



Get started

StorageGRID

NetApp
March 18, 2022

Table of Contents

- Get started 1
 - Grid primer 1
 - Networking guidelines 68

Get started

Grid primer

Grid primer: Overview

Use these introduction to get an overview of the StorageGRID system and to learn about StorageGRID architecture and networking topology, data management features, and user interface.

What is StorageGRID?

NetApp StorageGRID is a software-defined, object-based storage solution that supports industry-standard object APIs, including the Amazon Simple Storage Service (S3) API and the OpenStack Swift API.

StorageGRID provides secure, durable storage for unstructured data at scale. Integrated, metadata-driven lifecycle management policies optimize where your data lives throughout its life. Content is placed in the right location, at the right time, and on the right storage tier to reduce cost.

StorageGRID is composed of geographically distributed, redundant, heterogeneous nodes, which can be integrated with both existing and next-generation client applications.



Advantages of the StorageGRID system include the following:

- Massively scalable and easy-to-use a geographically distributed data repository for unstructured data.
- Standard object storage protocols:
 - Amazon Web Services Simple Storage Service (S3)
 - OpenStack Swift
- Hybrid cloud enabled. Policy-based information lifecycle management (ILM) stores objects to public clouds, including Amazon Web Services (AWS) and Microsoft Azure. StorageGRID platform services enable content replication, event notification, and metadata searching of objects stored to public clouds.
- Flexible data protection to ensure durability and availability. Data can be protected using replication and layered erasure coding. At-rest and in-flight data verification ensures integrity for long-term retention.
- Dynamic data lifecycle management to help manage storage costs. You can create ILM rules that manage data lifecycle at the object level, and customize data locality, durability, performance, cost, and retention

time. Tape is available as an integrated archive tier.

- High availability of data storage and some management functions, with integrated load balancing to optimize the data load across StorageGRID resources.
- Support for multiple storage tenant accounts to segregate the objects stored on your system by different entities.
- Numerous tools for monitoring the health of your StorageGRID system, including a comprehensive alert system, a graphical dashboard, and detailed statuses for all nodes and sites.
- Support for software or hardware-based deployment. You can deploy StorageGRID on any of the following:
 - Virtual machines running in VMware.
 - Container engines on Linux hosts.
 - StorageGRID engineered appliances.
 - Storage appliances provide object storage.
 - Services appliances provide grid administration and load balancing services.
- Compliant with the relevant storage requirements of these regulations:
 - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
 - Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
 - Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.
- Non-disruptive upgrade and maintenance operations. Maintain access to content during upgrade, expansion, decommission, and maintenance procedures.
- Federated identity management. Integrates with Active Directory, OpenLDAP, or Oracle Directory Service for user authentication. Supports single sign-on (SSO) using the Security Assertion Markup Language 2.0 (SAML 2.0) standard to exchange authentication and authorization data between StorageGRID and Active Directory Federation Services (AD FS).

Hybrid clouds with StorageGRID

You can use StorageGRID in a hybrid cloud configuration by implementing policy-driven data management to store objects in Cloud Storage Pools, by leveraging StorageGRID platform services, and by moving data to StorageGRID with NetApp FabricPool.

Cloud Storage Pools

Cloud Storage Pools allow you to store objects outside of the StorageGRID system. For example, you might want to move infrequently accessed objects to lower-cost cloud storage, such as Amazon S3 Glacier, S3 Glacier Deep Archive, or the Archive access tier in Microsoft Azure Blob storage. Or, you might want to maintain a cloud backup of StorageGRID objects, which can be used to recover data lost because of a storage volume or Storage Node failure.



Using Cloud Storage Pools with FabricPool is not supported because of the added latency to retrieve an object from the Cloud Storage Pool target.

S3 platform services

S3 platform services give you the ability to use remote services as endpoints for object replication, event notifications, or search integration. Platform services operate independently of the grid's ILM rules, and are enabled for individual S3 buckets. The following services are supported:

- The CloudMirror replication service automatically mirrors specified objects to a target S3 bucket, which can be on Amazon S3 or a second StorageGRID system.
- The Event notification service sends messages about specified actions to an external endpoint that supports receiving Simple Notification Service (SNS) events.
- The search integration service sends object metadata to an external Elasticsearch service, allowing metadata to be searched, visualized, and analyzed using third party tools.

For example, you might use CloudMirror replication to mirror specific customer records into Amazon S3 and then leverage AWS services to perform analytics on your data.

ONTAP data tiering with StorageGRID

You can reduce the cost of ONTAP storage by tiering data to StorageGRID using FabricPool. FabricPool is a NetApp Data Fabric technology that enables automated tiering of data to low-cost object storage tiers, either on or off premises.

Unlike manual tiering solutions, FabricPool reduces total cost of ownership by automating the tiering of data to lower the cost of storage. It delivers the benefits of cloud economics by tiering to public and private clouds including StorageGRID.

Related information

- [Administer StorageGRID](#)
- [Use a tenant account](#)
- [Manage objects with ILM](#)
- [Configure StorageGRID for FabricPool](#)

StorageGRID architecture and network topology

A StorageGRID system consists of multiple types of grid nodes at one or more data center sites.

For additional information about StorageGRID network topology, requirements, and grid communications, see the [Networking guidelines](#).

Deployment topologies

The StorageGRID system can be deployed to a single data center site or to multiple data center sites.

Single site

In a deployment with a single site, the infrastructure and operations of the StorageGRID system are centralized.



