管理不可信的客户端网络

StorageGRID

NetApp
April 10, 2024

目录

管理不可信的客户端网络

Manage Untrusted Client Networks： 概述

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 会信任所有可用外部端口上与每个网格节点的入站连接（请参见中有关外部通信的信息 网络连接准则）。

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，则节点仅接受显式配置为负载平衡器端点的端口上的入站连接。请参见 配置负载平衡器端点。

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. 在负载平衡器端点页面中，通过 HTTPS 在端口 443 上为 S3 配置负载平衡器端点。
2. 在不可信客户端网络页面中，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

假设您要从存储节点启用出站 S3 平台服务流量，但要阻止与客户端网络上的该存储节点建立任何入站连接。您应执行此常规步骤：

- 在不可信客户端网络页面中，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，但它仍允许向 Amazon Web Services 发出出站请求。

指定节点的客户端网络不可信

如果您使用的是客户端网络，则可以指定每个节点的客户端网络是可信还是不可信。您还可以为扩展中添加的新节点指定默认设置。

您需要的内容

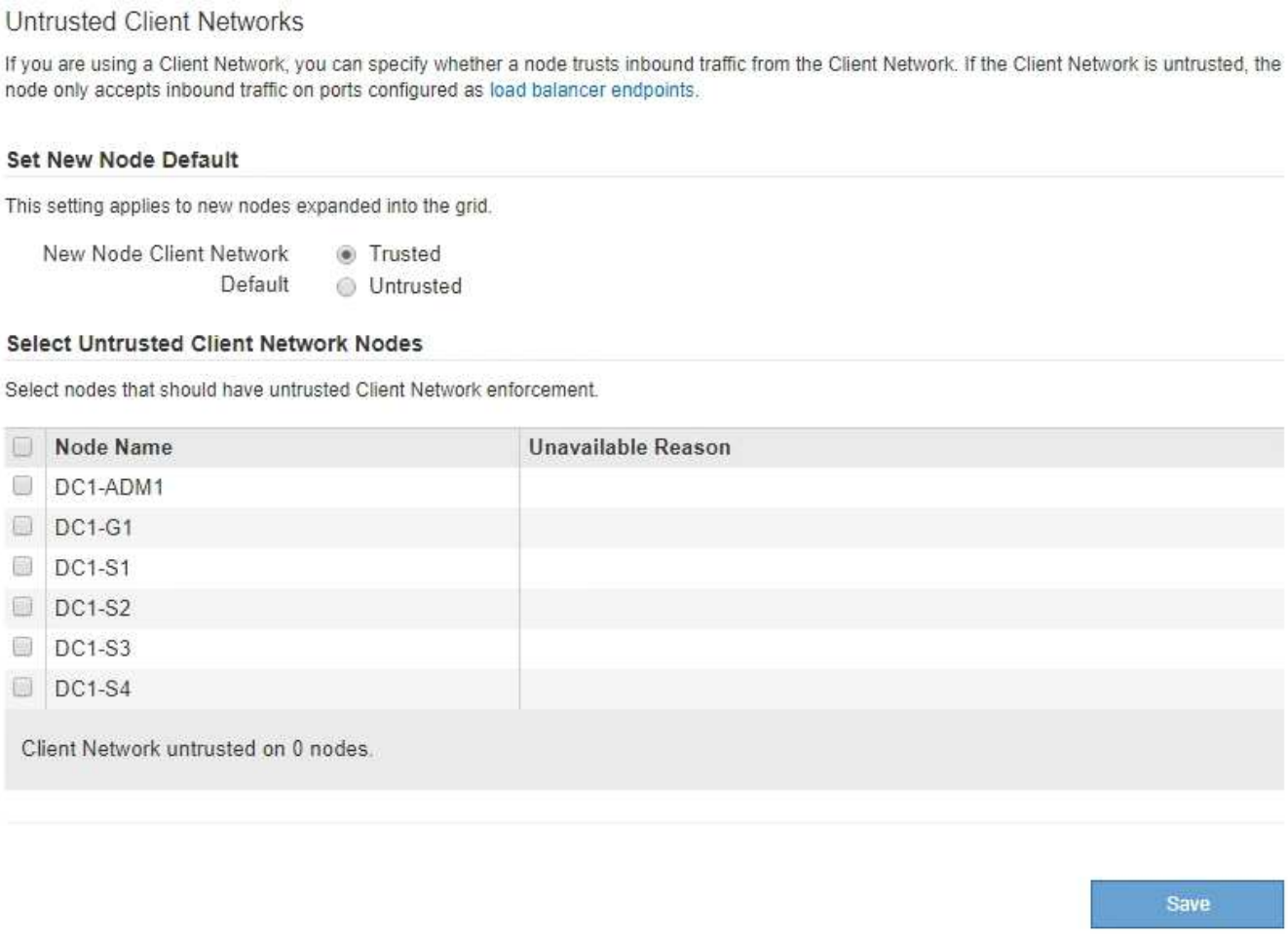
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 如果您希望管理节点或网关节点仅在显式配置的端点上接受入站流量，则已定义负载平衡器端点。

> 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。

步骤

1. 选择 * 配置 * > * 安全性 * > * 不可信客户端网络 * 。

   不可信客户端网络页面列出了 StorageGRID 系统中的所有节点。如果节点上的客户端网络必须可信，则不可用原因列将包含一个条目。



2. 在 * 设置新节点默认值 * 部分中，指定在扩展操作步骤 的网格中添加新节点时应采用的默认设置。

   - * 可信 * ： 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。根据需要，您可以返回此页面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. 在 * 选择不可信客户端网络节点 * 部分中，选择应仅允许在显式配置的负载平衡器端点上进行客户端连接的节点。

   您可以选中或取消选中标题中的复选框以选择或取消选择所有节点。

4. 选择 * 保存 * 。

   此时将立即添加并强制实施新的防火墙规则。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。

版权信息

商标信息