



配置客户端连接 StorageGRID software

NetApp
July 23, 2026

目录

配置客户端连接	1
配置 S3 客户端到 StorageGRID 的连接	1
配置任务	1
将 StorageGRID 附加到客户端应用程序所需的信息	2
StorageGRID 中 S3 客户端的安全性	3
摘要	3
StorageGRID 如何为客户端应用程序提供安全性	3
TLS 库支持的哈希和加密算法	4
\${post_edited_translations.segment}	4
StorageGRID S3 设置向导注意事项和要求	4
访问并完成 StorageGRID 中的 S3 设置向导	5
管理 HA 组	12
了解 StorageGRID 高可用性组	13
StorageGRID HA 组如何提供高可用性	15
StorageGRID 高可用性组的配置选项	16
在 StorageGRID 中配置高可用性组	17
管理负载均衡	22
了解 StorageGRID 负载均衡	22
配置 StorageGRID 负载均衡器端点	27
在 StorageGRID 中配置 S3 端点域名	35
\${post_edited_translations.segment}	35
重命名 S3 端点域名	36
删除 S3 端点域名	36
StorageGRID 客户端连接的 IP 地址和端口	36
示例 URL	37
\${post_edited_translations.segment}	37

配置客户端连接

配置 S3 客户端到 StorageGRID 的连接

作为网络管理员，您可以管理控制 S3 客户端应用程序如何连接到 StorageGRID 系统以存储和检索数据的配置选项。



此版本的文档网站中已删除 Swift 详细信息。请参阅 ["StorageGRID 11.8：配置 S3 和 Swift 客户端连接"](#)。

配置任务

1. 根据客户端应用程序连接到 StorageGRID 的方式，在 StorageGRID 中执行前提任务。

所需任务

您必须获得：

- IP 地址
- 域名
- SSL 证书

可选任务

(可选) 配置：

- 身份联合
- SSO

1. 使用 StorageGRID 获取应用程序连接到网格所需的值。您可以使用 S3 设置向导，也可以手动配置每个 StorageGRID 实体。+

`${post_edited_translations.segment}`

按照 S3 设置向导中的步骤操作。

手动配置

1. 创建高可用性组
2. 创建负载均衡器端点
3. 创建租户帐户
4. 创建存储桶和访问密钥
5. 配置 ILM 规则和策略

1. 使用 S3 应用程序完成与 StorageGRID 的连接。创建 DNS 条目，将 IP 地址与您计划使用的任何域名相关

联。

根据需要，执行其他应用程序设置。

- 2. 在应用程序和 StorageGRID 中执行持续任务，以便随时间推移管理和监控对象存储。

将 **StorageGRID** 附加到客户端应用程序所需的信息

在将 StorageGRID 连接到 S3 客户端应用程序之前，必须在 StorageGRID 中执行配置步骤并获取特定值。

我需要哪些值？

`${post_edited_translations.segment}`

值	配置值的位置	使用值的位置
虚拟 IP (VIP) 地址	StorageGRID > HA 组	DNS条目
端口	StorageGRID > 负载均衡器端点	客户端应用程序
SSL 证书	StorageGRID > 负载均衡器端点	客户端应用程序
服务器名称 (FQDN)	StorageGRID > 负载均衡器端点	• 客户端应用程序 • DNS条目
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	客户端应用程序
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	客户端应用程序

如何获得这些值？

根据您的要求，您可以执行以下操作之一来获取所需的信息：

- 使用 **"S3 设置向导"**。S3 设置向导可帮助您快速配置 StorageGRID 中所需的值，并输出一个或两个可在配置 S3 应用程序时使用的文件。该向导将引导您完成所需的步骤，并帮助确保您的设置符合 StorageGRID 最佳实践。



如果要配置 S3 应用程序，建议使用 S3 设置向导，除非您知道自己有特殊要求，或者您的实现需要大量自定义。

- 使用 **"FabricPool 设置向导"**。与 S3 设置向导类似，FabricPool 设置向导可帮助您快速配置所需的值，并输出一个文件，您可以在 ONTAP 中配置 FabricPool 云层时使用该文件。



如果您计划将 StorageGRID 用作 FabricPool 云分层的对象存储系统，除非您确定自己有特殊需求或您的实施需要进行大量自定义，否则建议使用 FabricPool 设置向导。

- 手动配置项目。如果您正在连接到 S3 应用程序，并且不希望使用 S3 设置向导，则可以通过手动执行配置来获取所需的值。请按照以下步骤操作：
 - a. 配置要用于 S3 应用程序的高可用性 (HA) 组。请参阅 ["配置高可用性组"](#)。
 - b. 创建 S3 应用程序将使用的负载均衡器端点。请参阅 ["配置负载均衡器端点"](#)。
 - c. 创建 S3 应用程序将使用的租户账户。参见 ["创建租户帐户"](#)。
 - d. 对于 S3 租户，请登录该租户账户，并为每个将访问该应用程序的用户生成一个访问密钥 ID 和机密访问密钥。请参见 ["\\${post_edited_translations.segment}"](#)。
 - e. 在租户帐户中创建一个或多个 S3 存储桶。有关 S3，请参见["创建 S3 存储桶"](#)。
 - f. 要为属于新租户或存储区/容器的对象添加特定放置说明，请创建新的 ILM 规则并激活新的 ILM 策略以使用该规则。请参阅 ["创建 ILM 规则"](#) 和 ["创建 ILM 策略"](#)。

StorageGRID 中 S3 客户端的安全性

StorageGRID 租户帐户使用 S3 客户端应用程序将对象数据保存至 StorageGRID。您应查看为客户端应用程序实施的安全措施。

摘要

以下列表总结了如何为 S3 REST API 实现安全性：

连接安全

TLS

服务器身份验证

由系统 CA 签名的 X.509 服务器证书或由管理员提供的自定义服务器证书

客户端身份验证

S3 账号访问密钥 ID 和密钥

客户端授权

存储桶所有权和所有适用的访问控制策略

StorageGRID 如何为客户端应用程序提供安全性

S3 客户端应用程序可以连接到网关节点或管理节点上的负载均衡器服务，也可以直接连接到存储节点。

- 连接到负载均衡器服务的客户端可以使用 HTTPS 或 HTTP，具体取决于您如何["配置负载均衡器端点"](#)。

HTTPS 提供安全的 TLS 加密通信，建议使用。您必须将安全证书附加到端点。

HTTP 提供安全性较低的未加密通信，应仅用于非生产或测试网络。

- 连接到存储节点的客户端也可以使用 HTTPS 或 HTTP。

HTTPS 是默认设置，建议使用。

HTTP 提供安全性较低的未加密通信，但可以选择["启用"](#)用于非生产或测试网格。

- StorageGRID 和客户端之间的通信使用 TLS 进行加密。
- 无论负载均衡器端点配置为接受 HTTP 还是 HTTPS 连接，网格中负载均衡器服务与存储节点之间的通信均会加密。
- 客户端必须向 StorageGRID 提供 ["HTTP 身份验证标头"](#) 才能执行 REST API 操作。

安全证书和客户端应用程序

在所有情况下，客户端应用程序都可以使用网格管理员上传的自定义服务器证书或 StorageGRID 系统生成的证书进行 TLS 连接：

- 当客户端应用程序连接到负载均衡器服务时，它们使用为负载均衡器端点配置的证书。每个负载均衡器端点都有自己的证书—由网格管理员上传的自定义服务器证书或网格管理员在配置端点时在 StorageGRID 中生成的证书。

请参阅 ["负载均衡注意事项"](#)。

- 当客户端应用程序直接连接到存储节点时，它们使用安装 StorageGRID 系统时为存储节点生成的系统生成的服务器证书（由系统证书颁发机构签名），或者使用网格管理员为网格提供的单个自定义服务器证书。请参阅 ["添加自定义 S3 API 证书"](#)。

应将客户端配置为信任对其用于建立 TLS 连接的任何证书进行签名的证书颁发机构。

TLS 库支持的哈希和加密算法

StorageGRID 系统支持一组密码套件，客户端应用程序可以在建立 TLS 会话时使用这些密码套件。要配置密码，请转到 [配置 > 安全 > 安全设置](#)，然后选择 **TLS** 和 **SSH** 策略。

支持的 TLS 版本

StorageGRID 支持 TLS 1.2 和 TLS 1.3。



SSLv3 和 TLS 1.1（或更早版本）不再受支持。

`${post_edited_translations.segment}`

StorageGRID S3 设置向导注意事项和要求

您可以使用 S3 设置向导将 StorageGRID 配置为 S3 应用程序的对象存储系统。

何时使用 **S3** 设置向导

S3 设置向导将指导您完成配置 StorageGRID 以用于 S3 应用程序的每个步骤。作为完成向导的一部分，您可以下载可用于在 S3 应用程序中输入值的文件。使用向导可以更快地配置您的系统，并确保您的设置符合 StorageGRID 最佳实践。