Multiple sites

In a deployment with multiple sites, different types and numbers of StorageGRID resources can be installed at each site. For example, more storage might be required at one data center than at another.

Different sites are often located in geographically different locations across different failure domains, such as an earthquake fault line or flood plain. Data sharing and disaster recovery are achieved by automated distribution of data to other sites.



Multiple logical sites can also exist within a single data center to allow the use of distributed replication and erasure coding for increase availability and resiliency.

Grid node redundancy

In a single-site or multi-site deployment, you can optionally include more than one Admin Node or Gateway Node for redundancy. For example, you can install more than one Admin Node at a single site or across several sites. However, each StorageGRID system can only have one primary Admin Node.

System architecture

This diagram shows how grid nodes are arranged within a StorageGRID system.



S3 and Swift clients store and retrieve objects in StorageGRID. Other clients are used to send email notifications, to access the StorageGRID management interface, and optionally to access the audit share.

S3 and Swift clients can connect to a Gateway Node or an Admin Node to use the load-balancing interface to Storage Nodes. Alternatively, S3 and Swift clients can connect directly to Storage Nodes using HTTPS.

Objects can be stored within StorageGRID on software or hardware-based Storage Nodes, on external archival media such as tape, or in Cloud Storage Pools, which consist of external S3 buckets or Azure Blob storage containers.

Grid nodes and services

The basic building block of a StorageGRID system is the grid node. Nodes contain services, which are software modules that provide a set of capabilities to a grid node.

The StorageGRID system uses four types of grid nodes:

- **Admin Nodes** provide management services such as system configuration, monitoring, and logging. When you sign in to the Grid Manager, you are connecting to an Admin Node. Each grid must have one primary Admin Node and might have additional non-primary Admin Nodes for redundancy. You can connect to any Admin Node, and each Admin Node displays a similar view of the StorageGRID system. However, maintenance procedures must be performed using the primary Admin Node.

Admin Nodes can also be used to load balance S3 and Swift client traffic.

- **Storage Nodes** manage and store object data and metadata. Each StorageGRID system must have at least three Storage Nodes. If you have multiple sites, each site within your StorageGRID system must also have three Storage Nodes.
- **Gateway Nodes (optional)** provide a load-balancing interface that client applications can use to connect to StorageGRID. A load balancer seamlessly directs clients to an optimal Storage Node, so that the failure of nodes or even an entire site is transparent. You can use a combination of Gateway Nodes and Admin Nodes for load balancing, or you can implement a third-party HTTP load balancer.
- **Archive Nodes (optional)** provide an interface through which object data can be archived to tape.

To learn more, see [Administer StorageGRID](#).

Software-based nodes

Software-based grid nodes can be deployed in the following ways:

- As virtual machines (VMs) in VMware vSphere
- Within container engines on Linux hosts. The following operating systems are supported:
 - Red Hat Enterprise Linux
 - CentOS
 - Ubuntu
 - Debian

See the following for more information:

- [Install VMware](#)
- [Install Red Hat Enterprise Linux or CentOS](#)
- [Install Ubuntu or Debian](#)

Use the [NetApp Interoperability Matrix Tool](#) to get a list of supported versions.

StorageGRID 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 that have no dependencies on external hypervisors, storage, or compute hardware.

Four types of StorageGRID appliances are available:

- The **SG100 and SG1000 services appliances** are 1-rack-unit (1U) servers that can each operate as the primary Admin Node, a non-primary Admin Node, or a Gateway Node. Both appliances can operate as

Gateway Nodes and Admin Nodes (primary and non-primary) at the same time.

- The **SG6000 storage appliance** operates as a Storage Node and combines the 1U SG6000-CN compute controller with a 2U or 4U storage controller shelf. The SG6000 is available in two models:
 - **SGF6024**: Combines the SG6000-CN compute controller with a 2U storage controller shelf that includes 24 solid state drives (SSDs) and redundant storage controllers.
 - **SG6060**: Combines the SG6000-CN compute controller with a 4U enclosure that includes 58 NL-SAS drives, 2 SSDs, and redundant storage controllers. Each SG6060 appliance supports one or two 60-drive expansion shelves, providing up to 178 drives dedicated to object storage.
- The **SG5700 storage appliance** is an integrated storage and computing platform that operates as a Storage Node. The SG5700 is available in two models:
 - **SG5712**: a 2U enclosure that includes 12 NL-SAS drives and integrated storage and compute controllers.
 - **SG5760**: a 4U enclosure that includes 60 NL-SAS drives and integrated storage and compute controllers.
- The **SG5600 storage appliance** is an integrated storage and computing platform that operates as a Storage Node. The SG5600 is available in two models:
 - **SG5612**: a 2U enclosure that includes 12 NL-SAS drives and integrated storage and compute controllers.
 - **SG5660**: a 4U enclosure that includes 60 NL-SAS drives and integrated storage and compute controllers.

See the following for more information:

- [NetApp Hardware Universe](#)
- [SG100 and SG1000 services appliances](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

Primary services for Admin Nodes

The following table shows the primary services for Admin Nodes; however, this table does not list all node services.

| Service | Key function |
|---|--|
| Audit Management System (AMS) | Tracks system activity. |
| Configuration Management Node (CMN) | Manages system-wide configuration. Primary Admin Node only. |
| Management Application Program Interface (mgmt-api) | Processes requests from the Grid Management API and the Tenant Management API. |

| Service | Key function |
|---------------------------------|--|
| High Availability | Manages high availability virtual IP addresses for groups of Admin Nodes and Gateway Nodes. Note: This service is also found on Gateway Nodes. |
| Load Balancer | Provides load balancing of S3 and Swift traffic from clients to Storage Nodes. Note: This service is also found on Gateway Nodes. |
| Network Management System (NMS) | Provides functionality for the Grid Manager. |
| Prometheus | Collects and stores metrics. |
| Server Status Monitor (SSM) | Monitors the operating system and underlying hardware. |

Primary services for Storage Nodes

The following table shows the primary services for Storage Nodes; however, this table does not list all node services.



