



# 系统强化

## StorageGRID 11.5

NetApp  
April 11, 2024

# 目录

系统强化	1
强化StorageGRID 系统	1
软件升级的强化准则	1
StorageGRID 网络强化准则	2
StorageGRID 节点的强化准则	3
服务器证书的强化准则	6
其他强化准则	7

# 系统强化

了解用于保护StorageGRID 系统免受安全威胁的系统设置、最佳实践和建议。

- ["强化StorageGRID 系统"](#)
- ["软件升级的强化准则"](#)
- ["StorageGRID 网络强化准则"](#)
- ["StorageGRID 节点的强化准则"](#)
- ["服务器证书的强化准则"](#)
- ["其他强化准则"\]](#)

## 强化StorageGRID 系统

系统强化是指尽可能消除 StorageGRID 系统中的安全风险的过程。

本文档概述了特定于 StorageGRID 的强化准则。这些准则是对行业标准系统强化最佳实践的补充。例如，这些准则假定您对 StorageGRID 使用强密码，使用 HTTPS 而不是 HTTP ，并在可用时启用基于证书的身份验证。

在安装和配置 StorageGRID 时，您可以使用这些准则来帮助您实现任何规定的安全目标，以确保信息系统的机密性，完整性和可用性。

StorageGRID 遵循 [\\_NetApp 漏洞处理策略\\_](#)。报告的漏洞会根据产品安全意外事件响应流程进行验证和解决。

### 强化StorageGRID 系统的一般注意事项

在强化 StorageGRID 系统时，必须考虑以下几点：

- 您实施了三个 StorageGRID 网络中的哪一个。所有 StorageGRID 系统都必须使用网格网络，但您也可以使用管理网络，客户端网络或这两者。每个网络都有不同的安全注意事项。
- StorageGRID 系统中各个节点使用的平台类型。StorageGRID 节点可以部署在VMware虚拟机上、Linux主机上的Docker容器中或作为专用硬件设备。每种类型的平台都有自己的一套强化最佳实践。
- 租户帐户的受信任程度。如果您是使用不可信租户帐户的服务提供商，则与仅使用可信的内部租户相比，您将面临不同的安全问题。
- 贵组织遵循哪些安全要求和约定。您可能需要遵守特定的法规或企业要求。

相关信息

["漏洞处理策略"](#)

## 软件升级的强化准则

您必须使 StorageGRID 系统和相关服务保持最新，以抵御攻击。

## 升级到 StorageGRID 软件

您应尽可能将 StorageGRID 软件升级到最新的主要版本或先前的主要版本。使 StorageGRID 保持最新有助于缩短已知漏洞处于活动状态的时间，并减少整体攻击面。此外，StorageGRID 的最新版本通常包含早期版本中不包括的安全强化功能。

如果需要修补程序，NetApp 会优先为最新版本创建更新。某些修补程序可能与早期版本不兼容。

要下载最新的 StorageGRID 版本和修补程序，请转到 StorageGRID 软件下载页面。有关升级 StorageGRID 软件的分步说明，请参见有关升级 StorageGRID 的说明。有关应用修补程序的说明，请参见恢复和维护说明。

## 升级到外部服务

外部服务可能存在间接影响 StorageGRID 的漏洞。您应确保 StorageGRID 所依赖的服务保持最新。这些服务包括 LDAP，KMS（或 KMIP 服务器），DNS 和 NTP。

使用 NetApp 互操作性表工具可获取受支持版本的列表。

## 升级到虚拟机管理程序

如果您的 StorageGRID 节点正在 VMware 或其他虚拟机管理程序上运行，则必须确保虚拟机管理程序软件和固件是最新的。

使用 NetApp 互操作性表工具可获取受支持版本的列表。

## 升级到Linux节点

如果 StorageGRID 节点使用的是 Linux 主机平台，则必须确保将安全更新和内核更新应用于主机操作系统。此外，如果存在固件更新，则必须将这些更新应用于容易受到影响的硬件。

使用 NetApp 互操作性表工具可获取受支持版本的列表。

相关信息

["NetApp 下载：StorageGRID"](#)

["升级软件"](#)

["保持并恢复\(\)"](#)

["NetApp 互操作性表工具"](#)