如果具有["root 访问权限"](#)，则可以在开始使用 StorageGRID 网格管理器时完成 S3 设置向导，也可以在以后的任何时候访问并完成该向导。根据您的要求，您还可以手动配置某些或所有必需项目，然后使用向导汇编 S3 应用

程序所需的值。

使用向导之前

在使用向导之前，请确认您已完成这些先决条件。

获取 IP 地址并设置 VLAN 接口

如果您将配置高可用性 (HA) 组，您将知道 S3 应用程序将连接到哪些节点以及将使用哪个 StorageGRID 网络。您还知道要为子网 CIDR、网关 IP 地址和虚拟 IP (VIP) 地址输入哪些值。

如果您计划使用虚拟 LAN 来隔离来自 S3 应用程序的流量，则表示您已经配置了 VLAN 接口。请参阅 ["配置 VLAN 接口"](#)。

配置身份联合和 SSO

如果您计划对 StorageGRID 系统使用身份联合或单点登录 (SSO)，则已启用这些功能。您还知道哪个联合组应具有 S3 应用程序将使用的租户帐户的根访问权限。请参阅 ["\\${post_edited_translations.segment}"](#) 和 ["\\${post_edited_translations.segment}"](#)。

获取并配置域名

您知道要用于 StorageGRID 的完全限定域名 (FQDN)。域名服务器 (DNS) 条目会将此 FQDN 映射到使用向导创建的 HA 组的虚拟 IP (VIP) 地址。

如果您计划使用 S3 虚拟托管风格的请求，则应该使用 ["配置的 S3 端点域名"](#)。建议使用虚拟主机式请求。

查看负载均衡器和安全证书要求

如果您计划使用 StorageGRID 负载均衡器，则已查看负载均衡的一般注意事项。您拥有要上传的证书或生成证书所需的值。

如果您计划使用外部（第三方）负载均衡器端点，则您具有该负载均衡器的完全限定域名 (FQDN)、端口和证书。

配置任何网格联合连接

如果要允许 S3 租户使用网格联合连接克隆帐户数据并将存储桶对象复制到另一个网格，请在启动向导之前确认以下内容：

- 您有 ["已配置网格联盟连接"](#)。
- 连接状态为*已连接*。
- [\\${post_edited_translations.segment}](#)

访问并完成 StorageGRID 中的 S3 设置向导

您可以使用 S3 设置向导将 StorageGRID 配置为与 S3 应用程序一起使用。设置向导提供应用程序访问 StorageGRID 存储桶和保存对象所需的值。

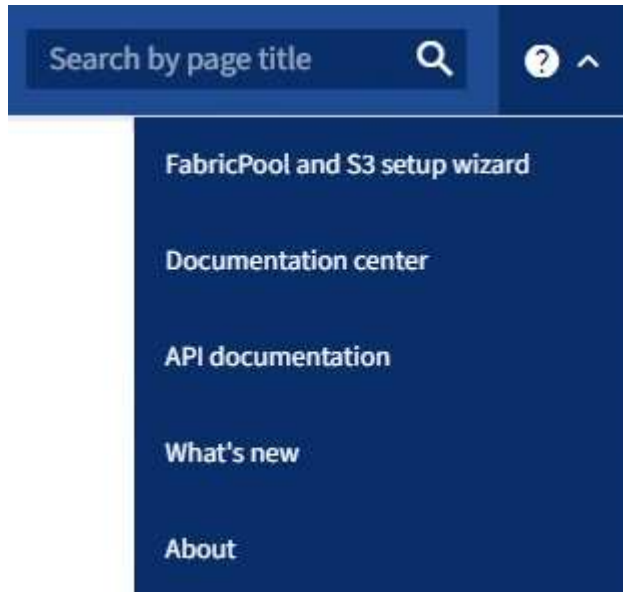
开始之前

- 您有 ["root 访问权限"](#)。
- 您已查阅["注意事项和要求"](#)以使用向导。

访问此向导

步骤

1. 使用 ["支持的 Web 浏览器"](#) 登录到网格管理器。
2. 如果仪表板上出现 **FabricPool and S3 setup wizard** 横幅，请选择横幅中的链接。如果横幅不再出现，请从 Grid Manager 中的标题栏中选择帮助图标，然后选择 **FabricPool and S3 setup wizard**。



3. 在 FabricPool 和 S3 设置向导页面的 S3 应用程序部分，选择*立即配置*。

步骤 1/6：配置 HA 组

HA 组是一组节点，每个节点都包含 StorageGRID 负载平衡器服务。HA 组可以包含网关节点、管理节点或两者。

您可以使用 HA 组来帮助保持 S3 数据连接可用。如果 HA 组中的活动接口出现故障，备份接口可以管理工作负载，对 S3 操作的影响很小。

有关此任务的详细信息，请参见 ["管理高可用性组"](#)。

步骤

1. 如果您计划使用外部负载均衡器，则无需创建 HA 组。选择 [跳过此步骤](#) 并转到 [步骤 2/6：配置负载均衡器端点](#)。
2. 要使用 StorageGRID 负载均衡器，您可以创建新的 HA 组或使用现有的 HA 组。

创建 HA 组

- a. 要创建新的HA组，请选择*创建HA组*。
- b. 对于*输入详细信息*步骤，请填写以下字段。

字段	问题描述
HA 组名称	此 HA 组的唯一显示名称。
<code>\${post_edited_translations.segment}</code>	此 HA 组的描述。

- c. 对于*添加接口*步骤，请选择要在此 HA 组中使用的节点接口。

`${post_edited_translations.segment}`

您可以选择一个或多个节点，但每个节点只能选择一个接口。

- d. 对于*Prioritize interfaces*步骤，请确定此 HA 组的主接口和任何备份接口。

拖动行以更改*优先级顺序*列中的值。

列表中的第一个接口是 Primary 接口。除非发生故障，否则 Primary 接口为活动接口。

如果 HA 组包含多个接口，并且活动接口发生故障，则虚拟 IP（VIP）地址按优先级顺序移动到第一个备份接口。如果该接口出现故障，VIP 地址将移动到下一个备份接口，依此类推。故障解决后，VIP 地址将移回可用的最高优先级接口。

- e. 对于*输入 IP 地址*步骤，请填写以下字段。

字段	问题描述
子网 CIDR	CIDR 表示法中 VIP 子网的地址 — IPv4 地址后跟斜杠和子网长度（0-32）。 网络地址不得设置任何主机位。例如，192.16.0.0/22。
网关 IP 地址（可选）	如果用于访问 StorageGRID 的 S3 IP 地址与 StorageGRID VIP 地址不在同一子网中，请输入 StorageGRID VIP 本地网关 IP 地址。本地网关 IP 地址必须在 VIP 子网内。
虚拟 IP 地址	为 HA 组中的活动接口输入至少一个且不超过十个 VIP 地址。所有 VIP 地址必须在 VIP 子网内。 必须至少有一个地址为 IPv4。或者，您可以指定其他 IPv4 和 IPv6 地址。

- f. 选择*创建HA组*，然后选择*完成*返回S3设置向导。
- g. 选择*继续*转到负载均衡器步骤。

使用现有 HA 组

- a. 要使用现有 HA 组，请从*选择 HA 组*中选择 HA 组名称。
- b. 选择*继续*转到负载均衡器步骤。

步骤 2/6：配置负载均衡器端点

StorageGRID 使用负载均衡器管理来自客户端应用程序的工作负载。负载均衡可最大限度地提高跨多个存储节点的速度和连接容量。

您可以使用 StorageGRID 负载均衡器服务，该服务存在于所有网关和管理节点上，也可以连接到外部（第三方）负载均衡器。建议使用 StorageGRID 负载均衡器。

有关此任务的详细信息，请参见 ["负载均衡注意事项"](#)。

要使用 StorageGRID 负载均衡器服务，请选择 **StorageGRID load balancer** 选项卡，然后创建或选择要使用的负载均衡器端点。要使用外部负载均衡器，请选择 **External load balancer** 选项卡，并提供有关已配置系统的详细信息。

创建端点

步骤

1. 要创建负载均衡器端点，请选择*Create endpoint*。
2. 对于*输入端点详细信息*步骤，请填写以下字段。

字段	问题描述
名称	终结点的描述性名称。
端口	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，但您可以输入任何未使用的外部端口。如果输入 80 或 443，则仅在网关节点上配置端点，因为这些端口在管理节点上保留。 注意：不允许使用其他网格服务使用的端口。请参阅 "StorageGRID 内部端口"。
客户端类型	必须是 S3 。
网络协议	选择 HTTPS。 注意：支持在不使用 TLS 加密的情况下与 StorageGRID 通信，但不建议这样做。

