配置客户端连接

StorageGRID 11.8

NetApp
May 17, 2024

目录

配置客户端连接

配置S3和Swift客户端连接：概述

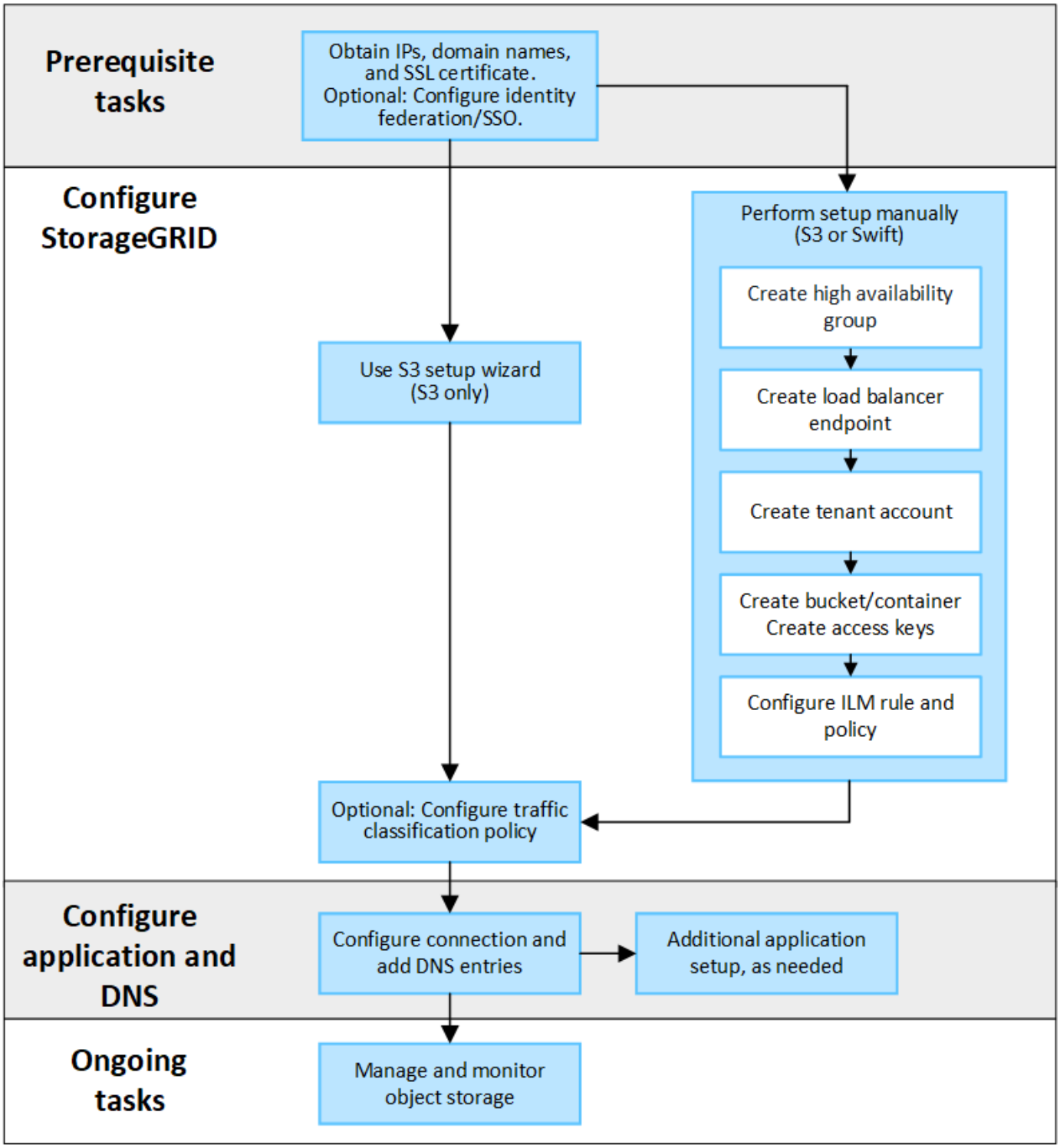
作为网格管理员、您可以管理一些配置选项、这些配置选项用于控制S3和Swift客户端应用程序如何连接到StorageGRID 系统以存储和检索数据。

> 对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

配置工作流

如工作流图所示、将StorageGRID 连接到任何S3或Swift应用程序主要有四个步骤：

1. 根据客户端应用程序连接到StorageGRID 的方式、在StorageGRID 中执行必备任务。
2. 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。
3. 使用S3或Swift应用程序完成与StorageGRID 的连接。创建DNS条目以将IP地址与计划使用的任何域名关联起来。
4. 在应用程序和StorageGRID 中执行持续任务、以管理和监控一段时间内的对象存储。



将StorageGRID 连接到客户端应用程序所需的信息

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

我需要什么值?

下表显示了您必须在StorageGRID 中配置的值、以及S3或Swift应用程序和DNS服务器使用这些值的位置。

价值	其中、值已配置	使用值的位置
虚拟IP (VIP)地址	StorageGRID > HA组	DNS条目
Port	StorageGRID >负载平衡器端点	客户端应用程序
SSL 证书	StorageGRID >负载平衡器端点	客户端应用程序
服务器名称(FQDN)	StorageGRID >负载平衡器端点	• 客户端应用程序 • DNS条目
S3访问密钥ID和机密访问密钥	StorageGRID >租户和存储分段	客户端应用程序
存储分段/容器名称	StorageGRID >租户和存储分段	客户端应用程序

如何获取这些值?

根据您的要求、您可以执行以下任一操作来获取所需信息:

- *使用 "S3设置向导"*S3设置向导可帮助您在StorageGRID 中快速配置所需的值、并输出一个或两个文件、您可以在配置S3应用程序时使用这些文件。此向导将指导您完成所需的步骤、并帮助您确保设置符合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、否则实施需要大量自定义。

- *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。

  > 如果您计划使用StorageGRID 作为FabricPool 云层的对象存储系统、建议使用FabricPool 设置向导、除非您知道自己有特殊要求或实施需要大量自定义。

- 手动配置项目。如果您要连接到Swift应用程序(或者要连接到S3应用程序而不想使用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或Swift应用程序的高可用性(HA)组。请参见 "配置高可用性组"。
  b. 创建S3或Swift应用程序要使用的负载平衡器端点。请参见 "配置负载平衡器端点"。
  c. 创建S3或Swift应用程序要使用的租户帐户。请参见 "创建租户帐户"。
  d. 对于S3租户、请登录到租户帐户、并为要访问该应用程序的每个用户生成访问密钥ID和机密访问密钥。请参见 "创建您自己的访问密钥"。
  e. 在租户帐户中创建一个或多个S3存储分段或Swift容器。对于S3、请参见 "创建 S3 存储分段"。对于Swift、请使用 "放置容器请求"。
  f. 要为属于新租户或存储分段/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。请参见 "创建 ILM 规则" 和 "创建 ILM 策略"。

S3或Swift客户端的安全性

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

摘要

下表总结了如何为S3和Swift REST API实施安全性：

Security 问题描述	实施 **REST API**
连接安全性	TLS
服务器身份验证	系统 CA 签名的 X.509 服务器证书或管理员提供的自定义服务器证书
客户端身份验证	**S3** S3帐户(访问密钥ID和机密访问密钥) **Swift** Swift帐户(用户名和密码)
客户端授权	**S3** 存储分段所有权和所有适用的访问控制策略 **Swift** 管理员角色访问