Some services, such as the ADC service and the RSM service, typically exist only on three Storage Nodes at each site.

| Service | Key function |
|--|---|
| Account (acct) | Manages tenant accounts. |
| Administrative Domain Controller (ADC) | Maintains topology and grid-wide configuration. |
| Cassandra | Stores and protects object metadata. |
| Cassandra Reaper | Performs automatic repairs of object metadata. |
| Chunk | Manages erasure-coded data and parity fragments. |
| Data Mover (dmv) | Moves data to Cloud Storage Pools. |
| Distributed Data Store (DDS) | Monitors object metadata storage. |
| Identity (idnt) | Federates user identities from LDAP and Active Directory. |

| Service | Key function |
|---------------------------------|---|
| Local Distribution Router (LDR) | Processes object storage protocol requests and manages object data on disk. |
| Replicated State Machine (RSM) | Ensures that S3 platform service requests are sent to their respective endpoints. |
| Server Status Monitor (SSM) | Monitors the operating system and underlying hardware. |

Primary services for Gateway Nodes

The following table shows the primary services for Gateway Nodes; however, this table does not list all node services.

| Service | Key function |
|--------------------------------|---|
| Connection Load Balancer (CLB) | Provides Layers 3 and 4 load balancing of S3 and Swift traffic from clients to Storage Nodes. Legacy load balancing mechanism. Note: The CLB service is deprecated. |
| High Availability | Manages high availability virtual IP addresses for groups of Admin Nodes and Gateway Nodes. Note: This service is also found on Admin Nodes. |
| Load Balancer | Provides Layer 7 load balancing of S3 and Swift traffic from clients to Storage Nodes. This is the recommended load balancing mechanism. Note: This service is also found on Admin Nodes. |
| Server Status Monitor (SSM) | Monitors the operating system and underlying hardware. |

Primary services for Archive Nodes

The following table shows the primary services for Archive Nodes; however, this table does not list all node services.

| Service | Key function |
|-----------------------------|--|
| Archive (ARC) | Communicates with a Tivoli Storage Manager (TSM) external tape storage system. |
| Server Status Monitor (SSM) | Monitors the operating system and underlying hardware. |

StorageGRID services

The following is a complete list of StorageGRID services.

- **Account Service Forwarder**

Provides an interface for the Load Balancer service to query the Account Service on remote hosts and provides notifications of Load Balancer Endpoint configuration changes to the Load Balancer service. The Load Balancer service is present on Admin Nodes and Gateway Nodes.

- **ADC service (Administrative Domain Controller)**

Maintains topology information, provides authentication services, and responds to queries from the LDR and CMN services. The ADC service is present on each of the first three Storage Nodes installed at a site.

- **AMS service (Audit Management System)**

Monitors and logs all audited system events and transactions to a text log file. The AMS service is present on Admin Nodes.

- **ARC service (Archive)**

Provides the management interface with which you configure connections to external archival storage, such as the cloud through an S3 interface or tape through TSM middleware. The ARC service is present on Archive Nodes.

- **Cassandra Reaper service**

Performs automatic repairs of object metadata. The Cassandra Reaper service is present on all Storage Nodes.

- **Chunk service**

Manages erasure-coded data and parity fragments. The Chunk service is present on Storage Nodes.

- **CLB service (Connection Load Balancer)**

Deprecated service that provides a gateway into StorageGRID for client applications connecting through HTTP. The CLB service is present on Gateway Nodes. The CLB service is deprecated and will be removed in a future StorageGRID release.

- **CMN service (Configuration Management Node)**

Manages system-wide configurations and grid tasks. Each grid has one CMN service, which is present on the primary Admin Node.

- **DDS service (Distributed Data Store)**

Interfaces with the Cassandra database to manage object metadata. The DDS service is present on Storage Nodes.

- **DMV service (Data Mover)**

Moves data to cloud endpoints. The DMV service is present on Storage Nodes.

- **Dynamic IP service**

Monitors the grid for dynamic IP changes and updates local configurations. The Dynamic IP (dynip) service is present on all nodes.

- **Grafana service**

Used for metrics visualization in the Grid Manager. The Grafana service is present on Admin Nodes.

- **High Availability service**

Manages high availability Virtual IPs on nodes configured on the High Availability Groups page. The High Availability service is present on Admin Nodes and Gateway Nodes. This service is also known as the keepalived service.

- **Identity (idnt) service**

Federates user identities from LDAP and Active Directory. The Identity service (idnt) is present on three Storage Nodes at each site.

- **Lambda Arbitrator service**

Manages S3 Select SelectObjectContent requests.

- **Load Balancer service**

Provides load balancing of S3 and Swift traffic from clients to Storage Nodes. The Load Balancer service can be configured through the Load Balancer Endpoints configuration page. The Load Balancer service is present on Admin Nodes and Gateway Nodes. This service is also known as the nginx-gw service.

