StorageGRID® 11.3

System Hardening Guide

November 2019 | 215-14607_2019-11_en-us
doccomments@netapp.com

NetApp®

Contents

Hardening a StorageGRID system

System hardening is the process of eliminating as many security risks as possible from a StorageGRID system.

About this guide

This document provides an overview of the hardening guidelines that are specific to StorageGRID. These guidelines are a supplement to industry-standard best practices for system hardening. For example, these guidelines assume that you use strong passwords for StorageGRID, use HTTPS instead of HTTP, and enable certificate-based authentication where available.

StorageGRID follows the *NetApp Vulnerability Handling Policy*. Reported vulnerabilities are verified and addressed according to the product security incident response process.

General considerations for hardening a StorageGRID system

When hardening a StorageGRID system, you must consider the following:

- Which of the three StorageGRID networks you have implemented. All StorageGRID systems must use the Grid Network, but you might also be using the Admin Network, the Client Network, or both. Each network has different security considerations.
- The type of platforms you use for the individual nodes in your StorageGRID system. StorageGRID nodes can be deployed on VMware virtual machines, within a Docker container on Linux hosts, or as dedicated hardware appliances. Each type of platform has its own set of hardening best practices.
- How trusted the tenant accounts are. If you are a service provider with untrusted tenant accounts, you will have different security concerns than if you only use trusted, in-house tenants.
- Which security requirements and conventions are followed by your organization. You might need to comply with specific regulatory or corporate requirements.

Related information

Vulnerability Handling Policy

System hardening guidelines

As you install and configure StorageGRID, you can use these guidelines to help you meet any prescribed security objectives for information system confidentiality, integrity, and availability.

Hardening guidelines for software upgrades

You must keep your StorageGRID system and related services up to date to defend against attacks.

Upgrades to StorageGRID software

Whenever possible, you should upgrade StorageGRID software to the most recent major release or to the previous major release. Keeping StorageGRID up to date helps reduce the amount of time that known vulnerabilities are active and reduces the overall attack surface area. In addition, the most recent releases of StorageGRID often contain security hardening features that are not included in earlier releases.

When a hotfix is required, NetApp prioritizes creating updates for the most recent releases. Some patches might not be compatible with earlier releases.

To download the most recent StorageGRID releases and hotfixes, go to the StorageGRID software download page. For step-by-step instructions for upgrading StorageGRID software, see the instructions for upgrading StorageGRID. For instructions on applying a hotfix, see the recovery and maintenance instructions.

Upgrades to external services

External services can have vulnerabilities that affect StorageGRID indirectly. You should ensure that the services that StorageGRID depends on are kept up to date. These services include LDAP, DNS, and NTP.

Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

Upgrades to hypervisors

If your StorageGRID nodes are running on VMware or another hypervisor, you must ensure that the hypervisor software and firmware are up to date.

Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

Upgrade to Linux nodes

If your StorageGRID nodes are using Linux host platforms, you must ensure that security updates and kernel updates are applied to the host OS. Additionally, you must apply firmware updates to vulnerable hardware when these updates become available.

Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

Related information

NetApp Downloads: StorageGRID
Upgrading StorageGRID
Recovery and maintenance
NetApp Interoperability Matrix Tool

Hardening guidelines for StorageGRID networks

The StorageGRID system supports up to three network interfaces per grid node, allowing you to configure the networking for each individual grid node to match your security and access requirements.

Guidelines for the Grid Network

You must configure a Grid Network for all internal StorageGRID traffic. All grid nodes are on the Grid Network, and they must be able to talk to all other nodes.

When configuring the Grid Network, follow these guidelines:

- Ensure that the network is secured from untrusted clients, such as those on the open internet.
- If the StorageGRID deployment spans multiple data centers, use a virtual private network (VPN) or equivalent on the Grid Network to provide additional protection for internal traffic.
- Some maintenance procedures require secure shell (SSH) access on port 22 between the primary Admin Node and all other grid nodes. Use an external firewall to restrict SSH access to trusted clients.

Guidelines for the Admin Network

The Admin Network is typically used for administrative tasks (trusted employees using the Grid Manager or SSH) and for communicating with other trusted services such as LDAP, DNS, or NTP. However, StorageGRID does not enforce this usage internally.

If you are using the Admin Network, follow these guidelines:

- Block all internal traffic ports on the Admin Network. See the list of internal ports in the installation guide for your platform.
- If untrusted clients can access the Admin Network, block access to StorageGRID on the Admin Network with an external firewall.

Guidelines for the Client Network

The Client Network is typically used for tenants and for communicating with external services, such as the CloudMirror replication service or another platform service. However, StorageGRID does not enforce this usage internally.

If you are using the Client Network, follow these guidelines:

- Block all internal traffic ports on the Client Network. See the list of internal ports in the installation guide for your platform.
- Accept inbound client traffic only on explicitly configured endpoints. See the information about managing untrusted Client Networks in the instructions for administering StorageGRID.