StorageGRID如何为客户端应用程序提供安全性

S3和Swift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平衡器服务、也可以直接连接到存储节点。

- 连接到负载平衡器服务的客户端可以根据您的方式使用HTTPS或HTTP "配置负载平衡器端点"。

  建议使用HTTPS提供安全的TLS加密通信。您必须向端点附加安全证书。

  HTTP提供的未加密通信安全性较低、只能用于非生产或测试网格。

- 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提供的未加密通信安全性较低、但也可以选择 "enabled" 用于非生产或测试网格。

- StorageGRID 与客户端之间的通信使用 TLS 进行加密。
- 无论将负载平衡器端点配置为接受 HTTP 或 HTTPS 连接，网格中的负载平衡器服务和存储节点之间的通信都会进行加密。
- 客户端必须向 StorageGRID 提供 HTTP 身份验证标头，才能执行 REST API 操作。请参见 "对请求进行身

份验证" 和 "支持的 Swift API 端点"。

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平衡器服务时、它们将使用为负载平衡器端点配置的证书。每个负载平衡器端点都有自己的证书##8212;网格管理员上传的自定义服务器证书，或者网格管理员在配置端点时在StorageGRID中生成的证书。

  请参见 "负载平衡注意事项"。

- 当客户端应用程序直接连接到存储节点时、它们会使用系统生成的服务器证书、这些证书是在安装StorageGRID 系统时为存储节点生成的(由系统证书颁发机构签名)。 或网格管理员为网格提供的单个自定义服务器证书。请参见 "添加自定义S3或Swift API证书"。

应将客户端配置为信任对用于建立 TLS 连接的任何证书签名的证书颁发机构。

支持 TLS 库的哈希和加密算法

StorageGRID系统支持一组密码套件、客户端应用程序可以在建立TLS会话时使用这些套件。要配置加密方法，请进入*configuration*>*Security*>*Security settings，然后选择*TLS和SSH policies*。

支持的 TLS 版本

StorageGRID 支持 TLS 1.2 和 TLS 1.3 。

> 不再支持 SSLv3 和 TLS 1.1 （或更早版本）。

使用S3设置向导

使用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。完成此向导期间、您可以下载一些文件、用于在S3应用程序中输入值。使用向导可以更快地配置系统、并确保您的设置符合StorageGRID 最佳实践。

如果您有 "root访问权限"，您可以在开始使用StorageGRID网格管理器时完成S3设置向导，也可以稍后访问并完成该向导。根据您的要求、您还可以手动配置部分或全部所需项、然后使用向导收集S3应用程序所需的值。

在使用向导之前

在使用向导之前、请确认您已满足这些前提条件。

获取**IP**地址并设置**VLAN**接口

如果要配置高可用性(HA)组、您就知道S3应用程序要连接到哪些节点以及要使用哪些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将流量与S3应用程序隔离、则已配置VLAN接口。请参见 "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。此外、您还知道哪个联盟组应该对S3应用程序要使用的租户帐户具有root访问权限。请参见 "使用身份联合" 和 "配置单点登录"。

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映射到您使用向导创建的HA组的虚拟IP (VIP)地址。

如果您计划使用S3虚拟托管模式请求、则应具有 "已配置S3端点域名"。建议使用虚拟托管模式请求。

查看负载平衡器和安全证书要求

如果您计划使用StorageGRID 负载平衡器、则已查看负载平衡的一般注意事项。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)负载平衡器端点、则具有该负载平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分段对象复制到另一个网格、请在启动向导之前确认以下内容：

- 您已拥有 "已配置网格联合连接"。
- 连接状态为*已连接*。
- 您具有 root 访问权限。

访问并完成**S3**设置向导

您可以使用S3设置向导配置StorageGRID 以用于S3应用程序。设置向导提供了应用程序访问StorageGRID 存储分段和保存对象所需的值。

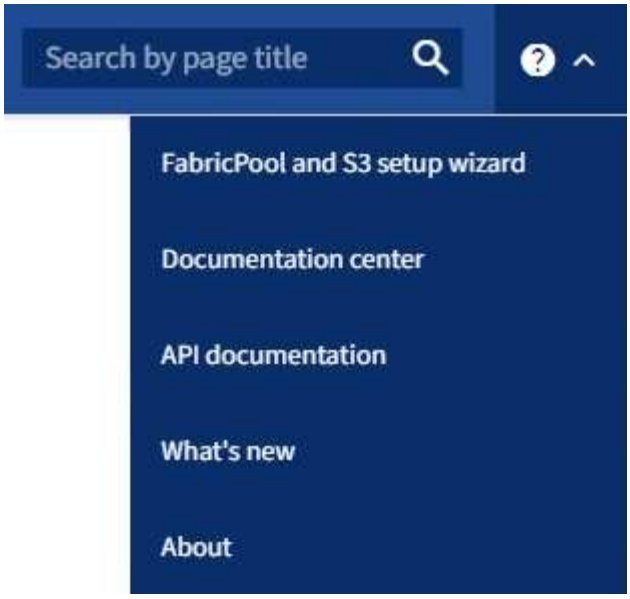
开始之前

- 您拥有 "root访问权限"。
- 您已查看 "注意事项和要求" 用于使用向导。

访问向导

步骤

1. 使用登录到网格管理器 "支持的 Web 浏览器"。
2. 如果信息板上显示了FabricPool and S3 setup wizard*横幅，请选择横幅中的链接。如果横幅不再显示，请从网格管理器的标题栏中选择帮助图标，然后选择FabricPool and S3 setup wizard*。



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

第**1**步(共**6**步)：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、管理节点或同时包含这两者。

您可以使用HA组帮助保持S3数据连接可用。如果HA组中的活动接口发生故障、备份接口可以管理工作负载、而对S3操作的影响微乎其微。

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平衡器、则无需创建HA组。选择*跳过此步骤*并转到 [第2步(共6步)：配置负载平衡器端点]。
2. 要使用StorageGRID 负载平衡器、您可以创建新的HA组或使用现有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	**Description**
HA组名称	此HA组的唯一显示名称。
问题描述 (可选)	此HA组的问题描述。

c. 对于*Add interfaces*步骤，选择要在此HA组中使用的节点接口。

使用列标题对行进行排序，或者输入搜索词以更快地找到接口。

您可以选择一个或多个节点、但只能为每个节点选择一个接口。

d. 对于“确定接口优先级”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主接口。主接口是活动接口，除非发生故障。

如果HA组包含多个接口、而活动接口发生故障、则虚拟IP (VIP)地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。解决故障后、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	**Description**
Subnet CIDR	采用CIDR表示法的VIP子网地址&#8212；后跟斜杠的IPv4地址和子网长度(0-32)。 网络地址不能设置任何主机位。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地址不在同一子网上、请输入StorageGRID VIP本地网关IP地址。本地网关 IP 地址必须位于 VIP 子网中。
虚拟IP地址	为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网内。 必须至少有一个地址为IPv4。您也可以指定其他 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*以转到负载平衡器步骤。

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*以转到负载平衡器步骤。

第**2**步**(**共**6**步**)**：配置负载平衡器端点

StorageGRID 使用负载平衡器管理客户端应用程序中的工作负载。负载平衡可最大限度地提高多个存储节点的速度和连接容量。

您可以使用所有网关和管理节点上的StorageGRID 负载平衡器服务、也可以连接到外部(第三方)负载平衡器。建议使用StorageGRID 负载平衡器。

有关此任务的详细信息，请参见 "负载平衡注意事项"。

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

创建端点

步骤

1. 要创建负载平衡器端点，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	Description
Name	端点的描述性名称。
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、因为这些端口是在管理节点上预留的。 *注意：*不允许使用其他网格服务使用的端口。请参见 "网络端口参考"。
客户端类型	必须为*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。绑定模式控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

模式	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。 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。 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。

4. 对于租户访问步骤、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。
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。