- **LDR service (Local Distribution Router)**

Manages the storage and transfer of content within the grid. The LDR service is present on Storage Nodes.

- **MISCd Information Service Control Daemon service**

Provides an interface for querying and managing services on other nodes and for managing environmental configurations on the node such as querying the state of services running on other nodes. The MISCd service is present on all nodes.

- **nginx service**

Acts as an authentication and secure communication mechanism for various grid services (such as Prometheus and Dynamic IP) to be able to talk to services on other nodes over HTTPS APIs. The nginx service is present on all nodes.

- **nginx-gw service**

Powers the Load Balancer service. The nginx-gw service is present on Admin Nodes and Gateway Nodes.

- **NMS service (Network Management System)**

Powers the monitoring, reporting, and configuration options that are displayed through the Grid Manager. The NMS service is present on Admin Nodes.

- **Persistence service**

Manages files on the root disk that need to persist across a reboot. The Persistence service is present on all nodes.

- **Prometheus service**

Collects time series metrics from services on all nodes. The Prometheus service is present on Admin Nodes.

- **RSM service (Replicated State Machine Service)**

Ensures platform service requests are sent to their respective endpoints. The RSM service is present on Storage Nodes that use the ADC service.

- **SSM service (Server Status Monitor)**

Monitors hardware conditions and reports to the NMS service. An instance of the SSM service is present on every grid node.

- **Trace collector service**

Performs trace collection to gather information for use by technical support. The trace collector service uses open source Jaeger software and is present on Admin Nodes.

Object management

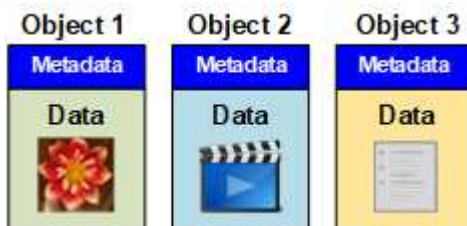
How StorageGRID manages data

As you begin working with the StorageGRID system, it is helpful to understand how the StorageGRID system manages data.

What an object is

With object storage, the unit of storage is an object, rather than a file or a block. Unlike the tree-like hierarchy of a file system or block storage, object storage organizes data in a flat, unstructured layout. Object storage decouples the physical location of the data from the method used to store and retrieve that data.

Each object in an object-based storage system has two parts: object data and object metadata.



Object data

Object data might be anything; for example, a photograph, a movie, or a medical record.

Object metadata

Object metadata is any information that describes an object. StorageGRID uses object metadata to track the locations of all objects across the grid and to manage each object's lifecycle over time.

Object metadata includes information such as the following:

- System metadata, including a unique ID for each object (UUID), the object name, the name of the S3 bucket or Swift container, the tenant account name or ID, the logical size of the object, the date and time

the object was first created, and the date and time the object was last modified.

- The current storage location of each object copy or erasure-coded fragment.
- Any user metadata associated with the object.

Object metadata is customizable and expandable, making it flexible for applications to use.

For detailed information about how and where StorageGRID stores object metadata, go to [Manage object metadata storage](#).

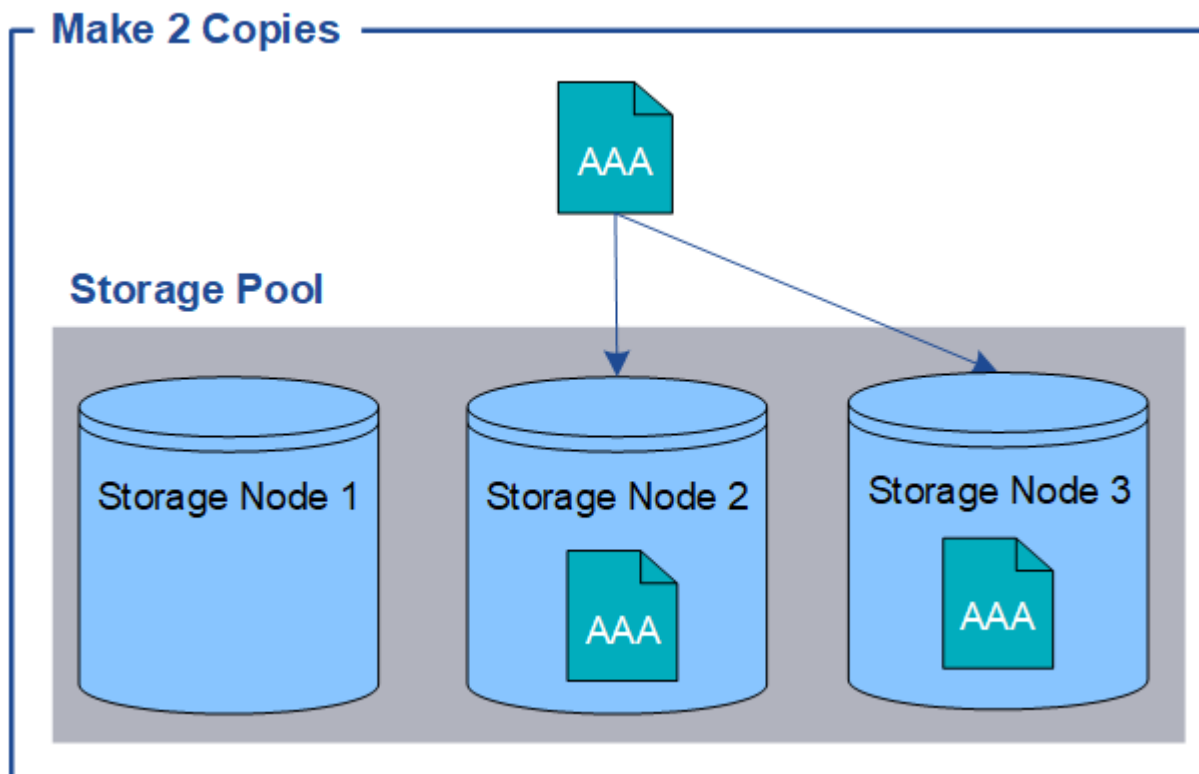
How object data is protected

The StorageGRID system provides you with two mechanisms to protect object data from loss: replication and erasure coding.

