



# 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 .....	1
Manage Untrusted Client Networks : 概述 .....	1
指定节点的客户端网络不可信 .....	1

# 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 *untrusted* 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均衡器端点的端口上的入站连接。请参见 [配置负载均衡器端点](#)。

### 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. 在负载均衡器端点页面中，通过 HTTPS 在端口 443 上为 S3 配置负载均衡器端点。
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，则已定义负载均衡器端点。



如果尚未配置负载均衡器端点，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。

### Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

#### Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network     Trusted  
Default                       Untrusted

#### Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

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均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。如果尚未配置负载均衡器端点，现有客户端连接可能会失败。

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。