



将 **StorageGRID** 附加为云层所需的信息

StorageGRID 11.5

NetApp
April 11, 2024

目录

将 StorageGRID 附加为云层所需的信息	1
负载均衡最佳实践	2
高可用性组的最佳实践	3
为DNS服务器配置StorageGRID IP地址	4
为FabricPool 创建高可用性(HA)组	4
为FabricPool 创建负载均衡器端点	6
为FabricPool 创建租户帐户	8
创建S3存储分段并获取访问密钥	9

将 StorageGRID 附加为云层所需的信息

在将StorageGRID 附加为FabricPool 的云层之前、您必须在StorageGRID 中执行一些配置步骤并获取某些值。

关于此任务

下表列出了在将 StorageGRID 作为 FabricPool 的云层附加时必须向 ONTAP 提供的信息。本节中的主题介绍如何使用 StorageGRID 网络管理器和租户管理器来获取所需信息。



列出的确切字段名称以及用于在 ONTAP 中输入所需值的过程取决于您使用的是 ONTAP 命令行界面（`storage aggregate object-store config create`）还是 ONTAP 系统管理器（* 存储 * > * 聚合和磁盘 * > * 云层 *）。

有关详细信息，请参见以下内容：

- ["TR-4598：《适用于ONTAP 9.8的FabricPool 最佳实践》"](#)
- ["ONTAP 9 文档中心"](#)

ONTAP 字段	Description
对象存储名称	任何唯一的描述性名称。例如： <code>StorageGRID_Cloud_Tier</code> 。
提供程序类型	StorageGRID (System Manager)或 <code>sgws</code> (命令行界面)。
Port	FabricPool 连接到 StorageGRID 时将使用的端口。您可以确定在定义 StorageGRID 负载均衡器端点时要使用的端口号。 "为FabricPool 创建负载均衡器端点"
服务器名称	StorageGRID 负载均衡器端点的完全限定域名（FQDN）。例如： <code>s3.storagegrid.company.com</code> 请注意以下事项： <ul style="list-style-type: none">• 此处指定的域名必须与您为 StorageGRID 负载均衡器端点上传的 CA 证书上的域名匹配。• 此域名的 DNS 记录必须映射到要用于连接到 StorageGRID 的每个 IP 地址。 "为DNS服务器配置StorageGRID IP地址"

ONTAP 字段	Description
容器名称	<p>要在此 ONTAP 集群中使用的 StorageGRID 存储分段的名称。例如：fabricpool-bucket。您可以在租户管理器中创建此分段。</p> <p>请注意以下事项：</p> <ul style="list-style-type: none"> • 创建配置后，无法更改存储分段名称。 • 存储分段不能启用版本控制。 • 您必须为每个 ONTAP 集群使用不同的分段，以便将数据分层到 StorageGRID 。 <p>"创建S3存储分段并获取访问密钥"</p>
访问密钥和机密密码	<p>StorageGRID 租户帐户的访问密钥和机密访问密钥。</p> <p>您可以在租户管理器中生成这些值。</p> <p>"创建S3存储分段并获取访问密钥"</p>
SSL	必须启用。
对象存储证书	<p>创建 StorageGRID 负载均衡器端点时上传的 CA 证书。</p> <ul style="list-style-type: none"> • 注意：* 如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。 <p>"为FabricPool 创建负载均衡器端点"</p>

完成后

获取所需的 StorageGRID 信息后，您可以转到 ONTAP 将 StorageGRID 添加为云层，将云层添加为聚合并设置卷分层策略。

负载均衡最佳实践

在将StorageGRID 附加为FabricPool 云层之前、您可以使用StorageGRID 网络管理器至少配置一个负载均衡器端点。

什么是负载均衡

在将数据从 FabricPool 分层到 StorageGRID 系统时， StorageGRID 会使用负载均衡器来管理载入和检索工作负载。负载均衡通过在多个存储节点之间分布 FabricPool 工作负载，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，每个节点上的负载均衡器服务会独立运行。通过加权过程，负载均衡器服务会