Replication

When StorageGRID matches objects to an information lifecycle management (ILM) rule that is configured to create replicated copies, the system creates exact copies of object data and stores them on Storage Nodes, Archive Nodes, or Cloud Storage Pools. ILM rules dictate the number of copies made, where those copies are stored, and for how long they are retained by the system. If a copy is lost, for example, as a result of the loss of a Storage Node, the object is still available if a copy of it exists elsewhere in the StorageGRID system.

In the following example, the Make 2 Copies rule specifies that two replicated copies of each object be placed in a storage pool that contains three Storage Nodes.

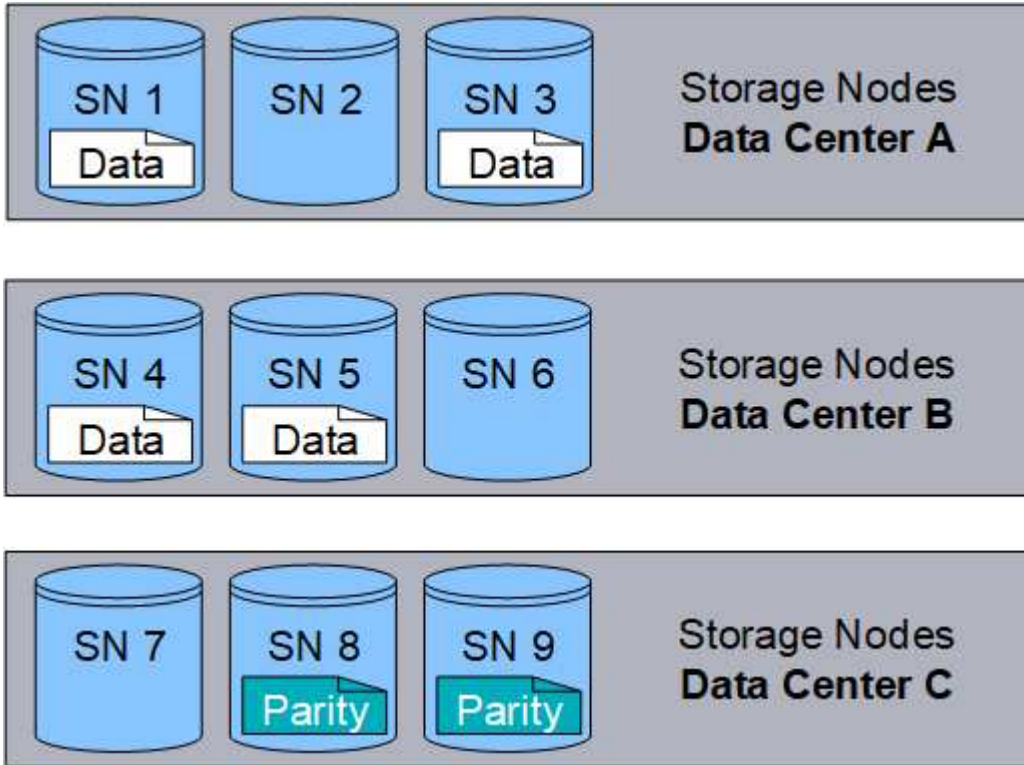


Erasure coding

When StorageGRID matches objects to an ILM rule that is configured to create erasure-coded copies, it slices object data into data fragments, computes additional parity fragments, and stores each fragment on a different Storage Node. When an object is accessed, it is reassembled using the stored fragments. If a data or a parity

fragment becomes corrupt or lost, the erasure coding algorithm can recreate that fragment using a subset of the remaining data and parity fragments. ILM rules and erasure coding profiles determine the erasure coding scheme used.

The following example illustrates the use of erasure coding on an object's data. In this example, the ILM rule uses a 4+2 erasure coding scheme. Each object is sliced into four equal data fragments, and two parity fragments are computed from the object data. Each of the six fragments is stored on a different Storage Node across three data centers to provide data protection for node failures or site loss.



Related information

- [Manage objects with ILM](#)
- [Use information lifecycle management](#)