Related information

Grid primer
Administering StorageGRID
Red Hat Enterprise Linux or CentOS installation
Ubuntu or Debian installation
VMware installation

Hardening guidelines for StorageGRID nodes

StorageGRID nodes can be deployed on VMware virtual machines, within a Docker container on Linux hosts, or as dedicated hardware appliances. Each type of platform and each type of node has its own set of hardening best practices.

Firewall configuration

As part of the system hardening process, you must review external firewall configurations and modify them so that traffic is accepted only from the IP addresses and on the ports from which it is strictly needed.

Nodes running on VMware platforms and StorageGRID appliances use an internal firewall that is managed automatically. While this internal firewall provides an additional layer of protection against some common threats, it does not remove the need for an external firewall.

Nodes running on Linux hosts are fully dependent on a correctly configured firewall that is external to the host.

For a list of all internal and external ports used by StorageGRID, see the installation guide for your platform.

Virtualization, containers, and shared hardware

For all StorageGRID nodes, avoid running StorageGRID on the same physical hardware as untrusted software. Do not assume that hypervisor protections will prevent malware from accessing StorageGRID-protected data if both StorageGRID and the malware exist on the same the physical hardware. For example, the Meltdown and Spectre attacks exploit critical vulnerabilities in modern processors and allow programs to steal data in memory on the same computer.

Disable unused services

For all StorageGRID nodes, you should disable or block access to unused services. For example, if you are not planning to configure client access to the audit shares for CIFS or NFS, block or disable access to these services.

Protect nodes during installation

Do not allow untrusted users to access StorageGRID nodes over the network when the nodes are being installed. Nodes are not fully secure until they have joined the grid.

Guidelines for Admin Nodes

Admin Nodes provide management services such as system configuration, monitoring, and logging. When you sign in to the Grid Manager or the Tenant Manager, you are connecting to an Admin Node.

Follow these guidelines to secure the Admin Nodes in your StorageGRID system:

- Secure all Admin Nodes from untrusted clients, such as those on the open internet. Ensure that no untrusted client can access any Admin Node on the Grid Network, the Admin Network, or the Client Network.
- When using StorageGRID load balancer endpoints, use Gateway Nodes instead of Admin Nodes for untrusted client traffic.
- If you have untrusted tenants, do not allow them to have direct access to the Tenant Manager or the Tenant Management API. Instead, have any untrusted tenants use a tenant portal or an external tenant management system, which interacts with the Tenant Management API.

- Optionally, use an Admin proxy for more control over AutoSupport communication from Admin Nodes to NetApp support. See the steps for creating an Admin proxy in the instructions for administering StorageGRID.
- Optionally, use the restricted 8443 and 9443 ports to separate Grid Manager and Tenant Manager communications. Block the shared port 443 and limit tenant requests to port 9443 for additional protection.
- Optionally, use separate Admin Nodes for grid administrators and tenant users.

For more information, see the instructions for administering StorageGRID.

Guidelines for Storage Nodes

Storage Nodes manage and store object data and metadata. Follow these guidelines to secure the Storage Nodes in your StorageGRID system.

- Do not enable outbound services for untrusted tenants. For example, when creating the account for an untrusted tenant, do not allow the tenant to use its own identity source and do not allow the use of platform services. See the steps for creating a tenant account in the instructions for administering StorageGRID.
- Use a third-party load balancer for untrusted client traffic. Third-party load balancing offers more control and additional layers of protection against attack.
- Optionally, use a Storage proxy for more control over Cloud Storage Pools and platform services communication from Storage Nodes to external services. See the steps for creating a Storage proxy in the instructions for administering StorageGRID.
- Optionally, connect to external services using the Client Network. Then, select **Configuration > Untrusted Client Network** and indicate that the Client Network on the Storage Node is untrusted. The Storage Node no longer accepts any incoming traffic on the Client Network, but it continues to allow outbound requests.

Guidelines for Gateway Nodes

Gateway Nodes provide an optional load-balancing interface that client applications can use to connect to StorageGRID. Follow these guidelines to secure any Gateway Nodes in your StorageGRID system:

- Configure and use load balancer endpoints instead of using the legacy CLB service on Gateway Nodes. See the steps for managing load balancing in the instructions for administering StorageGRID.
- Use a third-party load balancer for untrusted client traffic. Third-party load balancing offers more control and additional layers of protection against attack.
- If you are using load balancer endpoints, optionally have clients connect over the Client Network. Then, select **Configuration > Untrusted Client Network** and indicate that the Client Network on the Gateway Node is untrusted. The Gateway Node only accepts inbound traffic on the ports explicitly configured as load balancer endpoints.

Guidelines for hardware appliance nodes

StorageGRID hardware appliances are specially designed for use in a StorageGRID system. Some appliances can be used as Storage Nodes. Other appliances can be used as Admin Nodes or Gateway Nodes. You can combine appliance nodes with software-based nodes or deploy fully engineered, all-appliance grids.