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 负载均衡器服务来平衡负载，但您可能希望集成第三方负载均衡器。有关信息、请联系您的NetApp客户代表或参阅以下技术报告：

"StorageGRID 负载均衡器选项"



网关节点上的单独连接负载均衡器（CLB）服务已弃用，不再建议用于 FabricPool。

StorageGRID 负载均衡最佳实践

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均衡器服务的节点。例如、一个站点可能同时包含一个管理节点和一个网关节点、甚至包括两个管理节点。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，确保每个负载均衡节点都有足够的网络，硬件或虚拟化基础架构。

您必须配置 StorageGRID 负载均衡器端点，以定义网关节点和管理节点用于传入和传出 FabricPool 请求的端口。

负载均衡器端点证书的最佳实践

创建用于FabricPool 的负载均衡器端点时、必须使用HTTPS作为协议。然后、您可以上传由公共信任或私有证书颁发机构(CA)签名的证书、也可以生成自签名证书。此证书允许 ONTAP 向 StorageGRID 进行身份验证。

作为最佳实践，您应使用 CA 服务器证书来保护连接。由 CA 签名的证书可以无中断地轮换。

请求用于负载均衡器端点的 CA 证书时，请确保此证书上的域名与您在 ONTAP 中为该负载均衡器端点输入的服务器名称匹配。如果可能，请使用通配符（*）来支持虚拟主机模式的 URL。例如：

```
*.s3.storagegrid.company.com
```

在将 StorageGRID 添加为 FabricPool 云层时，必须将同一证书安装到 ONTAP 集群以及根证书颁发机构（CA）证书和任何从属证书颁发机构（CA）证书。



StorageGRID 将服务器证书用于多种用途。如果要连接到负载均衡器服务、则无需上传对象存储API服务端点服务器证书。

要了解有关负载均衡端点的服务器证书的详细信息，请执行以下操作：

- "管理负载均衡"
- "服务器证书的强化准则"

高可用性组的最佳实践

在将StorageGRID 附加为FabricPool 云层之前、您可以使用StorageGRID 网络管理器配置高可用性(HA)组。

什么是高可用性(HA)组

为了确保负载均衡器服务始终可用于管理 FabricPool 数据，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实体中，称为高可用性（ High Availability ， HA ）组。如果 HA 组中的活动节点发生故障，则组中的另一个节点可以继续管理工作负载。

每个 HA 组均可提供对关联节点上共享服务的高可用性访问。例如、由所有管理节点组成的HA组可提供对某些管理节点管理服务和负载均衡器服务的高可用性访问。仅包含网关节点或管理节点和网关节点的HA组可提供对共享负载均衡器服务的高可用性访问。

创建HA组时、您可以选择属于网格网络(eth0)或客户端网络(eth2)的网络接口。HA组中的所有接口必须位于同一网络子网中。

HA组维护一个或多个虚拟IP地址、这些地址会添加到组中的活动接口中。如果活动接口不可用、则虚拟IP地址将移至另一个接口。此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继续运行。

如果您配置了一个由负载均衡节点组成的HA组、则FabricPool 会连接到该HA组的虚拟IP地址。

高可用性（ HA ） 组的最佳实践

为 FabricPool 创建 StorageGRID HA 组的最佳实践取决于工作负载，如下所示：

- 如果您计划将 FabricPool 与主工作负载数据结合使用，则必须创建一个至少包含两个负载均衡节点的 HA 组，以防止数据检索中断。
- 如果您计划使用 FabricPool snapshot-only 卷分层策略或非主本地性能层（例如，灾难恢复位置或 NetApp SnapMirror® 目标），则只能为 HA 组配置一个节点。

以下说明介绍如何为主动备份 HA 设置 HA 组（一个节点为活动节点，一个节点为备份节点）。但是，您可能更喜欢使用 DNS 轮循或主动 - 主动 HA。要了解这些其他 HA 配置的优势，请参见 ["HA 组的配置选项"](#)。