Object lifecycle

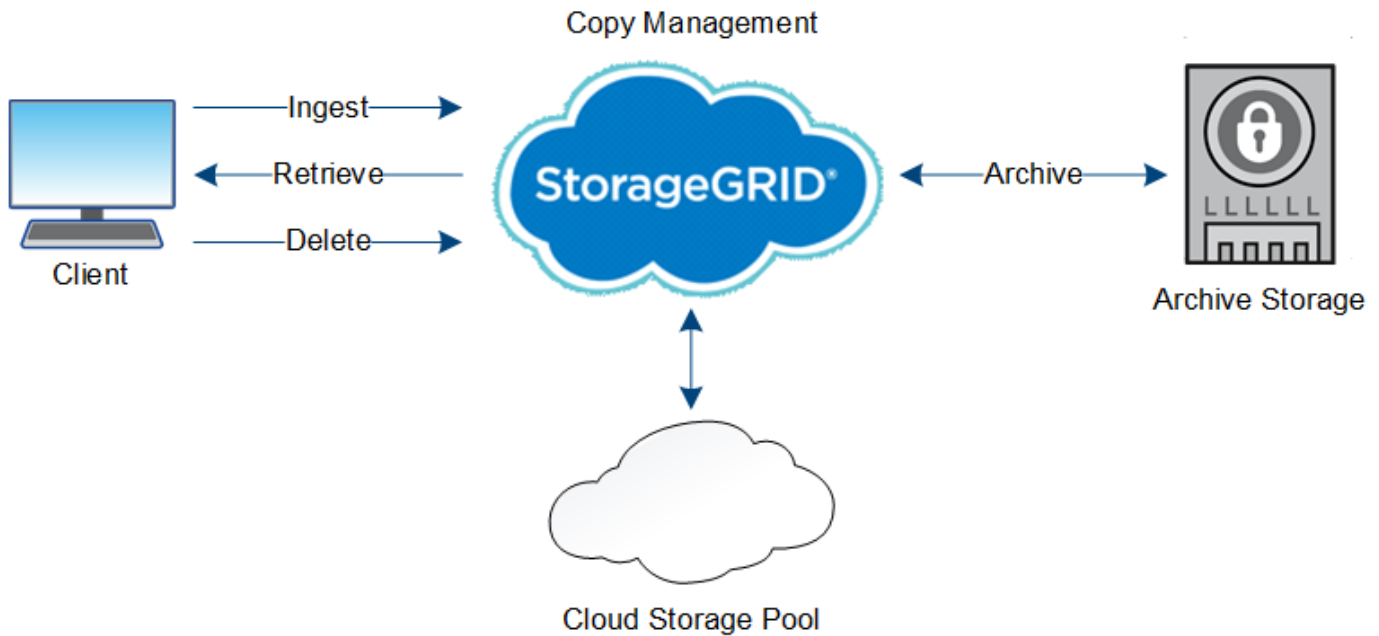
The life of an object

An object's life consists of various stages. Each stage represents the operations that occur with the object.

The life of an object includes the operations of ingest, copy management, retrieve, and delete.

- **Ingest:** The process of an S3 or Swift client application saving an object over HTTP to the StorageGRID system. At this stage, the StorageGRID system begins to manage the object.
- **Copy management:** The process of managing replicated and erasure-coded copies in StorageGRID, as described by the ILM rules in the active ILM policy. During the copy management stage, StorageGRID protects object data from loss by creating and maintaining the specified number and type of object copies on Storage Nodes, in a Cloud Storage Pool, or on Archive Node.
- **Retrieve:** The process of a client application accessing an object stored by the StorageGRID system. The client reads the object, which is retrieved from a Storage Node, Cloud Storage Pool, or Archive Node.

- **Delete:** The process of removing all object copies from the grid. Objects can be deleted either as a result of the client application sending a delete request to the StorageGRID system, or as a result of an automatic process that StorageGRID performs when the object's lifetime expires.



Related information

- [Manage objects with ILM](#)
- [Use information lifecycle management](#)

Ingest data flow

An ingest, or save, operation consists of a defined data flow between the client and the StorageGRID system.

Data flow

When a client ingests an object to the StorageGRID system, the LDR service on Storage Nodes processes the request and stores the metadata and data to disk.



1. The client application creates the object and sends it to the StorageGRID system through an HTTP PUT request.
2. The object is evaluated against the system's ILM policy.
3. The LDR service saves the object data as a replicated copy or as an erasure coded copy. (The diagram shows a simplified version of storing a replicated copy to disk.)
4. The LDR service sends the object metadata to the metadata store.
5. The metadata store saves the object metadata to disk.
6. The metadata store propagates copies of object metadata to other Storage Nodes. These copies are also saved to disk.
7. The LDR service returns an HTTP 200 OK response to the client to acknowledge that the object has been ingested.

Copy management

Object data is managed by the active ILM policy and its ILM rules. ILM rules make replicated or erasure coded copies to protect object data from loss.

Different types or locations of object copies might be required at different times in the object's life. ILM rules are periodically evaluated to ensure that objects are placed as required.

