控制防火墙

StorageGRID 11.7

NetApp
April 12, 2024

目录

控制防火墙

在外部防火墙处控制访问

您可以在外部防火墙处打开或关闭特定端口。

您可以通过在外部防火墙中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，除了使用其他方法控制系统访问之外，您可能还希望防止租户能够在防火墙处连接到网格管理器。

如果要配置StorageGRID 内部防火墙、请参见 "配置内部防火墙"。

Port	Description	端口是否已打开 ...
443.	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问网格管理器，网格管理 API ，租户管理器和租户管理 API 。 • 注： * 端口 443 也用于某些内部流量。
8443	管理节点上的网格管理器端口受限	• 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客户端无法访问租户管理器或租户管理API。 • 请求内部内容将被拒绝。
9443	管理节点上的租户管理器端口受限	• 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客户端无法访问网格管理器或网格管理API。 • 请求内部内容将被拒绝。

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过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"

管理内部防火墙控制

StorageGRID 在每个节点上都包含一个内部防火墙、可通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止对特定网格部署所需端口以外的所有端口进行网络访问。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自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡允许对关闭的端口进行选定访问。您可以使用CIDR表示法添加IP地址或子网、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：使用此选项卡关闭默认打开的端口，或重新打开先前关闭的端口。
- 不可信客户端网络：使用此选项卡指定节点是否信任来自客户端网络的入站流量。

  此选项卡还提供了指定在配置了不可信客户端网络时要打开的其他端口的选项。这些端口可以提供对网格管理器和/或租户管理器的访问。

  此选项卡上的设置将覆盖管理外部访问选项卡中的设置。

  - 具有不可信客户端网络的节点仅接受在该节点上配置的负载平衡器端点端口(全局端点、节点接口和受节点类型制约的端点)上的连接。
  - 在不可信客户端网络选项卡下打开的其他端口将在所有不可信客户端网络上打开、即使未配置负载平衡器端点也是如此。
  - 无论"管理外部网络"选项卡上的设置如何、负载平衡器端点端口和选定的其他端口_都是不可信客户端网络上唯一打开的端口_。
  - 如果受信任、则可以访问在"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。

> 您在一个选项卡上所做的设置可能会影响您在另一个选项卡上所做的访问更改。请务必检查所有选项卡上的设置、以确保您的网络按预期方式运行。

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、请参阅 "在外部防火墙处控制访问"。

特权地址列表和管理外部访问选项卡

通过特权地址列表选项卡、您可以注册一个或多个被授予对关闭的网格端口访问权限的IP地址。通过"管理外部访问"选项卡、您可以关闭对选定外部端口或所有打开的外部端口的外部访问(默认情况下、外部端口可由非网格节点访问)。这两个选项卡通常可结合使用来定制网格所需的确切网络访问。

> 默认情况下、有权限的IP地址不具有内部网格端口访问权限。

示例**1**：使用跳转主机执行维护任务

假设您要使用跳转主机(一个增强安全的主机)进行网络管理。您可以使用以下常规步骤：

1. 使用特权地址列表选项卡添加跳转主机的IP地址。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、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都将被阻止用于除跳转主机之外的所有主机。然后、您可以使用跳转主机更安全地在网格上执行维护任务。

示例**2**：限制对网格管理器和租户管理器的访问

假设出于安全原因、您希望限制对网格管理器和租户管理器的访问。您可以使用以下常规步骤：

1. 使用"管理外部访问"选项卡上的切换功能阻止端口443。
2. 使用管理外部访问选项卡上的切换以允许访问端口8443。
3. 使用管理外部访问选项卡上的切换以允许访问端口9443。

保存配置后、主机将无法访问端口443、但仍可通过端口8443访问网格管理器、并通过端口9443访问租户管理器。

示例**3**：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(例如、端口22上的SSH)。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服务的主机授予访问权限。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后、端口22和SSH服务将可供特权地址列表中的主机使用。无论请求来自哪个接口、所有其他主机都将被拒绝访问此服务。

示例**4**：禁止访问未使用的服务

在网络级别、您可以禁用一些不打算使用的服务。例如、如果您不提供Swift访问、则应执行以下常规步骤：

1. 使用管理外部访问选项卡上的切换功能阻止端口18083。
2. 使用管理外部访问选项卡上的切换功能阻止端口18085。

保存配置后、存储节点将不再允许Swift连接、而是继续允许访问未阻止的端口上的其他服务。

不可信客户端网络选项卡

如果您使用的是客户端网络、则可以通过仅在显式配置的端点或您在此选项卡上选择的其他端口上接受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均为 *trusted* 。也就是说、默认情况下、StorageGRID 信任所有网格节点的入站连接 "可用外部端口"。

您可以通过指定每个节点上的客户端网络为 *untrused_* 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可信、则该节点仅接受显式配置为负载平衡器端点的端口以及使用防火墙控制页面上的不可信客户端网络选项卡指定的任何其他端口上的入站连接。请参见 "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 请求以外的所有入站流量。您应执行以下常规步骤：

