



网络连接准则 StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/storagegrid-120/network/index.html> on July 23, 2026. Always check docs.netapp.com for the latest.

目录

网络连接准则	1
StorageGRID 网络准则	1
\${post_edited_translations.segment}	1
开始之前	1
StorageGRID 网络类型	2
流量类型	2
网络接口	2
网格网络	3
管理网络	4
客户端网络	4
可选 VLAN 网络	5
网络拓扑示例	5
StorageGRID 的网格网络拓扑	5
StorageGRID 的管理网络拓扑	6
StorageGRID 的客户端网络拓扑	8
所有三个 StorageGRID 网络的网络拓扑	10
StorageGRID 的网络要求	11
一般网络要求	11
适用于多个站点的广域网 (WAN)	12
管理节点和网关节点的连接	12
使用网络地址转换(NAT)	13
StorageGRID 的网络特定要求	13
网络网关和路由器	13
子网	13
网格网络	14
管理网络	14
客户端网络	14
特定于部署的网络注意事项	15
StorageGRID Linux 部署的网络配置	15
平台服务和云存储池的网络和端口	16
StorageGRID 设备节点的网络配置	17
StorageGRID 的网络安装和配置	17
节点的初始部署	18
使用主管理节点自动注册节点	18
禁用管理网络或客户端网络	18
StorageGRID 安装后指南	18
网络端口参考	18
StorageGRID 的内部网格节点通信	18
StorageGRID 的外部通信	21

网络连接准则

StorageGRID 网络准则

使用这些指南了解 StorageGRID 体系结构和网络拓扑，并了解网络配置和设置的要求。

`${post_edited_translations.segment}`

这些指南提供了在部署和配置 StorageGRID 节点之前可用于创建 StorageGRID 网络基础架构的信息。使用这些指南可帮助确保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能够进行通信。

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

- 存储和检索对象数据
- 接收电子邮件通知
- 访问 StorageGRID 管理接口（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(KMS)

必须适当配置 StorageGRID 网络，以处理这些功能及更多功能的流量。

开始之前

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 StorageGRID 架构，如 ["了解 StorageGRID"](#) 中所述。

确定要使用的 StorageGRID 网络以及这些网络的配置方式后，您可以按照相应的说明安装和配置 StorageGRID 节点。

安装设备节点

- ["安装设备硬件"](#)

安装基于软件的节点

- ["在基于软件的节点上安装 StorageGRID"](#)

配置并管理 StorageGRID 软件

- ["管理 StorageGRID"](#)
- ["发行说明"](#)。您必须使用您的 NetApp 帐户登录或创建帐户才能访问发行说明。

StorageGRID 网络类型

StorageGRID 系统中的网格节点处理_网络流量_、管理流量_和_客户端流量。您必须适当配置网络，以管理这三种类型的流量并提供控制 and 安全性。

流量类型

流量类型	问题描述	网络类型
网络流量	在网格中的所有节点之间传输的内部 StorageGRID 流量。所有网格节点必须能够通过此网络与所有其他网格节点通信。	网络网络（必填）
管理员流量	用于系统管理和维护的流量。	管理网络（可选）， VLAN 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 客户端的所有对象存储请求。	客户端网络（可选）， VLAN 网络（可选）

可以通过以下方式配置网络：

- 仅网络网络
- 网络和管理网络
- 网络和客户端网络
- 网络、管理和客户端网络

网络网络是强制性的，可以管理所有网络流量。管理网络和客户端网络可以在安装时加入，也可以稍后添加以适应需求变化。虽然管理网络和客户端网络是可选的，但当您使用这些网络来处理管理和客户端流量时，网络网络可以实现隔离和安全保护。

内部端口只能通过网络网络访问。外部端口可从所有网络类型访问。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 和端口过滤提供了多个选项。请参阅["内部网格节点通信"](#)和["外部通信"](#)。

网络接口

StorageGRID 节点通过以下特定接口连接到每个网络：

网络	接口名称
网络网络（必填）	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 ["在基于软件的节点上安装 StorageGRID"](#)。

设备节点

- ["SG6160 存储设备"](#)
- ["SGF6112 存储设备"](#)
- ["SG6000 存储设备"](#)
- ["SG5800 存储设备"](#)
- ["SG5700 存储设备"](#)
- ["SG110 和 SG1100 服务设备"](#)
- ["SG100 和 SG1000 服务设备"](#)

每个节点的网络信息

必须为在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

您只能为每个网络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，则应使用 IP 地址作为网关地址。

高可用性组

高可用性 (HA) 组提供将虚拟 IP (VIP) 地址添加到网格或客户端网络接口的功能。有关详细信息，请参见 ["管理高可用性组"](#)。

网格网络

网格网络是必需的。它用于所有内部 StorageGRID 流量。网格网络提供网格中所有节点之间、所有站点和子网之间的连接。网格网络上的所有节点必须能够与所有其他节点通信。网格网络可以由多个子网组成。包含关键网格服务（如 NTP）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 (NAT)。

即使配置了管理网络和客户端网络，也可以将网格网络用于所有管理流量和所有客户端流量。除非节点配置了客户端网络，否则网格网络网关是节点默认网关。



配置网格网络时，您必须确保网络免受不受信任的客户端（例如开放互联网上的客户端）的侵害。

请注意网格网络网关的以下要求和详细信息：

- 如果有多个网格子网，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。
- 系统会自动为全局网格网络子网列表中配置的所有子网的所有节点生成静态路由。
- 如果添加了客户端网络，则在完成网格配置后，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，可用于系统管理和维护流量。管理网络通常是专用网络，不需要在节点之间进行路由。

您可以选择哪些网格节点应启用管理网络。

使用管理网络时，管理和维护流量不需要跨网格网络传输。管理网络的典型用途包括以下内容：

- 访问 Grid Manager 和 Tenant Manager 用户界面。
- 访问关键服务，如 NTP 服务器、DNS 服务器、外部密钥管理服务器 (KMS) 和轻型目录访问协议 (LDAP) 服务器。
- 访问管理节点上的审核日志。
- 用于维护和支持的安全外壳协议 (SSH) 访问。