5. 对于*attach certificer*步骤，选择以下选项之一：

字段	Description
上传证书(建议)	使用此选项可上传CA签名的服务器证书、证书专用密钥和可选的CA包。
生成证书	使用此选项可生成自签名证书。请参见 "配置负载平衡器端点" 有关输入内容的详细信息。
使用StorageGRID S3和Swift证书	仅当您已上传或生成自定义版本的StorageGRID 全局证书时、才使用此选项。请参见 "配置 S3 和 Swift API 证书" 了解详细信息。

6. 选择*完成*以返回S3设置向导。
7. 选择*继续*转到租户和存储分段步骤。

> 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。

使用现有负载平衡器端点

步骤

1. 要使用现有端点，请从*选择负载平衡器端点*中选择其名称。
2. 选择*继续*转到租户和存储分段步骤。

使用外部负载平衡器

步骤

1. 要使用外部负载平衡器、请填写以下字段。

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

2. 选择*继续*转到租户和存储分段步骤。

第3步(共6步)：创建租户和存储分段

租户是一种可以使用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、分段、对象和一组特定功能。您必须先创建租户、然后才能创建S3应用程序用于存储其对象的存储分段。

分段是一种用于存储租户对象和对象元数据的容器。虽然某些租户可能具有许多存储分段、但此向导可帮助您以最快、最简单的方式创建租户和存储分段。您可以稍后使用租户管理器添加所需的任何其他分段。

您可以为此S3应用程序创建一个新租户。您也可以选择为新租户创建存储分段。最后、您可以允许向导为租户的root用户创建S3访问密钥。

有关此任务的详细信息，请参见 "创建租户帐户" 和 "创建 S3 存储分段"。

步骤

1. 选择 * 创建租户 * 。
2. 对于输入详细信息步骤、请输入以下信息。

字段	Description
Name	租户帐户的名称。租户名称不需要唯一。创建租户帐户时，它会收到一个唯一的数字帐户 ID 。
问题描述 (可选)	用于帮助识别租户的问题描述。
客户端类型	此租户将使用的客户端协议类型。对于S3设置向导，已选择*S3*，并且该字段已禁用。
存储配额(可选)	如果希望此租户具有存储配额、则为配额和单位指定一个数值。

3. 选择 * 继续 * 。
4. (可选)选择希望此租户拥有的任何权限。

其中某些权限还有其他要求。有关详细信息、请选择每个权限的帮助图标。

权限	如果选择...
允许平台服务	租户可以使用CloudMirror等S3平台服务。请参见 "管理 S3 租户帐户的平台服务"。
使用自己的身份源	租户可以为联盟组和用户配置和管理自己的身份源。如果您有、此选项将被禁用 "已配置SSO" 适用于您的StorageGRID 系统。

权限	如果选择...
允许S3选择	租户可以通过问题描述 S3选择对象内容API请求筛选和检索对象数据。请参见 "管理租户帐户的 S3 Select"。 重要：选择对象内容请求会降低所有S3客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。
使用网格联合连接	租户可以使用网格联合连接。 选择此选项： • 使此租户以及添加到帐户的所有租户组和用户从此网格(_ssource grid _)克隆到选定连接中的另一网格(_dDestination grid _)。 • 允许此租户在每个网格上的相应分段之间配置跨网格复制。 请参见 "管理网格联盟允许的租户"。

5. 如果选择了*使用网格联合连接*，请选择一个可用的网格联合连接。
6. 根据StorageGRID 系统是否使用、定义租户帐户的root访问权限 "身份联合"， "单点登录(SSO)"或两者。

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要使用的密码。
如果启用了身份联合	a. 选择一个现有联盟组、以便对租户具有root访问权限。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择一个现有联盟组、以便对租户具有root访问权限。没有本地用户可以登录。

7. 如果希望向导为root用户创建访问密钥ID和机密访问密钥，请选择*自动创建root用户S3访问密钥*。

> 如果租户的唯一用户是root用户、请选择此选项。如果其他用户要使用此租户、请使用租户管理器配置密钥和权限。

8. 选择 * 继续 * 。
9. 对于创建分段步骤、可以选择为租户的对象创建分段。否则、请选择*创建不含存储分段的租户*以转到 下载数据步骤。

> 如果为网格启用了S3对象锁定、则在此步骤中创建的分段不会启用S3对象锁定。如果需要对此S3应用程序使用S3对象锁定分段，请选择*创建不包含分段的租户*。然后、使用租户管理器 "创建存储分段" 而是。

   a. 输入S3应用程序要使用的存储分段的名称。例如： `S3-bucket`。

创建存储分段后、无法更改存储分段名称。

b. 为此存储分段选择*区域*。

   使用默认区域 (`us-east-1`)、除非您希望将来使用ILM根据存储分段的区域筛选对象。

c. 如果要将每个对象的每个版本存储在此存储分段中，请选择*启用对象版本控制*。

d. 选择*创建租户和存储分段*并转到下载数据步骤。

第4步(共6步)：下载数据

在下载数据步骤中、您可以下载一个或两个文件以保存刚刚配置的内容的详细信息。

步骤

1. 如果选择了*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 `.csv` 包含租户帐户名称、访问密钥ID和机密访问密钥的文件。
   - 选择复制图标()将访问密钥ID和机密访问密钥复制到剪贴板。
2. 选择*下载配置值*以下载 `.txt` 包含负载平衡器端点、租户、存储分段和root用户设置的文件。
3. 将此信息保存到安全位置。

   在复制两个访问密钥之前、请勿关闭此页面。关闭此页面后、密钥将不可用。请确保将此信息保存在安全位置、因为此信息可用于从StorageGRID 系统获取数据。

4. 如果出现提示、请选中此复选框以确认您已下载或复制密钥。
5. 选择*继续*以转到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、持续时间和加载行为。StorageGRID 附带的ILM策略会为所有对象创建两个复制副本。此策略在您至少激活一个新策略之前有效。

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分段的对象添加特定说明、请创建新规则和新策略。请参见 "创建 ILM 规则" 和 "ILM策略：概述"。
3. 选择*我已查看这些步骤并了解我需要执行的操作*。
4. 选中此复选框以指示您了解下一步要做什么。
5. 选择*继续*以转到*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、这些详细信息介绍了在连接到S3客户端之前可能需要的其他配置。例如，选

择*以root身份登录*将转到租户管理器，您可以在其中添加租户用户、创建其他存储分段以及更新存储分段设置。

3. 选择 * 完成 * 。
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

管理高可用性（ HA ）组：概述

您可以将多个管理节点和网关节点的网络接口分组到一个高可用性（ HA ）组中。如果 HA 组中的活动接口发生故障，则备份接口可以管理工作负载。

什么是 HA 组?

您可以使用高可用性（ High Availability ， HA ）组为 S3 和 Swift 客户端提供高可用性数据连接，或者为 Grid Manager 和租户管理器提供高可用性连接。

每个 HA 组均可访问选定节点上的共享服务。

- 包括网关节点，管理节点或两者在内的 HA 组可为 S3 和 Swift 客户端提供高可用性数据连接。
- 仅包含管理节点的 HA 组可提供与网格管理器和租户管理器的高可用性连接。
- 仅包含服务设备和基于VMware的软件节点的HA组可以为提供高可用性连接 "使用 S3 Select 的 S3 租户"。建议在使用 S3 Select 时使用 HA 组，但不要求使用 HA 组。

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。

   > 如果某个接口具有DHCP分配的IP地址、则无法将其添加到HA组。

2. 您可以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其中任何 VIP 地址连接到 StorageGRID 。

有关说明，请参见 "配置高可用性组"。

什么是活动接口?

