# 网络连接准则

## StorageGRID 11.5

NetApp
April 11, 2024

# 目录

# 网络连接准则

了解StorageGRID 架构和网络拓扑。熟悉网络配置和配置的要求。

- "StorageGRID 网络概述"
- "网络连接要求和准则"
- "部署特定的网络注意事项"
- "网络安装和配置"
- "安装后准则"
- "网络端口参考"

# StorageGRID 网络概述

为 StorageGRID 系统配置网络需要在以太网交换， TCP/IP 网络，子网，网络路由和防火墙方面具有丰富的经验。

在配置网络之前、请熟悉_Grid primer_中所述的StorageGRID 架构。

在部署和配置StorageGRID 之前、您必须配置网络基础架构。网格中的所有节点之间以及网格与外部客户端和服务之间都需要进行通信。

外部客户端和外部服务需要连接到 StorageGRID 网络才能执行如下功能：

- 存储和检索对象数据
- 接收电子邮件通知
- 访问 StorageGRID 管理界面（网格管理器和租户管理器）
- 访问审核共享（可选）
- 提供以下服务：
  - 网络时间协议（ NTP ）
  - 域名系统（ DNS ）
  - 密钥管理服务器（ KMS ）

必须正确配置 StorageGRID 网络，才能处理这些功能等的流量。

在确定要使用的三个StorageGRID 网络中的哪一个以及这些网络的配置方式之后、您可以按照相应的说明安装和配置StorageGRID 节点。

相关信息

"网格入门"

"管理 StorageGRID"

"发行说明"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

## StorageGRID 网络类型

StorageGRID 系统中的网格节点处理 _grid traffic ， _admin traffic _ 和 _client traffic 。您必须正确配置网络，以管理这三种类型的流量并提供控制和安全性。

流量类型

| 流量类型 | **Description** | 网络类型 |
| --- | --- | --- |
| 网格流量 | 网格中所有节点之间传输的内部 StorageGRID 流量。所有网格节点都必须能够通过此网络与所有其他网格节点进行通信。 | 网格网络（必需） |
| 管理流量 | 用于系统管理和维护的流量。 | 管理网络（可选） |
| 客户端流量 | 在外部客户端应用程序和网格之间传输的流量，包括来自 S3 和 Swift 客户端的所有对象存储请求。 | 客户端网络（可选） |

您可以通过以下方式配置网络：

- 仅限网格网络
- 网格和管理网络
- 网格和客户端网络
- 网格网络，管理网络和客户端网络

网格网络是必需的，可以管理所有网格流量。管理员和客户端网络可以在安装时包括在内，也可以稍后添加，以适应需求的变化。尽管管理网络和客户端网络是可选的，但在使用这些网络处理管理和客户端流量时，网格网络可以实现隔离和安全。

网络接口

StorageGRID 节点使用以下特定接口连接到每个网络：

| 网络 | 接口名称 |
| --- | --- |
| 网格网络（必需） | eth0 |
| 管理网络（可选） | Eth1 |
| 客户端网络（可选） | Eth2 |

有关将虚拟或物理端口映射到节点网络接口的详细信息、请参见安装说明。

您必须为节点上启用的每个网络配置以下内容：

- IP 地址
- 子网掩码
- 网关 IP 地址

您只能为每个网格节点上的三个网络中的每个网络配置一个 IP 地址 / 掩码 / 网关组合。如果不想为网络配置网关，应使用 IP 地址作为网关地址。

通过高可用性(High Availability、HA)组、可以向网格或客户端网络接口添加虚拟IP地址。有关详细信息，请参见有关管理 StorageGRID 的说明。

网格网络

网格网络为必填项。它用于所有内部 StorageGRID 流量。网格网络可在网格中的所有节点之间以及所有站点和子网之间建立连接。网格网络上的所有节点必须能够与所有其他节点进行通信。网格网络可以包含多个子网。包含 NTP 等关键网格服务的网络也可以添加为网格子网。

StorageGRID 不支持节点之间的网络地址转换（ Network Address Translation ， NAT ）。

网格网络可用于所有管理流量和所有客户端流量，即使已配置管理网络和客户端网络也是如此。除非节点配置了客户端网络，否则网格网络网关是节点的默认网关。

在配置网格网络时，您必须确保网络不受不可信客户端的保护，例如在开放式 Internet 上的客户端。

请注意网格网络的以下要求和详细信息：

- 如果存在多个网格子网，则必须配置网格网络网关。
- 网格网络网关是节点默认网关，直到网格配置完成为止。
- 系统会自动为所有节点生成静态路由，并发送到全局网格网络子网列表中配置的所有子网。
- 如果添加了客户端网络，则在网格配置完成后，默认网关将从网格网络网关切换到客户端网络网关。

管理网络

管理网络是可选的。配置后，它可用于系统管理和维护流量。管理网络通常是一个专用网络，不需要在节点之间进行路由。

您可以选择应在哪些网格节点上启用管理网络。

通过使用管理网络、管理和维护流量无需通过网格网络传输。管理网络的典型用途包括：访问Grid Manager用户界面；访问NTP、DNS、外部密钥管理(KMS)和轻型目录访问协议(LDAP)等关键服务；访问管理节点上的审核日志；以及访问安全Shell协议(SSH)进行维护和支持。

管理网络决不用于内部网格流量。提供了一个管理网络网关，允许管理网络与多个外部子网进行通信。但是，管理网络网关绝不会用作节点默认网关。

请注意管理网络的以下要求和详细信息：

- 如果要从管理网络子网外部进行连接或配置了多个管理网络子网，则需要使用管理网络网关。
- 系统会为节点的管理网络子网列表中配置的每个子网创建静态路由。

客户端网络

客户端网络是可选的。配置后，它可用于为 S3 和 Swift 等客户端应用程序提供对网格服务的访问。如果您计划使外部资源（例如云存储池或 StorageGRID CloudMirror 复制服务）可以访问 StorageGRID 数据，则外部资源也可以使用客户端网络。网格节点可以与可通过客户端网络网关访问的任何子网进行通信。

您可以选择应在哪些网格节点上启用客户端网络。所有节点不必位于同一客户端网络上，并且节点永远不会通过客户端网络彼此通信。网格安装完成后，客户端网络才会运行。

为了提高安全性，您可以指定节点的客户端网络接口不可信，以便客户端网络在允许的连接方面更具限制性。如果节点的客户端网络接口不可信，则该接口会接受出站连接，例如 CloudMirror 复制使用的连接，但仅接受已明确配置为负载平衡器端点的端口上的入站连接。有关不可信客户端网络功能和负载平衡器服务的详细信息、请参见有关管理StorageGRID 的说明。

使用客户端网络时，客户端流量不需要通过网格网络传输。网格网络流量可以分隔到安全的不可路由网络上。以下节点类型通常配置有客户端网络：

- 网关节点，因为这些节点可提供对 StorageGRID 负载平衡器服务的访问以及 S3 和 Swift 客户端对网格的访问。
- 存储节点，因为这些节点提供对 S3 和 Swift 协议以及云存储池和 CloudMirror 复制服务的访问。
- 管理节点、以确保租户用户无需使用管理网络即可连接到租户管理器。