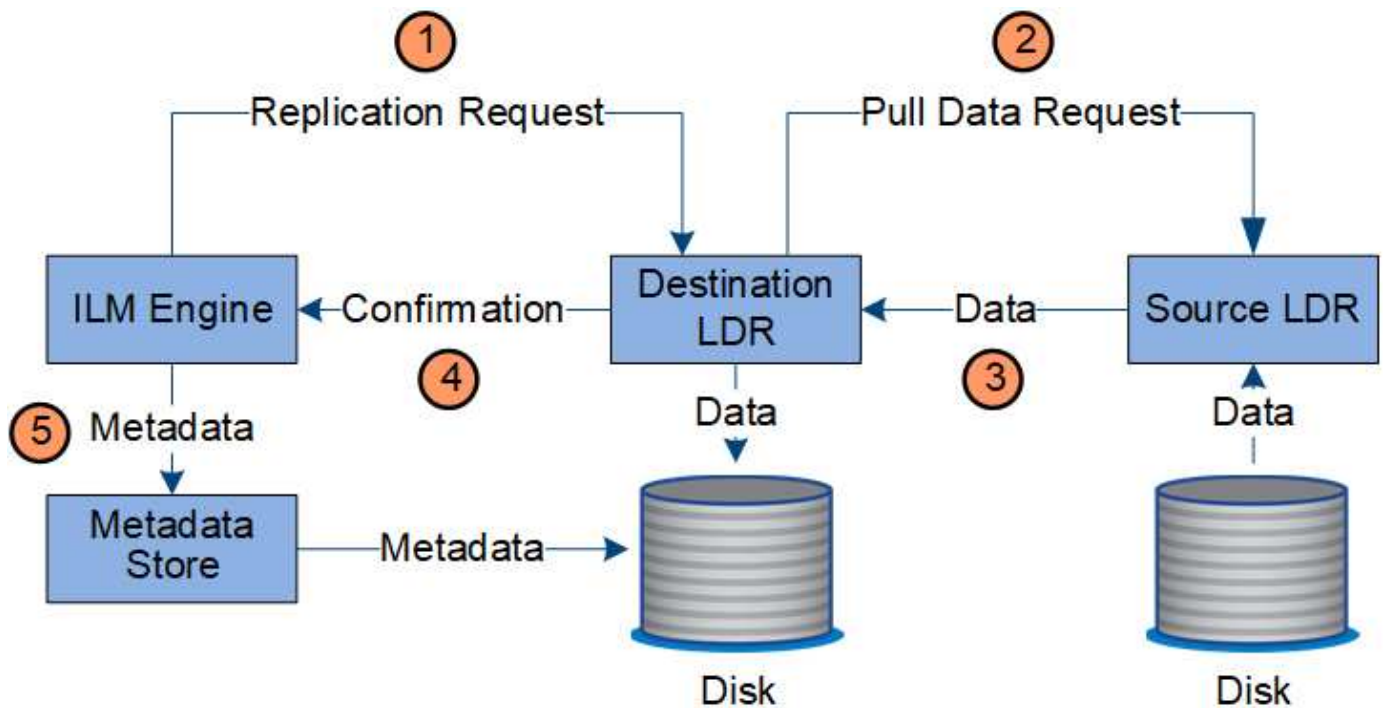
Object data is managed by the LDR service.

Content protection: replication

If an ILM rule's content placement instructions require replicated copies of object data, copies are made and stored to disk by the Storage Nodes that make up the configured storage pool.

Data flow

The ILM engine in the LDR service controls replication and ensures that the correct number of copies are stored in the correct locations and for the correct amount of time.



1. The ILM engine queries the ADC service to determine the best destination LDR service within the storage pool specified by the ILM rule. It then sends that LDR service a command to initiate replication.
2. The destination LDR service queries the ADC service for the best source location. It then sends a replication request to the source LDR service.
3. The source LDR service sends a copy to the destination LDR service.
4. The destination LDR service notifies the ILM engine that the object data has been stored.
5. The ILM engine updates the metadata store with object location metadata.

Content protection: erasure coding

If an ILM rule includes instructions to make erasure coded copies of object data, the applicable erasure coding scheme breaks object data into data and parity fragments and distributes these fragments across the Storage Nodes configured in the Erasure Coding profile.

Data flow

The ILM engine, which is a component of the LDR service, controls erasure coding and ensures that the Erasure Coding profile is applied to object data.



1. The ILM engine queries the ADC service to determine which DDS service can best perform the erasure coding operation. Once determined, the ILM engine sends an "initiate" request to that service.
2. The DDS service instructs an LDR to erasure code the object data.
3. The source LDR service sends a copy to the LDR service selected for erasure coding.
4. Once broken into the appropriate number of parity and data fragments, the LDR service distributes these fragments across the Storage Nodes (Chunk services) that make up the Erasure Coding profile's storage pool.
5. The LDR service notifies the ILM engine, confirming that object data is successfully distributed.
6. The ILM engine updates the metadata store with object location metadata.

Content protection: Cloud Storage Pool

If an ILM rule's content placement instructions require that a replicated copy of object data is stored on a Cloud Storage Pool, object data is duplicated to the external S3 bucket or Azure Blob storage container that was specified for the Cloud Storage Pool.

Data flow

The ILM engine, which is a component of the LDR service, and the Data Mover service control the movement of objects to the Cloud Storage Pool.



1. The ILM engine selects a Data Mover service to replicate to the Cloud Storage Pool.
2. The Data Mover service sends the object data to the Cloud Storage Pool.
3. The Data Mover service notifies the ILM engine that the object data has been stored.
4. The ILM engine updates the metadata store with object location metadata.

Content protection: archive

An archive operation consists of a defined data flow between the StorageGRID system and the client.

If the ILM policy requires that a copy of object data be archived, the ILM engine, which is a component of the LDR service, sends a request to the Archive Node, which in turn sends a copy of the object data to the targeted archival storage system.



1. The ILM engine sends a request to the ARC service to store a copy on archive media.
2. The ARC service queries the ADC service for the best source location and sends a request to the source LDR service.
3. The ARC service retrieves object data from the LDR service.
4. The ARC service sends the object data to the archive media destination.
5. The archive media notifies the ARC service that the object data has been stored.
6. The ARC service notifies the ILM engine that the object data has been stored.

Retrieve data flow

A retrieve operation consists of a defined data flow between the StorageGRID system and the client. The system uses attributes to track the retrieval of the object from a Storage Node or, if necessary, a Cloud Storage Pool or Archive Node.