在正常操作期间， HA 组的所有 VIP 地址都会添加到主接口，这是优先级顺序中的第一个接口。只要主接口保持可用，客户端就会连接到组的任何 VIP 地址。也就是说、在正常操作期间、主接口是组的"活动"接口。

同样、在正常操作期间、HA组中任何优先级较低的接口都会充当"备份"接口。除非主(当前处于活动状态)接口不可用、否则不会使用这些备份接口。

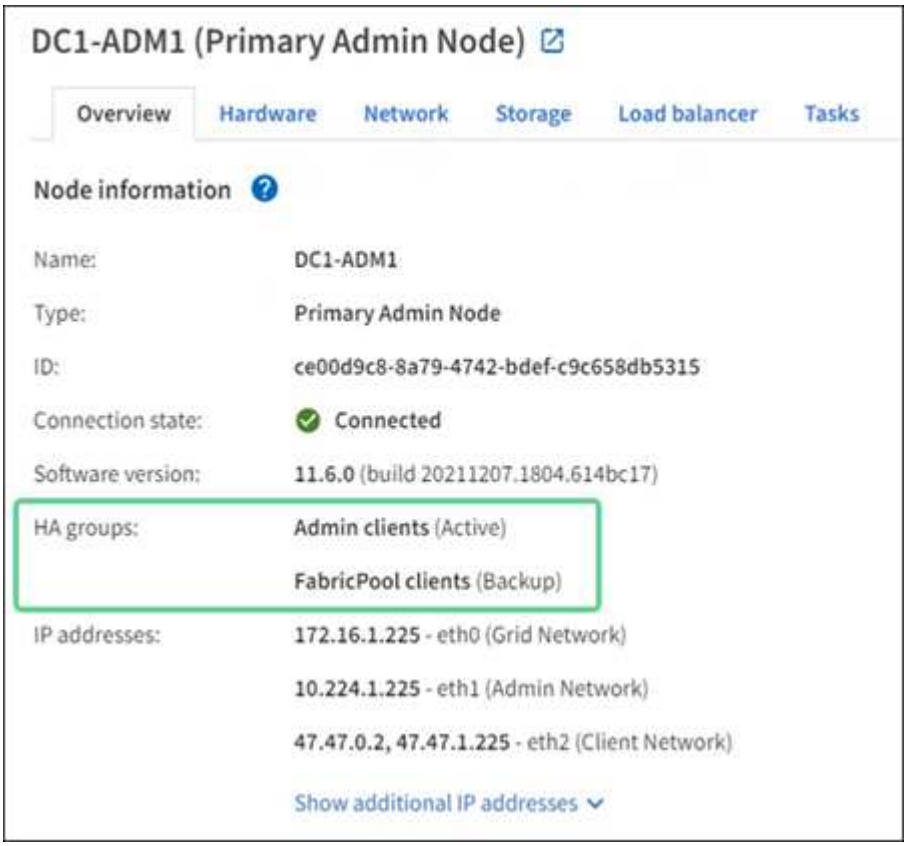
查看节点的当前 **HA** 组状态

要查看节点是否已分配给 HA 组并确定其当前状态，请选择 * 节点 * > * 节点 _节点 _* 。

如果 * 概述 * 选项卡包含 * HA 组 * 的条目，则节点将分配给列出的 HA 组。组名称后面的值是 HA 组中节点的当前状态：

- * 活动 *： HA 组当前正在此节点上托管。
- * 备份 *： HA 组当前未使用此节点；这是一个备份接口。
- 已停止：无法在此节点上托管HA组、因为已手动停止高可用性(keepalived)服务。
- 故障：由于以下一项或多项原因、无法在此节点上托管HA组：
  - 此节点上未运行负载平衡器（ nginx -gw ）服务。
  - 节点的 eth0 或 VIP 接口已关闭。
  - 节点已关闭。

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



活动接口发生故障时会发生什么情况?

当前托管 VIP 地址的接口是活动接口。如果 HA 组包含多个接口且活动接口发生故障，则 VIP 地址将按优先级顺序移至第一个可用的备份接口。如果该接口发生故障， VIP 地址将移至下一个可用备份接口，依此类推。

触发故障转移的原因如下：

- 配置接口的节点将关闭。
- 配置了该接口的节点与所有其他节点的连接至少断开 2 分钟。
- 活动接口关闭。
- 负载平衡器服务将停止。
- 高可用性服务将停止。

> 托管活动接口的节点外部的网络故障可能不会触发故障转移。同样、网格管理器或租户管理器的服务也不会触发故障转移。

故障转移过程通常只需几秒钟，并且速度足以使客户端应用程序不会受到任何影响，并且可以依靠正常的重试行为来继续运行。

解决故障后，如果更高优先级的接口再次可用，则 VIP 地址会自动移至可用的最高优先级接口。

如何使用 **HA** 组?

您可以使用高可用性（High Availability， HA）组提供与 StorageGRID 的高可用性连接，以用于对象数据和管理目的。

- 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 和 Swift 客户端提供高可用性数据连接。
- 如果 HA 组仅包含一个接口，则可以提供多个 VIP 地址并明确设置 IPv6 地址。

只有当 HA 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 *：包括负载平衡器服务，并允许访问网格管理器或租户管理器。
- 网关节点：包括负载平衡器服务。

HA 组的用途	将此类型的节点添加到 **HA** 组
访问 Grid Manager	• 主管理节点（* 主 *） • 非主管理节点 • 注： * 主管理节点必须为主接口。某些维护过程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 或 Swift 客户端访问—负载平衡器服务	• 管理节点 • 网关节点

HA 组的用途	将此类型的节点添加到 HA 组
的 S3 客户端访问 "S3 Select"	• 服务设备 • 基于 VMware 的软件节点 • 注 * ： 使用 S3 Select 时建议使用 HA 组，但不要求使用 HA 组。

将 **HA** 组与 **Grid Manager** 或租户管理器结合使用的限制

如果 Grid Manager 或租户管理器服务失败，则不会触发 HA 组故障转移。

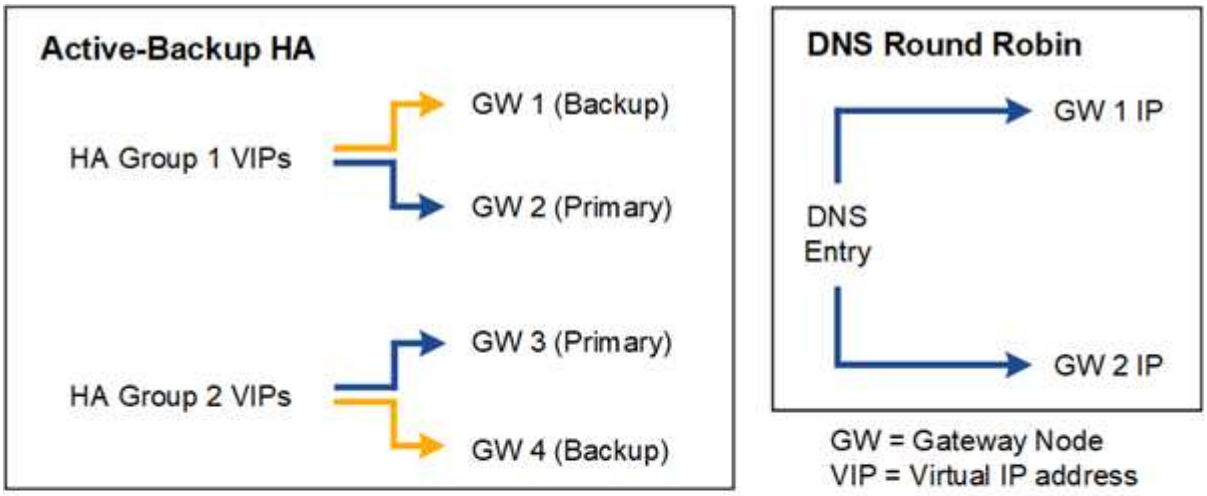
如果在发生故障转移时登录到网格管理器或租户管理器，则您将注销并必须重新登录才能恢复任务。

