控制防火墙
StorageGRID software

NetApp
July 23, 2026

目录

控制防火墙

在外部防火墙处控制 StorageGRID 访问

您可以在外部防火墙上打开或关闭特定端口。

您可以通过在外部防火墙上打开或关闭特定端口来控制对 StorageGRID 管理节点上用户界面和 API 的访问。例如，除了使用其他方法来控制系统访问之外，您可能还希望阻止租户在防火墙处连接到 Grid Manager。

如果要配置 StorageGRID 内部防火墙，请参见 "配置内部防火墙"。

端口	问题描述	如果端口打开.....
443	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问 Grid Manager、Grid Management API、Tenant Manager 和 Tenant Management API。 注意： 端口 443 也用于一些内部流量。
8443	管理节点上的受限 Grid Manager 端口	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问网格管理器和网格管理 API。 • Web 浏览器和管理 API 客户端无法访问 Tenant Manager 或 Tenant Management API。 • 对内部内容的请求将被拒绝。
9443	管理节点上的受限租户管理器端口	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问租户管理器和租户管理 API。 • Web 浏览器和管理 API 客户端无法访问 Grid Manager 或网格管理 API。 • 对内部内容的请求将被拒绝。

单点登录 (SSO) 在受限 Grid Manager 或 Tenant Manager 端口上不可用。如果希望用户使用单点登录进行身份验证，则必须使用默认 HTTPS 端口 (443)。

相关信息

- "登录到网格管理器"
- "创建租户帐户"
- "外部通信"

管理 StorageGRID 中的内部防火墙控制

StorageGRID 在每个节点上包含一个内部防火墙，通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止所有端口上的网络访问，特定网格部署所必需的端口除外。在防火墙控制页面上所做的配置更改将部署到每个节点。

使用防火墙控制页面上的三个选项卡可自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡可允许选定访问已关闭的端口。您可以添加 CIDR 表示法的 IP 地址或子网，这些地址或子网可以访问使用"管理外部访问"选项卡关闭的端口。
- 管理外部访问：使用此选项卡可关闭默认打开的端口，或重新打开先前已关闭的端口。
- 不受信任的客户端网络：使用此选项卡可指定节点是否信任来自客户端网络的入站流量。

  此选项卡上的设置将覆盖"管理外部访问"选项卡中的设置。

  - 具有不受信任客户端网络的节点将仅接受在该节点上配置的负载均衡器端点端口上的连接（全局、节点接口和节点类型绑定端点）。
  - 无论 Manage external networks 选项卡上的设置如何，在不受信任的客户端网络上，负载均衡器端点端口_是唯一开放的端口_。
  - 受信任时，可以访问在"管理外部访问"选项卡下打开的所有端口，以及在客户端网络上打开的任何负载平衡器端点。

> 您在一个选项卡上进行的设置可能会影响您在另一个选项卡上进行的访问更改。请务必检查所有选项卡上的设置，以确保您的网络按预期运行。

要配置内部防火墙控制，请参见 "配置防火墙控件"。

有关外部防火墙和网络安全的详细信息，请参见 "控制外部防火墙的访问"。

${post_edited_translations.segment}

“特权地址列表”选项卡使您能够注册一个或多个被授予访问已关闭网格端口权限的 IP 地址。“管理外部访问”选项卡使您能够关闭对选定外部端口或所有打开的外部端口的外部访问（外部端口是默认情况下非网格节点可访问的端口）。这两个选项卡通常可以结合使用，以自定义允许网格访问的精确网络访问权限。

> ${post_edited_translations.segment}

示例 **1**：使用跳板机执行维护任务

假设您要使用跳板机（经过安全加固的主机）进行网络管理。您可以使用以下常规步骤：

1. ${post_edited_translations.segment}
2. 使用"管理外部访问"选项卡可阻止所有端口。

> 在阻止端口 443 和 8443 之前，请先添加特权 IP 地址。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。

保存配置后，网格中管理节点上的所有外部端口将对除跳转主机之外的所有主机被阻止。然后，您可以使用跳转主机更安全地对网格执行维护任务。

示例 **2**：锁定敏感端口

假设您要锁定敏感端口以及该端口上的服务。您可以使用以下常规步骤：

1. 使用"特权地址列表"选项卡，仅向需要访问该服务的主机授予访问权限。
2. 使用"管理外部访问"选项卡可阻止所有端口。

> 在阻止访问分配给 Grid Manager 和 Tenant Manager 的任何端口（预设端口为 443 和 8443）之前，请先添加特权 IP 地址。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。