管理网络绝不会用于内部网格流量。提供了管理网络网关，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。

请注意管理网络网关的以下要求和详细信息：

- 如果将从管理网络子网外部进行连接，或者配置了多个管理网络子网，则需要管理网络网关。
- 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，它用于为 S3 等客户端应用程序提供对网格服务的访问。如果您计划使 StorageGRID 数据可供外部资源（例如，云存储池或 StorageGRID CloudMirror 复制服务）访问，则外部资源也可以使用客户端网络。网格节点可以与通过客户端网络网关可访问的任何子网通信。

您可以选择哪些网格节点应启用客户端网络。所有节点不必在同一个客户端网络上，并且节点永远不会通过客户端网络相互通信。在网格安装完成之前，客户端网络不会开始运行。

为了增加安全性，您可以指定节点的客户端网络接口不受信任，以便客户端网络对允许的连接进行更严格的限制。如果节点的客户端网络接口不受信任，则该接口将接受 CloudMirror 复制使用的出站连接，但仅接受已显式配置为负载均衡器端点的端口上的入站连接。请参阅 ["管理防火墙控件"](#) 和 ["配置负载均衡器端点"](#)。

使用客户端网络时，客户端流量不需要跨网格网络传输。网格网络流量可以分离到安全、不可路由的网络上。以下节点类型通常配置有客户端网络：

- 网关节点，因为这些节点提供对 StorageGRID 负载均衡器服务的访问权限以及对网格的 S3 客户端访问权限。
- 存储节点，因为这些节点提供对 S3 协议以及云存储池和 CloudMirror 复制服务的访问。
- 管理节点，以确保租户用户可以连接到 Tenant Manager，而无需使用管理网络。

对于客户端网络网关，请注意以下内容：

- 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。

可选 VLAN 网络

根据需要，您可以选择将虚拟 LAN (VLAN) 网络用于客户端流量和某些类型的管理员流量。但是，网络流量不能使用 VLAN 接口。节点之间的内部 StorageGRID 流量必须始终使用 eth0 上的网络网络。

要支持使用 VLAN，必须将节点上的一个或多个接口配置为交换机上的中继接口。您可以将网络网络接口 (eth0) 或客户端网络接口 (eth2) 配置为中继，也可以将中继接口添加到该节点。

如果将 eth0 配置为中继，则网络网络流量将按照交换机上的配置通过中继本机接口。同样，如果将 eth2 配置为中继，并且客户端网络也配置在同一节点上，则客户端网络将使用交换机上配置的中继端口的本征 VLAN。

仅在 VLAN 网络上支持入站管理流量，例如用于 SSH、Grid Manager 或 Tenant Manager 流量。出站流量（例如用于 NTP、DNS、LDAP、KMS 和 Cloud Storage Pools）不支持通过 VLAN 网络传输。



VLAN 接口只能添加到管理节点和网关节点。您不能将 VLAN 接口用于客户端或管理员对存储节点的访问。

有关说明和指南，请参见 ["配置 VLAN 接口"](#)。

VLAN 接口仅在 HA 组中使用，并在活动节点上分配 VIP 地址。有关说明和指南，请参阅 ["管理高可用性组"](#)。

网络拓扑示例

StorageGRID 的网络网络拓扑

最简单的网络拓扑仅通过配置网络网络来创建。

配置网络网络时，为每个网络节点的 eth0 接口建立主机 IP 地址、子网掩码和网关 IP 地址。

在配置过程中，您必须将所有网络网络子网添加到网络网络子网列表 (GNSL)。此列表包括所有站点的所有子网，还可能包括提供对 NTP、DNS 或 LDAP 等关键服务的访问权限的外部子网。

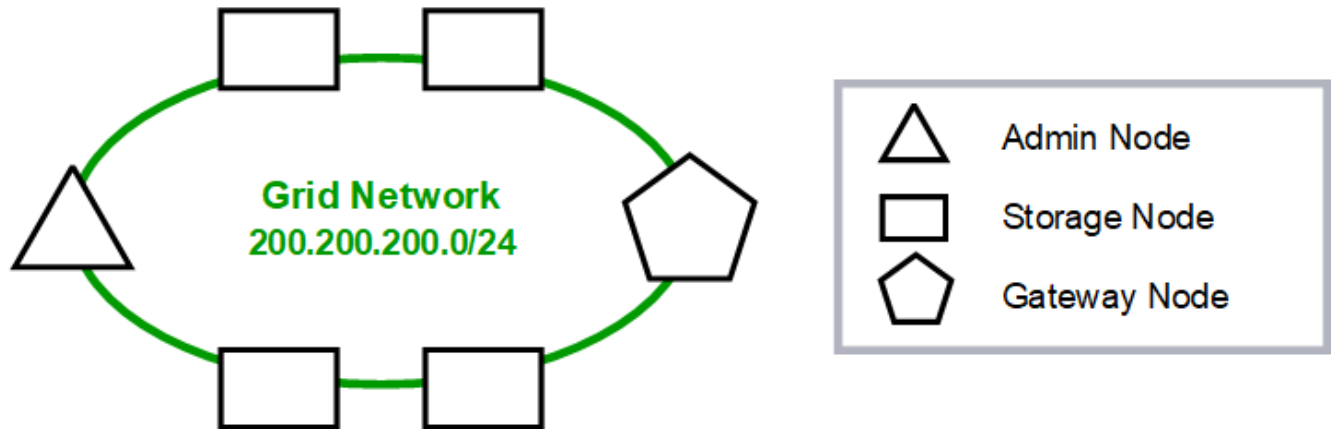
安装时，网络网络接口为 GNSL 中的所有子网应用静态路由，并将节点的默认路由设置为网络网络网关（如果已配置）。如果没有客户端网络，且网络网络网关是节点的默认路由，则不需要 GNSL。此外，还会生成指向网络中所有其他节点的主机路由。