## StorageGRID 网络强化准则

StorageGRID 系统支持每个网格节点最多三个网络接口，使您可以根据安全和访问要求为每个网格节点配置网络。

### 网格网络准则

您必须为所有内部 StorageGRID 流量配置网格网络。所有网格节点均位于网格网络上，它们必须能够与所有其他节点进行通信。

配置网格网络时，请遵循以下准则：

- 确保网络不受不可信客户端的保护，例如在开放式互联网上的客户端。
- 如果可能，请仅对内部流量使用网格网络。管理网络和客户端网络都具有其他防火墙限制，可阻止外部向内部服务发送流量。支持对外部客户端流量使用网格网络，但这种使用可提供更少的保护层。
- 如果 StorageGRID 部署跨越多个数据中心，请使用网格网络上的虚拟专用网络（VPN）或等效网络为内部流量提供额外保护。
- 某些维护过程要求在主管理节点与所有其他网格节点之间的端口 22 上进行安全 Shell（SSH）访问。使用外部防火墙将 SSH 访问限制为受信任的客户端。

## 管理网络准则

管理网络通常用于执行管理任务（使用网格管理器或 SSH 的受信任员工）以及与 LDAP，DNS，NTP 或 KMS（或 KMIP 服务器）等其他受信任服务进行通信。但是，StorageGRID 不会在内部强制使用此用法。

如果您使用的是管理网络，请遵循以下准则：

- 阻止管理网络上的所有内部流量端口。请参见适用于您的平台的安装指南中的内部端口列表。
- 如果不可信的客户端可以访问管理网络，请使用外部防火墙阻止对管理网络上 StorageGRID 的访问。

## 客户端网络准则

客户端网络通常用于租户以及与外部服务（例如 CloudMirror 复制服务或其他平台服务）进行通信。但是，StorageGRID 不会在内部强制使用此用法。

如果您使用的是客户端网络，请遵循以下准则：

- 阻止客户端网络上的所有内部流量端口。请参见适用于您的平台的安装指南中的内部端口列表。
- 仅接受显式配置的端点上的入站客户端流量。请参见有关管理 StorageGRID 的说明中有关管理不可信客户端网络的信息。

相关信息

["网络准则"](#)

["网格入门"](#)

["管理 StorageGRID"](#)

["安装 Red Hat Enterprise Linux 或 CentOS"](#)

["安装 Ubuntu 或 Debian"](#)

["安装 VMware"](#)

## StorageGRID 节点的强化准则

StorageGRID 节点可以部署在VMware虚拟机上、Linux主机上的Docker容器中或作为专用硬件设备。每种类型的平台和每种类型的节点都有自己的一组强化最佳实践。

## 防火墙配置

在系统强化过程中，您必须查看外部防火墙配置并对其进行修改，以便仅接受来自 IP 地址和严格需要的端口的流量。

在VMware平台和StorageGRID设备上运行的节点使用内部防火墙、该防火墙会自动进行管理。虽然此内部防火墙可为应对某些常见威胁提供额外的保护层，但它不会消除对外部防火墙的需求。

有关 StorageGRID 使用的所有内部和外部端口的列表，请参见适用于您的平台的安装指南。

## 虚拟化，容器和共享硬件

对于所有 StorageGRID 节点，请避免在与不可信软件相同的物理硬件上运行 StorageGRID。如果 StorageGRID 和恶意软件都位于同一物理硬件上，则不要假定虚拟机管理程序保护将防止恶意软件访问受 StorageGRID 保护的数据。例如，Meltdown 和 Spectre 攻击会利用现代处理器中的关键漏洞，并允许程序在同一台计算机的内存中窃取数据。

## 禁用未使用的服务

对于所有 StorageGRID 节点，您应禁用或阻止对未使用服务的访问。例如，如果您不打算配置客户端对 CIFS 或 NFS 的审核共享的访问权限，请阻止或禁用对这些服务的访问。