为DNS服务器配置StorageGRID IP地址

配置高可用性组和负载均衡器端点后，您必须确保 ONTAP 系统的域名系统（ DNS ）包含一条记录，用于将 StorageGRID 服务器名称（完全限定域名）与 FabricPool 用于建立连接的 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均衡节点组成的 HA 组：

- 如果已配置 HA 组， FabricPool 将连接到该 HA 组的虚拟 IP 地址。
- 如果您不使用 HA 组，则 FabricPool 可以使用任何网关节点或管理节点的 IP 地址连接到 StorageGRID 负载均衡器服务。

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。

为FabricPool 创建高可用性(HA)组

在配置 StorageGRID 与 FabricPool 结合使用时，您可以选择创建一个或多个高可用性（ HA ）组。HA 组由管理节点，网关节点或这两者上的一个或多个网络接口组成。

您需要的内容

- 您必须使用支持的浏览器登录到网络管理器。
- 您必须具有 root 访问权限。

关于此任务

每个 HA 组都使用虚拟 IP 地址（VIP）来提供对关联节点上共享服务的高可用性访问。

有关此任务的详细信息。请参见 ["管理高可用性组"](#)。

步骤

1. 选择*配置*>*网络设置*>*高可用性组*。
2. 选择一个或多个网络接口。网络接口必须属于网格网络(eth0)或客户端网络(eth2)上的同一子网。
3. 将一个节点分配为首选主节点。

首选主接口是活动接口、除非发生故障、导致VIP地址重新分配给备份接口。

4. 为HA组最多输入十个IPv4地址。

这些地址必须位于所有成员接口共享的IPv4子网中。

Create High Availability Group

High Availability Group

Name HA Group for LB

Description HA for FabricPool load balancing

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.98.0/23	<input checked="" type="radio"/>
DC1-G1	eth0	10.96.98.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.98.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1

10.96.98.1

+

Cancel

Save

为FabricPool 创建负载均衡器端点

在配置StorageGRID 与FabricPool 结合使用时、您需要配置负载均衡器端点并上传负载均衡器端点证书、该证书用于保护ONTAP 和StorageGRID 之间的连接。

您需要的内容

- 您必须使用支持的浏览器登录到网络管理器。
- 您必须具有 root 访问权限。
- 您具有以下文件：
 - Server Certificate : 自定义服务器证书文件。
 - 服务器证书专用密钥: 自定义服务器证书专用密钥文件。

- CA Bundle：一个文件、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。

关于此任务

有关此任务的详细信息，请参见 ["配置负载均衡器端点"](#)。

步骤

1. 选择*配置*>*网络设置*>*负载均衡器端点*。

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

2. 选择*添加端点*。
3. 输入以下信息。

字段	Description
显示名称	端点的描述性名称
Port	<p>要用于负载均衡的 StorageGRID 端口。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，则仅会在网关节点上配置端点，因为这些端口是在管理节点上保留的。</p> <ul style="list-style-type: none"> • 注：* 不允许使用其他网格服务使用的端口。请参见用于内部和外部通信的端口列表： <p>"网络端口参考"</p> <p>在将 StorageGRID 附加为 FabricPool 云层时，您必须向 ONTAP 提供此相同端口号。</p>
协议	必须为* HTTPS *。
端点绑定模式	<p>使用 * 全局 * 设置（建议）或将此端点的可访问性限制为以下选项之一：</p> <ul style="list-style-type: none"> • 特定高可用性（High Availability，HA）虚拟 IP 地址（VIP）。只有在需要更高级别的工作负载隔离时，才使用此选项。 • 特定节点的特定网络接口。

4. 选择 * 保存 *。

此时将显示编辑端点对话框。

5. 对于*端点服务类型*、选择* S3 *。

6. 选择*上传证书*(建议)、然后浏览到您的服务器证书、证书专用密钥和CA捆绑包。

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate	<input type="button" value="Browse"/>
Certificate Private Key	<input type="button" value="Browse"/>
CA Bundle	<input type="button" value="Browse"/>

