StorageGRID 系统加固

StorageGRID software

NetApp
July 23, 2026

目录

StorageGRID 系统加固

了解 StorageGRID 的系统加固

系统强化是从 StorageGRID 系统中消除尽可能多的安全风险的过程。

在安装和配置 StorageGRID 时，请使用这些指南来帮助您实现任何规定的机密性、完整性和可用性安全目标。

您应该已经使用行业标准的最佳实践来进行系统加固。例如，您对 StorageGRID 使用强密码、使用 HTTPS 而不是 HTTP，并启用基于证书的身份验证（如果可用）。这些最佳实践必须包括限制物理访问的物理和环境安全，以及保护物理数据中心和支持基础设施。您还必须参考任何适用于您的业务和地区的监管标准和建议。

StorageGRID 遵循 "NetApp 漏洞处理策略"。报告的漏洞将根据产品安全事件响应流程进行验证和解决。

加固 StorageGRID 系统时，请考虑以下内容：

- 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，但也可能使用管理网络、客户端网络或两者。每个网络都有不同的安全注意事项。
- 您用于 **StorageGRID** 系统中各个节点的平台类型。StorageGRID 节点可以部署在 VMware 虚拟机上、Linux 主机上的容器引擎内或作为专用硬件设备。每种类型的平台都有其自己的一套加固最佳实践。
- 租户账号的可信度。如果您是一家拥有不受信任的租户帐户的服务提供商，则与仅使用受信任的内部租户相比，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监管或公司要求。

StorageGRID 软件升级的强化准则

您必须保持 StorageGRID 系统和相关服务处于最新状态，以防御攻击。

升级到 StorageGRID 软件

尽可能将 StorageGRID 软件升级到最新的主要版本或以前的主要版本。及时更新 StorageGRID 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，最新版本的 StorageGRID 通常包含早期版本中未包含的安全强化功能。

请参阅 "NetApp 互操作性表工具" (IMT)，以确定您应该使用哪个版本的 StorageGRID 软件。当需要修补程序时，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 "NetApp 下载：StorageGRID"。
- 要升级 StorageGRID 软件，请参见 "升级说明"。
- 要应用修补程序，请参见 "StorageGRID 修补程序过程"。

升级到外部服务

外部服务可能存在间接影响 StorageGRID 的漏洞。请确保 StorageGRID 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。

有关受支持版本的列表，请参见 "NetApp 互操作性表工具"。

升级到虚拟机监控程序

如果您的 StorageGRID 节点在 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。

有关受支持版本的列表，请参见 "NetApp 互操作性表工具"。

升级到 Linux 节点

如果您的 StorageGRID 节点正在使用 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，当这些更新可用时，您必须将固件更新应用于易受攻击的硬件。

有关受支持版本的列表，请参见 "NetApp 互操作性表工具"。

StorageGRID 网络的加固准则

StorageGRID 系统为每个网格节点最多支持三个网络接口，允许您为每个单独的网格节点配置网络，以满足您的安全和访问要求。

有关 StorageGRID 网络的详细信息，请参见 "StorageGRID 网络类型"。

网格网络准则

您必须为所有内部 StorageGRID 流量配置网格网络。所有网格节点都在网格网络上，它们必须能够与所有其他节点通信。

配置网格网络时，请遵循以下指南：

- 确保网络免受不受信任的客户端（例如开放互联网上的客户端）的侵害。
- 如果可能，请仅将网格网络用于内部流量。管理网络和客户端网络都有额外的防火墙限制，可阻止外部流量访问内部服务。支持将网格网络用于外部客户端流量，但这种用法提供的保护层较少。
- 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) 或同等网络为内部流量提供额外保护。
- 某些维护程序要求在主管理节点和所有其他网格节点之间的端口 22 上进行安全外壳 (SSH) 访问。使用外部防火墙将 SSH 访问限制为受信任的客户端。

管理网络指南

管理网络通常用于管理任务（使用 Grid Manager 或 SSH 的受信任员工）以及与其他受信任服务（如 LDAP、DNS、NTP 或 KMS（或 KMIP 服务器））进行通信。但是，StorageGRID 不会在内部强制执行此用法。

如果要使用管理员网络，请遵循以下指南：

- 阻止管理网络上的所有内部流量端口。请参见 "内部端口列表"。
- 如果不受信任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。

客户端网络指南

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 不会在内部强制执行此用法。

如果要使用客户端网络，请遵循以下指南：

- 阻止客户端网络上的所有内部流量端口。请参见 "内部端口列表"。
- 仅在显式配置的端点上接受入站客户端流量。请参阅有关 "管理防火墙控制" 的信息。

StorageGRID 节点的加固准则

StorageGRID 节点可以部署在 VMware 虚拟机上、Linux 主机上的容器引擎内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套强化最佳实践。