对于客户端网络、请注意以下事项：

- 如果配置了客户端网络，则需要客户端网络网关。
- 网格配置完成后，客户端网络网关将成为网格节点的默认路由。

相关信息

"网络连接要求和准则"

"管理 StorageGRID"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

## 网络拓扑示例

### 除了所需的网格网络之外、在为单站点或多站点部署设计网络拓扑时、您还可以选择是配置管理网络接口还是客户端网络接口。

内部端口只能通过网格网络访问。可以从所有网络类型访问外部端口。这种灵活性为设计 StorageGRID 部署以及在交换机和防火墙中设置外部 IP 和端口筛选提供了多种选项。有关内部和外部端口的详细信息、请参见网络端口参考。

如果您指定节点的客户端网络接口不可信、请配置负载平衡器端点以接受入站流量。有关配置不可信客户端网络和负载平衡器端点的信息、请参见有关管理StorageGRID 的说明。

相关信息

"管理 StorageGRID"

"网络端口参考"

网格网络拓扑

### 最简单的网络拓扑只能通过配置网格网络来创建。

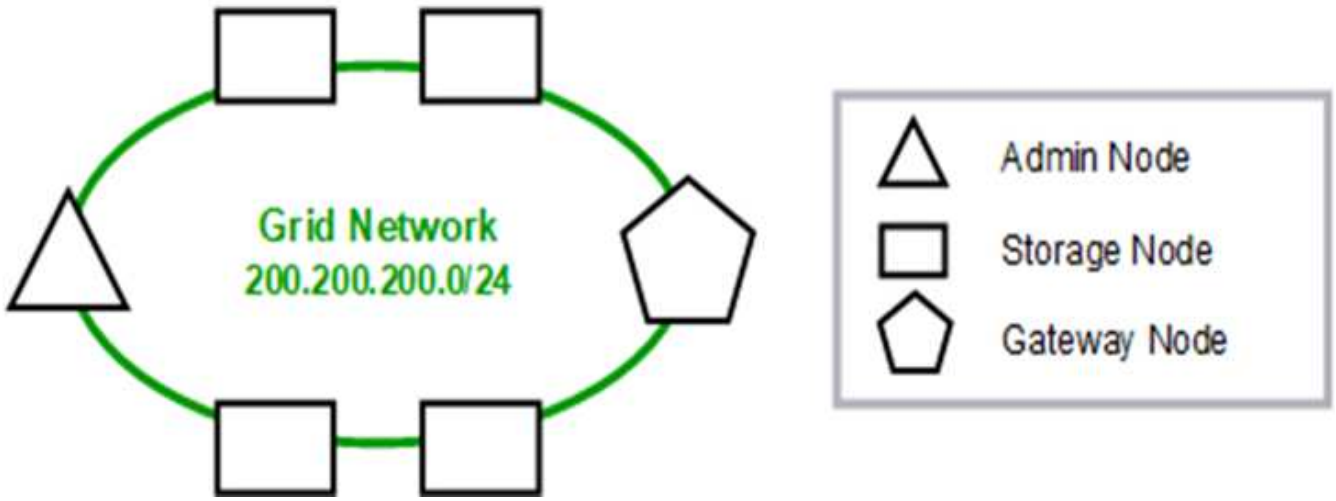
配置网格网络时，您需要为每个网格节点的 eth0 接口建立主机 IP 地址，子网掩码和网关 IP 地址。

在配置期间，必须将所有网格网络子网添加到网格网络子网列表（ GSLL ）中。此列表包括所有站点的所有子网，并且可能还包括外部子网，这些子网可提供对 NTP ， DNS 或 LDAP 等关键服务的访问权限。

在安装时，网格网络接口会对 GNSL 中的所有子网应用静态路由，如果配置了网格网络网关，则会将节点的默认路由设置为网格网络网关。如果没有客户端网络，并且网格网络网关是节点的默认路由，则不需要使用 GNSL 。此外，还会生成到网格中所有其他节点的主机路由。

在此示例中，所有流量共享同一网络，包括与 S3 和 Swift 客户端请求以及管理和维护功能相关的流量。

> 此拓扑适用于外部不可用的单站点部署，概念验证或测试部署，或者当第三方负载平衡器充当客户端访问边界时。如果可能，网格网络应专门用于内部流量。管理网络和客户端网络都具有其他防火墙限制，可阻止外部向内部服务发送流量。支持对外部客户端流量使用网格网络，但这种使用可提供更少的保护层。




*Provisioned*

**GNSL → 200.200.200.0/24**

| | Grid Network | |
|---|---|---|
| **Nodes** | **IP/mask** | **Gateway** |
| Admin | 200.200.200.32/24 | 200.200.200.1 |
| Storage | 200.200.200.33/24 | 200.200.200.1 |
| Storage | 200.200.200.34/24 | 200.200.200.1 |
| Storage | 200.200.200.35/24 | 200.200.200.1 |
| Storage | 200.200.200.36/24 | 200.200.200.1 |
| Gateway | 200.200.200.37/24 | 200.200.200.1 |

*System Generated*

| Nodes | Routes | | | Type | From |
|---|---|---|---|---|---|
| All | 0.0.0.0/0 | → | 200.200.200.1 | Default | Grid Network gateway |
| | 200.200.200.0/24 | → | eth0 | Link | Interface IP/mask |