3. 对于*选择绑定模式*步骤，指定绑定模式。绑定模式控制使用任何 IP 地址或使用特定 IP 地址和网络接口访问端点的方式。

模式	问题描述
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、任何网络上的任何 HA 组的虚拟 IP (VIP) 地址或相应的 FQDN 来访问端点。 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）来访问此端点。 具有此绑定模式的端点都可以使用相同的端口号，只要您为端点选择的 HA 组不重叠即可。
节点接口	<code>\${post_edited_translations.segment}</code>
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。

4. 对于租户访问步骤，请选择以下选项之一：

字段	问题描述
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存储区。
允许选定的租户	只有选定租户帐户可以使用此端点访问其存储桶。
阻止选定租户	选定的租户帐户无法使用此端点来访问其存储桶。所有其他租户都可以使用此端点。

5. 对于*附加证书*步骤，请选择以下选项之一：

字段	问题描述
上传证书（推荐）	使用此选项可上传 CA 签名的服务器证书、证书私钥和可选的 CA 捆绑包。
生成证书	使用此选项可生成自签名证书。有关要输入内容的详细信息，请参见 "配置负载均衡器端点" 。
使用 StorageGRID S3 证书	仅当已上传或生成 StorageGRID 全局证书的自定义版本时，才使用此选项。有关详细信息，请参见 "配置 S3 API 证书" 。

6. 选择*完成*返回 S3 设置向导。

7. 选择*继续*转到租户和存储桶步骤。



对端点证书的更改可能需要长达 15 分钟才能应用于所有节点。

使用现有负载均衡器端点

步骤

1. 要使用现有端点，请从*选择负载均衡器端点*中选择其名称。
2. 选择*继续*转到租户和存储桶步骤。

使用外部负载均衡器

步骤

1. 要使用外部负载均衡器，请完成以下字段。

字段	问题描述
FQDN	外部负载均衡器的完全限定域名(FQDN)。
端口	S3 应用程序将用于连接到外部负载均衡器的端口号。
证书	复制外部负载均衡器的服务器证书并将其粘贴到此字段中。

2. 选择*继续*转到租户和存储桶步骤。

步骤 3/6：创建租户和存储区

租户是可以使用 S3 应用程序在 StorageGRID 中存储和检索对象的实体。每个租户都有自己的用户、访问密钥、存储桶、对象和一组特定的功能。

存储区是用于存储租户的对象和对象元数据的容器。虽然租户可能有很多存储区，但此向导可帮助您以最快捷、最简单的方式创建租户和存储区。如果稍后需要添加存储区或设置选项，可以使用 Tenant Manager。

有关此任务的详细信息，请参见 ["创建租户帐户"](#) 和 ["创建 S3 存储桶"](#)。

步骤

- 1. 输入租户帐户的名称。

租户名称不必是唯一的。创建租户帐户时，它将收到一个唯一的数字帐户 ID。

- 2. 根据您的 StorageGRID 系统使用 ["身份联合"](#)、["单点登录 \(SSO\)"](#) 还是同时使用两者，定义租户帐户的根访问权限。

选项	执行此操作
如果未启用身份联合	指定以本地 root 用户身份登录租户时使用的密码。
如果启用了身份联合	a. 选择现有联合组，以便为租户提供 "root 访问权限" 。 b. （可选）指定以本地 root 用户身份登录租户时使用的密码。
如果已启用身份联合和单一登录(SSO)	选择现有联合组，使其拥有 "root 访问权限" 租户权限。没有本地用户可以登录。

- 3. 如果要向导为 root 用户创建访问密钥 ID 和秘密访问密钥，请选择 **Create root user S3 access key automatically**。

如果租户的唯一用户是 root 用户，请选择此选项。如果其他用户将使用此租户，["使用租户管理器"](#)以配置密钥和权限。
- 4. 如果要立即为此租户创建存储桶，请选择**Create bucket for this tenant**。



如果为网格启用了 S3 对象锁定，则此步骤中创建的存储桶未启用 S3 对象锁定。如果需要为此 S3 应用程序使用 S3 对象锁定存储桶，请不要选择立即创建存储桶。请改用 Tenant Manager ["创建存储桶"](#) 稍后执行此操作。

- a. 输入 S3 应用程序将使用的存储桶的名称。例如， s3-bucket。

创建存储桶后，您无法更改存储桶名称。

- b. 选择此存储桶的***区域***。

使用默认区域(us-east-1) ，除非您希望将来使用 ILM 根据存储桶的区域筛选对象。

- 5. 选择***创建并继续***。

步骤 4/6：下载数据

在下载数据步骤中，您可以下载一个或两个文件来保存刚刚配置的详细信息。

步骤

1. 如果您选择了*自动创建 root 用户 S3 访问密钥*，请执行以下一项或两项操作：
 - 选择*下载访问密钥*以下载包含租户帐户名称、访问密钥 ID 和机密访问密钥的`.csv`文件。
 - 选择复制图标 () 将访问密钥 ID 和秘密访问密钥复制到剪贴板。
2. 选择*下载配置值*以下载包含负载均衡器端点、租户、存储桶和 root 用户设置的`.txt`文件。
3. 请将此信息保存到安全位置。



在复制两个访问密钥之前，请不要关闭此页面。关闭此页面后，密钥将不可用。请务必将此信息保存在安全的位置，因为它可用于从 StorageGRID 系统获取数据。

4. 如果出现提示，请选中复选框以确认已下载或复制密钥。
5. 选择 **Continue** 转到 ILM 规则和策略步骤。

第 5 步，共 6 步：查看 S3 的 ILM 规则和 ILM 策略

信息生命周期管理 (ILM) 规则控制 StorageGRID 系统中所有对象的放置、持续时间和接收行为。StorageGRID 附带的 ILM 策略会生成所有对象的两个复制副本。在您激活至少一项新策略之前，此策略有效。

步骤

1. 查看页面上提供的信息。
2. 如果要为属于新租户或存储区的对象添加特定说明，请创建新规则和新策略。请参阅["创建 ILM 规则"](#)和["使用 ILM 策略"](#)。
3. 选择*我已查看这些步骤并了解需要执行的操作*。
4. 选中复选框表示您了解下一步该怎么做。
5. 选择*继续*前往*摘要*。

第6步（共6步）：查看摘要

步骤

1. 查看摘要。
2. 记下后续步骤中的详细信息，其中描述了连接到 S3 客户端之前可能需要的其他配置。例如，选择 **Sign in as root** 会将您转至租户管理器，您可以在其中添加租户用户、创建其他存储桶并更新存储桶设置。
3. 选择 **Finish**。
4. 使用从 StorageGRID 下载的文件或手动获取的值配置应用程序。

管理 HA 组

了解 StorageGRID 高可用性组

高可用性(HA)组为S3客户端提供高可用性数据连接，并为网格管理器和租户管理器提供高可用性连接。

您可以将多个管理节点和网关节点的网络接口分组到高可用性 (HA) 组中。如果 HA 组中的活动接口出现故障，备份接口可以管理工作负载。

每个HA组都提供对选定节点上共享服务的访问权限。

- 包括网关节点、管理节点或两者的 HA 组为 S3 客户端提供高可用数据连接。
- 仅包含管理节点的 HA 组提供到 Grid Manager 和 Tenant Manager 的高可用性连接。
- 仅包括服务设备和基于 VMware 的软件节点的 HA 组可以为 ["使用 S3 Select 的 S3 租户"](#) 提供高可用性连接。使用 S3 Select 时建议使用 HA 组，但不是必需的。

如何创建 HA 组？

1. 您可以为一个或多个管理节点或网关节点选择一个网络接口。您可以使用网格网络 (eth0) 接口、客户端网络 (eth2) 接口、VLAN 接口或已添加到节点的访问接口。



如果接口具有 DHCP 分配的 IP 地址，则无法将其添加到 HA 组。

2. 指定一个接口作为主接口。主接口是活动接口，除非发生故障。
3. 您可以确定任何备份接口的优先级顺序。
4. 您可以为组分配 1 到 10 个虚拟 IP (VIP) 地址。客户端应用程序可以使用这些 VIP 地址中的任何一个连接到 StorageGRID。

有关说明，请参阅 ["配置高可用性组"](#)。

什么是活动接口？

在正常运行过程中，HA 组的所有 VIP 地址都会添加到主接口中，这是优先级顺序中的第一个接口。只要主接口保持可用，当客户端连接到组的任何 VIP 地址时，就会使用该接口。也就是说，在正常运行期间，主接口是组的"活动"接口。