## 在安装期间保护节点

安装 StorageGRID 节点时，请勿允许不可信的用户通过网络访问这些节点。节点在加入网格之前不会完全安全。

## 管理节点准则

管理节点可提供系统配置，监控和日志记录等管理服务。登录到网格管理器或租户管理器时，您正在连接到管理节点。

请按照以下准则保护 StorageGRID 系统中的管理节点：

- 保护所有管理节点不受不可信客户端的安全，例如在开放式 Internet 上的客户端。确保任何不可信的客户端都不能访问网格网络，管理网络或客户端网络上的任何管理节点。
- StorageGRID 组控制对网格管理器和租户管理器功能的访问。为每个用户组授予其角色所需的最低权限，并使用只读访问模式防止用户更改配置。
- 在使用 StorageGRID 负载均衡器端点时，请对不可信的客户端流量使用网关节点，而不是管理节点。
- 如果您的租户不可信，请勿允许他们直接访问租户管理器或租户管理 API。相反，让任何不可信的租户使用与租户管理 API 交互的租户门户或外部租户管理系统。
- 或者，也可以使用管理员代理更好地控制从管理节点到 NetApp 支持的 AutoSupport 通信。请参见管理 StorageGRID 说明中的创建管理员代理的步骤。
- 或者，也可以使用受限的 8443 和 9443 端口分隔 Grid Manager 和租户管理器通信。阻止共享端口 443 并将租户请求限制为端口 9443 以提供额外保护。
- 也可以为网格管理员和租户用户使用单独的管理节点。

有关详细信息，请参见有关管理 StorageGRID 的说明。

## 存储节点准则

存储节点可管理和存储对象数据和元数据。请按照以下准则保护 StorageGRID 系统中的存储节点。

- 请勿为不可信租户启用出站服务。例如，在为不可信租户创建帐户时，请勿允许租户使用自己的身份源，也不允许使用平台服务。请参见管理 StorageGRID 的说明中有关创建租户帐户的步骤。
- 对不可信的客户端流量使用第三方负载均衡器。第三方负载均衡可提供更多控制和更多保护层，防止受到攻击。
- 或者，也可以使用存储代理更好地控制云存储池以及从存储节点到外部服务的平台服务通信。请参见管理 StorageGRID 的说明中有关创建存储代理的步骤。
- 也可以使用客户端网络连接到外部服务。然后、选择\*配置\*>\*网络设置\*>\*不可信客户端网络\*、并指示存储节点上的客户端网络不可信。存储节点不再接受客户端网络上的任何传入流量，但仍允许对平台服务发出出站请求。

## 网关节点准则

网关节点提供了一个可选的负载均衡接口，客户端应用程序可以使用该接口连接到 StorageGRID 。请按照以下准则保护 StorageGRID 系统中的所有网关节点：

- 在网关节点上配置和使用负载均衡器端点，而不是使用 CLB 服务。请参见管理 StorageGRID 说明中的负载均衡管理步骤。



CLB 服务已弃用。

- 在客户端和网关节点或存储节点之间使用第三方负载均衡器处理不可信的客户端流量。第三方负载均衡可提供更多控制和更多保护层，防止受到攻击。如果您使用的是第三方负载均衡器，则仍然可以选择将网络流量配置为通过内部负载均衡器端点或直接发送到存储节点。
- 如果您使用的是负载均衡器端点，则可以选择让客户端通过客户端网络进行连接。然后、选择\*配置\*>\*网络设置\*>\*不可信客户端网络\*、并指示网关节点上的客户端网络不可信。网关节点仅接受显式配置为负载均衡器端点的端口上的入站流量。

## 硬件设备节点准则

StorageGRID 硬件设备经过专门设计，可在 StorageGRID 系统中使用。某些设备可用作存储节点。其他设备可以用作管理节点或网关节点。您可以将设备节点与基于软件的节点结合使用，也可以部署经过全面设计的全设备网络。

请按照以下准则保护 StorageGRID 系统中的所有硬件设备节点：

- 如果设备使用 SANtricity 系统管理器管理存储控制器，请防止不可信的客户端通过网络访问 SANtricity 系统管理器。
- 如果设备具有基板管理控制器（ Baseboard Management Controller ， BMC ），请注意， BMC 管理端口允许低级别硬件访问。请仅将 BMC 管理端口连接到安全可信的内部管理网络。如果没有此类网络可用，请保持 BMC 管理端口未连接或被阻止，除非技术支持请求 BMC 连接。
- 如果设备支持使用智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）标准通过以太网远程管理控制器硬件，请阻止端口 623 上的不可信流量。
- 如果设备中的存储控制器包含 FDE 或 FIPS 驱动器，并且已启用驱动器安全功能，请使用 SANtricity 配置驱动器安全密钥。

- 对于没有 FDE 或 FIPS 驱动器的设备，请使用密钥管理服务器（KMS）启用节点加密。

请参见 StorageGRID 硬件设备的安装和维护说明。

相关信息

["安装 Red Hat Enterprise Linux 或 CentOS"](#)

["安装 Ubuntu 或 Debian"](#)

["安装 VMware"](#)

["管理 StorageGRID"](#)

["使用租户帐户"](#)

["SG100和AMP；SG1000服务设备"](#)

["SG5600 存储设备"](#)