Follow these guidelines to secure any hardware appliance nodes in your StorageGRID system:

- If the appliance uses SANtricity System Manager for storage controller management, prevent untrusted clients from accessing SANtricity System Manager over the network.
- If the appliance has a baseboard management controller (BMC), be aware that the BMC management port allows low-level hardware access. Connect the BMC management port only to a secure, trusted, internal management network. If no such network is available, leave the BMC management port unconnected or blocked, unless a BMC connection is requested by technical support.
- If the appliance supports remote management of the controller hardware over Ethernet using the Intelligent Platform Management Interface (IPMI) standard, block untrusted traffic on port 623.
- If the storage controller in the appliance includes FDE or FIPS drives and the Drive Security feature is enabled, use SANtricity to configure Drive Security keys.

See the installation and maintenance instructions for your StorageGRID hardware appliance.

Related information

Red Hat Enterprise Linux or CentOS installation
Ubuntu or Debian installation
VMware installation
Administering StorageGRID
Using tenant accounts
SG1000 appliance installation and maintenance
SG5600 appliance installation and maintenance
SG5700 appliance installation and maintenance
SG6000 appliance installation and maintenance

Hardening guidelines for NAS Bridge

StorageGRID NAS Bridge is a virtual appliance that allows file-based workloads to run on StorageGRID.

If you are using NAS Bridge, follow these guidelines to harden your system:

- When defining the StorageGRID endpoint during the initial configuration of NAS Bridge, check the **Certificate Validation** check box. When this check box is selected, the certificate for the Transport Layer Security (TLS) connection to StorageGRID is validated.
- Ensure that NFS and SMB traffic run over a secure network. NAS Bridge does not support encrypted NFS or SMB.

See the instructions for NAS Bridge installation and setup.

Related information

NAS Bridge installation and setup

Other hardening guidelines

In addition to following the hardening guidelines for StorageGRID networks and nodes, you should follow the hardening guidelines for other areas of the StorageGRID system.

Custom server certificates

You should replace the default certificates created during installation with your own custom certificates.

- For many organizations, the self-signed digital certificate for StorageGRID web access is not compliant with their information security policies. On production systems, you should install a CA-signed digital certificate for use in authenticating StorageGRID.
- Certificates should have a `subjectAltName` that matches DNS entries for StorageGRID. For details, see section 4.2.1.6, “Subject Alternative Name,” in *RFC 5280: PKIX Certificate and CRL Profile.*
- Clients should use strict hostname checking when communicating with StorageGRID.

Specifically, you should use custom server certificates instead of these default certificates:

- **Management Interface Server Certificate**: Used to secure access to the Grid Manager, the Tenant Manager, the Grid Management API, and the Tenant Management API.
- **Object Storage API Service Endpoints Server Certificate**: Used to secure access to Storage Nodes and Gateway Nodes, which S3 and Swift client applications use to upload and download object data.

Note: StorageGRID manages the certificates used for load balancer endpoints separately. To configure load balancer certificates, see the steps for configuring load balancer endpoints in the instructions for administering StorageGRID.

Logs and audit messages

Always protect StorageGRID logs and audit message output in a secure manner. StorageGRID logs and audit messages provide invaluable information from a support and system availability standpoint. In addition, the information and details contained in StorageGRID logs and audit message output are generally of a sensitive nature.

See the instructions for monitoring and troubleshooting for more information about StorageGRID logs. See the instructions for audit messages for more information about StorageGRID audit messages.

NetApp AutoSupport

The AutoSupport feature of StorageGRID allows you to proactively monitor the health of your system and automatically send messages and details to NetApp technical support, your organization’s internal support team, or a support partner. By default, AutoSupport messages to NetApp technical support are enabled when StorageGRID is configured for the first time.

The AutoSupport feature can be disabled. However, NetApp recommends enabling it because AutoSupport helps speed problem identification and resolution should an issue arise on your StorageGRID system.

AutoSupport supports HTTPS, HTTP, and SMTP for transport protocols. Because of the sensitive nature of AutoSupport messages, NetApp strongly recommends using HTTPS as the default transport protocol for sending AutoSupport messages to NetApp support.

Optionally, you can configure an Admin proxy for more control over AutoSupport communication from Admin Nodes to NetApp technical support. See the steps for creating an Admin proxy in the instructions for administering StorageGRID.

Cross-Origin Resource Sharing (CORS)

You can configure Cross-Origin Resource Sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains. In general, do not enable CORS unless it is required. If CORS is required, restrict it to trusted origins.

See the steps for configuring Cross-Origin Resource Sharing (CORS) in the instructions for using tenant accounts.

External security devices

A complete hardening solution must address security mechanisms outside of StorageGRID. Using additional infrastructure devices for filtering and limiting access to StorageGRID is an effective way to establish and maintain a stringent security posture. These external security devices include firewalls, intrusion prevention systems (IPSs), and other security devices.

A third-party load balancer is recommended for untrusted client traffic. Third-party load balancing offers more control and additional layers of protection against attack.

Related information

Monitoring and troubleshooting StorageGRID
Understanding audit messages
Using tenant accounts
Administering StorageGRID

Copyright

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277