同样，在正常操作期间，HA 组的任何优先级较低的接口都充当"备份"接口。除非主（当前活动）接口不可用，否则不会使用这些备份接口。

查看节点的当前HA组状态

要查看是否将节点分配给 HA 组并确定其当前状态，请选择 节点 > *node*。

如果*概述*选项卡包含 *HA 组*的条目，则该节点将被分配到列出的 HA 组。组名后面的值是该节点在 HA 组中的当前状态：

- **Active**：HA 组当前托管在此节点上。
- **Backup**：HA 组当前未使用此节点；此为备份接口。
- **已停止**：HA 组无法在此节点上托管，因为高可用性（keepalived）服务已手动停止。

- **Fault:** 由于以下一个或多个原因，HA 组无法在此节点上托管：
 - 节点上未运行负载均衡器(nginx-gw)服务。
 - 节点的 eth0 或 VIP 接口已关闭。
 - 此节点已关闭。

在此示例中，主管理节点已添加到两个 HA 组。此节点当前是 Admin 客户端组的活动接口和 FabricPool 客户端组的备份接口。

DC1-ADM1 (Primary Admin Node) [🔗](#)

[Overview](#)
[Hardware](#)
[Network](#)
[Storage](#)
[Load balancer](#)
[Tasks](#)

Node information [?](#)

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	🟢 Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	Admin clients (Active) FabricPool clients (Backup)
IP addresses:	172.16.1.225 - eth0 (Grid Network) 10.224.1.225 - eth1 (Admin Network) 47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses ▼](#)

活动接口出现故障时会发生什么？

当前承载 VIP 地址的接口是活动接口。如果 HA 组包含多个接口，并且活动接口发生故障，则 VIP 地址将按优先级顺序移动到第一个可用的备份接口。如果该接口出现故障，VIP 地址将移动到下一个可用的备份接口，依此类推。

可以出于以下任意原因触发故障转移：

- 配置此接口的节点已关闭。
- 配置该接口的节点将与所有其他节点断开连接至少 2 分钟。
- 活动接口关闭。
- 负载均衡器服务停止。
- 高可用性服务停止。



故障转移可能不会由托管活动接口的节点外部的网络故障触发。同样，故障转移不会由 Grid Manager 或 Tenant Manager 的服务触发。

故障转移过程通常只需几秒钟，速度足够快，客户端应用程序受到的影响极小，可以依靠正常的重试行为继续运行。

当故障得到解决且更高优先级的接口再次可用时，VIP 地址将自动移动到可用的最高优先级接口。

StorageGRID HA 组如何提供高可用性

您可以使用高可用性 (HA) 组为对象数据和管理用途提供到 StorageGRID 的高可用性连接。

- HA组可以为网格管理器或租户管理器提供高度可用的管理连接。
- HA组可以为S3客户端提供高可用性数据连接。
- 仅包含一个接口的 HA 组允许您提供多个 VIP 地址并显式设置 IPv6 地址。

只有组中包含的所有节点都提供相同的服务时，HA 组才能提供高可用性。创建 HA 组时，请从提供所需服务的节点类型中添加接口。

- 管理节点：包括负载均衡器服务，并启用对 Grid Manager 或 Tenant Manager 的访问。
- 网关节点：包括负载均衡器服务。

HA 组的目的	将此类型的节点添加到HA组
访问 Grid Manager	• 主管理节点（ Primary ） • 非主管理节点 注意： 主管理节点必须是主界面。某些维护程序只能从主管理节点执行。
仅访问租户管理器	• 主管理节点或非主管理节点
S3 客户端访问——负载均衡器服务	• 管理节点 • 网关节点
S3 客户端访问 "S3 Select"	• 服务设备 • 基于VMware的软件节点 注意： 建议在使用 S3 Select 时使用 HA 组，但不是必需的。

对网格管理器或租户管理器使用HA组的限制

如果 Grid Manager 或 Tenant Manager 服务失败，则不会触发 HA 组故障转移。

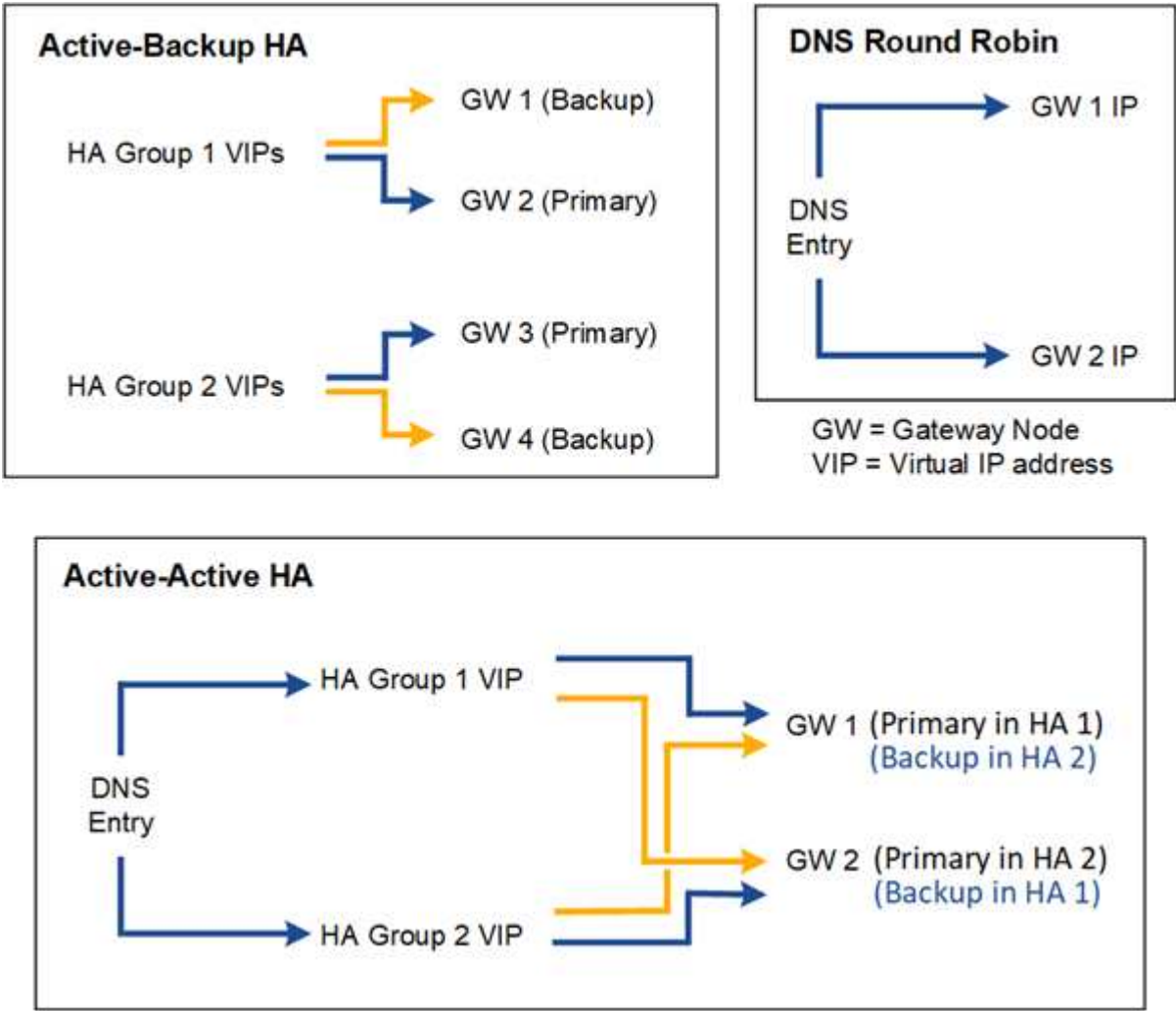
如果在发生故障转移时已登录到 Grid Manager 或 Tenant Manager，则您将被注销，必须重新登录才能继续执行任务。

当主管理节点不可用时，无法执行某些维护程序。在故障转移期间，您可以使用 Grid Manager 监控您的 StorageGRID 系统。

StorageGRID 高可用性组的配置选项

以下图表提供了配置高可用性 (HA) 组的不同方法的示例。每个选项都有优点和缺点。

在图中，蓝色表示 HA 组中的主接口，黄色表示 HA 组中的备份接口。



下表总结了图中所示的每个 HA 配置的优点。

配置	优势	劣势
活动-备份 HA	• 由 StorageGRID 管理，无外部依赖关系。 • 快速故障转移。	• HA 组中只有一个节点处于活动状态。每个 HA 组至少有一个节点将处于空闲状态。
DNS 轮询	• 提高聚合吞吐量。 • 无空闲主机。	• 故障转移速度较慢，这可能取决于客户端行为。 • 需要在 StorageGRID 外部配置硬件。 • 需要客户实施的运行状况检查。