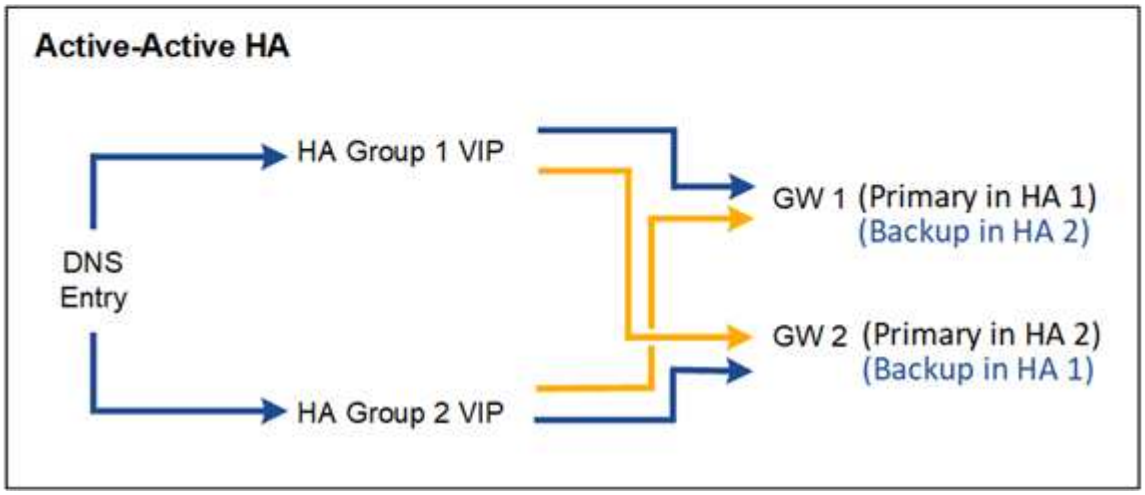
当主管理节点不可用时、无法执行某些维护过程。在故障转移期间，您可以使用网格管理器监控 StorageGRID 系统。

HA 组的配置选项

下图举例说明了配置 HA 组的不同方式。每个选项都有优缺点。

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每个 HA 配置的优势。

Configuration	优势	缺点
主动备份 HA	• 由 StorageGRID 管理，无外部依赖关系。 • 快速故障转移。	• 一个 HA 组中只有一个节点处于活动状态。每个 HA 组至少有一个节点处于空闲状态。
DNS 轮循	• 提高聚合吞吐量。 • 无闲置主机。	• 故障转移速度较慢，这可能取决于客户端行为。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。
主动 - 主动 HA	• 流量分布在多个 HA 组中。 • 可随 HA 组数量扩展的高聚合吞吐量。 • 快速故障转移。	• 配置更复杂。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。

配置高可用性组

您可以配置高可用性（ High Availability ， 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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "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。请参见 "配置 VLAN 接口"。
- 如果您计划对 HA 组中的节点使用访问接口，则已创建此接口：
  - **Red Hat Enterprise Linux (**安装节点之前**)**： "创建节点配置文件"
  - * Ubuntu 或 Debian （安装节点之前） *： "创建节点配置文件"
  - * Linux （安装节点后） *： "Linux ： 向节点添加中继或访问接口"
  - * VMware （安装节点后） *： "VMware ： 向节点添加中继或访问接口"

创建高可用性组

创建高可用性组时，您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，您将一个或多个 VIP 地址分配给该组。

接口必须是要将网关节点或管理节点包含在 HA 组中的接口。一个 HA 组只能对任何给定节点使用一个接口；但是，同一节点的其他接口也可以在其他 HA 组中使用。

访问向导

步骤

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

输入 **HA** 组的详细信息

步骤

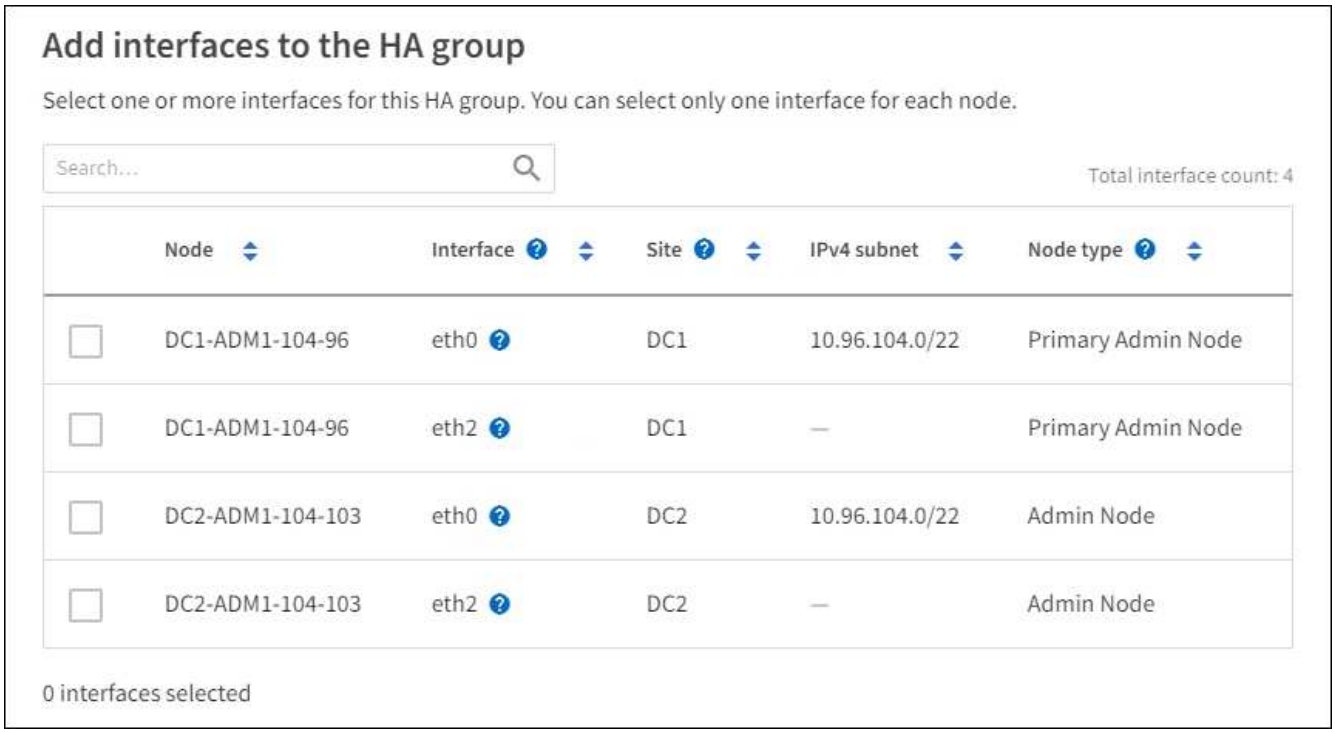
1. 为 HA 组提供一个唯一名称。
2. 或者，输入 HA 组的问题描述 。
3. 选择 * 继续 * 。