控制对 **BMC** 的远程 **IPMI** 访问

您可以为所有包含 BMC 的设备启用或禁用远程 IPMI 访问。远程 IPMI 接口允许拥有 BMC 帐户和密码的任何人对您的 StorageGRID 设备进行低级硬件访问。如果不需要远程 IPMI 访问 BMC，请禁用此选项。

- 要在 Grid Manager 中控制对 BMC 的远程 IPMI 访问，请转到 **Configuration** > **Security** > **Security settings** > **Appliances**：
  - 清除*启用远程 IPMI 访问*复选框以禁用对 BMC 的 IPMI 访问。
  - 选中*启用远程 IPMI 访问*复选框以启用对 BMC 的 IPMI 访问。

有关 BMC 加固的其他信息，请参见 "加固基板管理控制器"来自 "国家安全局（NSA）"和 "网络安全和基础设施安全局（CISA）"的网络安全信息表。

防火墙配置

作为系统强化过程的一部分，您必须查看外部防火墙配置并进行修改，以便仅接受来自严格需要的 IP 地址和端口的流量。

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。您应该"管理内部防火墙控制"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。

具体来说，您可以管理以下方面：

- 特权地址：您可以允许选定的 IP 地址或子网访问通过"管理外部访问"选项卡上的设置关闭的端口。
- 管理外部访问：您可以关闭默认打开的端口，或重新打开以前关闭的端口。
- 不受信任的客户端网络：您可以指定节点是否信任来自客户端网络的入站流量，以及在配置不受信任的客户端网络时要打开的其他端口。

虽然此内部防火墙提供了针对某些常见威胁的额外保护层，但它并不能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 "StorageGRID 内部端口" 和 "用于外部通信的端口"。

禁用未使用的服务

对于所有 StorageGRID 节点，应禁用或阻止对未使用服务的访问。例如，如果您不打算使用 DHCP，请使用 Grid Manager 关闭端口 68。选择 **Configuration** > **Firewall control** > **Manage external access**。然后将端口 68 的状态切换从 **Open** 更改为 **Closed**。

虚拟化、容器和共享硬件

对于所有 StorageGRID 节点，请避免在与不受信任的软件相同的物理硬件上运行 StorageGRID。如果 StorageGRID 和恶意软件都存在于同一物理硬件上，请勿假设虚拟机监控程序保护能够阻止恶意软件访问受 StorageGRID 保护的数据。例如，Meltdown 和 Spectre 攻击利用了现代处理器中的关键漏洞，允许程序窃取同一台计算机内存中的数据。

在安装过程中保护节点

在安装节点时，不允许不受信任的用户通过网络访问 StorageGRID 节点。节点在加入网格之前不会完全安全。

限制对硬件的物理访问

您必须将对 StorageGRID 硬件设备节点以及运行 StorageGRID 的 VMware 虚拟机主机和 Linux 主机的物理访问权限限制为仅授权管理员。物理访问控制的一些示例包括锁、防护装置、物理屏障和视频监控。

硬件设备节点仅供授权管理员安装和操作。不允许未经授权的管理员访问硬件设备节点。

管理节点指南

管理节点提供系统配置、监控和日志记录等管理服务。登录到 Grid Manager 或 Tenant Manager 时，您将连接到管理节点。

请遵循以下指南来保护 StorageGRID 系统中的管理节点：

- 保护所有管理节点免受不受信任的客户端（例如开放互联网上的客户端）的攻击。确保任何不受信任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 Grid Manager 和 Tenant Manager 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以防止用户更改配置。
- 使用 StorageGRID 负载均衡器端点时，对于不受信任的客户端流量，请使用网关节点而不是管理节点。
- 如果您有不受信任的租户，请不要允许他们直接访问租户管理器或租户管理 API。相反，让任何不受信任的租户使用租户门户或与租户管理 API 交互的外部租户管理系统。
- （可选）使用管理代理可以更好地控制从管理节点到 NetApp 支持的 AutoSupport 通信。请参见 "创建管理员代理" 的步骤。
- 可选地，使用受限的 8443 和 9443 端口将 Grid Manager 和 Tenant Manager 通信分开。阻止共享端口 443，并将租户请求限制到端口 9443 以获得额外保护。
- （可选）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 "管理 StorageGRID" 的说明。