1. 从 "负载平衡器端点" 页面上、通过端口443为基于HTTPS的S3配置负载平衡器端点。

2. 在防火墙控制页面中、选择不可信以指定网关节点上的客户端网络不可信。

保存配置后，网关节点客户端网络上的所有入站流量都会被丢弃，但端口 443 上的 HTTPS S3 请求和 ICMP 回显（ping）请求除外。

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与该存储节点的任何入站连接。您应执行此常规步骤：

- 在防火墙控制页面的不可信客户端网络选项卡中、指示存储节点上的客户端网络不可信。

保存配置后、存储节点将不再接受客户端网络上的任何传入流量、但仍允许向已配置的平台服务目标发出出站请求。

示例**3**：限制对网格管理器的子网访问

假设您希望仅允许对特定子网进行网格管理器访问。您应执行以下步骤：

1. 将管理节点的客户端网络连接到子网。
2. 使用不可信客户端网络选项卡将客户端网络配置为不可信。
3. 在选项卡的*在不可信客户端网络上打开的其他端口*部分，添加端口443或8443。
4. 使用管理外部访问选项卡阻止所有外部端口(无论是否为该子网以外的主机设置了特权IP地址)。

保存配置后、只有指定子网上的主机才能访问网格管理器。所有其他主机均被阻止。

配置内部防火墙

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

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您已查看中的信息 "管理防火墙控制" 和 "网络连接准则"。
- 如果您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、如果未配置负载平衡器端点、现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上都有一个内部防火墙、可用于打开或关闭网格节点上的部分端口。您可以使用防火墙控制选项卡打开或关闭网格网络、管理网络和客户端网络上默认打开的端口。您还可以创建一个可访问关闭的网格端口的特权IP地址列表。如果您使用的是客户端网络、则可以指定节点是否信任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。

将向网格外部的IP地址开放的端口数限制为仅限绝对必要的端口、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来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 "管理防火墙控制"。

有关外部防火墙和网络安全的详细信息、请参阅 "在外部防火墙处控制访问"。

访问防火墙控件

步骤

1. 选择*configuration*>*Security*>*Firewall control*。

   介绍了此页面上的三个选项卡 "管理防火墙控制"。

2. 选择任何选项卡以配置防火墙控件。

   您可以按任意顺序使用这些选项卡。您在一个选项卡上设置的配置不会限制在其他选项卡上可以执行的操作；但是、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、有权限的IP地址和子网不具有内部网格访问权限。此外、即使在"管理外部访问"选项卡中阻止了负载平衡器端点和在"特权地址列表"选项卡中打开的其他端口、也可以访问。

> 特权地址列表选项卡上的设置不能覆盖不可信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*以CIDR表示法添加其他IP地址或子网*以添加其他有权限的客户端。

   > 向特权列表中添加尽可能少的地址。

3. (可选)选择*允许有权限的IP地址访问StorageGRID 内部端口*。请参见 "StorageGRID 内部端口"。

   > 此选项会删除对内部服务的一些保护。如果可能、请将其禁用。

4. 选择 * 保存 * 。

管理外部访问

在"管理外部访问"选项卡中关闭某个端口后、任何非网格IP地址都无法访问该端口、除非您将该IP地址添加到特权地址列表中。您只能关闭默认情况下处于打开状态的端口、并且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"不可信客户端网络"选项卡上的设置。例如、如果节点不可信、则客户端网络上会阻止端口SSH/ 22、即使此端口在管理外部访问选项卡上打开也是如此。不可信客户端网络选项卡上的设置会覆盖客户端网络上已关闭的端口(例如443、8443、9443)。

步骤

1. 选择*管理外部访问*。此选项卡将显示一个表、其中包含网格中节点的所有外部端口(默认情况下可由非网格节点访问的端口)。
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键打开或关闭选定端口。
   - 选择*打开所有显示的端口*以打开表中列出的所有端口。
   - 选择*关闭所有显示的端口*以关闭表中列出的所有端口。

     如果关闭网格管理器端口443或8443、则当前连接到被阻止端口的任何用户(包括您)将无法访问网格管理器、除非其IP地址已添加到特权地址列表中。

     使用表右侧的滚动条确保您已查看所有可用端口。使用搜索字段输入端口号以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 * 保存 *

不可信客户端网络

如果节点的客户端网络不可信、则该节点仅接受配置为负载平衡器端点的端口以及您在此选项卡上选择的其他端口(可选)上的入站流量。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。

如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

在*不可信客户端网络*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*不可信客户端网络*。
2. 在设置新节点默认值部分中、指定在扩展操作步骤 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。
   - * 不可信 * ：在扩展中添加节点时，其客户端网络不可信。

     您可以根据需要返回此选项卡来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. 使用以下选项选择仅允许在显式配置的负载平衡器端点或其他选定端口上进行客户端连接的节点：
   - 选择*在显示的节点上取消信任*，将表中显示的所有节点添加到不可信客户端网络列表中。
   - 选择*在显示的节点上信任*，从不可信客户端网络列表中删除表中显示的所有节点。
   - 使用每个端口旁边的切换功能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*Untrust on displayed N点*将所有节点添加到Untrusted Client Network列表中，然后使用单个节点旁边的切换将该单个节点添加到Trusted Client Network列表中。

> 使用表右侧的滚动条确保您已查看所有可用节点。使用搜索字段输入节点名称以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. (可选)选择要在不可信客户端网络上打开的任何其他端口。这些端口可以提供对网格管理器和/或租户管理器的访问。

   例如、您可能希望使用此选项来确保可以在客户端网络上访问网格管理器进行维护。

   > 这些附加端口在客户端网络上处于打开状态、无论它们是否在管理外部访问选项卡中关闭。

5. 选择 * 保存 * 。

   此时将立即应用并实施新的防火墙设置。如果尚未配置负载平衡器端点，现有客户端连接可能会失败。