向 **HA** 组添加接口

步骤

1. 选择一个或多个接口以添加到此 HA 组。

   使用列标题对行进行排序，或者输入搜索词以更快地找到接口。



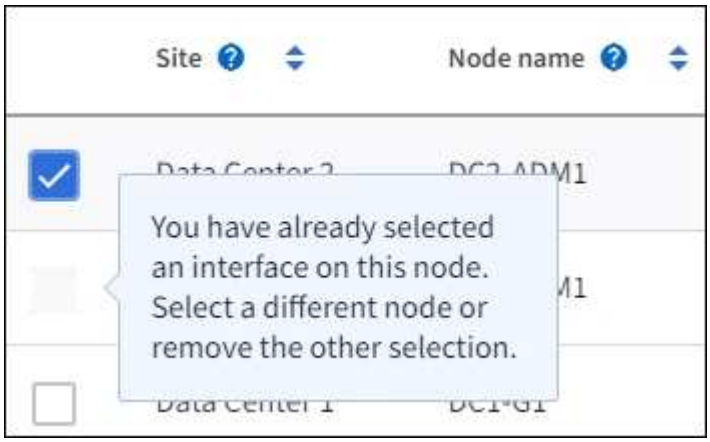
   创建 VLAN 接口后，请等待最多 5 分钟，使新接口显示在表中。

   选择接口的准则

   - 必须至少选择一个接口。
   - 您只能为一个节点选择一个接口。
   - 如果 HA 组用于管理节点服务（包括网格管理器和租户管理器）的 HA 保护，请仅选择管理节点上的接口。
   - 如果 HA 组用于对 S3 或 Swift 客户端流量进行 HA 保护，请选择管理节点，网关节点或两者上的接口。
   - 如果选择不同类型节点上的接口，则会显示一条信息性注释。系统会提醒您，如果发生故障转移，则新

活动节点上可能无法使用先前活动节点提供的服务。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、则会禁用其复选框。工具提示提供了更多信息。



- 如果某个接口的子网值或网关与另一个选定接口冲突、则无法选择该接口。
- 如果已配置接口没有静态IP地址、则无法选择该接口。

2. 选择 * 继续 * 。

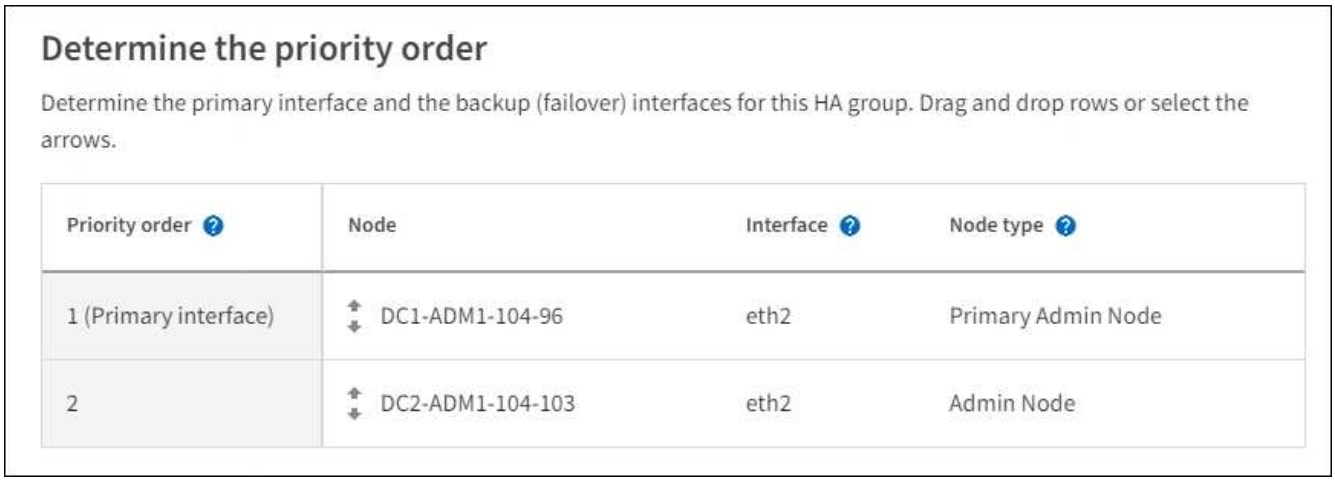
确定优先级顺序

如果HA组包含多个接口、则可以确定哪个是主接口、哪些是备份(故障转移)接口。 如果主接口发生故障、VIP地址将移至可用的最高优先级接口。如果该接口发生故障， VIP 地址将移至可用的下一个最高优先级接口，依此类推。

步骤

1. 拖动*优先级顺序*列中的行以确定主接口和任何备份接口。

   列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。



> 如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行。

2. 选择 * 继续 * 。

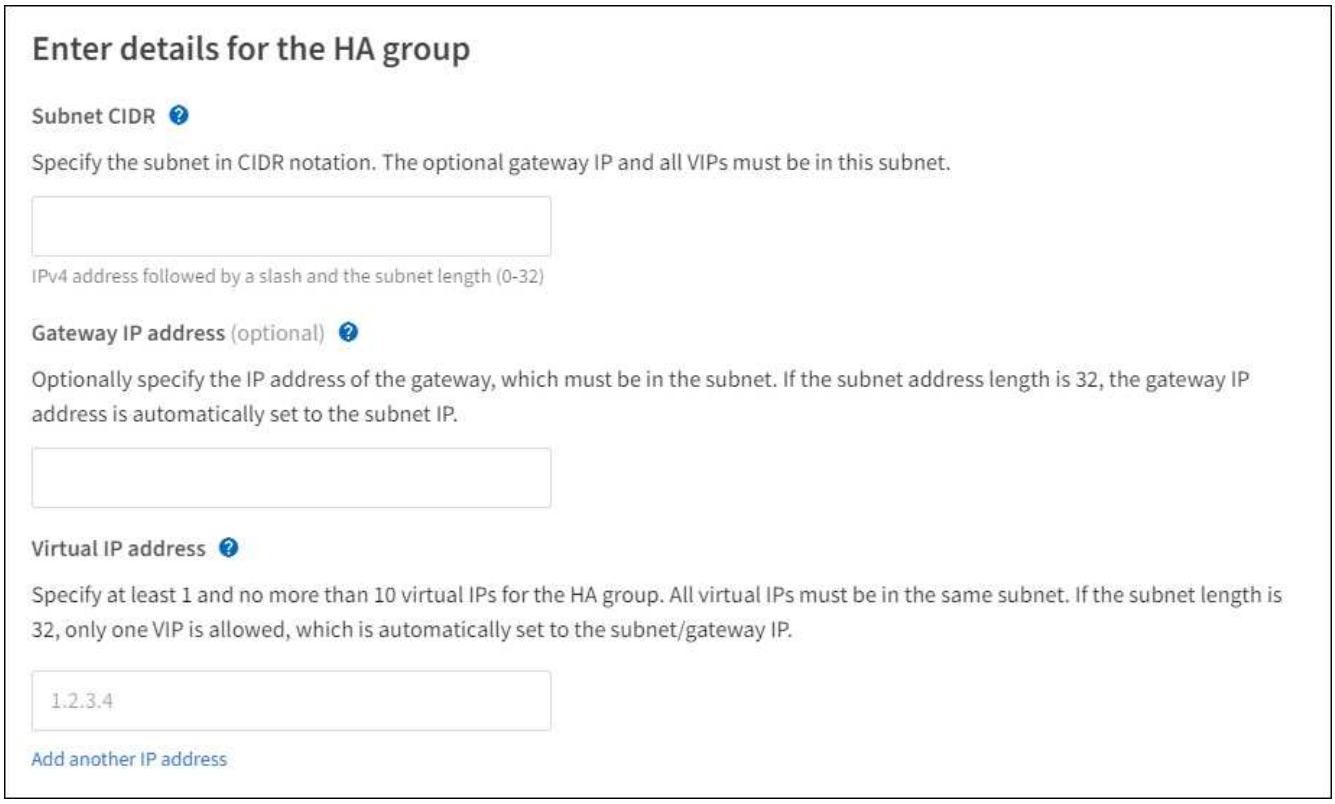
输入 **IP** 地址

步骤

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

   网络地址不能设置任何主机位。例如： `192.16.0.0/22`。

   > 如果使用 32 位前缀，则 VIP 网络地址也会用作网关地址和 VIP 地址。

2. 或者，如果任何 S3 ， Swift ，管理或租户客户端要从其他子网访问这些 VIP 地址，请输入 * 网关 IP 地址 * 。网关地址必须在 VIP 子网中。