存储节点指南

存储节点管理和存储对象数据和元数据。按照以下指南保护 StorageGRID 系统中的存储节点。

- 不允许不受信任的客户端直接连接到存储节点。使用由网关节点或第三方负载平衡器提供的负载平衡器端点。
- 请勿为不受信任的租户启用出站服务。例如，为不受信任的租户创建帐户时，不允许租户使用自己的身份源，也不允许使用平台服务。请参阅 "创建租户帐户" 的步骤。
- 对于不受信任的客户端流量，请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额外的防御层。
- （可选）使用存储代理来更好地控制云存储池和平台服务从存储节点到外部服务的通信。查看"创建存储代理"的步骤。
- （可选）使用客户端网络连接到外部服务。然后，选择*配置* > 安全 > 防火墙控制 > 不受信任的客户端网络，并指示存储节点上的客户端网络不受信任。存储节点不再接受客户端网络上的任何传入流量，但它继续允许平台服务的出站请求。

网关节点指南

网关节点提供了一个可选的负载平衡接口，客户端应用程序可以使用它来连接至 StorageGRID。请遵循以下指南来保护 StorageGRID 系统中的任何网关节点：

- 配置和使用负载平衡器端点。请参阅 "负载平衡注意事项"。
- 使用客户端与网关节点或存储节点之间的第三方负载均衡器来处理不受信任的客户端流量。第三方负载均衡提供了更多的控制和额外的防御层。如果使用第三方负载均衡器，则仍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。
- 如果使用负载平衡器端点，可以选择让客户端通过客户端网络连接。然后，选择 配置 > 安全 > 防火墙控制 > 不受信任的客户端网络，并指示网关节点上的客户端网络不受信任。网关节点仅接受显式配置为负载平衡器端点的端口上的入站流量。

硬件设备节点指南

StorageGRID 硬件设备专为用于 StorageGRID 系统而设计。有些设备可以用作存储节点。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相结合，或部署完全设计的全设备网格。

请遵循以下指南来保护 StorageGRID 系统中的任何硬件设备节点：

- 如果设备使用 SANtricity System Manager 进行存储控制器管理，请防止不受信任的客户端通过网络访问 SANtricity System Manager。
- 如果设备具有基板管理控制器 (BMC)，请注意 BMC 管理端口允许低级硬件访问。仅将 BMC 管理端口连接到安全、可信的内部管理网络。

  您可以建立 VLAN 来隔离 BMC 网络连接，并将 BMC Internet 访问限制为受信任的网络。有关强制 VLAN 分离的其他信息，请参见 "加固基板管理控制器"中的网络安全信息表，来源为 "国家安全局（NSA）"和 "网络安全和基础设施安全局（CISA）"。

  如果安全、受信任的内部管理网络不可用，请保持 BMC 管理端口未连接或被阻止。技术支持可能会在支持案例期间请求临时访问权限。

- 如果设备支持使用智能平台管理接口(IPMI)标准通过以太网远程管理控制器硬件，请阻止端口 623 上的不受信任流量。

> 您可以为所有包含 BMC 的设备启用或禁用远程 IPMI 访问。远程 IPMI 接口允许任何拥有 BMC 帐户和密码的人对您的 StorageGRID 设备进行低级硬件访问。如果您不需要远程 IPMI 访问 BMC，请使用以下方法之一禁用此选项：+ 在 Grid Manager 中，转到 **Configuration** > **Security** > **Security settings** > **Appliances**，然后清除 **Enable remote IPMI access** 复选框。+ 在 Grid management API 中，使用专用端点： `PUT /private/bmc`。

+ 您也可以 禁用远程 IPMI 访问。

- 对于包含使用 SANtricity System Manager 管理的 SED、FDE 或 FIPS NL-SAS 驱动器的设备型号， "启用和配置 SANtricity Drive Security"。
- 对于包含使用 StorageGRID Appliance Installer 和 Grid Manager 管理的 SED 或 FIPS NVMe SSD 的设备型号， "启用并配置 StorageGRID 驱动器加密"。
- 对于没有 SED、FDE 或 FIPS 驱动器的设备，请使用密钥管理服务器 (KMS) "启用并配置 StorageGRID 软件节点加密"。

相关信息

"了解 SANtricity System Manager 中的驱动器安全性"

StorageGRID 中 TLS 和 SSH 的强化准则

您应该控制 SSH 访问，替换默认 TLS 证书，并为 TLS 和 SSH 连接选择适当的安全策略。

证书的强化准则

应将安装过程中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，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，应安装 CA 签名的数字证书以用于验证 StorageGRID。

具体来说，您应该使用自定义服务器证书，而不是以下默认证书：

- 管理接口证书：用于保护对 Grid Manager、Tenant Manager、Grid Management API 和 Tenant Management API 的访问。
- **S3 API** 证书：用于保护对存储节点和网关节点的访问，S3 客户端应用程序使用这些节点上传和下载对象数据。