配置	优势	劣势
主动-主动 HA	• <code>\$(post_edited_translations.segment)</code> • <code>\$(post_edited_translations.segment)</code> • 快速故障转移。	• 配置更复杂。 • 需要在 StorageGRID 外部配置硬件。 • 需要客户实施的运行状况检查。

在 StorageGRID 中配置高可用性组

您可以配置高可用性(HA)组，以提供对管理节点或网关节点上服务的高可用性访问。



`$(post_edited_translations.segment)`

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到网格管理器。
- 您有 ["root 访问权限"](#)。
- 如果您计划在 HA 组中使用 VLAN 接口，则已创建 VLAN 接口。请参阅 ["配置 VLAN 接口"](#)。
- `$(post_edited_translations.segment)`
 - **Linux** (安装节点之前)： ["创建节点配置文件"](#)
 - **Linux** (安装节点后)： ["将中继或接入接口添加到节点"](#)
 - **VMware** (安装节点后): ["将中继或接入接口添加到节点"](#)



"Linux"是指 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参见 ["NetApp 互操作性矩阵工具 \(IMT\)"](#)。

创建高可用性组

创建高可用性组时，可以选择一个或多个接口，并按优先级顺序对其进行组织。然后，将一个或多个 VIP 地址分配给该组。

接口必须是网关节点或管理节点的接口，才能包含在 HA 组中。HA 组只能为任何给定节点使用一个接口；但是，同一节点的其他接口可以在其他 HA 组中使用。

访问此向导

步骤

1. 选择*配置* > 网络 > 高可用性组。
2. 选择 **Create**。

输入HA组的详细信息

步骤

1. 为 HA 组提供唯一名称。
2. (可选) 输入HA组的说明。

3. 选择 **Continue**。

向 **HA** 组添加接口

步骤

1. `${post_edited_translations.segment}`
`${post_edited_translations.segment}`

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Total interface count: 4

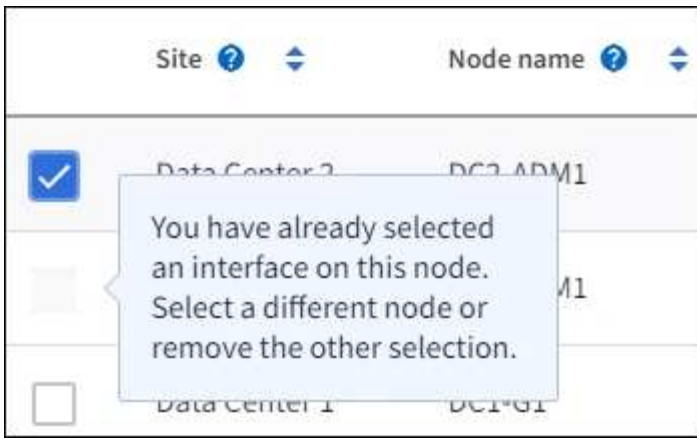
	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected

`${post_edited_translations.segment}`

接口选择指南

- `${post_edited_translations.segment}`
- 您只能为节点选择一个接口。
- 如果 HA 组用于管理节点服务（包括 Grid Manager 和 Tenant Manager）的 HA 保护，请仅选择管理节点上的接口。
- `${post_edited_translations.segment}`
- 如果选择不同类型的节点上的接口，则会显示信息说明。系统会提醒您，如果发生故障转移，以前活动节点提供的服务可能在新活动节点上不可用。例如，备份网关节点无法为管理节点服务提供 HA 保护。同样，备份管理节点无法执行主管理节点可以提供的所有维护过程。
- 如果无法选择接口，其复选框将被禁用。工具提示提供了更多信息。



- 如果接口的子网值或网关与另一个选定的接口冲突，则无法选择该接口。
- 如果配置的接口没有静态 IP 地址，则无法选择该接口。

2. 选择 **Continue**。

确定优先级顺序

如果 HA 组包括多个接口，则可以确定哪个是主接口，哪个是备份（故障转移）接口。如果主接口出现故障，VIP 地址将移动到可用的最高优先级接口。如果该接口出现故障，VIP 地址将移动到下一个可用的最高优先级接口，依此类推。

步骤

1. 在*优先级顺序*列中拖动行以确定主接口和任何备份接口。

列表中的第一个接口是 Primary 接口。除非发生故障，否则 Primary 接口为活动接口。

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	DC1-ADM1-104-96	eth2	Primary Admin Node
2	DC2-ADM1-104-103	eth2	Admin Node



如果 HA 组提供对 Grid Manager 的访问权限，则必须在主管理节点上选择一个接口作为主接口。某些维护程序只能从主管理节点执行。

2. 选择 **Continue**。

输入 IP 地址

步骤

1. 在 **Subnet CIDR** 字段中，以 CIDR 表示法指定 VIP 子网——一个 IPv4 地址，后跟斜杠和子网长度（0-32）。

网络地址不得设置任何主机位。例如，192.16.0.0/22。



`${post_edited_translations.segment}`

Enter details for the HA group

Subnet CIDR

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional)

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

2. 可选地，如果任何 S3 管理或租户客户端将从不同的子网访问这些 VIP 地址，请输入*网关 IP 地址*。网关地址必须在 VIP 子网内。

客户端和管理员用户将使用此网关访问虚拟 IP 地址。

3. 为 HA 组中的活动接口输入至少一个且不超过十个 VIP 地址。所有 VIP 地址必须位于 VIP 子网内，并且所有地址都将在活动接口上同时处于活动状态。

您必须至少提供一个 IPv4 地址。您也可以指定其他 IPv4 和 IPv6 地址。

4. 选择*创建HA组*并选择*完成*。

已创建 HA 组，您现在可以使用已配置的虚拟 IP 地址。

后续步骤

如果要使用此 HA 组进行负载平衡，请创建负载平衡器端点以确定端口和网络协议并附加任何所需的证书。请参阅 ["配置负载平衡器端点"](#)。

编辑高可用性组

您可以编辑高可用性(HA)组以更改其名称和描述、添加或删除接口、更改优先级顺序或添加或更新虚拟 IP 地址。

例如，如果要删除与站点或节点停用过程中的选定接口关联的节点，则可能需要编辑 HA 组。

步骤

1. 选择*配置* > 网络 > 高可用性组。

高可用性组页面显示所有现有 HA 组。

2. 选中要编辑的 HA 组的复选框。
3. 根据您要更新的内容，执行以下操作之一：
 - 选择*操作* > *编辑虚拟 IP 地址*以添加或删除 VIP 地址。
 - 选择*操作* > *编辑 HA 组*以更新组的名称或描述、添加或删除接口、更改优先级顺序或添加或删除 VIP 地址。
4. 如果您选择了*编辑虚拟 IP 地址*：
 - a. 更新HA组的虚拟IP地址。
 - b. 选择 **Save**。
 - c. 选择 **Finish**。
5. 如果选择 **Edit HA group**：
 - a. (可选) 更新组的名称或描述。
 - b. (可选) 选中或清除复选框以添加或删除接口。



如果 HA 组提供对 Grid Manager 的访问权限，则必须在主管理节点上选择一个接口作为主接口。某些维护程序只能从主管理节点执行

- c. 可选操作：拖动行以更改此 HA 组的主接口和任何备份接口的优先级顺序。
- d. (可选) 更新虚拟 IP 地址。
- e. 选择 **Save**，然后选择 **Finish**。

删除高可用性组

您可以一次删除一个或多个高可用性 (HA) 组。



如果高可用性 (HA) 组已绑定到负载均衡器端点，则无法将其删除。要删除 HA 组，必须将其从使用该组的任何负载均衡器端点中移除。

为了防止客户端中断，请在删除 HA 组之前更新任何受影响的 S3 客户端应用程序。更新每个客户端以使用另一个 IP 地址进行连接，例如，其他 HA 组的虚拟 IP 地址或在安装期间为接口配置的 IP 地址。

步骤

1. 选择*配置* > 网络 > 高可用性组。

2. 查看要删除的每个 HA 组的*负载均衡器端点*列。如果列出了任何负载均衡器端点：
 - a. `${post_edited_translations.segment}`
 - b. 选中端点的复选框。
 - c. 选择*操作* > 编辑端点绑定模式。
 - d. `${post_edited_translations.segment}`
 - e. 选择 **Save changes**。
3. 如果未列出负载均衡器端点，请选中要删除的每个 HA 组的复选框。
4. 选择*操作* > 删除 HA 组。
5. 查看消息并选择 **Delete HA group** 以确认您的选择。