在此示例中，所有流量共享同一个网络，包括与 S3 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，或第三方负载均衡器充当客户端访问边界的情况。在可能的情况下，网络网络应仅用于内部流量。管理网络和客户端网络都有额外的防火墙限制，可以阻止到内部服务的外部流量。支持将网络网络用于外部客户端流量，但这种使用提供的保护层较少。

Topology example: Grid Network only



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

StorageGRID 的管理网络拓扑

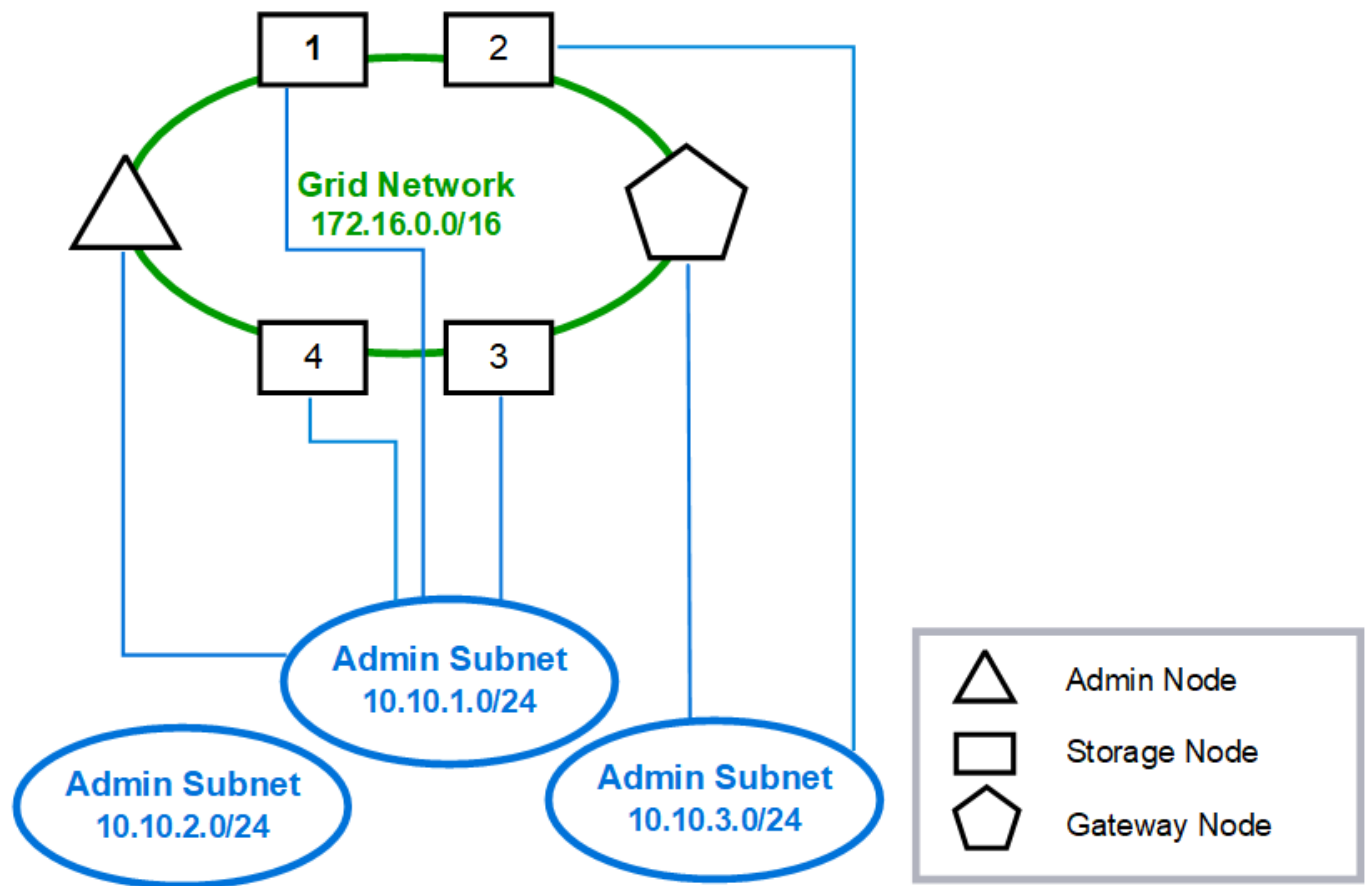
拥有管理网络是可选的。使用管理网络和网格网络的一种方法是为每个节点配置可路由的网格网络和有界管理网络。

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

管理网络可以对每个节点都是唯一的，并且可以由多个子网组成。可以为每个节点配置管理外部子网列表 (AESL)。AESL 列出每个节点通过管理网络可访问的子网。AESL 还必须包括网格将通过管理网络访问的任何服务的子网，例如 NTP、DNS、KMS 和 LDAP。静态路由应用于 AESL 中的每个子网。

在此示例中，网格网络用于与 S3 客户端请求和对象管理相关的流量，而管理网络用于管理功能。

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

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

Nodes	Grid Network		Admin Network	
	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