管理网络拓扑

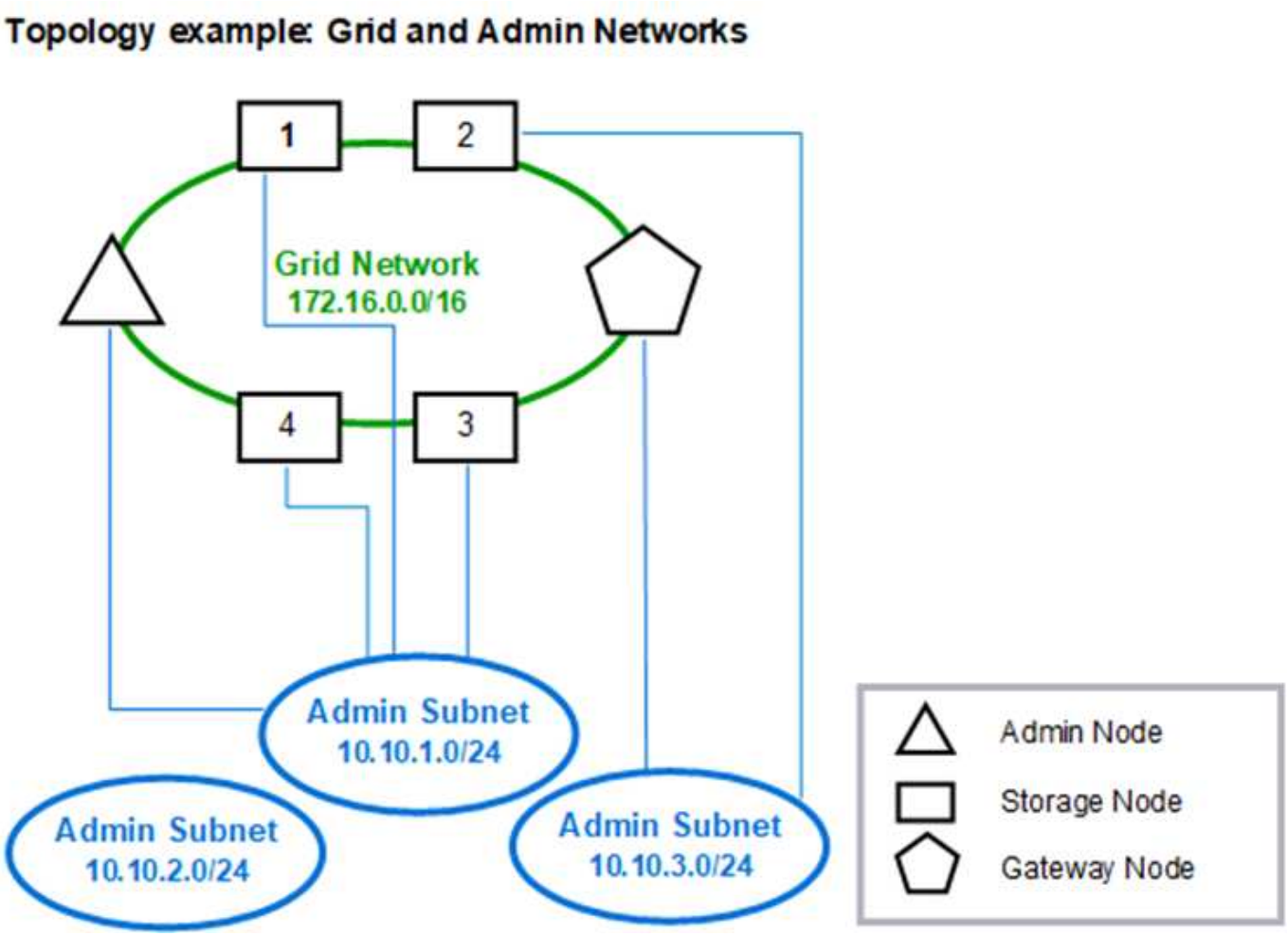
## 可以选择使用管理网络。使用管理网络和网格网络的一种方法是，为每个节点配置可路由的网格网络和有限制的管理网络。

配置管理网络时，您需要为每个网格节点的 eth1 接口建立主机 IP 地址，子网掩码和网关 IP 地址。

管理网络对于每个节点都是唯一的，并且可以包含多个子网。可以为每个节点配置一个管理外部子网列表（ Admin External Subnet List ， AESL ）。AESL 列出了每个节点可通过管理网络访问的子网。AESL 还必须包括网格通过管理网络访问的任何服务的子网，例如 NTP ， DNS ， KMS 和 LDAP 。AESL 中的每个子网都应用静态路由。

在此示例中，网格网络用于处理与 S3 和 Swift 客户端请求以及对象管理相关的流量。而管理网络则用于管理功

能。


Topology example: Grid and Admin Networks
1
2
Grid Network
172.16.0.0/16
4
3
Admin Subnet
10.10.1.0/24
Admin Subnet
10.10.2.0/24
Admin Subnet
10.10.3.0/24
Admin Node
Storage Node
Gateway Node

*Provisioned*

**GNSL → 172.16.0.0/16**

**AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24**

| | Grid Network | | Admin Network | |
|---|---|---|---|---|
| **Nodes** | **IP/mask** | **Gateway** | **IP/mask** | **Gateway** |
| Admin | 172.16.200.32/24 | 172.16.200.1 | 10.10.1.10/24 | 10.10.1.1 |
| Storage 1 | 172.16.200.33/24 | 172.16.200.1 | 10.10.1.11/24 | 10.10.1.1 |
| Storage 2 | 172.16.200.34/24 | 172.16.200.1 | 10.10.3.65/24 | 10.10.3.1 |
| Storage 3 | 172.16.200.35/24 | 172.16.200.1 | 10.10.1.12/24 | 10.10.1.1 |
| Storage 4 | 172.16.200.36/24 | 172.16.200.1 | 10.10.1.13/24 | 10.10.1.1 |
| Gateway | 172.16.200.37/24 | 172.16.200.1 | 10.10.3.66/24 | 10.10.3.1 |

*System Generated*

| **Nodes** | **Routes** | | | **Type** | **From** |
|---|---|---|---|---|---|
| All | 0.0.0.0/0 | → | 172.16.200.1 | Default | Grid Network gateway |
| Admin, Storage 1, 3, and 4 | 172.16.0.0/16 | → | eth0 | Static | GNSL |
| | 10.10.1.0/24 | → | eth1 | Link | Interface IP/mask |
| | 10.10.2.0/24 | → | 10.10.1.1 | Static | AESL |
| | 10.10.3.0/24 | → | 10.10.1.1 | Static | AESL |
| Storage 2, Gateway | 172.16.0.0/16 | → | eth0 | Static | GNSL |
| | 10.10.1.0/24 | → | 10.10.3.1 | Static | AESL |
| | 10.10.2.0/24 | → | 10.10.3.1 | Static | AESL |
| | 10.10.3.0/24 | → | eth1 | Link | Interface IP/mask |

客户端网络拓扑

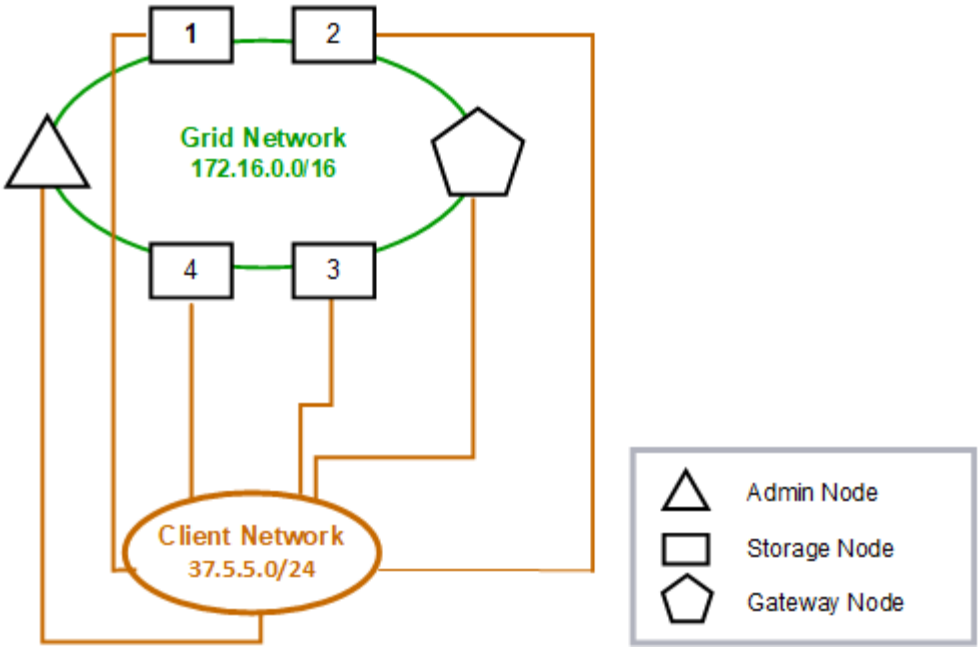
可以选择使用客户端网络。使用客户端网络可以将客户端网络流量（例如 S3 和 Swift ）与网格内部流量分隔开，从而提高网格网络连接的安全性。如果未配置管理网络，则可通过客户端网络或网格网络处理管理流量。

