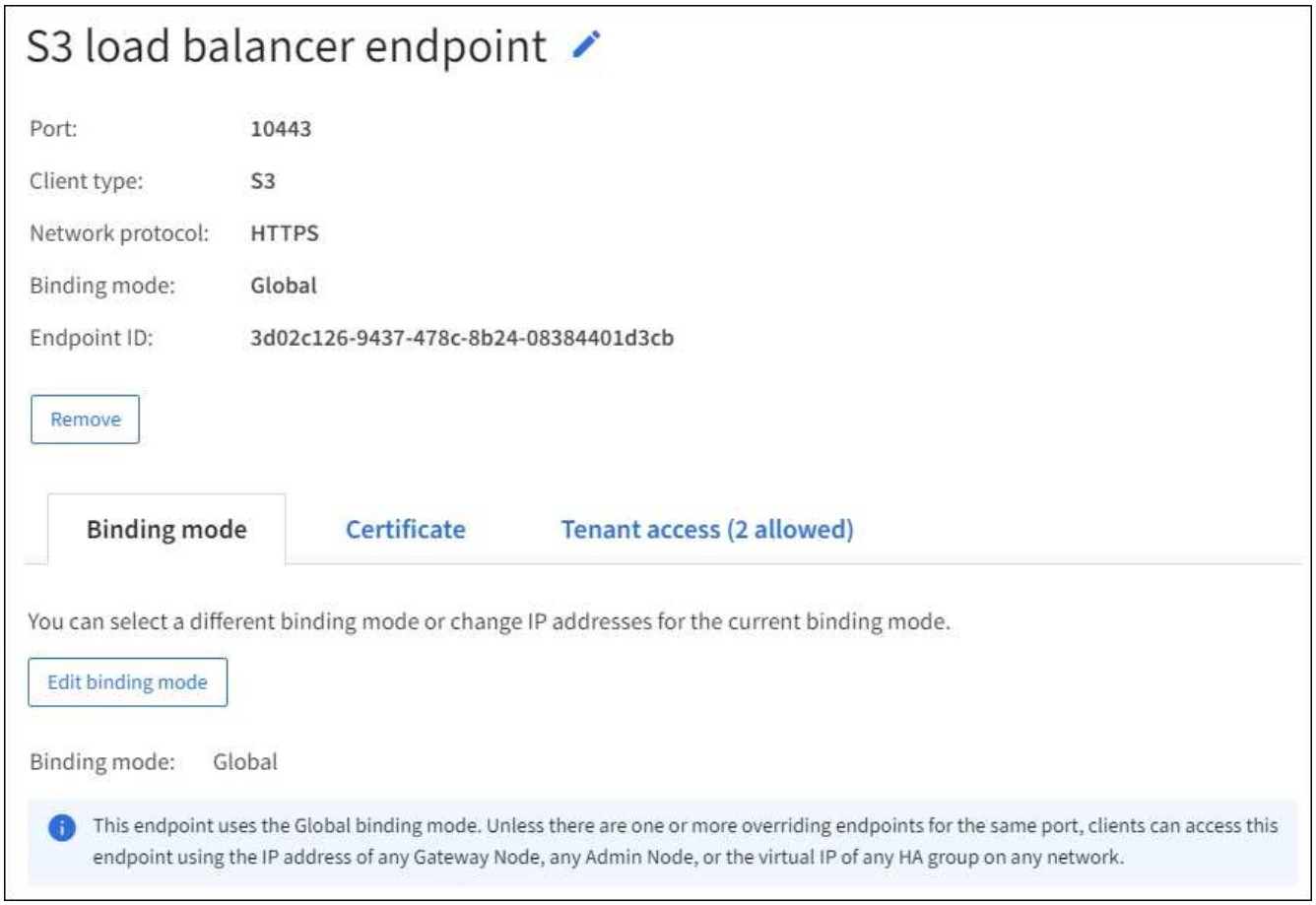
，并更新任何关联的证书。

您不能更改服务类型(S3或Swift)、端口或协议(HTTP或HTTPS)。

- 要查看所有负载平衡器端点的基本信息，请查看负载平衡器端点页面上的表。




- 要查看有关特定端点的所有详细信息，包括证书元数据，请在表中选择端点的名称。




- 要编辑端点，请使用负载平衡器端点页面上的 * 操作 * 菜单或特定端点的详细信息页面。

> 编辑端点后，您可能需要等待长达 15 分钟，才能将所做的更改应用于所有节点。

| 任务 | 操作菜单 | 详细信息页面 |
| --- | --- | --- |
| 编辑端点名称 | a. 选中此端点对应的复选框。<br>b. 选择 * 操作 * > * 编辑端点名称 * 。<br>c. 输入新名称。<br>d. 选择 * 保存 * 。 | a. 选择端点名称以显示详细信息。<br>b. 选择编辑图标 。<br>c. 输入新名称。<br>d. 选择 * 保存 * 。 |
| 编辑端点绑定模式 | a. 选中此端点对应的复选框。<br>b. 选择 * 操作 * > * 编辑端点绑定模式 * 。<br>c. 根据需要更新绑定模式。<br>d. 选择 * 保存更改 * 。 | a. 选择端点名称以显示详细信息。<br>b. 选择 * 编辑绑定模式 * 。<br>c. 根据需要更新绑定模式。<br>d. 选择 * 保存更改 * 。 |
| 编辑端点证书 | a. 选中此端点对应的复选框。<br>b. 选择 * 操作 * > * 编辑端点证书 * 。<br>c. 根据需要上传或生成新的自定义证书或开始使用全局 S3 和 Swift 证书。<br>d. 选择 * 保存更改 * 。 | a. 选择端点名称以显示详细信息。<br>b. 选择 * 证书 * 选项卡。<br>c. 选择 * 编辑证书 * 。<br>d. 根据需要上传或生成新的自定义证书或开始使用全局 S3 和 Swift 证书。<br>e. 选择 * 保存更改 * 。 |
| 编辑租户访问 | a. 选中此端点对应的复选框。<br>b. 选择*操作*>*编辑租户访问*。<br>c. 选择其他访问选项、从列表中选择或删除租户、或者同时执行这两项操作。<br>d. 选择 * 保存更改 * 。 | a. 选择端点名称以显示详细信息。<br>b. 选择*租户访问*选项卡。<br>c. 选择*编辑租户访问*。<br>d. 选择其他访问选项、从列表中选择或删除租户、或者同时执行这两项操作。<br>e. 选择 * 保存更改 * 。 |

## 删除负载平衡器端点

您可以使用 * 操作 * 菜单删除一个或多个端点，也可以从详细信息页面中删除单个端点。

> 为防止客户端中断，请在删除负载平衡器端点之前更新任何受影响的 S3 或 Swift 客户端应用程序。更新每个客户端以使用分配给另一个负载平衡器端点的端口进行连接。请务必同时更新所需的任何证书信息。

- 删除一个或多个端点：
  a. 在"负载平衡器"页面中、选中要删除的每个端点对应的复选框。
  b. 选择 * 操作 * > * 删除 * 。
  c. 选择 * 确定 * 。

- 从详细信息页面中删除一个端点：
  a. 从负载平衡器页面。选择端点名称。
  b. 在详细信息页面上选择 * 删除 * 。
  c. 选择 * 确定 * 。