StorageGRID 网络概述

StorageGRID 11.5

NetApp
April 11, 2024

目录

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。

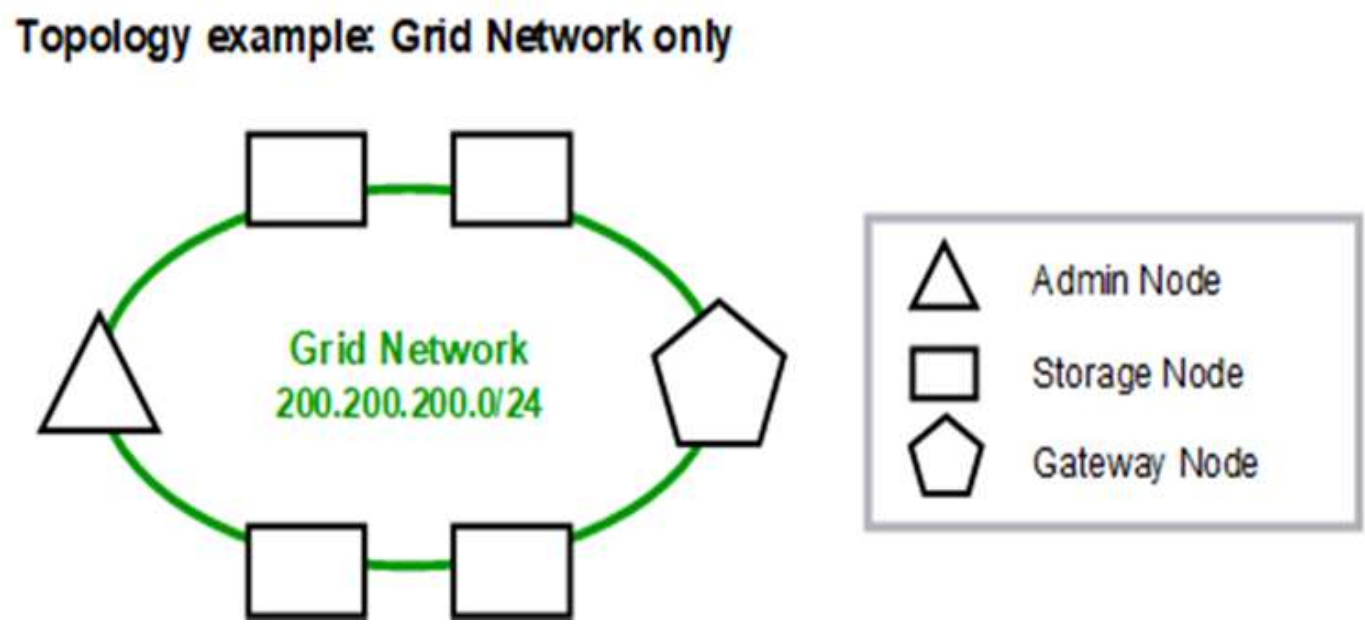
配置网格网络时，您需要为每个网格节点的 eth0 接口建立主机 IP 地址，子网掩码和网关 IP 地址。