保存配置后，特权地址列表中的主机可以使用该敏感端口及其上的服务。无论请求来自哪个接口，所有其他主机均被拒绝访问该服务。

示例 **3**：禁用对未使用服务的访问

在网络级别，您可以禁用某些不打算使用的服务。例如，要阻止 HTTP S3 客户端流量，您可以使用"管理外部访问"选项卡上的切换来阻止端口 18084。

不受信任的客户端网络选项卡

如果使用客户端网络，则可以通过仅接受显式配置的端点上的入站客户端流量来帮助保护 StorageGRID 免受恶意攻击。

默认情况下，每个网格节点上的客户端网络为_trusted_。也就是说，默认情况下，StorageGRID 信任所有 "可用外部端口" 上每个网格节点的入站连接。

您可以通过指定每个节点上的客户端网络_不可信_来减少对 StorageGRID 系统的恶意攻击威胁。如果节点的客户端网络不受信任，则该节点仅接受明确配置为负载平衡器端点的端口上的入站连接。请参阅"配置负载平衡器端点"和"配置防火墙控件"。

示例 **1**：网关节点仅接受 **HTTPS S3** 请求

假设您希望网关节点拒绝客户端网络上除 HTTPS S3 请求之外的所有入站流量。您将执行以下一般步骤：

1. 在"负载平衡器端点"页面中，通过端口 443 上的 HTTPS 为 S3 配置负载平衡器端点。
2. 在防火墙控制页面中，选择"不受信任"以指定网关节点上的客户端网络不受信任。

保存配置后，除端口 443 上的 HTTPS S3 请求和 ICMP echo (ping) 请求外，网关节点客户端网络上的所有入站流量都将被丢弃。

示例 **2**：存储节点发送 **S3** 平台服务请求

假设您要启用来自存储节点的出站 S3 平台服务流量，但要阻止客户端网络上该存储节点的任何入站连接。您将执行以下常规步骤：

- 在防火墙控制页面的"不受信任的客户端网络"选项卡中，指示存储节点上的客户端网络不受信任。

保存配置后，存储节点不再接受客户端网络上的任何传入流量，但它继续允许向已配置的平台服务目标发出出站请求。

示例 **3**：将对 **Grid Manager** 的访问限制为子网

假设您只想允许 Grid Manager 访问特定子网。您将执行以下步骤：

1. 将管理节点的客户端网络附加到子网。
2. 使用"不受信任的客户端网络"选项卡将客户端网络配置为不受信任。
3. 在创建管理接口负载均衡器端点时，输入端口并选择该端口将访问的管理接口。
4. 对于不受信任的客户端网络，选择*是*。
5. 使用管理外部访问选项卡可阻止所有外部端口（为该子网外的主机设置或不设置特权 IP 地址）。

保存配置后，只有您指定的子网上的主机才能访问 Grid Manager。所有其他主机均被屏蔽。

配置 StorageGRID 内部防火墙

您可以配置 StorageGRID 防火墙，以控制对 StorageGRID 节点上特定端口的网络访问。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 您已查看 "管理防火墙控件" 和 "网络连接准则" 中的信息。
- 如果希望管理节点或网关节点仅在显式配置的端点上接受入站流量，则已定义负载平衡器端点。

> 更改客户端网络的配置时，如果未配置负载均衡器端点，则现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上包含一个内部防火墙，使您能够打开或关闭网格节点上的某些端口。您可以使用防火墙控制选项卡打开或关闭默认情况下在网格网络、管理网络和客户端网络上打开的端口。您还可以创建可访问已关闭网格端口的特权 IP 地址列表。如果使用客户端网络，则可以指定节点是否信任来自客户端网络的入站流量，并且可以配置客户端网络上特定端口的访问权限。

将对网格外部 IP 地址开放的端口数量限制为仅绝对必要的端口，可增强网格的安全性。您可以使用三个防火墙控制选项卡中每个选项卡上的设置，以确保仅打开所需的端口。

有关使用防火墙控件的详细信息，包括示例，请参见 "管理防火墙控件"。

有关外部防火墙和网络安全的详细信息，请参见 "控制外部防火墙的访问"。

访问防火墙控件

步骤

1. 选择*配置* > 安全 > 防火墙控制。

   本页上的三个选项卡如 "管理防火墙控件" 中所述。

2. 选择任意选项卡以配置防火墙控件。

   您可以按任何顺序使用这些选项卡。您在一个选项卡上设置的配置不限制您可以在其他选项卡上执行的操作；但是，您在一个选项卡上进行的配置更改可能会更改在其他选项卡上配置的端口的行为。