您选择的所有 HA 组均已删除。"高可用性组"页面上将显示绿色成功横幅。

管理负载均衡

了解 StorageGRID 负载均衡

您可以使用负载均衡来处理来自 S3 客户端的接收和检索工作负载。

什么是负载均衡？

当客户端应用程序从 StorageGRID 系统保存或检索数据时，StorageGRID 使用负载均衡器来管理摄取和检索工作负载。负载均衡通过将工作负载分布在多个存储节点上，最大限度地提高速度和连接容量。

StorageGRID 负载均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 层负载均衡。它执行客户端请求的传输层安全性 (TLS) 终止，检查请求，并建立到存储节点的新安全连接。

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



虽然 StorageGRID 负载均衡器服务是推荐的负载均衡机制，但您可能需要集成第三方负载均衡器。有关信息，请联系您的 NetApp 客户代表或参阅 ["将第三方负载均衡器与 StorageGRID 结合使用"](#)。

我需要多少个负载均衡节点？

作为一般最佳做法，StorageGRID 系统中的每个站点都应包含具有负载均衡器服务的两个或多个节点。例如，站点可能包括两个网关节点，或者同时包括管理节点和网关节点。确保每个负载均衡节点都有足够的网络、硬件或虚拟化基础架构，无论您是使用服务设备、裸机节点还是基于虚拟机 (VM) 的节点。

什么是负载均衡器端点？

负载均衡器端点定义传入和传出客户端应用程序请求将用于访问包含负载均衡器服务的那些节点的端口和网络协议 (HTTPS 或 HTTP)。端点还定义了客户端类型 (S3)、绑定模式，以及可选的允许或阻止的租户列表。

要创建负载均衡器端点，请使用 Grid Manager 或完成 S3 设置和 FabricPool 向导：

- ["配置负载均衡器端点"](#)
- ["使用 S3 设置向导"](#)
- ["使用 FabricPool 设置向导"](#)

负载均衡器缓存的注意事项

当工作负载对数据子集进行操作并多次访问对象时，缓存会显著提高性能。此外，缓存提供对对象存储的远程访问，而无需完整的网格部署。负载均衡器缓存仅适用于网关节点。

创建负载均衡器端点时：

- 仅对可缓存的工作负载启用缓存。与未缓存数据相比，访问缓存数据频率更低的工作负载，其性能将比未使用缓存服务时更差。在某些情况下，覆盖率和逐出率较高的工作负载也可能超过保修的驱动器写入耐久性。
- 考虑添加额外的端点或节点，以缓存适合缓存的各个工作负载。
- 对可缓存和不可缓存的工作负载使用不同的端点。这种分离可确保适当应用缓存机制，并且不会干扰不可缓存的数据处理。
- 通过将其定向到启用缓存的端点来评估潜在的可缓存工作负载。监控并验证缓存命中率，以确定工作负载是否适合缓存。此评估有助于优化性能并确保高效使用缓存资源。
- ["查看审核日志"](#) 以确定现有工作负载是否适合缓存。在给定的时间段内，确定唯一对象的 GET 百分比。要适合缓存，此值应低于 50%。

可能适合缓存的工作负载示例

- 数据湖
- 高性能计算 (HPC)
- AI/ML 训练
- 内容分发网络 (CDN)
- 媒体资产管理
- 视频制作



- 可以缓存多个对象版本。
- 支持范围读取操作。

不适合缓存的工作负载示例

- Fabric Pool
- 备份应用程序
- 存储分层



如果要由缓存提供的任何内容需要静态加密，["启用节点或驱动器加密"](#)在缓存节点上。

不会缓存的对象和请求的类型

- The response-content-encoding 查询参数
- The partNumber 查询参数
- 条件标头
 - If-Match
 - If-Modified-Since
 - If-None-Match
 - If-Unmodified-Since
- 使用以下任何内容进行静态加密的请求：
 - SSE（使用 StorageGRID 管理的密钥的服务器端加密）
 - SSE-C（使用客户提供的密钥的服务器端加密）
 - 存储对象加密

未缓存的任何请求都将转发到上游 LDR，就像未启用缓存一样。

相关信息

- ["对负载均衡器缓存进行故障排除"](#)
- 有关负载均衡器缓存的详细信息，请与技术支持联系。

端口注意事项

对于您创建的第一个端点，负载均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。如果您使用端口 80 或 443，则端点将仅在网关节点上使用负载均衡器服务。这些端口在管理节点上保留。如果您对多个端点使用相同的端口，则必须为每个端点指定不同的绑定模式。

不允许使用其他网格服务所用的端口。请参阅["StorageGRID 内部端口"](#)。

网络协议的注意事项

在大多数情况下，客户端应用程序与 StorageGRID 之间的连接应使用传输层安全性 (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 负载均衡器端点选择网络协议时，应选择 **HTTPS**。

负载均衡器端点证书的注意事项

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

- 上传已签名的证书（推荐）。此证书可以由公用信任的证书颁发机构或专用证书颁发机构 (CA) 签名。使用公开可信的 CA 服务器证书来保护连接是最佳做法。与生成的证书不同，由 CA 签名的证书可以无中断地轮换，这有助于避免过期问题。

在创建负载均衡器端点之前，必须获取以下文件：

- 自定义服务器证书文件。

- 自定义服务器证书私钥文件。
- 可选，来自每个中间颁发证书颁发机构的证书的 CA 捆绑包。
- 生成自签名证书。
- 使用全局 **StorageGRID S3** 证书。必须上传或生成此证书的自定义版本，然后才能将其选择用于负载平衡器端点。请参阅 ["配置 S3 API 证书"](#)。

我需要哪些值？

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

证书的使用者 **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，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 虚拟托管样式请求，则证书还必须为您配置的每个 **"S3端点域名"** 包含*备用名称*条目，包括任何通配符名称。例如：

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



如果对域名使用通配符，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 DNS 条目。

如何管理过期的证书？



如果用于保护 S3 应用程序和 StorageGRID 之间连接的证书过期，则应用程序可能会暂时失去对 StorageGRID 的访问权限。

要避免证书过期问题，请遵循以下最佳实践：

- 仔细监控任何警告证书过期日期即将到来的警报，例如*负载平衡器端点证书过期*和*S3 API 全局服务器证书过期*警报。
- 始终保持 StorageGRID 和 S3 应用程序的证书版本同步。如果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。
- 使用公开签名的 CA 证书。如果使用由 CA 签名的证书，则可以无中断地替换即将过期的证书。
- 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

绑定模式可让您控制哪些 IP 地址可用于访问负载均衡器端点。如果端点使用绑定模式，则客户端应用程序只有在使用允许的 IP 地址或其相应的完全限定域名 (FQDN) 时才能访问端点。使用任何其他 IP 地址或 FQDN 的客户端应用程序无法访问端点。

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、任何网络上的任何 HA 组的虚拟 IP (VIP) 地址或相应的 FQDN 来访问端点。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**。客户端必须使用所选节点接口的 IP 地址（或相应的 FQDN）。
- **节点类型**。根据您选择的节点类型，客户端必须使用任意管理节点的 IP 地址（或相应的 FQDN）或任意网关节点的 IP 地址（或相应的 FQDN）。

租户访问的注意事项

租户访问是一项可选安全功能，允许您控制哪些 StorageGRID 租户帐户可以使用负载均衡器端点来访问其存储桶。您可以允许所有租户访问端点（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拥有的绝密或高度机密的材料对其他租户完全不可访问。



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确定的，如果请求中未提供访问密钥（例如匿名访问），则使用存储桶所有者来确定租户。

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. 您已创建两个负载均衡器端点，如下所示：
 - ***公共***端点：使用端口 10443，并允许访问所有租户。
 - **Top secret** 端点：使用端口 10444，仅允许访问 **Top secret** 租户。所有其他租户均无法访问此端点。
2. The `top-secret.pdf` 位于*绝密*租户拥有的存储桶中。

要访问 `top-secret.pdf`，*绝密*租户中的用户可以向 `\https://w.x.y.z:10444/top-secret.pdf` 发出 GET 请求。由于允许此租户使用 10444 端点，因此用户可以访问该对象。但是，如果属于任何其他租户的用户向相同的 URL 发出相同的请求，则会立即收到“拒绝访问”消息。即使凭据和签名有效，也会拒绝访问。