["SG5700 存储设备"](#)

["SG6000 存储设备"](#)

## 服务器证书的强化准则

您应将安装期间创建的默认证书替换为您自己的自定义证书。

对于许多组织来说，用于 StorageGRID Web 访问的自签名数字证书不符合其信息安全策略。在生产系统上，您应安装 CA 签名的数字证书以用于对 StorageGRID 进行身份验证。

具体而言，您应使用自定义服务器证书，而不是这些默认证书：

- 管理接口服务器证书：用于确保对网络管理器、租户管理器、网络管理API和租户管理API的访问安全。
- 对象存储API服务端点服务器证书：用于保护对存储节点和网关节点的访问安全、S3和Swift客户端应用程序使用这些节点上传和下载对象数据。



StorageGRID 单独管理用于负载均衡器端点的证书。要配置负载均衡器证书，请参见管理 StorageGRID 的说明中配置负载均衡器端点的步骤。

使用自定义服务器证书时，请遵循以下准则：

- 证书应具有 `subjectAltName` 与 StorageGRID 的 DNS 条目匹配。有关详细信息，请参见中的第 4.2.1.6 节 "SSubject Alternative Name"，"[RFC 5280：PKIX 证书和 CRL 配置文件](#)"。
- 尽可能避免使用通配符证书。此准则的一个例外是 S3 虚拟托管模式端点的证书，如果事先不知道分段名称，则需要使用通配符。
- 如果必须在证书中使用通配符，则应执行其他步骤以降低风险。使用通配符模式、例如 `*.s3.example.com`和、请勿使用 `s3.example.com` 其他应用程序的后缀。此模式也适用于路径模式 S3 访问、例如 `dc1-s1.s3.example.com/mybucket`。



- 将证书到期时间设置为较短（例如 2 个月），并使用网络管理 API 自动轮换证书。这对于通配符证书尤其重要。

此外，客户端在与 StorageGRID 通信时应使用严格的主机名检查。

## 其他强化准则

除了遵循 StorageGRID 网络和节点的强化准则之外，您还应遵循 StorageGRID 系统其他方面的强化准则。

### 日志和审核消息

始终以安全的方式保护 StorageGRID 日志和审核消息输出。从支持和系统可用性角度来看，StorageGRID 日志和审核消息可提供宝贵的信息。此外，StorageGRID 日志和审核消息输出中包含的信息和详细信息通常具有敏感性。

有关 StorageGRID 日志的详细信息，请参见有关监控和故障排除的说明。有关 StorageGRID 审核消息的详细信息，请参见审核消息的说明。

### NetApp AutoSupport

通过 StorageGRID 的 AutoSupport 功能，您可以主动监控系统的运行状况，并自动向 NetApp 技术支持，贵组织的内部支持团队或支持合作伙伴发送消息和详细信息。默认情况下，首次配置 StorageGRID 时，会启用发送给 NetApp 技术支持的 AutoSupport 消息。

可以禁用 AutoSupport 功能。但是，NetApp 建议启用此功能，因为如果您的 StorageGRID 系统上出现问题描述，AutoSupport 有助于加快识别和解决问题的速度。

对于传输协议，AutoSupport 支持 HTTPS，HTTP 和 SMTP。由于 AutoSupport 消息的敏感性，NetApp 强烈建议使用 HTTPS 作为向 NetApp 支持部门发送 AutoSupport 消息的默认传输协议。

您也可以配置一个管理员代理，以便更好地控制从管理节点到 NetApp 技术支持的 AutoSupport 通信。请参见管理 StorageGRID 说明中的创建管理员代理的步骤。

### 跨源资源共享（CORS）

如果您希望 S3 存储分段中的存储分段和对象可供其他域中的 Web 应用程序访问，则可以为该存储分段配置跨源资源共享（CORS）。通常，除非需要，否则请勿启用 CORS。如果需要 CORS，请将其限制为可信源。

请参见使用租户帐户说明中的配置跨源资源共享（CORS）的步骤。

### 外部安全设备

全面强化的解决方案必须解决 StorageGRID 之外的安全机制问题。使用其他基础架构设备筛选和限制对 StorageGRID 的访问是建立和保持严格安全防护的有效方法。这些外部安全设备包括防火墙，入侵防护系统（IP）和其他安全设备。

对于不可信的客户端流量，建议使用第三方负载平衡器。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。

相关信息

"监控和放大; 故障排除"

"查看审核日志"

"使用租户帐户"

"管理 StorageGRID"

## 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。