配置客户端网络时，您需要为所配置节点的 eth2 接口建立主机 IP 地址，子网掩码和网关 IP 地址。每个节点的客户端网络可以独立于任何其他节点上的客户端网络。

如果在安装期间为节点配置客户端网络，则在安装完成后，节点的默认网关将从网格网络网关切换到客户端网络网关。如果稍后添加客户端网络，则节点的默认网关将以相同方式进行切换。

在此示例中，客户端网络用于处理 S3 和 Swift 客户端请求以及管理功能，而网格网络则专用于内部对象管理操作。

**Topology example: Grid and Client Networks**




*Provisioned*

**GNSL → 172.16.0.0/16**

| Nodes | Grid Network IP/mask | Client Network IP/mask | Client Network Gateway |
|---|---|---|---|
| Admin | 172.16.200.32/24 | 37.5.5.10/24 | 37.5.5.1 |
| Storage | 172.16.200.33/24 | 37.5.5.11/24 | 37.5.5.1 |
| Storage | 172.16.200.34/24 | 37.5.5.12/24 | 37.5.5.1 |
| Storage | 172.16.200.35/24 | 37.5.5.13/24 | 37.5.5.1 |
| Storage | 172.16.200.36/24 | 37.5.5.14/24 | 37.5.5.1 |
| Gateway | 172.16.200.37/24 | 37.5.5.15/24 | 37.5.5.1 |

*System Generated*

| Nodes | Routes | | | Type | From |
|---|---|---|---|---|---|
| All | 0.0.0.0/0 | → | 37.5.5.1 | Default | Client Network gateway |
| | 172.16.0.0/16 | → | eth0 | Link | Interface IP/mask |
| | 37.5.5.0/24 | → | eth2 | Link | Interface IP/mask |

所有这三个网络的拓扑结构

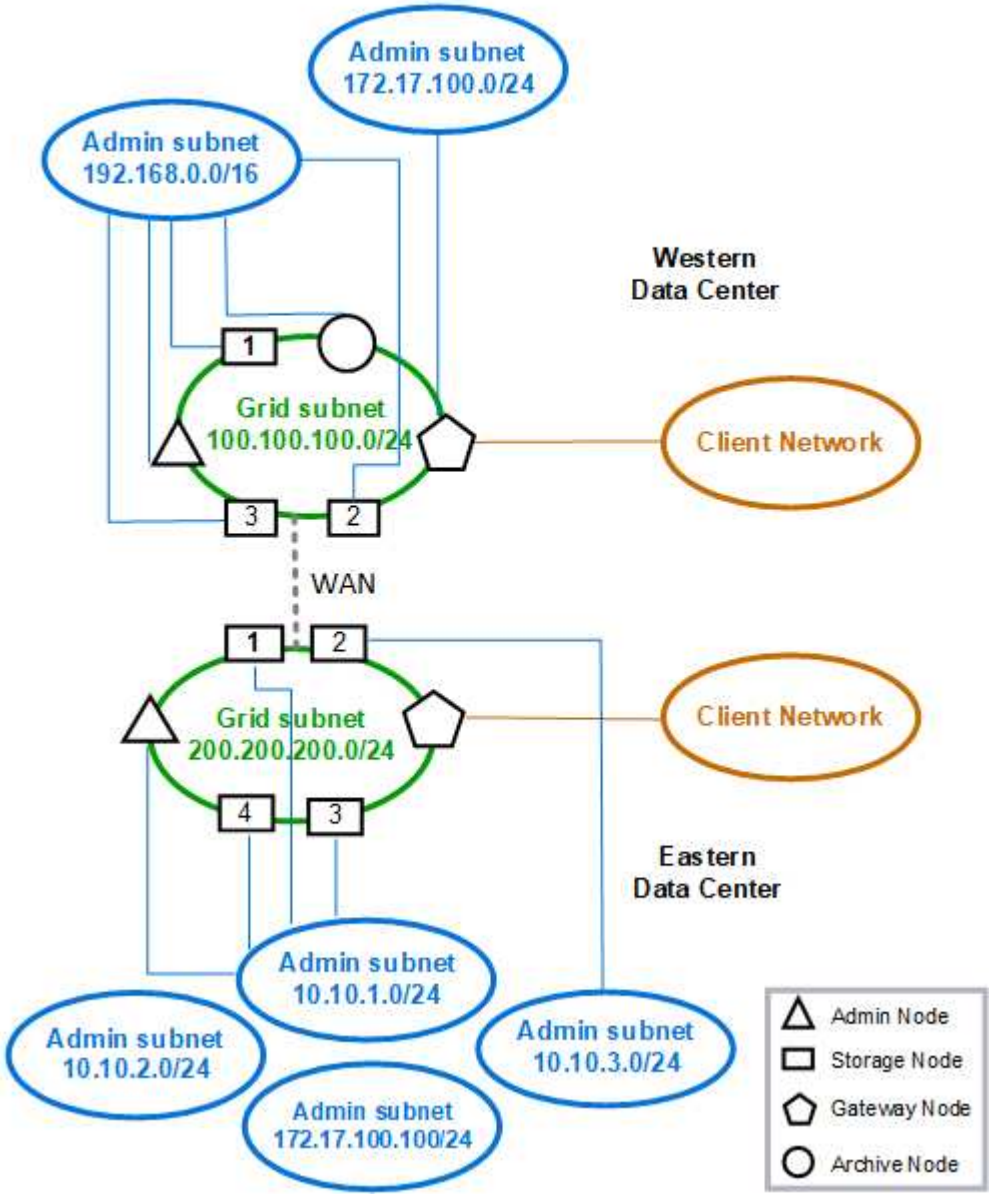
您可以将所有这三个网络配置为一个网络拓扑，其中包括专用网格网络，特定于特定于站点的受限制管理网络和开放式客户端网络。如果需要，使用负载平衡器端点和不可信的客

户端网络可以提供额外的安全性。

在此示例中：

- 网格网络用于处理与内部对象管理操作相关的网络流量。
- 管理网络用于处理与管理功能相关的流量。
- 客户端网络用于处理与 S3 和 Swift 客户端请求相关的流量。

**Topology example: Grid, Admin, and Client Networks**




# 网络要求

您必须验证当前的网络基础架构和配置是否可以支持计划的 StorageGRID 网络设计。

## 一般网络连接要求

所有 StorageGRID 部署都必须能够支持以下连接。

这些连接可以通过网格网络，管理网络或客户端网络进行，也可以通过这些网络的组合进行，如网络拓扑示例所示。

- * 管理连接 * ： 管理员到节点的入站连接，通常通过 SSH 。通过 Web 浏览器访问网格管理器，租户管理器和 StorageGRID 设备安装程序。
- * NTP 服务器连接 * ： 接收入站 UDP 响应的出站 UDP 连接。

  主管理节点必须至少可访问一个 NTP 服务器。

- * DNS 服务器连接 * ： 接收入站 UDP 响应的出站 UDP 连接。
- * LDAP/Active Directory 服务器连接 * ： 从存储节点上的身份服务发出的出站 TCP 连接。
- * AutoSupport ： 从管理节点到eithersupport.netapp.com或客户配置的代理的出站TCP连接。
- * 外部密钥管理服务器 * ： 启用节点加密的每个设备节点的出站 TCP 连接。
- 来自 S3 和 Swift 客户端的入站 TCP 连接。
- 来自云镜像复制等StorageGRID 平台服务或云存储池的出站请求。