   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组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网中、并且所有VIP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 * 。

   此时将创建 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，请创建一个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。请参见 "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（ High Availability ， HA ）组以更改其名称和问题描述 ，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操作步骤 中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 " 页面显示所有现有的 HA 组。

2. 选中要编辑的HA组对应的复选框。
3. 根据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 * 可更新组的名称或问题描述 ，添加或删除接口，更改优先级顺序或添加或删除 VIP 地址。
4. 如果选择了 * 编辑虚拟 IP 地址 * ：
   a. 更新 HA 组的虚拟 IP 地址。
   b. 选择 * 保存 * 。
   c. 选择 * 完成 * 。
5. 如果选择了 * 编辑 HA 组 * ：
   a. （可选）更新组的名称或问题描述 。
   b. (可选)选中或清除相应复选框以添加或删除接口。

      > 如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行

   c. (可选)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. 也可以更新虚拟 IP 地址。
   e. 选择 * 保存 * ，然后选择 * 完成 * 。

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HA组绑定到负载平衡器端点、则无法删除该HA组。要删除HA组、必须将其从使用该组的任何负载平衡器端点中删除。

为防止客户端中断，请在删除 HA 组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其他 IP 地址进行连接，例如，安装期间为接口配置的不同 HA 组的虚拟 IP 地址或 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*负载平衡器端点*列。如果列出了任何负载平衡器端点：
   a. 转到*configuration*>*Network*>*负载平衡器端点*。
   b. 选中此端点对应的复选框。
   c. 选择 * 操作 * > * 编辑端点绑定模式 * 。
   d. 更新绑定模式以删除HA组。
   e. 选择 * 保存更改 * 。
3. 如果未列出负载平衡器端点、请选中要删除的每个HA组对应的复选框。
4. 选择*Actions*>*Remove HA group*。
5. 查看此消息并选择 * 删除 HA 组 * 以确认您的选择。

   选定的所有 HA 组都将被删除。高可用性组页面上会显示一个绿色的成功横幅。

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。无论您使用的是服务设备、裸机节点还是基于虚拟机(VM)的节点、请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。您还可以使用端点访问网格管理器、租户管理器或这两者。

> 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"。
- 您拥有 "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服务设备和基于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S3或Swift客户端负载平衡器端点指定一个端口、一种客户端类型(S3或Swift)和一种网络协议(HTTP或HTTPS)。管理接口负载平衡器端点指定端口、接口类型和不可信的客户端网络。

访问向导

步骤

1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。
2. 要为S3或Swift客户端创建端点，请选择*S3或Swift client*选项卡。
3. 要创建端点以访问网格管理器、租户管理器或这两者，请选择*管理接口*选项卡。
4. 选择 * 创建 * 。

输入端点详细信息

步骤

1. 选择相应的说明、为要创建的端点类型输入详细信息。

S3或Swift客户端

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。 如果输入*80*或*8443*，则仅在网关节点上配置端点，除非释放端口8443。然后、您可以使用端口8443作为S3端点、此端口将同时在网关节点和管理节点上进行配置。
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。 • 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。 • 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 。

管理接口

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	要用于访问网格管理器和/或租户管理器的StorageGRID端口。 • 网格管理器：**8443** • 租户管理器：**9443** • 网格管理器和租户管理器：**443** 注：您可以使用这些预设端口或其他可用端口。
接口类型	选择要使用此端点访问的StorageGRID接口对应的单选按钮。
不可信客户端网络	如果此端点应可供不可信的客户端网络访问，请选择*是*。否则，请选择*No*。 选择*是*时，端口在所有不可信的客户端网络上打开。 注意：创建负载平衡器端点时，只能将端口配置为对不可信客户端网络开放或关闭。

1. 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。

   某些绑定模式可用于客户端端点或管理接口端点。此处列出了这两种端点类型的所有模式。

模式	**Description**
全局(默认用于客户端端点)	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。 除非需要限制此端点的可访问性，否则请使用*Global"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)才能访问此端点。 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(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(默认用于管理接口端点)	客户端必须使用任何管理节点的IP地址(或相应的FQDN)才能访问此端点。

   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"。

   如果要创建管理接口端点、则仅允许使用管理节点。

2. 如果选择了 * HA 组的虚拟 IP * ，请选择一个或多个 HA 组。

   如果要创建管理接口端点、请选择仅与管理节点关联的VIP。

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

> 只有当管理接口端点具有时、该端点才能控制租户访问 租户管理器的接口类型。

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。 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"。

   - 使用管理接口证书。如果要使用全局管理接口证书、则选择此选项、此证书也可用于直接连接到管理节点。
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 * 。+ 此时将创建负载平衡器端点。自定义证书将用于S3和Swift客户端或管理接口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)。 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。 这些扩展定义了证书中所含密钥的用途。 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*以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。自定义证书将用于S3和Swift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. 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。

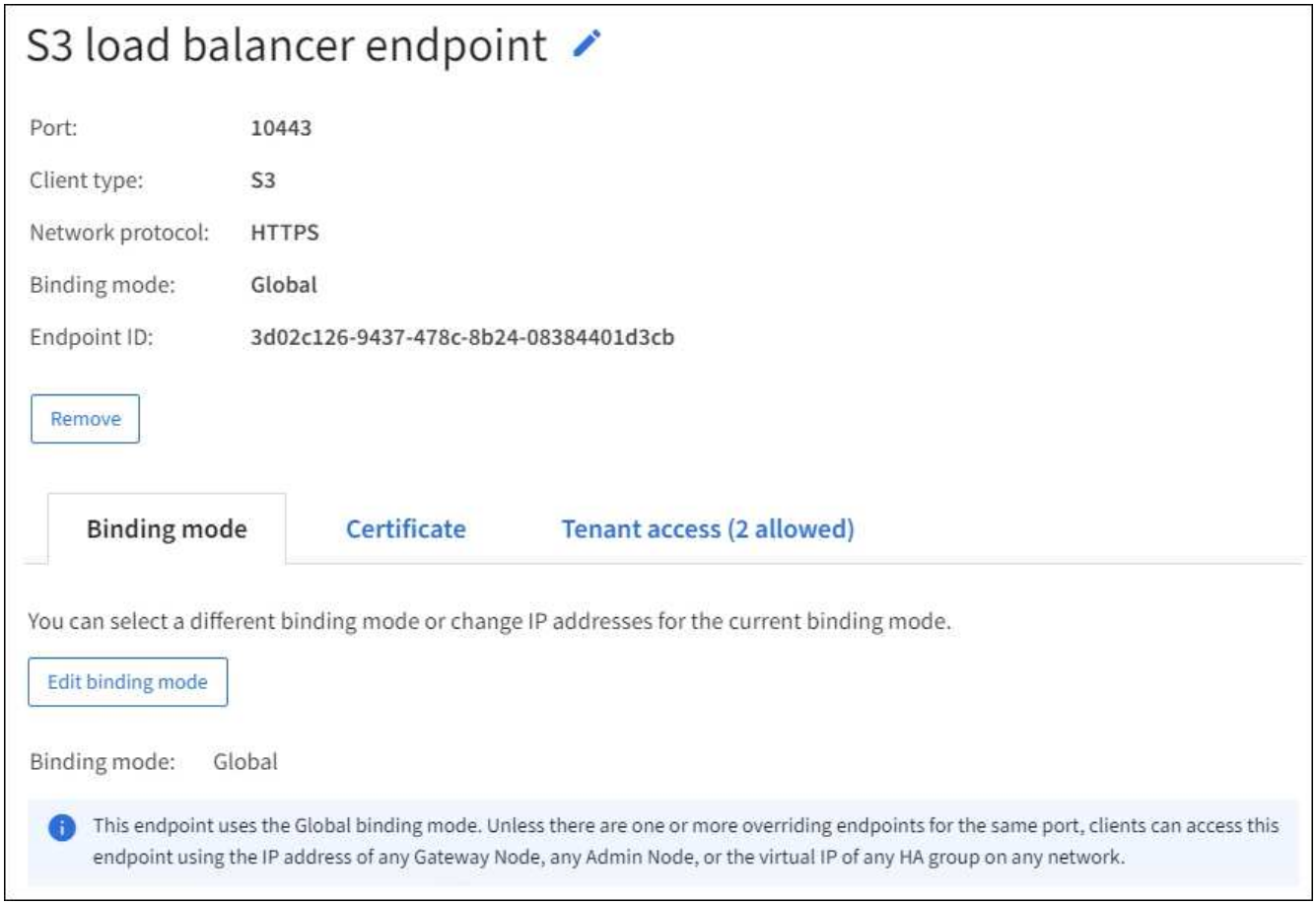
     此外，还必须确保 DNS 记录引用所有必需的端点域名，包括任何通配符名称。