7. 选择 * 保存 *。

为FabricPool 创建租户帐户

您必须在网络管理器中创建一个租户帐户以供 FabricPool 使用。

您需要的内容

- 您必须使用支持的浏览器登录到网络管理器。
- 您必须具有特定的访问权限。

关于此任务

租户帐户允许客户端应用程序在 StorageGRID 上存储和检索对象。每个租户帐户都有自己的帐户 ID ， 授权组 和用户， 分段和对象。

您可以对多个 ONTAP 集群使用相同的租户帐户。或者，您也可以根据需要在每个 ONTAP 集群创建一个专用租户帐户。



以下说明假定您已为网络管理器配置单点登录（ Single Sign-On ， SSO ）。如果不使用SSO、请按照的说明进行操作 ["如果StorageGRID 未使用SSO、则创建租户帐户"](#)。

步骤

1. 选择*租户*。
2. 选择 * 创建 *。
3. 输入FabricPool 租户帐户的显示名称。
4. 选择 * 。 s3*。

5. 保持选中*允许平台服务*复选框以启用平台服务。

如果启用了平台服务，则租户可以使用 CloudMirror 复制等功能来访问外部服务。

6. 将*存储配额*字段留空。

7. 在*根访问组*字段中、从网格管理器中选择一个现有联合组、以便为租户提供初始根访问权限。

8. 选择 * 保存 *。

创建S3存储分段并获取访问密钥

在将 StorageGRID 与 FabricPool 工作负载结合使用之前，您必须为 FabricPool 数据创建一个 S3 存储分段。您还需要为要用于 FabricPool 的租户帐户获取访问密钥和机密访问密钥。

您需要的内容

- 您必须已创建用于FabricPool 的租户帐户。

关于此任务

以下说明介绍如何使用 StorageGRID 租户管理器创建存储分段并获取访问密钥。您也可以使用租户管理 API 或 StorageGRID S3 REST API 执行这些任务。

了解更多信息：

- ["使用租户帐户"](#)
- ["使用 S3"](#)

步骤

1. 登录到租户管理器。

您可以执行以下任一操作：

- 从网格管理器的租户帐户页面中，选择此租户的 * 登录 * 链接，然后输入您的凭据。
- 在 Web 浏览器中输入租户帐户的 URL ，然后输入凭据。

2. 为 FabricPool 数据创建 S3 存储分段。

您必须为计划使用的每个 ONTAP 集群创建一个唯一的存储分段。

- 选择 * 存储 (S3) * > * 分段 * 。
- 选择 * 创建存储分段 * 。
- 输入要与 FabricPool 结合使用的 StorageGRID 存储分段的名称。例如： `fabricpool-bucket`。



创建存储分段后，您无法更改存储分段名称。

存储分段名称必须符合以下规则：

- 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。

- 必须符合 DNS 要求。
- 必须至少包含 3 个字符，并且不能超过 63 个字符。
- 可以是一个或多个标签的序列，并使用一个句点分隔相邻标签。每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。
- 不能与文本格式的 IP 地址类似。
- 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。

d. 为此存储分段选择区域。

默认情况下、所有分段都在中创建 us-east-1 区域。

Create bucket
×

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

us-east-1
▼

Cancel
Create bucket

- a. 选择 * 创建存储分段 *。
3. 创建访问密钥和机密访问密钥。
 - a. 选择 * 存储 (S3) * > * 我的访问密钥 *。
 - b. 选择 * 创建密钥 *。
 - c. 选择 * 创建访问密钥 *。
 - d. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

将 StorageGRID 配置为 FabricPool 云层时，您将在 ONTAP 中输入这些值。



如果您将来创建新的访问密钥和机密访问密钥，请务必立即更新 ONTAP 中的相应值，以确保 ONTAP 可以在 StorageGRID 中存储和检索数据，而不会造成中断。

版权信息

版权所有 © 2024 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。