如果 StorageGRID 无法使用默认路由规则与任何已配置的 NTP 或 DNS 服务器建立联系，则只要指定了 DNS 和 NTP 服务器的 IP 地址，它就会自动尝试在所有网络（网格，管理员和客户端）上进行联系。如果可以在任何网络上访问 NTP 或 DNS 服务器， StorageGRID 将自动创建其他路由规则，以确保将来尝试连接到该网络时都使用该网络。

> 虽然您可以使用这些自动发现的主机路由，但通常应手动配置 DNS 和 NTP 路由，以确保在自动发现失败时连接。

如果您尚未准备好在部署期间配置可选的管理和客户端网络，则可以在配置步骤期间批准网格节点时配置这些网络。此外、您还可以使用恢复和维护说明中所述的更改IP工具在安装完成后配置这些网络。

## 管理节点和网关节点的连接

管理节点必须始终受到不可信客户端的保护，例如在开放式 Internet 上的客户端。您必须确保任何不可信的客户端都不能访问网格网络，管理网络或客户端网络上的任何管理节点。

要添加到高可用性组的管理节点和网关节点必须使用静态 IP 地址进行配置。请参见有关管理StorageGRID 的说明中有关高可用性组的信息。

## 使用网络地址转换（ **Network Address Translation ， NAT** ）

请勿在网格节点之间或 StorageGRID 站点之间的网格网络上使用网络地址转换（ Network Address Translation ， NAT ）。如果您对网格网络使用专用 IPv4 地址，则这些地址必须可从每个站点的每个网格节点直接路由。但是，您可以根据需要在外部客户端和网格节点之间使用 NAT ，例如为网关节点提供公有 IP 地址。只有在使用对网格中的所有节点都透明的通道应用程序时，才支持使用 NAT 桥接公有 网段，这意味着网格节点不需要了解公有 IP 地址。

相关信息

"网格入门"

"管理 StorageGRID"

"保持并恢复()"

# 网络特定要求

请按照每种 StorageGRID 网络类型的要求进行操作。

## 网络网关和路由器

- 如果设置了此值，则给定网络的网关必须位于特定网络的子网内。
- 如果使用静态寻址配置接口，则必须指定 0.0.0.0 以外的网关地址。
- 如果您没有网关，则最佳做法是将网关地址设置为网络接口的 IP 地址。

## Subnets

每个网络都必须连接到其自身的子网，而该子网不会与节点上的任何其他网络重叠。

网格管理器会在部署期间强制实施以下限制。此处提供这些配置文件，用于协助进行部署前网络规划。

- 任何网络 IP 地址的子网掩码不能为 255.255.255.254 或 255.255.255.255 （ CIDR 表示法为 /31 或 /32 ）。
- 网络接口 IP 地址和子网掩码（ CIDR ）定义的子网不能与同一节点上配置的任何其他接口的子网重叠。
- 每个节点的网格网络子网必须包含在 GNSL 中。
- 管理网络子网不能与网格网络子网，客户端网络子网或 GNSL 中的任何子网重叠。
- AESL 中的子网不能与 GNSL 中的任何子网重叠。
- 客户端网络子网不能与网格网络子网，管理网络子网， GNSL 中的任何子网或 AESL 中的任何子网重叠。

## 网格网络

- 在部署时，每个网格节点都必须连接到网格网络，并且必须能够使用部署节点时指定的网络配置与主管理节点进行通信。
- 在正常网格操作期间，每个网格节点都必须能够通过网格网络与所有其他网格节点进行通信。

网格网络必须在每个节点之间直接可路由。不支持节点之间的网络地址转换（ Network Address Translation ， NAT ）。

- 如果网格网络包含多个子网，请将其添加到网格网络子网列表（ GSLL ）中。在 GNSL 中的每个子网的所有节点上创建静态路由。

## 管理网络

管理网络是可选的。如果您计划配置管理网络，请遵循以下要求和准则。

管理网络的典型用途包括管理连接， AutoSupport ， KMS 以及与 NTP ， DNS 和 LDAP 等关键服务器的连接（如果这些连接不是通过网格网络或客户端网络提供的）。

只要所需的网络服务和客户端可访问，管理网络和 AESL 就可以对每个节点唯一。

要从外部子网启用入站连接，必须在管理网络上至少定义一个子网。AESL 中的每个子网都会在每个节点上自动生成静态路由。

### 客户端网络

客户端网络是可选的。如果您计划配置客户端网络，请注意以下事项。

客户端网络用于支持来自 S3 和 Swift 客户端的流量。如果已配置，客户端网络网关将成为节点的默认网关。

如果您使用客户端网络，则可以通过仅接受显式配置的负载平衡器端点上的入站客户端流量来帮助保护 StorageGRID 免受恶意攻击。请参见有关管理StorageGRID 的说明中有关管理负载平衡和管理不可信客户端网络的信息。

相关信息

"管理 StorageGRID"

# 部署特定的网络注意事项

根据您使用的部署平台、您可能还需要考虑StorageGRID 网络设计的其他注意事项。

网格节点可部署为：

- 在VMware vSphere Web Client中部署为虚拟机的基于软件的网格节点
- 基于软件的网格节点、部署在Linux主机上的Docker容器中
- 基于设备的节点

有关网格节点的追加信息 、请参见_Grid primer_。

相关信息

"网格入门"

### Linux 部署

为了提高效率、可靠性和安全性、StorageGRID 系统在Linux上作为一组Docker容器运行。StorageGRID 系统不需要配置与Docker相关的网络。

使用非绑定设备作为容器网络接口，例如 VLAN 或虚拟以太网（ Veth ）对。在节点配置文件中指定此设备作为网络接口。

请勿直接使用绑定或网桥设备作为容器网络接口。这样做可能会由于内核问题描述 在容器命名空间中对绑定和网桥设备使用 macvlan 而阻止节点启动。

请参见Red Hat Enterprise Linux/CentOS或Ubuntu或Debian部署的安装说明。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

## 适用于**Docker**部署的主机网络配置

在Docker容器平台上开始StorageGRID 部署之前、请确定每个节点要使用的网络(网格、管理、客户端)。您必须确保在正确的虚拟或物理主机接口上配置每个节点的网络接口，并且每个网络都有足够的带宽。

物理主机

如果使用物理主机支持网格节点：

- 确保所有主机对每个节点接口使用相同的主机接口。此策略可简化主机配置，并支持将来的节点迁移。
- 获取物理主机本身的 IP 地址。

> 主机本身以及主机上运行的一个或多个节点均可使用主机上的物理接口。分配给使用此接口的主机或节点的任何 IP 地址都必须是唯一的。主机和节点不能共享 IP 地址。