StorageGRID 的客户端网络拓扑

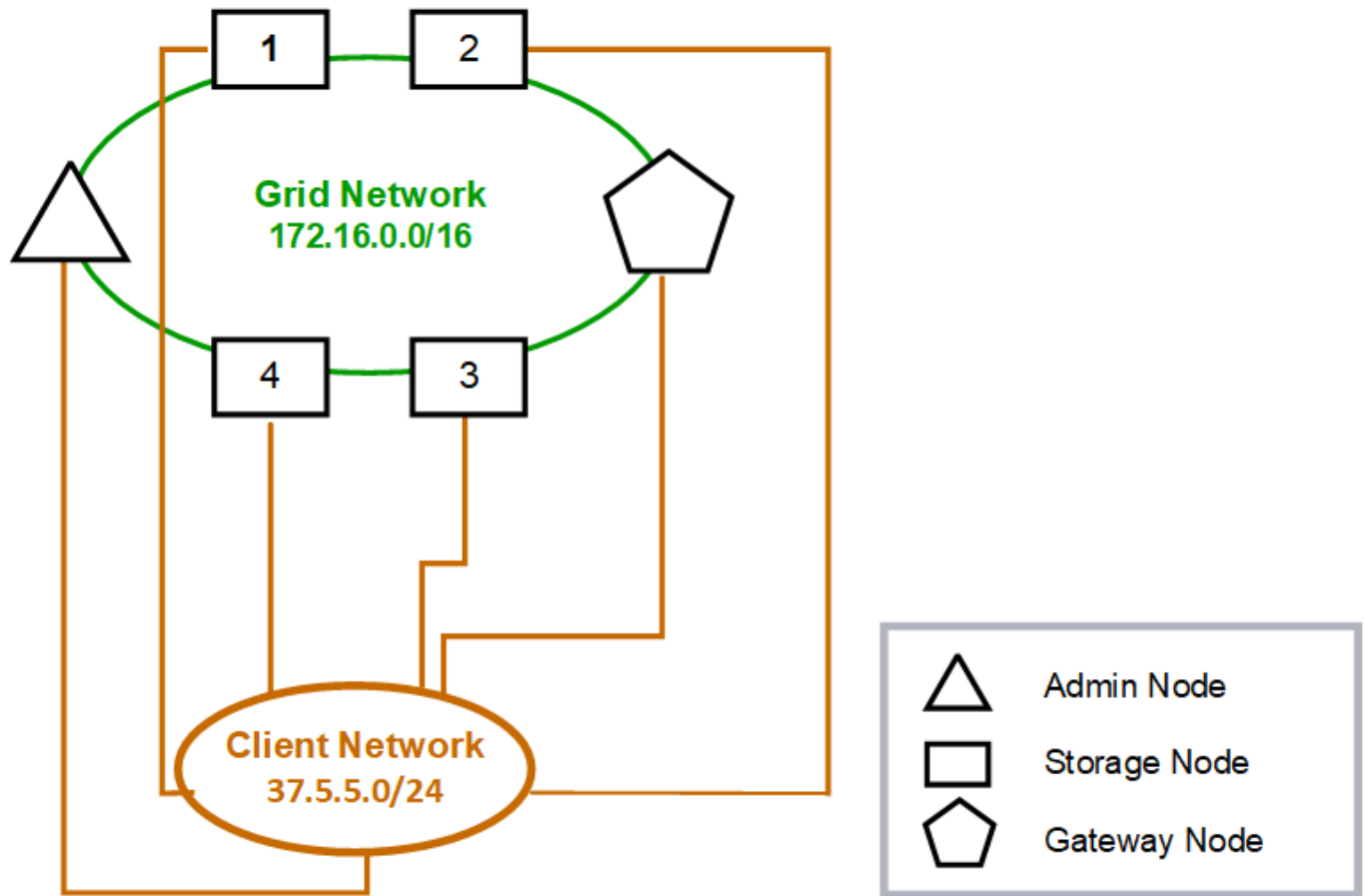
拥有客户端网络是可选的。使用客户端网络允许将客户端网络流量（例如 S3）与网格内部流量分开，从而使网格网络更加安全。未配置管理网络时，可由客户端或网格网络处理管理流量。

配置客户端网络时，需要为配置的节点的 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。

如果在安装过程中为节点配置客户端网络，则在安装完成后，该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。如果稍后添加了客户端网络，则节点的默认网关将以相同的方式切换。

在此示例中，客户端网络用于 S3 客户端请求和管理功能，而网格网络专用于内部对象管理操作。

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	IP/mask	IP/mask	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

相关信息

["更改节点网络配置"](#)