特权地址列表

您可以使用"特权地址列表"选项卡授予主机对默认关闭或通过"管理外部访问"选项卡上的设置关闭的端口的访问权限。

默认情况下，特权 IP 地址和子网没有内部网格访问权限。此外，即使在"管理外部访问"选项卡中被阻止，也可以访问在"特权地址列表"选项卡中打开的负载均衡器端点和其他端口。

"特权地址列表"选项卡上的设置无法覆盖"不受信任的客户端网络"选项卡上的设置。

步骤

1. 在"特权地址列表"选项卡上，输入要授予对已关闭端口的访问权限的地址或 IP 子网。
2. （可选）选择 **Add another IP address or subnet in CIDR notation** 以添加其他特权客户端。

   将尽可能少的地址添加到特权列表。

3. 可选，选择*允许特权 IP 地址访问 StorageGRID 内部端口*。请参阅 "StorageGRID 内部端口"。

   此选项将删除对内部服务的一些保护。如有可能，请将其停用。

4. 选择 **Save**。

管理外部访问

在"管理外部访问"选项卡中关闭端口时，除非您将 IP 地址添加到特权地址列表，否则任何非网格 IP 地址都无法访问该端口。您只能关闭默认情况下处于打开状态的端口，也只能打开已关闭的端口。

"管理外部访问"选项卡上的设置无法覆盖"不受信任的客户端网络"选项卡上的设置。例如，如果节点不受信任，端口 SSH/22 在客户端网络上被阻止，即使它在"管理外部访问"选项卡上已打开。"不受信任的客户端网络"选项卡上的设置将覆盖客户端网络上的封闭端口（如 443、8443、9443）。

步骤

1. 选择*管理外部访问权限*。该选项卡显示一个表格，其中包含网格中节点的所有外部端口（默认情况下非网格节点可访问的端口）。
2. 使用以下选项配置要打开和关闭的端口：
   - 使用每个端口旁边的切换开关打开或关闭选定端口。
   - 选择*Open all displayed ports*以打开表格中列出的所有端口。
   - 选择*关闭所有显示的端口*以关闭表中列出的所有端口。

     如果关闭 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。

使用表格右侧的滚动条，确保您已查看所有可用端口。使用搜索字段通过输入端口号来查找任何外部端口的设置。您可以输入部分端口号。例如，如果输入 **2**，则会显示名称中包含字符串"2"的所有端口。

3. 选择 **Save**

不受信任的客户端网络

如果节点的客户端网络不受信任，则该节点仅接受配置为负载平衡器端点的端口上的入站流量，以及您在此选项卡上选择的其他端口（可选）。您还可以使用此选项卡为扩展中添加的新节点指定默认设置。

如果未配置负载均衡器端点，则现有客户端连接可能会失败。

您在*不受信任的客户端网络*选项卡上所做的配置更改将覆盖*管理外部访问*选项卡上的设置。

步骤

1. 选择*不受信任的客户端网络*。
2. 在设置新节点默认值部分，指定在扩展过程中向网格添加新节点时的默认设置。
   - 可信（默认）：在扩展中添加节点时，其客户端网络是可信的。
   - 不受信任：在扩展中添加节点时，其客户端网络不受信任。

   根据需要，您可以返回此选项卡以更改特定新节点的设置。

   此设置不会影响 StorageGRID 系统中的现有节点。

3. 使用以下选项选择应仅在显式配置的负载平衡器端点或其他选定端口上允许客户端连接的节点：
   - 选择*显示的节点不受信任*，将表中显示的所有节点添加到不受信任的客户端网络列表中。
   - 选择*Trust on displayed nodes*，从不受信任的客户端网络列表中删除表中显示的所有节点。
   - 使用每个节点旁边的切换开关将选定节点的客户端网络设置为可信或不可信。

   例如，您可以选择*对显示的节点不信任*将所有节点添加到不受信任的客户端网络列表中，然后使用单个节点旁边的切换开关将该单个节点添加到受信任的客户端网络列表中。

   使用表格右侧的滚动条，确保您已查看所有可用节点。使用搜索字段通过输入节点名称来查找任何节点的设置。您可以输入部分名称。例如，如果输入 **GW**，则会显示名称中包含字符串"GW"的所有节点。

4. 选择 **Save**。

   新的防火墙设置将立即应用和实施。如果未配置负载均衡器端点，现有客户端连接可能会失败。