- 打开主机所需的端口。

最小带宽建议

下表提供了每种类型的 StorageGRID 节点和每种网络的最小带宽建议。您必须为每个物理或虚拟主机配置足够的网络带宽，以满足计划在该主机上运行的 StorageGRID 节点总数和类型的聚合最小带宽要求。

| 节点类型 | 网络类型 | | |
|---|---|---|---|
| | 网格 | 管理员 | 客户端 |
| 管理员 | 10 Gbps | 1 Gbps | 1 Gbps |
| 网关 | 10 Gbps | 1 Gbps | 10 Gbps |
| 存储 | 10 Gbps | 1 Gbps | 10 Gbps |
| 归档 | 10 Gbps | 1 Gbps | 10 Gbps |

> 此表不包括访问共享存储所需的 SAN 带宽。如果您使用的是通过以太网（ iSCSI 或 FCoE ）访问的共享存储，则应在每个主机上配置单独的物理接口，以提供足够的 SAN 带宽。为了避免出现瓶颈，给定主机的 SAN 带宽应大致与该主机上运行的所有存储节点的聚合存储节点网络带宽匹配。

使用下表根据计划在每个主机上运行的 StorageGRID 节点的数量和类型确定要在该主机上配置的最小网络接口

数。

例如，要在单个主机上运行一个管理节点，一个网关节点和一个存储节点，请执行以下操作：

- 连接管理节点上的网格和管理网络（需要 10 + 1 = 11 Gbps ）
- 连接网关节点上的网格和客户端网络（需要 10 + 10 = 20 Gbps ）
- 在存储节点上连接网格网络（需要 10 Gbps ）

在这种情况下，您应至少提供 11 + 20 + 10 = 41 Gbps 的网络带宽， 可通过两个 40 Gbps 接口或五个 10 Gbps 接口来满足，这些接口可能聚合为中继，然后由三个或更多 VLAN 共享，这些 VLAN 承载主机所在物理数据中心的本地网格，管理和客户端子网。

有关在StorageGRID 集群中的主机上配置物理和网络资源以准备StorageGRID 部署的一些建议方法、请参见适用于Linux平台的安装说明中有关配置主机网络的信息。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

## 用于平台服务和云存储池的网络和端口

如果您计划使用 StorageGRID 平台服务或云存储池，则必须配置网格网络和防火墙以确保可以访问目标端点。平台服务包括提供搜索集成、事件通知和CloudMirror复制的外部服务。

平台服务需要从托管 StorageGRID ADA 服务的存储节点访问外部服务端点。提供访问权限的示例包括：

- 在具有 ADE 服务的存储节点上，使用路由到目标端点的 AESL 条目配置唯一管理网络。
- 依靠客户端网络提供的默认路由。在此示例中、可以使用不可信客户端网络功能限制入站连接。

云存储池还需要从存储节点访问所使用的外部服务提供的端点，例如 Amazon S3 Glacier 或 Microsoft Azure Blob 存储。

默认情况下，平台服务和云存储池通信使用以下端口：

- * 80*：对于以开头的端点URI `http`
- * 443：对于以开头的端点URI `https`

创建或编辑端点时，可以指定其他端口。

如果您使用的是非透明代理服务器、则还必须配置代理设置、以允许将消息发送到外部端点、例如Internet上的端点。请参见管理StorageGRID 以了解如何配置代理设置。

有关不可信客户端网络的详细信息、请参见有关管理StorageGRID 的说明。有关平台服务的详细信息、请参见有关使用租户帐户的说明。有关云存储池的详细信息、请参见有关通过信息生命周期管理来管理对象的说明。

相关信息

"网络端口参考"

"网格入门"

"管理 StorageGRID"

"使用租户帐户"

"使用 ILM 管理对象"

### 设备节点

您可以将 StorageGRID 设备上的网络端口配置为使用符合吞吐量，冗余和故障转移要求的端口绑定模式。

可以在固定或聚合绑定模式下配置 StorageGRID 设备上的 10/225-GbE 端口，以便连接到网格网络和客户端网络。

可以在独立或主动备份模式下配置 1-GbE 管理网络端口，以便连接到管理网络。

请参见设备安装和维护说明中有关端口绑定模式的信息。

相关信息

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

## 网络安装和配置

您必须了解在节点部署和网格配置期间如何使用网格网络以及可选的管理和客户端网络。

### 节点的初始部署

首次部署节点时，必须将节点连接到网格网络，并确保其能够访问主管理节点。如果网格网络已隔离，则可以在主管理节点上配置管理网络，以便从网格网络外部进行配置和安装访问。

配置了网关的网格网络将在部署期间成为节点的默认网关。默认网关允许不同子网上的网格节点在配置网格之前与主管理节点进行通信。

如有必要，还可以将包含 NTP 服务器或需要访问网格管理器或 API 的子网配置为网格子网。

### 自动向主管理节点注册节点

部署节点后，它们会使用网格网络向主管理节点注册自己。然后、您可以使用网格管理器、即 `configure-storagegrid.py` Python脚本或安装API、用于配置网格并批准注册的节点。在网格配置期间，您可以配置多个网格子网。完成网格配置后，系统将在每个节点上创建通过网格网络网关到这些子网的静态路由。

### 禁用管理网络或客户端网络

如果要禁用管理网络或客户端网络、您可以在节点批准过程中从其中删除配置、也可以在安装完成后使用更改IP工具。请参见恢复和维护说明中有关网络维护过程的信息。

相关信息

"保持并恢复()"

# 安装后准则

完成网格节点部署和配置后，请按照以下准则更改 DHCP 地址和网络配置。

- 如果使用 DHCP 分配 IP 地址，请为所使用网络上的每个 IP 地址配置 DHCP 预留。

  您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。

  > 当节点的 IP 地址发生更改时，节点会重新启动，如果 DHCP 地址更改同时影响多个节点，则发生原因 可能会中断。

- 如果要更改网格节点的 IP 地址，子网掩码和默认网关，必须使用更改 IP 过程。请参见恢复和维护说明中有关配置IP地址的信息。
- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改，您可能需要重新建立这些连接。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

"保持并恢复()"

# 网络端口参考

您必须确保网络基础架构能够在网格内的节点之间以及与外部客户端和服务之间提供内部和外部通信。您可能需要跨内部和外部防火墙，交换系统和路由系统进行访问。

使用为内部网格节点通信和外部通信提供的详细信息来确定如何配置每个所需端口。

- "内部网格节点通信"
- "外部通信"

## 内部网格节点通信

StorageGRID 内部防火墙仅允许传入网格网络上的特定端口，但端口 22 ， 80 ， 123 和 443 除外（请参见有关外部通信的信息）。负载平衡器端点定义的端口也接受连接。

NetApp 建议您在网格节点之间启用 Internet 控制消息协议（ Internet Control Message Protocol ， ICMP ）流量。如果无法访问网格节点，则允许 ICMP 流量可以提高故障转移性能。

除了 ICMP 和表中列出的端口之外， StorageGRID 还使用虚拟路由器冗余协议（ VRRP ）。VRRP 是一种使用 IP 协议编号 112 的 Internet 协议。StorageGRID 仅在单播模式下使用 VRRP 。只有在配置了高可用性(HA)组时、才需要VRRP。

### 基于 **Linux** 的节点的准则

如果企业网络策略限制对其中任何端口的访问，则可以在部署时使用部署配置参数重新映射端口。有关端口重新映射和部署配置参数的详细信息、请参见适用于Linux平台的安装说明。