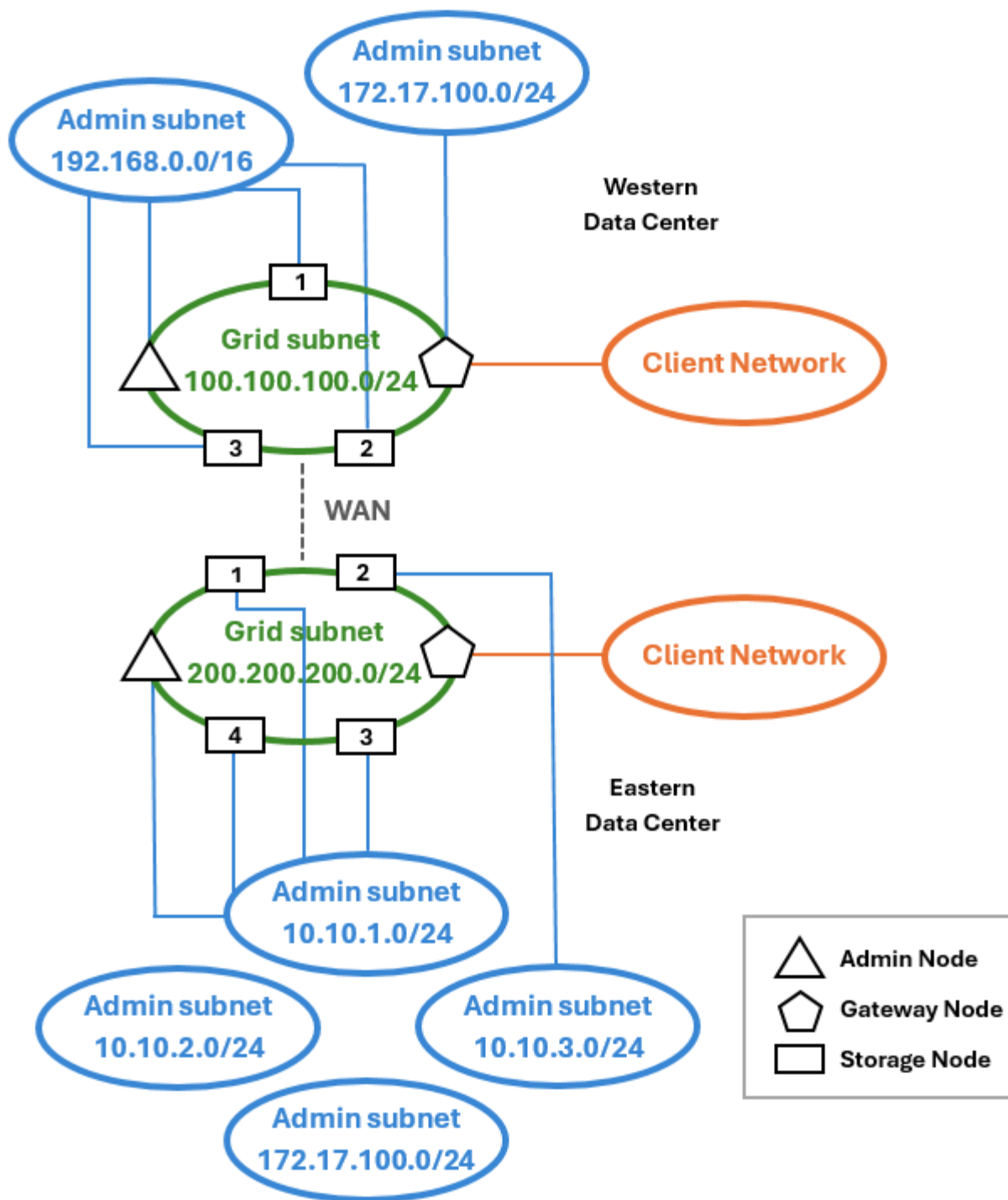
所有三个 **StorageGRID** 网络的网络拓扑

您可以将所有三个网络配置为由专用网格网络、特定于站点的有界管理网络和开放客户端网络组成的网络拓扑。如果需要，使用负载均衡器端点和不受信任的客户端网络可以提供额外的安全性。

在此示例中：

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

拓扑示例：网格、管理和客户端网络



StorageGRID 的网络要求

您必须验证当前的网络基础设施和配置是否能够支持计划的 StorageGRID 网络设计。

一般网络要求

所有 StorageGRID 部署必须能够支持以下连接。

这些连接可以通过网格、管理或客户端网络，或网络拓扑示例中所示的这些网络的组合来实现。

- **管理连接**：从管理员到节点的入站连接，通常通过 SSH。Web 浏览器访问 Grid Manager、Tenant Manager 和 StorageGRID Appliance Installer。
- **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**：来自存储节点上身份服务的出站 TCP 连接。
- **AutoSupport**：从管理节点到 `support.netapp.com` 或客户配置代理的出站 TCP 连接。
- **外部密钥管理服务器**：从每个已启用节点加密的设备节点出站 TCP 连接。
- 来自 S3 客户端的入站 TCP 连接。
- 来自 StorageGRID 平台服务（如 CloudMirror 复制）或来自云存储池的出站请求。

如果 StorageGRID 无法使用默认路由规则联系任何已配置的 NTP 或 DNS 服务器，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，以确保该网络用于将来所有的连接尝试。



虽然您可以使用这些自动发现的主机路由，但一般来说，您应该手动配置 DNS 和 NTP 路由，以确保在自动发现失败时的连接性。

如果您尚未准备好在部署期间配置可选的管理员和客户端网络，则可以在配置步骤中批准网格节点时配置这些网络。此外，您可以在安装后使用 Change IP 工具配置这些网络（请参阅[配置 IP 地址](#)）。

仅支持通过 VLAN 接口进行 S3 客户端连接以及 SSH、Grid Manager 和 Tenant Manager 管理连接。出站连接（例如与 NTP、DNS、LDAP、AutoSupport 和 KMS 服务器的连接）必须直接通过客户端、管理员或网格网络接口。如果将接口配置为中继以支持 VLAN 接口，则此流量将按照交换机的配置在接口的本机 VLAN 上流动。

适用于多个站点的广域网 (WAN)

在配置具有多个站点的 StorageGRID 系统时，站点之间的 WAN 连接在考虑客户端流量之前，每个方向的最小带宽必须为 25 Mbit/秒。站点之间的数据复制或纠删编码、节点或站点扩展、节点恢复以及其他操作或配置将需要额外的带宽。

实际的最小 WAN 带宽要求取决于客户端活动和 ILM 保护方案。如需在估算最小 WAN 带宽要求方面获得帮助，请联系您的 NetApp 专业服务顾问。

管理节点和网关节点的连接

必须始终保护管理节点不受不受信任的客户端（例如开放互联网上的客户端）的攻击。您必须确保任何不受信任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。

计划添加到高可用性组的管理节点和网关节点必须配置静态 IP 地址。有关详细信息，请参见[管理高可用性组](#)。

使用网络地址转换(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 (NAT)。当您为网格网络使用私有 IPv4 地址时，这些地址必须能够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端客户端和网格节点之间使用 NAT，例如为网关节点提供公共 IP 地址。仅当您使用对网格中所有节点透明的隧道应用程序时，才支持使用 NAT 来桥接公网段，这意味着网格节点不需要知道公共 IP 地址。

StorageGRID 的网络特定要求

请遵循每个 StorageGRID 网络类型的要求。

网络网关和路由器

- 如果设置，给定网络的网关必须在特定网络的子网内。
- 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。
- 如果没有网关，最佳做法是将网关地址设置为网络接口的 IP 地址。

子网



每个网络必须连接到自己的子网，该子网不与节点上的任何其他网络重叠。

网络管理器在部署期间强制执行以下限制。此处提供这些信息以协助部署前的网络规划。

- 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 表示法中为 /31 或 /32）。
- 由网络接口 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。
- 对于任何节点的网格网络、管理网络或客户端网络，请勿使用包含以下 IPv4 地址的子网：
 - 192.168.130.101
 - 192.168.130.121
 - 192.168.131.101
 - 192.168.131.121
 - 192.168.130.102
 - 192.168.130.122
 - 192.168.131.102
 - 192.168.131.122
 - 198.51.100.2
 - 198.51.100.4