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。您可以更改端点的某些设置。

- 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。显示的信息因端点类型及其配置方式而异。



- 要编辑端点，请使用“负载平衡器端点”页面上的*Actions*菜单。

> 如果在编辑管理接口端点的端口时无法访问网格管理器、请更新URL和端口以重新获取访问权限。

> 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。 b. 选择 * 操作 * > * 编辑端点名称 * 。 c. 输入新名称。 d. 选择 * 保存 * 。	a. 选择端点名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存 * 。

任务	操作菜单	详细信息页面
编辑端点端口	a. 选中此端点对应的复选框。 b. 选择*Actions*>*编辑端点端口* c. 输入有效的端口号。 d. 选择 * 保存 * 。	*n/A*
编辑端点绑定模式	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 编辑绑定模式 * 。 c. 根据需要更新绑定模式。 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。 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 和 Swift 证书。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 证书 * 选项卡。 c. 选择 * 编辑证书 * 。 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。 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。 b. 选择*操作*>*编辑租户访问*。 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。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择*租户访问*选项卡。 c. 选择*编辑租户访问*。 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。 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。

> 如果在删除管理接口端点时无法访问网格管理器、请更新此URL。

- 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 * 。

配置S3端点域名

要支持S3虚拟托管模式请求、必须使用网格管理器配置S3客户端连接到的S3端点域名列表。

> 不支持使用IP地址作为端点域名。未来版本将禁止此配置。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您已确认网格升级未在进行中。

> 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，您必须执行以下所有操作：

- 使用网格管理器将 S3 端点域名添加到 StorageGRID 系统。
- 确保 "客户端用于与StorageGRID 进行HTTPS连接的证书" 已针对客户端所需的所有域名进行签名。

  例如、如果端点为 `s3.company.com`、您必须确保用于HTTPS连接的证书包括 `s3.company.com` 端点和端点的通配符使用者备用名称(SAN)： `*.s3.company.com`。

- 配置客户端使用的 DNS 服务器。包括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 地址或连接到高可用性组的虚拟 IP 地址连接到 StorageGRID 。您应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。

使用 HTTPS 连接（建议）连接到网格的客户端可以使用以下任一证书：

- 连接到负载平衡器端点的客户端可以对该端点使用自定义证书。可以对每个负载平衡器端点进行配置、使其能够识别不同的S3端点域名。
- 连接到负载平衡器端点或直接连接到存储节点的客户端可以自定义全局S3和Swift API证书、以包含所有必需的S3端点域名。

如果不添加S3端点域名且此列表为空、则会禁用对S3虚拟托管模式请求的支持。

添加S3端点域名

步骤

1. 选择*配置*>*网络*>* S3端点域名*。
2. 在*域名1*字段中输入域名。选择*添加其他域名*以添加更多域名。
3. 选择 * 保存 * 。
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自己的证书的负载平衡器端点、 "更新与此端点关联的证书"。
   - 如果客户端连接到使用全局S3和Swift API证书的负载平衡器端点、或者直接连接到存储节点、 "更新全局S3和Swift API证书"。
5. 添加所需的 DNS 记录，以确保可以解决端点域名请求。

结果

现在、当客户端使用端点时 `bucket.s3.company.com`、DNS服务器解析到正确的端点、证书将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、虚拟托管模式请求将失败。

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 * 保存 * 。
4. 选择*是*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、虚拟托管模式请求将失败。

步骤

1. 选择*配置*>*网络*>* S3端点域名*。
2. 选择删除图标 ✕ 域名旁边。
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"

摘要：客户端连接的 IP 地址和端口

要存储或检索对象、S3和Swift客户端应用程序会连接到负载平衡器服务(包含在所有管理节点和网关节点上)或本地分发路由器(LDR)服务(包含在所有存储节点上)。

客户端应用程序可以使用网格节点的IP地址以及该节点上服务的端口号连接到StorageGRID。或者、您也可以为负载平衡节点创建高可用性(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 、则可以配置DNS条目。

此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。如果已创建负载平衡器端点和高可用性(HA)组、请参见 从何处查找IP地址 在网格管理器中查找这些值。

建立连接的位置	客户端连接到的服务	**IP** 地址	**Port**
HA 组	负载平衡器	HA 组的虚拟 IP 地址	分配给负载平衡器端点的端口
管理节点	负载平衡器	管理节点的 IP 地址	分配给负载平衡器端点的端口
网关节点	负载平衡器	网关节点的 IP 地址	分配给负载平衡器端点的端口
存储节点	LDR	存储节点的 IP 地址	默认 S3 端口： • HTTPS： 18082 • HTTP： 18084 默认 Swift 端口： • HTTPS： 18083 • HTTP： 18085

示例URL

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

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

例如、如果HA组的虚拟IP地址为192.0.2.5、负载平衡器端点的端口号为10443、则应用程序可以使用以下URL连接到StorageGRID ：

```
https://192.0.2.5:10443
```

从何处查找IP地址

1. 使用登录到网格管理器 "支持的 Web 浏览器"。

2. 要查找网格节点的 IP 地址，请执行以下操作：
   a. 选择 * 节点 * 。
   b. 选择要连接到的管理节点，网关节点或存储节点。
   c. 选择 * 概述 * 选项卡。
   d. 在节点信息部分中，记下节点的 IP 地址。
   e. 选择 * 显示更多 * 可查看 IPv6 地址和接口映射。

      您可以建立从客户端应用程序到列表中任何 IP 地址的连接：

      - * eth0 ： * 网格网络
      - * eth1 ： * 管理网络（可选）
      - * eth2 ： * 客户端网络（可选）

      > 如果您正在查看管理节点或网关节点，并且该节点是高可用性组中的活动节点，则 eth2 上会显示 HA 组的虚拟 IP 地址。

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. 在表中，记下 HA 组的虚拟 IP 地址。
4. 查找负载平衡器端点的端口号：
   a. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。
   b. 记下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、因为这些端口是在管理节点上预留的。所有其他端口都在网关节点和管理节点上进行配置。

   c. 从表中选择端点的名称。
   d. 确认*客户端类型*(S3或Swift)与要使用端点的客户端应用程序匹配。