### 基于 **VMware** 的节点的准则

只有在需要定义 VMware 网络外部的防火墙限制时，才配置以下端口。

如果企业网络策略限制对其中任何端口的访问，则可以在使用 VMware vSphere Web Client 部署节点时重新映射端口，也可以在自动部署网格节点时使用配置文件设置重新映射端口。有关端口重新映射和部署配置参数的详细信息、请参见VMware的安装说明。

### 设备存储节点准则

如果企业网络策略限制对其中任何端口的访问，则可以使用 StorageGRID 设备安装程序重新映射端口。有关设备端口重新映射的详细信息、请参见存储设备的安装说明。

### **StorageGRID** 内部端口

| Port | TCP 或 UDP | from | 收件人： | 详细信息 |
|---|---|---|---|---|
| 22. | TCP | 主管理节点 | 所有节点 | 在维护过程中，主管理节点必须能够通过端口 22 上的 SSH 与所有其他节点进行通信。允许来自其他节点的 SSH 流量是可选的。 |
| 80 | TCP | 设备 | 主管理节点 | StorageGRID 设备使用此节点与主管理节点进行通信以启动安装。 |

| | | | | |
|---|---|---|---|---|
| 123. | UDP | 所有节点 | 所有节点 | 网络时间协议服务。每个节点都使用 NTP 与其他节点同步其时间。 |
| 443. | TCP | 所有节点 | 主管理节点 | 用于在安装和其他维护过程中与主管理节点进行状态通信。 |
| 1139. | TCP | 存储节点 | 存储节点 | 存储节点之间的内部流量。 |
| 1501 | TCP | 所有节点 | 具有模块转换器的存储节点 | 报告，审核和配置内部流量。 |
| 1502 | TCP | 所有节点 | 存储节点 | 与 S3 和 Swift 相关的内部流量。 |
| 1504 | TCP | 所有节点 | 管理节点 | NMS 服务报告和配置内部流量。 |
| 1505. | TCP | 所有节点 | 管理节点 | AMS 服务内部流量。 |
| 1506. | TCP | 所有节点 | 所有节点 | 服务器状态内部流量。 |
| 1507. | TCP | 所有节点 | 网关节点 | 负载平衡器内部流量。 |
| 1508. | TCP | 所有节点 | 主管理节点 | 配置管理内部流量。 |
| 1509. | TCP | 所有节点 | 归档节点 | 归档节点内部流量。 |
| 1511 | TCP | 所有节点 | 存储节点 | 元数据内部流量。 |
| 5353 | UDP | 所有节点 | 所有节点 | 也可用于在安装，扩展和恢复期间进行全网格 IP 更改以及主管理节点发现。 |
| 7001 | TCP | 存储节点 | 存储节点 | Cassandra TLS 节点间集群通信。 |
| 7443 | TCP | 所有节点 | 管理节点 | 维护过程和错误报告的内部流量。 |

| | | | | |
|---|---|---|---|---|
| 9042 | TCP | 存储节点 | 存储节点 | Cassandra 客户端端口。 |
| 9999 | TCP | 所有节点 | 所有节点 | 多个服务的内部流量。包括维护过程，指标和网络更新。 |
| 10226 | TCP | 存储节点 | 主管理节点 | 由 StorageGRID 设备使用，用于将 AutoSupport 消息从 E 系列 SANtricity 系统管理器转发到主管理节点。 |
| 11139. | TCP | 归档 / 存储节点 | 归档 / 存储节点 | 存储节点和归档节点之间的内部流量。 |
| 18000 | TCP | 管理 / 存储节点 | 具有模块转换器的存储节点 | 帐户服务内部流量。 |
| 18001 | TCP | 管理 / 存储节点 | 具有模块转换器的存储节点 | 身份联合内部流量。 |
| 18002 | TCP | 管理 / 存储节点 | 存储节点 | 与对象协议相关的内部 API 流量。 |
| 18003 | TCP | 管理 / 存储节点 | 具有模块转换器的存储节点 | 平台为内部流量提供服务。 |
| 18017 | TCP | 管理 / 存储节点 | 存储节点 | 数据移动服务为云存储池提供内部流量。 |
| 18019 | TCP | 存储节点 | 存储节点 | 用于纠删编码的区块服务内部流量。 |
| 18082 | TCP | 管理 / 存储节点 | 存储节点 | 与 S3 相关的内部流量。 |
| 18083. | TCP | 所有节点 | 存储节点 | 与 Swift 相关的内部流量。 |
| 18200 年 | TCP | 管理 / 存储节点 | 存储节点 | 有关客户端请求的其他统计信息。 |
| 19000 | TCP | 管理 / 存储节点 | 具有模块转换器的存储节点 | Keystone 服务内部流量。 |

- 相关信息 *

"外部通信"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

## 外部通信

客户端需要与网格节点进行通信才能载入和检索内容。使用的端口取决于所选的对象存储协议。这些端口需要可供客户端访问。

如果企业网络策略限制对任何端口的访问、则可以使用负载平衡器端点允许对用户定义的端口进行访问。不可信客户端网络功能只能用于允许对负载平衡器端点端口进行访问。

要使用 SMTP ， DNS ， SSH 或 DHCP 等系统和协议，您必须在部署节点时重新映射端口。但是、不应重新映射平衡器端点。有关端口重新映射的信息、请参见适用于您的平台的安装说明。

下表显示了用于向节点进行流量的端口。

此列表不包含可能配置为负载平衡器端点的端口。有关详细信息、请参见有关配置负载平衡器端点的说明。

| Port | TCP 或 UDP | 协议 | from | 收件人： | 详细信息 |
| --- | --- | --- | --- | --- | --- |
| 22. | TCP | SSH | 服务笔记本电脑 | 所有节点 | 要执行控制台步骤，需要 SSH 或控制台访问。您也可以选择使用端口 2022 ，而不是 22 。 |
| 25. | TCP | SMTP | 管理节点 | 电子邮件服务器 | 用于警报和基于电子邮件的 AutoSupport 。您可以使用电子邮件服务器页面覆盖默认端口设置 25 。 |
| 53. | TCP/UDP | DNS | 所有节点 | DNS 服务器 | 用于域名系统。 |

| Port | TCP 或 UDP | 协议 | from | 收件人： | 详细信息 |
| --- | --- | --- | --- | --- | --- |
| 67 | UDP | DHCP | 所有节点 | DHCP 服务 | 也可用于支持基于 DHCP 的网络配置。dhclient 服务不会对静态配置的网格运行。 |
| 68 | UDP | DHCP | DHCP 服务 | 所有节点 | 也可用于支持基于 DHCP 的网络配置。对于使用静态 IP 地址的网格，不会运行 dhclient 服务。 |
| 80 | TCP | HTTP | 浏览器 | 管理节点 | 端口 80 重定向到管理节点用户界面的端口 443 。 |
| 80 | TCP | HTTP | 浏览器 | 设备 | 端口 80 重定向到 StorageGRID 设备安装程序的端口 8443 。 |
| 80 | TCP | HTTP | 具有模块转换器的存储节点 | AWS | 用于发送到 AWS 或其他使用 HTTP 的外部服务的平台服务消息。创建端点时，租户可以覆盖默认的 HTTP 端口设置 80 。 |
| 80 | TCP | HTTP | 存储节点 | AWS | 发送到使用 HTTP 的 AWS 目标的云存储池请求。配置云存储池时，网格管理员可以覆盖默认的 HTTP 端口设置 80 。 |
| 111. | TCP/UDP | rpcbind | NFS 客户端 | 管理节点 | 由基于 NFS 的审核导出（ portmap ）使用。<br>• 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。 |
| 123. | UDP | NTP | 主要 NTP 节点 | 外部 NTP | 网络时间协议服务。选择为主 NTP 源的节点还会将时钟时间与外部 NTP 时间源同步。 |
| 137. | UDP | NetBIOS | SMB 客户端 | 管理节点 | 由基于 SMB 的审核导出用于需要 NetBIOS 支持的客户端。<br>• 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。 |