例如，对于任何节点的网格网络、管理网络或客户端网络，请不要使用以下子网范围：

- 192.168.130.0/24，因为此子网范围包含 IP 地址 192.168.130.101 和 192.168.130.102
- 192.168.131.0/24，因为此子网范围包含 IP 地址 192.168.131.101 和 192.168.131.102
- \${post_edited_translations.segment}

- 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，每个网格节点必须连接到网格网络，并且必须能够使用您在部署节点时指定的网络配置与主管理节点通信。
- 在正常网格操作期间，每个网格节点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路由。不支持节点之间的网络地址转换（NAT）。

- 如果网格网络由多个子网组成，请将其添加到网格网络子网列表 (GNSL)。系统会为 GNSL 中每个子网的所有节点创建静态路由。
- 如果将网格网络接口配置为中继以支持 VLAN 接口，则中继本征 VLAN 必须是用于网格网络流量的 VLAN。必须能够通过中继本征 VLAN 访问所有网格节点。

管理网络

管理网络是可选的。如果您计划配置管理网络，请遵循这些要求和准则。

管理网络的典型用途包括管理连接、AutoSupport、KMS 以及与关键服务器（如 NTP、DNS 和 LDAP）的连接（如果未通过网格网络或客户端网络提供这些连接）。



只要所需的网络服务和客户端可访问，管理网络和 AESL 对于每个节点都可以是唯一的。



要启用来自外部子网的入站连接，必须至少在管理网络上定义一个子网。系统会自动为 AESL 中每个子网的每个节点生成静态路由。

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，请注意以下注意事项。

- 客户端网络旨在支持来自 S3 客户端的流量。如果已配置，则客户端网络网关将成为该节点的默认网关。
- 如果使用客户端网络，则可以通过仅接受显式配置的负载均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。请参阅 ["配置负载均衡器端点"](#)。
- 如果将客户端网络接口配置为中继以支持 VLAN 接口，请考虑是否需要配置客户端网络接口（eth2）。如果已配置，客户端网络流量将按照交换机中的配置通过中继本征 VLAN。

相关信息

["更改节点网络配置"](#)

特定于部署的网络注意事项

StorageGRID Linux 部署的网络配置

为了提高效率、可靠性和安全性，StorageGRID 系统在 Linux 上作为容器引擎的集合运行。StorageGRID 系统中不需要与容器引擎相关的网络配置。

为容器网络接口使用非绑定设备，例如 VLAN 或虚拟以太网 (veth) 对。在节点配置文件中将此设备指定为网络接口。



不要直接使用绑定或桥接设备作为容器网络接口。这样做可能会阻止节点启动，因为在容器命名空间中使用带有绑定和桥接设备的 macvlan 存在内核问题。

请参阅["安装说明"](#)。

用于容器引擎部署的主机网络配置

在容器引擎平台上启动 StorageGRID 部署之前，请确定每个节点将使用哪些网络（网络、管理、客户端）。您必须确保每个节点的网络接口配置在正确的虚拟或物理主机接口上，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络节点：

- 确保所有主机对每个节点接口使用相同的主机接口。此策略简化了主机配置，并为未来的节点迁移提供了便利。
- 获取物理主机本身的 IP 地址。



主机上的物理接口可以由主机本身和主机上运行的一个或多个节点使用。使用此接口分配给主机或节点的任何 IP 地址必须是唯一的。主机和节点无法共享 IP 地址。

- 打开到主机的所需端口。
- 如果您打算在 StorageGRID 中使用 VLAN 接口，则主机必须具有一个或多个中继接口，以提供对所需 VLAN 的访问。这些接口可以作为 eth0、eth2 或附加接口传入节点容器。要添加中继或接入接口，请参见以下内容：
 - **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"](#)



"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 \(IMT\)"](#)。

最小带宽建议

下表提供了每种 StorageGRID 节点类型和每种网络类型的最低 LAN 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，以满足您计划在该主机上运行的 StorageGRID 节点总数和类型的最低带宽要求。

节点类型	网络类型		
	Grid	管理员	客户端
	最小局域网带宽	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



此表不包括访问共享存储所需的 SAN 带宽。如果使用通过以太网访问的共享存储（iSCSI 或 FCoE），则应在每台主机上配置单独的物理接口，以提供足够的 SAN 带宽。为了避免引入瓶颈，给定主机的 SAN 带宽应与该主机上运行的所有存储节点的总存储节点网络带宽大致匹配。

根据计划在每台主机上运行的 StorageGRID 节点的数量和类型，使用该表确定要在该主机上设置的最小网络接口数量。

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：

- 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）
- 连接存储节点上的网格网络（需要 10 Gbps）

在这种情况下，您应提供至少 $11 + 20 + 10 = 41$ Gbps 的网络带宽，这可以通过两个 40 Gbps 接口或五个 10 Gbps 接口来满足，这些接口可能会聚合到中继，然后由三个或更多承载 Grid、Admin 和 Client 子网的 VLAN 共享，这些子网位于包含主机的物理数据中心本地。

有关在 StorageGRID 集群中的主机上配置物理和网络资源以准备 StorageGRID 部署的一些推荐方法，请参见 "[配置主机网络](#)"。

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，以确保可以到达目标端点。

平台服务的网络

如"[为租户管理平台服务](#)"和"[管理平台服务](#)"中所述，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 ADC 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 ADC 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。如果您使用默认路由，则可以使用 "[不受信任的客户端网络功能](#)" 限制入站连接。

云存储池的网络

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。有关信息，请参见 ["什么是云存储池"](#)。

平台服务和云存储池的端口

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 `'https'` 开头的端点 URI

可以在创建或编辑端点时指定不同的端口。请参阅["网络端口参考"](#)。

如果使用不透明的代理服务器，则还必须["配置存储代理设置"](#)以允许将消息发送到外部端点，例如 Internet 上的端点。

VLAN 和平台服务以及云存储池

不能将 VLAN 网络用于平台服务或云存储池。目标端点必须可通过网格、管理或客户端网络访问。

StorageGRID 设备节点的网络配置

您可以配置 StorageGRID 设备上的网络端口，以使用满足吞吐量、冗余和故障转移要求的端口绑定模式。

StorageGRID 设备上的 10/25-GbE 端口可以配置为固定或聚合绑定模式，以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，以连接到管理网络。

