网络端口参考

StorageGRID 11.7

NetApp
April 12, 2024

目录

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。

请使用为提供的详细信息 "内部网格节点通信" 和 "外部通信" 以确定如何配置所需的每个端口。

内部网格节点通信

StorageGRID 内部防火墙允许与网格网络上的特定端口建立传入连接。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 。只有在满足条件时才需要 VRRP "高可用性组" 已配置。

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：

- "安装 Red Hat Enterprise Linux 或 CentOS"
- "安装 Ubuntu 或 Debian"

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"安装 VMware"。

设备节点准则

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。请参见 "可选：重新映射设备的网络端口"。

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。
1055年	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护过程的内部流量。
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。
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、其他维护过程和错误报告的内部流量。

Port	TCP 或 UDP	from	收件人：	详细信息
8011.	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护过程的内部流量。
8443	TCP	主管理节点	设备节点	与维护模式操作步骤 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。
10342.	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护过程的内部流量。
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。

Port	TCP 或 UDP	from	收件人：	详细信息
18086	TCP	所有网格节点	所有存储节点	与LDR服务相关的内部流量。
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"

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。

对端口的访问受限

如果企业网络策略限制对任何端口的访问，您可以使用 "负载平衡器端点" 允许对用户定义的端口进行访问。然后，您可以使用 "不可信的客户端网络" 仅允许对负载平衡器端点端口进行访问。

端口重新映射

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，您不应重新映射负载平衡器端点。有关端口重新映射的信息、请参见安装说明：

- "安装 Red Hat Enterprise Linux 或 CentOS"
- "安装 Ubuntu 或 Debian"
- "安装 VMware"
- "可选：重新映射设备的网络端口"

用于外部通信的端口

下表显示了用于向节点进行流量的端口。

> 此列表不包括可能配置为的端口 "负载平衡器端点" 或用于 "系统日志服务器"。

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DNS。
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。 • 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。 • 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。 • 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。 • 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 。 • 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。 • 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 。 • 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。 • 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。
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。 注意：如果关闭Grid Manager端口443或8443，则当前连接到被阻止端口的任何用户(包括您在内)将无法访问Grid Manager，除非其IP地址已添加到特权地址列表中。请参见 "配置防火墙控件" 配置有权限的IP地址。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
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。 • 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`）。 • 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。 • 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。
5353	UDP	mDNS	所有节点	所有节点	提供多播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。
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。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
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。
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。 注意：如果关闭Grid Manager端口443或8443，则当前连接到被阻止端口的任何用户(包括您在内)将无法访问Grid Manager，除非其IP地址已添加到特权地址列表中。请参见 "配置防火墙控件" 配置有权限的IP地址。
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。 • 注： * 只有在启用了基于证书的 Prometheus 访问时，才需要此端口。
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	直接发送到存储节点（ HTTPS ）的 S3 客户端流量。
18083.	TCP	HTTPS	Swift 客户端	存储节点	Swift 客户端流量直接发送到存储节点（ HTTPS ）。
18084	TCP	HTTP	S3 客户端	存储节点	直接发送到存储节点（ HTTP ）的 S3 客户端流量。
18085	TCP	HTTP	Swift 客户端	存储节点	Swift 客户端流量直接发送到存储节点（ HTTP ）。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
23000-23999	TCP	HTTPS	源网格上用于跨网格复制的所有节点	目标网格上用于跨网格复制的管理节点和网关节点	此端口范围是为网格联合连接预留的。给定连接中的两个网格使用相同的端口。