有关详细信息和说明，请参见 "管理安全证书"。

> 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 "配置负载平衡器端点"。

使用自定义服务器证书时，请遵循以下准则：

- 证书应具有与 StorageGRID 的 DNS 条目匹配的 *subjectAltName*。有关详细信息，请参见 "RFC 5280：PKIX 证书和 CRL 配置文件"中的第 4.2.1.6 节"使用者备用名称"。
- 尽可能避免使用通配符证书。此准则的一个例外是 S3 虚拟托管样式端点的证书，如果事先不知道存储桶名称，则需要使用通配符。

- 当您必须在证书中使用通配符时，您应该采取其他步骤来降低风险。使用通配符模式（如 `*.s3.example.com`），并且不要为其他应用程序使用 `s3.example.com`后缀。此模式也适用于路径样式的 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 Grid Management API 自动进行证书轮换。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。

TLS 和 SSH 策略的强化准则

您可以选择一个安全策略，以确定使用哪些协议和密码与客户端应用程序建立安全的 TLS 连接，以及与内部 StorageGRID 服务建立安全的 SSH 连接。

安全策略控制 TLS 和 SSH 如何加密传输中的数据。作为最佳做法，应禁用应用程序兼容性不需要的加密选项。使用默认的 Modern 策略，除非您的系统需要符合 Common Criteria、符合 FIPS 140-2，或者您需要使用其他密码

有关详细信息和说明，请参见 "管理 TLS 和 SSH 策略"。

管理外部 SSH 访问

为增强系统安全性，默认情况下会阻止外部 SSH 访问。仅在需要执行需要入站 SSH 访问的任务（如故障排除）时才启用 SSH 访问。有关详细信息和说明，请参阅 "管理外部 SSH 访问"。

StorageGRID 中日志、密码和审核消息的加固准则

除了遵循 StorageGRID 网络和节点的加固准则外，您还应遵循 StorageGRID 系统其他区域的加固准则。

临时安装密码

要在安装期间保护 StorageGRID 系统，请在 StorageGRID 安装 UI 的临时安装程序密码页面或安装 API 中设置密码。设置后，此密码适用于安装 StorageGRID 的所有方法，包括用户界面、安装 API 和 `configure-storagegrid.py`脚本。

有关更多信息，请参阅：

- "在基于软件的节点上安装 StorageGRID"
- "安装 StorageGRID 设备"

日志和审计消息

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的角度来看，StorageGRID 日志和审核消息提供了宝贵的信息。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。

将 StorageGRID 配置为将安全事件发送到外部 syslog 服务器。如果使用 syslog 导出，请为传输协议选择 TLS 和 RELP/TLS。

有关 StorageGRID 日志的详细信息，请参见 "日志文件引用"。有关 StorageGRID 审计消息的详细信息，请参见 "审核消息"。

NetApp AutoSupport

StorageGRID 的 AutoSupport 功能允许您主动监控系统的运行状况，并自动将数据包发送到 NetApp 支持站点、您组织的内部支持团队或支持合作伙伴。默认情况下，在首次配置 StorageGRID 时，系统会启用向 NetApp 发送 AutoSupport 数据包的功能。

AutoSupport 功能可以禁用。但是，NetApp 建议启用此功能，因为如果 StorageGRID 系统出现问题，AutoSupport 可帮助加快问题识别和解决速度。

AutoSupport 支持将 HTTPS、HTTP 和 SMTP 作为传输协议。由于 AutoSupport 包的敏感性质，NetApp 强烈建议使用 HTTPS 作为默认传输协议，以便向 NetApp 发送 AutoSupport 包。

跨源资源共享(CORS)

如果您希望其他域中的 Web 应用程序可以访问 S3 存储桶中的存储桶和对象，则可以为该存储桶配置跨源资源共享 (CORS)。一般来说，除非需要，否则不要启用 CORS。如果需要 CORS，请将其限制为受信任的来源。

请参见 "配置存储桶和对象的 CORS" 的步骤。

外部安全设备

完整的加固解决方案必须解决 StorageGRID 之外的安全机制。使用额外的基础设施设备来过滤和限制对 StorageGRID 的访问，是建立和维护严格安全态势的有效方法。这些外部安全设备包括防火墙、入侵防御系统 (IPS) 和其他安全设备。

对于不受信任的客户端流量，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额外的防御层。

勒索软件缓解

按照 "使用 StorageGRID 防御勒索软件"中的建议，帮助保护您的对象数据免受勒索软件攻击。