请参见有关设备的端口绑定模式的信息：

- ["端口绑定模式 \(SG6160\)"](#)
- ["端口绑定模式 \(SGF6112\)"](#)
- ["端口绑定模式 \(SG6000-CN 控制器\) "](#)
- ["端口绑定模式 \(SG5800 控制器\) "](#)
- ["端口绑定模式 \(E5700SG 控制器\) "](#)
- ["端口绑定模式 \(SG110 和 SG1100\) "](#)
- ["端口绑定模式 \(SG100 和 SG1000\) "](#)

StorageGRID 的网络安装和配置

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。如果网格网络是隔离的，您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，包含 NTP 服务器或需要访问 Grid Manager 或 API 的子网也可以配置为网格子网。

使用主管理节点自动注册节点

部署节点后，它们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、`configure-storagegrid.py` Python 脚本或安装 API 来配置网格并批准注册的节点。在网格配置过程中，您可以配置多个网格子网。完成网格配置后，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删除它们的配置，也可以在安装完成后使用更改 IP 工具（请参阅[配置 IP 地址](#)）。

StorageGRID 安装后指南

完成网格节点部署和配置后，请按照以下指导原则进行 DHCP 寻址和网络配置更改。

- 如果使用 DHCP 分配 IP 地址，请为正在使用的网络上的每个 IP 地址配置 DHCP 保留。

您只能在部署阶段设置 DHCP。您无法在配置期间设置 DHCP。



当 DHCP 更改网格网络配置时，节点将重新启动，如果 DHCP 更改同时影响多个节点，则可能会导致中断。

- 如果要更改网格节点的 IP 地址、子网掩码和默认网关，则必须使用更改 IP 过程。请参阅 [配置 IP 地址](#)。
- 如果进行网络配置更改，包括路由和网关更改，则客户端与主管理节点和其他网格节点的连接可能会丢失。根据应用的网络更改，您可能需要重新建立这些连接。

网络端口参考

StorageGRID 的内部网格节点通信

StorageGRID 内部防火墙允许传入到网格网络上的特定端口的连接。负载均衡器端点定义的端口也接受连接。



NetApp 建议您启用网格节点之间的互联网控制消息协议 (ICMP) 流量。当无法访问网格节点时，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 使用虚拟路由器冗余协议 (VRRP)。VRRP 是一种使用 IP 协议编号 112 的互联网协议。StorageGRID 仅在单播模式下使用 VRRP。仅当配置了 [高可用性组](#) 时才需要

VRRP。

基于 Linux 的节点指南

如果企业网络策略限制对任何这些端口的访问，则可以使用部署配置参数在部署时重新映射端口。有关端口重映射和部署配置参数的详细信息，请参见 ["在基于软件的节点上安装 StorageGRID"](#)。



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 ["删除裸机主机上的端口重映射"](#)。

基于 VMware 的节点指南

仅当需要定义 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任何这些端口的访问，则可以在使用 VMware vSphere Web Client 部署节点时或在自动化网络节点部署时使用配置文件设置来重新映射端口。有关端口重映射和部署配置参数的详细信息，请参见 ["在 VMware 上安装 StorageGRID"](#) 的说明。



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 ["删除裸机主机上的端口重映射"](#)。

设备节点指南

如果企业网络策略限制对任何这些端口的访问，则可以使用 StorageGRID 设备安装程序重新映射端口。请参阅 ["可选：重新映射设备的网络端口"](#)。



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 ["删除 StorageGRID 设备上的端口重映射"](#)。

StorageGRID 内部端口

端口	TCP 或 UDP	自	至	详细信息
22	TCP	主管理节点	所有节点	对于维护过程，主管理节点必须能够使用端口 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	由 StorageGRID 设备用于与主管理节点通信以开始安装。
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 与其他每个节点同步其时间。
443	TCP	所有节点	主管理节点	用于在安装和其他维护过程中向主管理节点传达状态。
1055	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护程序的内部流量。

端口	TCP 或 UDP	自	至	详细信息
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	带 ADC 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	S3 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	负载均衡器内部流量。
1508	TCP	所有节点	主管理节点	配置管理内部流量。
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	提供组播 DNS (mDNS) 服务，用于在安装、扩展和恢复期间进行全网格 IP 更改和主管理节点发现。 注意：配置此端口是可选的。
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	主管理节点	用于安装、扩展、恢复、其他维护程序和错误报告的内部流量。
8011	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护程序的内部流量。
8443	TCP	主管理节点	设备节点	与维护模式过程相关的内部流量。
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。包括维护程序、指标和网络更新。
10226	TCP	存储节点	主管理节点	由 StorageGRID 设备用于将 AutoSupport 包从 E 系列 SANtricity System Manager 转发到主管理节点。

端口	TCP 或 UDP	自	至	详细信息
10342	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护程序的内部流量。
18000	TCP	管理/存储节点	带 ADC 的存储节点	帐户服务内部流量。
18001	TCP	管理/存储节点	带 ADC 的存储节点	Identity Federation 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	带 ADC 的存储节点	平台服务内部流量。
18017	TCP	管理/存储节点	存储节点	Data Mover 服务用于云存储池的内部流量。
18019	TCP	所有节点	所有节点	用于擦除编码和复制的区块服务内部流量
18082	TCP	管理/存储节点	存储节点	S3 相关的内部流量。
18086	TCP	所有节点	存储节点	与 LDR 服务相关的内部流量。
18200	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	带 ADC 的存储节点	Keystone 服务内部流量。

相关信息

["外部通信"](#)