CPU可用性

每个管理节点和网关节点上的负载均衡器服务在将 S3 流量转发到存储节点时独立运行。通过加权过程，负载均衡器服务将更多请求路由到具有更高 CPU 可用性的存储节点。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 100% 的利用率或未能报告其利用率，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均衡器服务所在的站点。

配置 StorageGRID 负载均衡器端点

负载均衡器端点确定 S3 客户端在连接到网关和管理节点上的 StorageGRID 负载均衡器时可以使用的端口和网络协议。您还可以使用端点访问 Grid Manager、Tenant Manager 或两者。

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到网格管理器。
- 您有 ["root 访问权限"](#)。
- 您已审阅 ["负载均衡的注意事项"](#)。
- 如果您之前重新映射了要用于负载均衡器端点的端口，则您有 ["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，但不是必需的。请参阅 ["管理高可用性组"](#)。
- 如果负载均衡器端点将由 ["S3 Select 的 S3 租户"](#) 使用，则不得使用任何裸机节点的 IP 地址或 FQDN。用于 S3 Select 的负载均衡器端点仅允许使用服务设备和基于 VMware 的软件节点。
- 已配置计划使用的任何 VLAN 接口。请参阅 ["配置 VLAN 接口"](#)。
- 如果要创建 HTTPS 端点（推荐），则需要具备服务器证书的相关信息。



对端点证书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，需要服务器证书、证书私钥以及 CA 捆绑包（可选）。
- 要生成证书，您需要 S3 客户端用于访问端点的所有域名和 IP 地址。您还必须了解主题（可分辨名称）。
- 如果要使用 StorageGRID S3 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。请参阅 ["配置 S3 API 证书"](#)。

创建负载均衡器端点

每个 S3 客户端负载均衡器端点都指定端口、客户端类型 (S3) 和网络协议 (HTTP 或 HTTPS)。管理接口负载均衡器端点指定端口、接口类型和不受信任的客户端网络。

访问此向导

步骤

1. 选择*配置* > 网络 > 负载均衡器端点。
2. 要为 S3 客户端创建端点，请选择 **S3 client** 选项卡。
3. 要创建用于访问 Grid Manager、Tenant Manager 或两者的端点，请选择*管理界面*选项卡。
4. 选择 **Create**。

输入端点详细信息

步骤

1. 选择适当的说明以输入要创建的端点类型的详细信息。

S3客户端

字段	问题描述
名称	端点的描述性名称，将显示在负载均衡器端点页面的表格中。
端口	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 1 到 65535 之间的任何未使用的外部端口。 如果您输入 80 或 8443，则仅在网关节点上配置端点，除非您已释放端口 8443。然后，您可以使用端口 8443 作为 S3 端点，该端口将在网关节点和管理节点上进行配置。
客户端类型	必须是 S3 。
网络协议	客户端在连接到此端点时将使用的网络协议。 • 选择 HTTPS 进行安全的 TLS 加密通信（推荐）。必须先附加安全证书，然后才能保存端点。 • 选择 HTTP 进行不太安全的未加密通信。仅对非生产网格使用 HTTP。
启用缓存	为此负载均衡器端点启用或禁用 "网关节点上的缓存"。 如果缓存出现问题，请参阅 "对负载均衡器缓存进行故障排除"。

管理界面

字段	问题描述
名称	端点的描述性名称，将显示在负载均衡器端点页面的表格中。
端口	要用于访问 Grid Manager、Tenant Manager 或两者的 StorageGRID 端口。 • 网格管理器：8443 • 租户管理器：9443 • Grid Manager 和 Tenant Manager：443 注意：您可以使用这些预设端口或其他可用端口。
接口类型	选择您将使用此端点访问的 StorageGRID 接口的单选按钮。

字段	问题描述
不受信任的客户端网络	如果此端点应可供不受信任的客户端网络访问，请选择*是*。否则，请选择*否*。 当您选择*是*时，该端口将在所有不受信任的客户端网络上打开。 注意：创建负载均衡器端点时，只能将端口配置为对不受信任的客户端网络开放或关闭。

1. 选择 **Continue**。

选择绑定模式

步骤

1. 选择端点的绑定模式，以控制使用任何 IP 地址或使用特定 IP 地址和网络接口访问端点的方式。

某些绑定模式可用于客户端端点或管理接口端点。此处列出了两种端点类型的所有模式。

模式	问题描述
全局(客户端端点的默认值)	客户端可以使用任何网关节点或管理节点的 IP 地址、任何网络上的任何 HA 组的虚拟 IP (VIP) 地址或相应的 FQDN 来访问端点。 除非需要限制此端点的可访问性，否则请使用*全局*设置。
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）来访问此端点。 具有此绑定模式的端点都可以使用相同的端口号，只要您为端点选择的 HA 组不重叠即可。
节点接口	<code>#{post_edited_translations.segment}</code>
节点类型（仅限客户端端点）	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。
所有管理节点（管理接口端点的默认值）	客户端必须使用任何管理节点的 IP 地址（或相应的 FQDN）来访问此端点。

如果多个端点使用相同的端口，StorageGRID 使用此优先级顺序来决定使用哪个端点：**HA 组的虚拟 IP** > 节点接口 > 节点类型 > 全局。

如果要创建管理接口端点，则仅允许使用管理节点。

2. 如果您选择了 **Virtual IPs of HA groups**，请选择一个或多个 HA 组。

如果要创建管理界面端点，请选择仅与管理节点关联的 VIP。

- 3. 如果选择*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. 如果您选择了*节点类型*，请选择管理节点（其中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



只有当终结点具有 **Tenant Manager 的接口类型** 时，管理接口终结点才能控制租户访问。

步骤

- 1. 对于*租户访问*步骤，请选择以下选项之一：

字段	问题描述
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存储区。 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，可以编辑负载均衡器端点以允许或阻止特定帐户。
允许选定的租户	只有选定租户帐户可以使用此端点访问其存储桶。
阻止选定租户	选定的租户帐户无法使用此端点来访问其存储桶。所有其他租户都可以使用此端点。

- 2. 如果您正在创建 **HTTP** 端点，则无需附加证书。选择 **创建** 以添加新的负载均衡器端点。然后，转到 **完成后**。否则，选择 **继续** 以附加证书。

`${post_edited_translations.segment}`

步骤

- 1. `${post_edited_translations.segment}`

该证书保护 S3 客户端与管理节点或网关节点上的负载均衡器服务之间的连接。

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

除非您已将由网格 CA 签名的默认 S3 API 证书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 API 证书"**。

- 使用管理接口证书。如果您要使用全局管理接口证书，请选择此选项，该证书也可用于直接连接到 Admin Nodes。

- 2. `${post_edited_translations.segment}`

上传证书

- a. 选择*上传证书*。
- b. 上传所需的服务器证书文件：
 - `${post_edited_translations.segment}`
 - 证书私钥：自定义服务器证书私钥文件（.key）。



EC 私钥必须为 224 位或更大。RSA 私钥必须为 2048 位或更大。

- **CA bundle**：包含来自每个中间颁发证书颁发机构 (CA) 的证书的单个可选文件。该文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。
- 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 捆绑包，则每个证书都会显示在自己的选项卡上。
 - 选择*下载证书*保存证书文件，或选择*下载 CA 捆绑包*保存证书捆绑包。

指定证书文件名和下载位置。使用扩展名 .pem 保存文件。

例如：storagegrid_certificate.pem

- `${post_edited_translations.segment}`
- d. 选择 **Create**。+ 此时将创建负载均衡器端点。自定义证书将用于 S3 客户端或管理界面与该端点之间后续的所有新连接。

生成证书

- a. 选择*生成证书*。
- b. 指定证书信息：

字段	问题描述
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 主题或标识名 (DN)。 如果在此字段中未输入任何值，则生成的证书将使用第一个域名或 IP 地址作为使用者通用名称 (CN)。
有效天数	创建后证书过期的天数。

字段	问题描述
添加密钥使用扩展	<code>\${post_edited_translations.segment}</code>
	<code>\${post_edited_translations.segment}</code>
	<code>\${post_edited_translations.segment}</code>

c. 选择 **Generate**。

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 `.pem` 保存文件。

例如: `storagegrid_certificate.pem`

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

e. 选择 **Create**。

已创建负载均衡器端点。自定义证书用于 S3 客户端或管理接口与此端点之间的所有后续新连接。

完成后

步骤

1. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

2. 请向 S3 客户端提供连接到端点所需的信息：

- `${post_edited_translations.segment}`
- 完全限定的域名或 IP 地址
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

您可以查看现有负载均衡器端点的详细信息，包括安全端点的证书元数据。您可以更改端点的某些设置。

- `${post_edited_translations.segment}`
- 要查看有关特定端点的所有详细信息（包括证书元数据），请在表中选择该端点的名称。显示的信息因端点类型及其配置方式而异。