| Port | TCP 或 UDP | 协议 | from | 收件人： | 详细信息 |
| --- | --- | --- | --- | --- | --- |
| 138. | UDP | NetBIOS | SMB 客户端 | 管理节点 | 由基于 SMB 的审核导出用于需要 NetBIOS 支持的客户端。<br>• 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。 |
| 139. | TCP | SMB | SMB 客户端 | 管理节点 | 由基于 SMB 的审核导出用于需要 NetBIOS 支持的客户端。<br>• 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。 |
| 161. | TCP/UDP | SNMP | SNMP 客户端 | 所有节点 | 用于 SNMP 轮询。所有节点均提供基本信息；管理节点还提供警报和警报数据。配置后，默认为 UDP 端口 161 。<br>• 注： * 仅需要此端口，只有在配置了 SNMP 的情况下，才会在节点防火墙上打开此端口。如果您计划使用 SNMP ，则可以配置备用端口。<br>• 注： * 有关将 SNMP 与 StorageGRID 结合使用的信息，请联系您的 NetApp 客户代表。 |
| 162. | TCP/UDP | SNMP 通知 | 所有节点 | 通知目标 | 出站 SNMP 通知和陷阱默认为 UDP 端口 162 。<br>• 注： * 只有在启用 SNMP 并配置通知目标时，才需要此端口。如果您计划使用 SNMP ，则可以配置备用端口。<br>• 注： * 有关将 SNMP 与 StorageGRID 结合使用的信息，请联系您的 NetApp 客户代表。 |
| 389. | TCP/UDP | LDAP | 具有模块转换器的存储节点 | Active Directory/LDAP | 用于连接到 Active Directory 或 LDAP 服务器以实现身份联合。 |

| Port | TCP 或 UDP | 协议 | from | 收件人： | 详细信息 |
| --- | --- | --- | --- | --- | --- |
| 443. | TCP | HTTPS | 浏览器 | 管理节点 | 供 Web 浏览器和管理 API 客户端用于访问 Grid Manager 和租户管理器。 |
| 443. | TCP | HTTPS | 管理节点 | Active Directory | 如果启用了单点登录（ SSO ），则由连接到 Active Directory 的管理节点使用。 |
| 443. | TCP | HTTPS | 归档节点 | Amazon S3 | 用于从归档节点访问 Amazon S3 。 |
| 443. | TCP | HTTPS | 具有模块转换器的存储节点 | AWS | 用于发送到 AWS 或其他使用 HTTPS 的外部服务的平台服务消息。创建端点时，租户可以覆盖默认的 HTTP 端口设置 443 。 |
| 443. | TCP | HTTPS | 存储节点 | AWS | 发送到使用 HTTPS 的 AWS 目标的云存储池请求。配置云存储池时，网格管理员可以覆盖默认 HTTPS 端口设置 443 。 |
| 445 | TCP | SMB | SMB 客户端 | 管理节点 | 由基于 SMB 的审核导出使用。<br>• 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。 |
| 903 | TCP | NFS | NFS 客户端 | 管理节点 | 由基于NFS的审核导出使用（`rpc.mountd`）。<br>• 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。 |
| 2022 年 | TCP | SSH | 服务笔记本电脑 | 所有节点 | 要执行控制台步骤，需要 SSH 或控制台访问。您也可以选择使用端口 22 ，而不是 2022 。 |
| 2049. | TCP | NFS | NFS 客户端 | 管理节点 | 由基于 NFS 的审核导出（ NFS ）使用。<br>• 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。 |

| Port | TCP 或 UDP | 协议 | from | 收件人： | 详细信息 |
| --- | --- | --- | --- | --- | --- |
| 5696 | TCP | KMIP | 设备 | 公里 | 从配置了节点加密的设备到密钥管理服务器（ KMS ）的密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）外部流量，除非在 StorageGRID 设备安装程序的 KMS 配置页面上指定了其他端口。 |
| 8022 | TCP | SSH | 服务笔记本电脑 | 所有节点 | 端口 8022 上的 SSH 允许访问设备和虚拟节点平台上的基本操作系统，以便进行支持和故障排除。此端口不用于基于 Linux 的（裸机）节点，并且不需要在网格节点之间或在正常操作期间访问。 |
| 8082 | TCP | HTTPS | S3 客户端 | 网关节点 | 连接到网关节点(HTTPS)的S3相关外部流量。 |
| 8083. | TCP | HTTPS | Swift 客户端 | 网关节点 | 与Swift相关的外部流量传输到网关节点(HTTPS)。 |
| 8084 | TCP | HTTP | S3 客户端 | 网关节点 | 连接到网关节点(HTTP)的S3相关外部流量。 |
| 8085 | TCP | HTTP | Swift 客户端 | 网关节点 | 与Swift相关的外部流量传输到网关节点(HTTP)。 |
| 8443 | TCP | HTTPS | 浏览器 | 管理节点 | 可选。供 Web 浏览器和管理 API 客户端用于访问网格管理器。可用于分隔网格管理器和租户管理器通信。 |
| 9022 | TCP | SSH | 服务笔记本电脑 | 设备 | 在预配置模式下授予对 StorageGRID 设备的访问权限，以便提供支持和进行故障排除。在网格节点之间或正常操作期间，不需要访问此端口。 |
| 9091. | TCP | HTTPS | 外部 Grafana 服务 | 管理节点 | 由外部 Grafana 服务使用，用于安全访问 StorageGRID Prometheus 服务。<br>• 注： * 只有在启用了基于证书的 Prometheus 访问时，才需要此端口。 |

| Port | TCP 或 UDP | 协议 | from | 收件人： | 详细信息 |
| --- | --- | --- | --- | --- | --- |
| 9443 | TCP | HTTPS | 浏览器 | 管理节点 | 可选。供 Web 浏览器和管理 API 客户端用于访问租户管理器。可用于分隔网格管理器和租户管理器通信。 |
| 18082 | TCP | HTTPS | S3 客户端 | 存储节点 | 与S3相关的到存储节点的外部流量(HTTPS)。 |
| 18083. | TCP | HTTPS | Swift 客户端 | 存储节点 | 与Swift相关的存储节点外部流量(HTTPS)。 |
| 18084 | TCP | HTTP | S3 客户端 | 存储节点 | 与S3相关的存储节点外部流量(HTTP)。 |
| 18085 | TCP | HTTP | Swift 客户端 | 存储节点 | 与Swift相关的存储节点外部流量(HTTP)。 |

相关信息

"内部网格节点通信"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

## 版权信息



## 商标信息