StorageGRID 的外部通信

客户端需要与网格节点进行通信，以获取和检索内容。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。

限制访问端口

如果企业网络策略限制对任何端口的访问，则可以执行以下操作之一：

- 使用 ["负载均衡器端点"](#) 允许访问用户定义的端口。

- 部署节点时重新映射端口。但是，不应重新映射负载均衡器端口。请参阅有关 StorageGRID 节点端口重新映射的信息：



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 ["删除 StorageGRID 设备上的端口重映射"](#) 或 ["删除裸机主机上的端口重映射"](#)。

- ["StorageGRID on Red Hat Enterprise Linux 的端口重映射密钥"](#)
- ["在 VMware 上重新映射 StorageGRID 的端口"](#)
- ["可选：重新映射设备的网络端口"](#)

用于外部通信的端口

下表显示了流入节点的流量所使用的端口。



此列表不包括可能配置为 ["负载均衡器端点"](#) 的端口。

端口	TCP 或 UDP	协议	自	至	详细信息
22	TCP	SSH	维修笔记本电脑	所有节点	具有控制台步骤的操作步骤需要 SSH 或控制台访问权限。您也可以选择使用端口 2022 而非端口 22。 注意：仅当需要为某些维护操作启用 SSH 访问时，才需要此端口。
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 DNS。
67	UDP	DHCP	所有节点	DHCP 服务	可选用于支持基于 DHCP 的网络配置。dhclient 服务不为静态配置的网格运行。
68	UDP	DHCP	DHCP 服务	所有节点	可选用于支持基于 DHCP 的网络配置。dhclient 服务不会为使用静态 IP 地址的网格运行。
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 将重定向到 StorageGRID 设备安装程序的端口 8443。

端口	TCP 或 UDP	协议	自	至	详细信息
80	TCP	HTTP	带 ADC 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。租户可以在创建端点时覆盖默认的 HTTP 端口设置 80。
80	TCP	HTTP	存储节点	AWS	云存储池请求发送到使用 HTTP 的 AWS 目标。网络管理员可以在配置云存储池时覆盖默认的 HTTP 端口设置 80。
123	UDP	NTP	主 NTP 节点	外部 NTP	网络时间协议服务。被选为主 NTP 源的节点也与外部 NTP 时间源同步时钟时间。
161	TCP/UDP	SNMP	SNMP 客户端	所有节点	用于 SNMP 轮询。所有节点都提供基本信息；管理节点还提供警报数据。配置时默认为 UDP 端口 161。 注意：此端口仅为必需端口，并且仅在配置 SNMP 时在节点防火墙上打开。如果您计划使用 SNMP，则可以配置备用端口。 注意：有关在 StorageGRID 中使用 SNMP 的信息，请联系您的 NetApp 客户代表。
162	TCP/UDP	SNMP 通知	所有节点	通知目的地	出站 SNMP 通知和陷阱默认为 UDP 端口 162。 *注意：*仅当启用了 SNMP 并配置了通知目的地时，才需要此端口。如果您计划使用 SNMP，则可以配置备用端口。 注意：有关在 StorageGRID 中使用 SNMP 的信息，请联系您的 NetApp 客户代表。
389	TCP/UDP	LDAP	带 ADC 的存储节点	Active Directory/LDAP	用于连接到 Active Directory 或 LDAP 服务器以进行 Identity Federation。
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 Tenant Manager。 注意：如果您关闭 Grid Manager 端口 443 或 8443，则当前连接到被阻止端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。请参阅配置防火墙控件以配置特权 IP 地址。
443	TCP	HTTPS	管理节点	Active Directory	如果启用单一登录 (SSO)，则由连接到 Active Directory 的管理节点使用。

端口	TCP 或 UDP	协议	自	至	详细信息
443	TCP	HTTPS	带 ADC 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。租户可以在创建端点时覆盖默认的 HTTP 端口设置 443。
443	TCP	HTTPS	存储节点	AWS	云存储池请求发送到使用 HTTPS 的 AWS 目标。网络管理员可以在配置云存储池时覆盖默认 HTTPS 端口设置 443。
5353	UDP	mDNS	所有节点	所有节点	提供组播 DNS (mDNS) 服务，用于在安装、扩展和恢复期间进行全网格 IP 更改和主管理节点发现。 注意：配置此端口是可选的。
5696	TCP	KMIP	设备	KMS	从配置为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 (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。
8443	TCP	HTTPS	浏览器	管理节点	可选。由 Web 浏览器和管理 API 客户端用于访问 Grid Manager。可用于分隔 Grid Manager 和 Tenant Manager 通信。 注意：如果您关闭 Grid Manager 端口 443 或 8443，则当前连接到受阻端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。请参阅 配置防火墙控件 以配置特权 IP 地址。
8443	TCP	HTTPS	浏览器	设备	由 Web 浏览器和管理 API 客户端用于访问 StorageGRID 设备安装程序。 注意：端口 443 重定向到 StorageGRID 设备安装程序的端口 8443。
9022	TCP	SSH	维修笔记本电脑	设备	在预配置模式下授予对 StorageGRID 设备的访问权限，以进行支持和故障排除。此端口无需在网格节点之间或正常操作期间访问。
9091	TCP	HTTPS	外部 Grafana 服务	管理节点	由外部 Grafana 服务用于安全访问 StorageGRID Prometheus 服务。 注意：仅当启用了基于证书的 Prometheus 访问权限时，才需要此端口。

端口	TCP 或 UDP	协议	自	至	详细信息
9092	TCP	Kafka	带 ADC 的存储节点	Kafka 集群	用于发送到 Kafka 集群的平台服务消息。租户可以在创建端点时覆盖默认的 Kafka 端口设置 9092。
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。可用于分离 Grid Manager 和租户管理器通信。
18082	TCP	HTTPS	S3 客户端	存储节点	S3 客户端流量直接到达存储节点 (HTTPS)。
18084	TCP	HTTP	S3 客户端	存储节点	S3 客户端流量直接到达存储节点 (HTTP)。
23000-23999	TCP	HTTPS	跨网格复制的源网格上的所有节点	用于跨网格复制的目标网格上的管理节点和网关节点	此端口范围保留用于网格联合连接。给定连接中的两个网格使用相同的端口。

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。