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

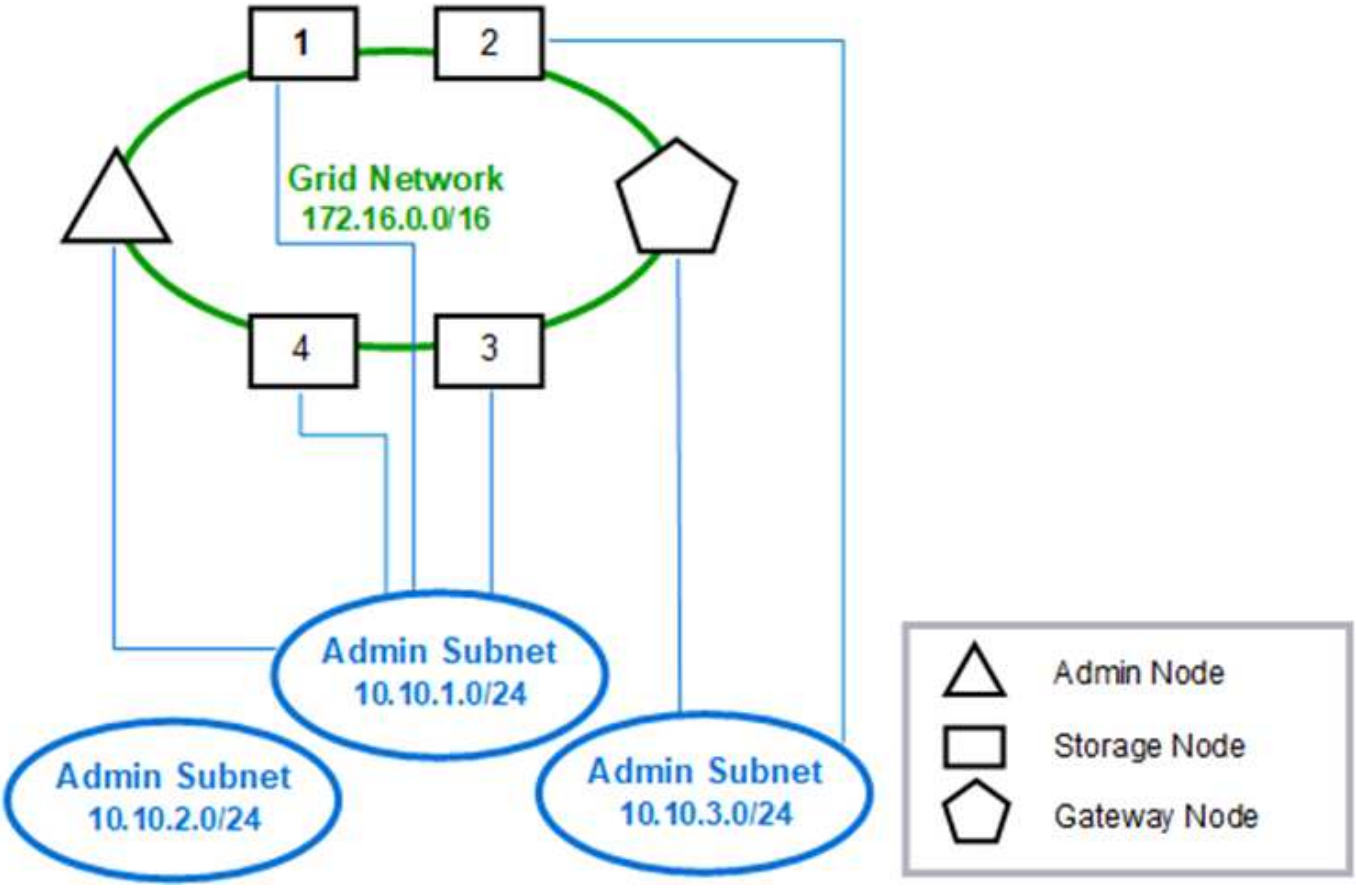
可以选择使用管理网络。使用管理网络和网格网络的一种方法是，为每个节点配置可路由的网格网络和有限制的管理网络。

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



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

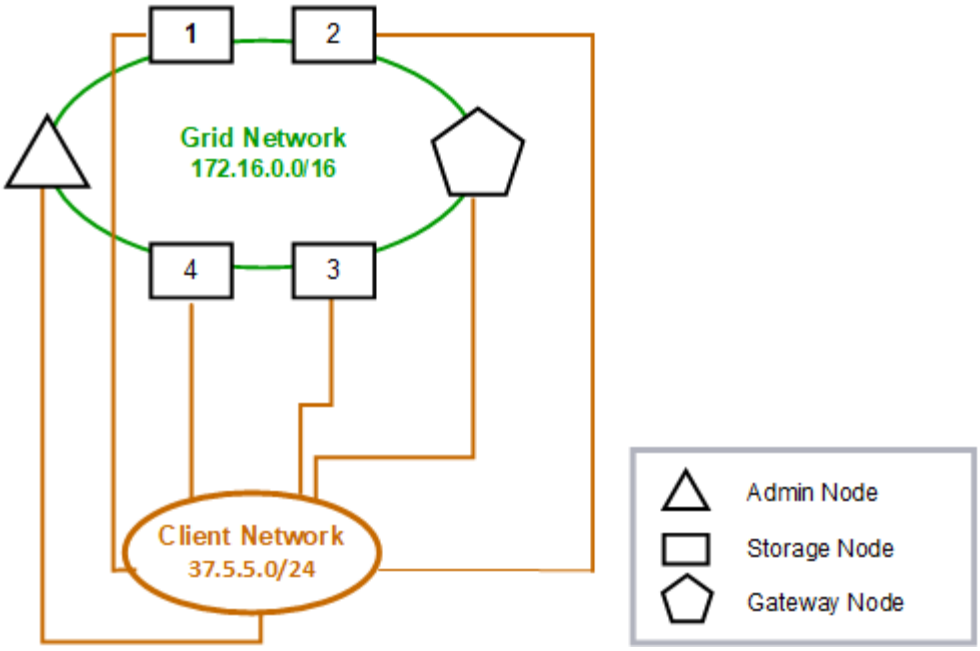
可以选择使用客户端网络。使用客户端网络可以将客户端网络流量（例如 S3 和 Swift ）与网格内部流量分隔开，从而提高网格网络连接的安全性。如果未配置管理网络，则可通过客户端网络或网格网络处理管理流量。

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

	Grid Network	Client Network	
Nodes	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

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。