S3 load balancer endpoint

Port:

10443

Client type:

S3

Network protocol:

HTTPS

Binding mode:

Global

Endpoint ID:

3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

• `${post_edited_translations.segment}`

- 

如果在编辑管理接口端点端口时无法访问 Grid Manager，请更新 URL 和端口以重新获得访问权限。
- 

`${post_edited_translations.segment}`

任务	<code>\${post_edited_translations.segment}</code>	详细信息页面
编辑端点名称	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点名称。 c. 输入新名称。 d. 选择 Save 。	a. <code>\${post_edited_translations.segment}</code> b. 选择编辑图标  。 c. 输入新名称。 d. 选择 Save 。
<code>\${post_edited_translations.segment}</code>	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点端口 c. <code>\${post_edited_translations.segment}</code> d. 选择 Save 。	不适用

任务	<code>\${post_edited_translations.segment}</code>	详细信息页面
编辑端点绑定模式	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点绑定模式。 c. <code>\${post_edited_translations.segment}</code> d. 选择 Save changes 。	a. <code>\${post_edited_translations.segment}</code> b. 选择*编辑绑定模式*。 c. <code>\${post_edited_translations.segment}</code> d. 选择 Save changes 。
编辑端点证书	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点证书。 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 证书。 d. 选择 Save changes 。	a. <code>\${post_edited_translations.segment}</code> b. 选择 Certificate 选项卡。 c. <code>\${post_edited_translations.segment}</code> 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 证书。 e. 选择 Save changes 。
<code>\${post_edited_translations.segment}</code>	a. 选中端点的复选框。 b. <code>\${post_edited_translations.segment}</code> c. 选择其他访问选项，从列表中选择或删除租户，或同时执行这两项操作。 d. 选择 Save changes 。	a. <code>\${post_edited_translations.segment}</code> b. <code>\${post_edited_translations.segment}</code> c. 选择*编辑租户访问权限*。 d. 选择其他访问选项，从列表中选择或删除租户，或同时执行这两项操作。 e. 选择 Save changes 。

删除负载均衡器端点

`${post_edited_translations.segment}`



为防止客户端中断，请在删除负载均衡器端点之前更新任何受影响的 S3 客户端应用程序。更新每个客户端，使其使用分配给另一个负载均衡器端点的端口进行连接。请务必同时更新任何所需的证书信息。



`${post_edited_translations.segment}`

- 要删除一个或多个端点：
 - a. 从"负载均衡器"页面中，选中要删除的每个端点的复选框。
 - b. 选择*操作* > 删除。
 - c. 选择 **OK**。
- 从详细信息页面中删除一个端点：
 - a. 从负载均衡器页面，选择端点名称。
 - b. 在详细信息页面上选择*移除*。
 - c. 选择 **OK**。

在 StorageGRID 中配置 S3 端点域名

要支持 S3 虚拟托管样式的请求，必须使用 Grid Manager 配置 S3 客户端连接到的 S3 端点域名列表。



不支持为端点域名使用 IP 地址。未来的版本将阻止此配置。

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到网格管理器。
- 您有 ["特定访问权限"](#)。
- 您已确认未进行网格升级。



正在进行网格升级时，请勿对域名配置进行任何更改。

关于此任务

要使客户端能够使用 S3 端点域名，必须执行以下所有操作：

- `${post_edited_translations.segment}`
- 确保已针对客户端所需的所有域名对 ["客户端用于与 StorageGRID 建立 HTTPS 连接的证书"](#) 进行了签名。

例如，如果端点为 `s3.company.com`，则必须确保用于 HTTPS 连接的证书包含 `s3.company.com` 端点以及该端点的通配符主题备用名称 (SAN)： `*.s3.company.com`。

- 配置客户端使用的 DNS 服务器。包含客户端用于建立连接的 IP 地址的 DNS 记录，并确保这些记录引用所有必需的 S3 端点域名，包括任何通配符名称。



客户端可以使用网关节点、管理节点或存储节点的 IP 地址连接到 StorageGRID，也可以通过连接到高可用性组的虚拟 IP 地址进行连接。您应该了解客户端应用程序如何连接到网格，以便在 DNS 记录中包含正确的 IP 地址。

`${post_edited_translations.segment}`

- 连接到负载均衡器端点的客户端可以使用该端点的自定义证书。每个负载均衡器端点都可以配置为识别不同的 S3 端点域名。
- `${post_edited_translations.segment}`



`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

步骤

1. 选择 **配置** > **网络** > **S3 端点域名**。
2. 在 **Domain name 1** 字段中输入域名。选择 **Add another domain name** 以添加更多域名。
3. 选择 **Save**。

4. 确保客户端使用的服务器证书与所需的 S3 端点域名匹配。
 - 如果客户端连接到使用其自己的证书的负载平衡器端点，"[更新与端点关联的证书](#)"。
 - 如果客户端连接到使用全局 S3 API 证书的负载平衡器端点或直接连接到存储节点，则 "[更新全局 S3 API 证书](#)"。
5. 添加确保可以解析端点域名请求所需的 DNS 记录。

结果

现在，当客户端使用端点 `bucket.s3.company.com` 时，DNS 服务器解析到正确的端点，证书按预期对端点进行身份验证。

重命名 S3 端点域名

如果更改 S3 应用程序使用的名称，则虚拟托管样式的请求将失败。

步骤

1. 选择*配置* > 网络 > **S3** 端点域名。
2. 选择要编辑的域名字段并进行必要的更改。
3. 选择 **Save**。
4. 选择*是*以确认更改。

删除 S3 端点域名

如果删除 S3 应用程序使用的名称，则虚拟托管风格的请求将失败。

步骤

1. 选择*配置* > 网络 > **S3** 端点域名。
2. 选择域名旁边的删除图标 .
3. 选择*是*确认删除。

相关信息

- "[使用 S3 REST API](#)"
- "[查看 IP 地址](#)"
- "[配置高可用性组](#)"

StorageGRID 客户端连接的 IP 地址和端口

`${post_edited_translations.segment}`

客户端应用程序可以使用网格节点的 IP 地址和该节点上的服务端口号连接到 StorageGRID。也可以创建负载平衡节点的高可用性 (HA) 组，以提供使用虚拟 IP (VIP) 地址的高可用性连接。如果要使用完全限定域名 (FQDN) 而不是 IP 或 VIP 地址连接到 StorageGRID，可以配置 DNS 条目。

下表总结了客户端连接到 StorageGRID 的不同方式，以及每种连接类型所使用的 IP 地址和端口。如果您已创建负载均衡器端点和高可用性 (HA) 组，请参见 `<<${post_edited_translations.segment}>>` 以在 Grid Manager 中

找到这些值。

在何处进行连接	<code>\${post_edited_translations.segment}</code>	IP 地址	端口
HA 组	负载均衡器	HA 组的虚拟 IP 地址	<code>\${post_edited_translations.segment}</code>
管理节点	负载均衡器	管理节点的 IP 地址	<code>\${post_edited_translations.segment}</code>
网关节点	负载均衡器	网关节点的 IP 地址	<code>\${post_edited_translations.segment}</code>
存储节点	LDR	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code> • HTTPS: 18082 • HTTP: 18084

示例 URL

要将客户端应用程序连接到网关节点的 HA 组的负载均衡器端点，请使用如下所示的 URL 结构：

`https://VIP-of-HA-group:LB-endpoint-port`

`${post_edited_translations.segment}`

`https://192.0.2.5:10443`

`${post_edited_translations.segment}`

1. 使用 "支持的 Web 浏览器" 登录到网格管理器。
2. 要查找网格节点的 IP 地址：
 - a. 选择 **Nodes**。
 - b. `${post_edited_translations.segment}`
 - c. 选择 **Overview** 选项卡。
 - d. 在节点信息部分，记下节点的 IP 地址。
 - e. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`
 - `${post_edited_translations.segment}`
 - **eth1**: 管理网络（可选）
 - **eth2**: 客户端网络（可选）



`${post_edited_translations.segment}`

3. 要查找高可用性组的虚拟 IP 地址，请执行以下操作：

- a. 选择*配置* > 网络 > 高可用性组。
- b. `${post_edited_translations.segment}`

4. `${post_edited_translations.segment}`

- a. 选择*配置* > 网络 > 负载均衡器端点。
- b. 请记住要使用的端点的端口号。



如果端口号为 80 或 443，则仅在网关节点上配置端点，因为这些端口在管理节点上保留。所有其他端口都配置在网关节点和管理节点上。

- c. `${post_edited_translations.segment}`
- d. `${post_edited_translations.segment}`

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。