The Storage Node's LDR service queries the metadata store for the location of the object data and retrieves it from the source LDR service. Preferentially, retrieval is from a Storage Node. If the object is not available on a Storage Node, the retrieval request is directed to a Cloud Storage Pool or to an Archive Node.



If the only object copy is on AWS Glacier storage or the Azure Archive tier, the client application must issue an S3 POST Object restore request to restore a retrievable copy to the Cloud Storage Pool.



1. The LDR service receives a retrieval request from the client application.
2. The LDR service queries the metadata store for the object data location and metadata.
3. LDR service forwards the retrieval request to the source LDR service.
4. The source LDR service returns the object data from the queried LDR service and the system returns the object to the client application.

Delete data flow

All object copies are removed from the StorageGRID system when a client performs a delete operation or when the object's lifetime expires, triggering its automatic removal. There is a defined data flow for object deletion.

Deletion hierarchy

StorageGRID provides several methods for controlling when objects are retained or deleted. Objects can be deleted by client request or automatically. StorageGRID always prioritizes any S3 Object Lock settings over client delete requests, which are prioritized over S3 bucket lifecycle and ILM placement instructions.

- **S3 Object Lock:** If the global S3 Object Lock setting is enabled for the grid, S3 clients can create buckets with S3 Object Lock enabled and then use the S3 REST API to specify retain-until-date and legal hold settings for each object version added to that bucket.
 - An object version that is under a legal hold cannot be deleted by any method.
 - Before an object version's retain-until-date is reached, that version cannot be deleted by any method.
 - Objects in buckets with S3 Object Lock enabled are retained by ILM "forever". However, after its retain-until-date is reached, an object version can be deleted by a client request or the expiration of the bucket lifecycle.
 - If S3 clients apply a default retain-until-date to the bucket, they do not need to specify a retain-until-

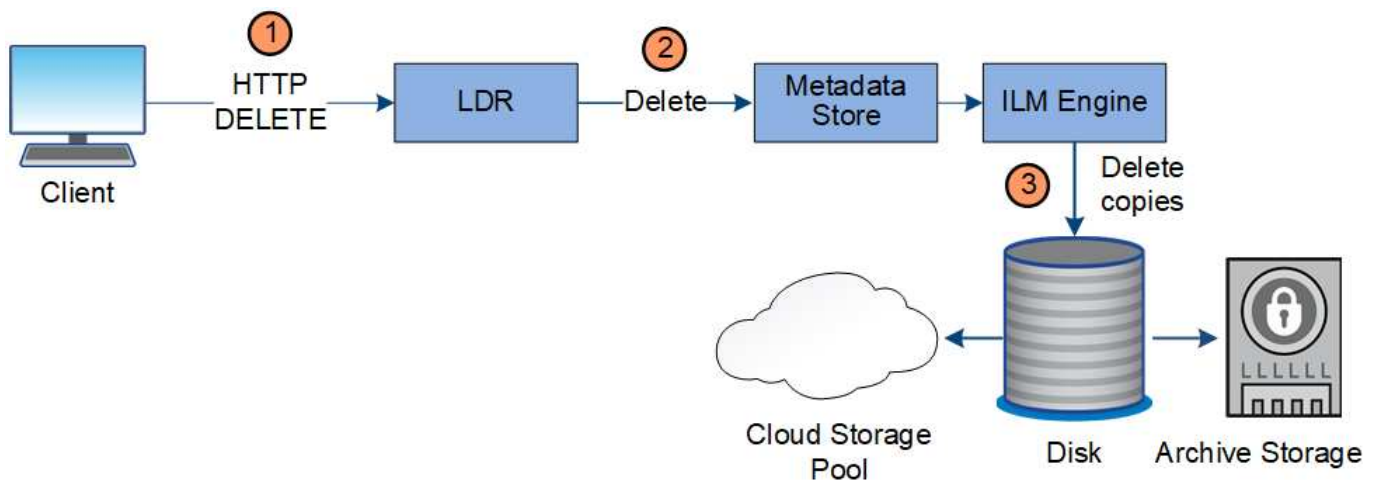
date for each object.

- **Client delete request:** An S3 or Swift client can issue a delete object request. When a client deletes an object, all copies of the object are removed from the StorageGRID system.
- **S3 bucket lifecycle:** S3 clients can add a lifecycle configuration to their buckets that specifies an Expiration action. If a bucket lifecycle exists, StorageGRID automatically deletes all copies of an object when the date or number of days specified in the Expiration action are met, unless the client deletes the object first.
- **ILM placement instructions:** Assuming that the bucket does not have S3 Object Lock enabled and that there is no bucket lifecycle, StorageGRID automatically deletes an object when the last time period in the ILM rule ends and there are no further placements specified for the object.



The Expiration action in an S3 bucket lifecycle always overrides ILM settings. As a result, an object might be retained on the grid even after any ILM instructions for placing the object have lapsed.

Data flow for client deletes



1. The LDR service receives a delete request from the client application.
2. The LDR service updates the metadata store so the object looks deleted to client requests, and instructs the ILM engine to remove all copies of object data.
3. The object is removed from the system. The metadata store is updated to remove object metadata.

Data flow for ILM deletes



1. The ILM engine determines that the object needs to be deleted.
2. The ILM engine notifies the metadata store. The metadata store updates object metadata so that the object looks deleted to client requests.
3. The ILM engine removes all copies of the object. The metadata store is updated to remove object metadata.

How to use StorageGRID

Explore the Grid Manager

The Grid Manager is the browser-based graphical interface that allows you to configure, manage, and monitor your StorageGRID system.

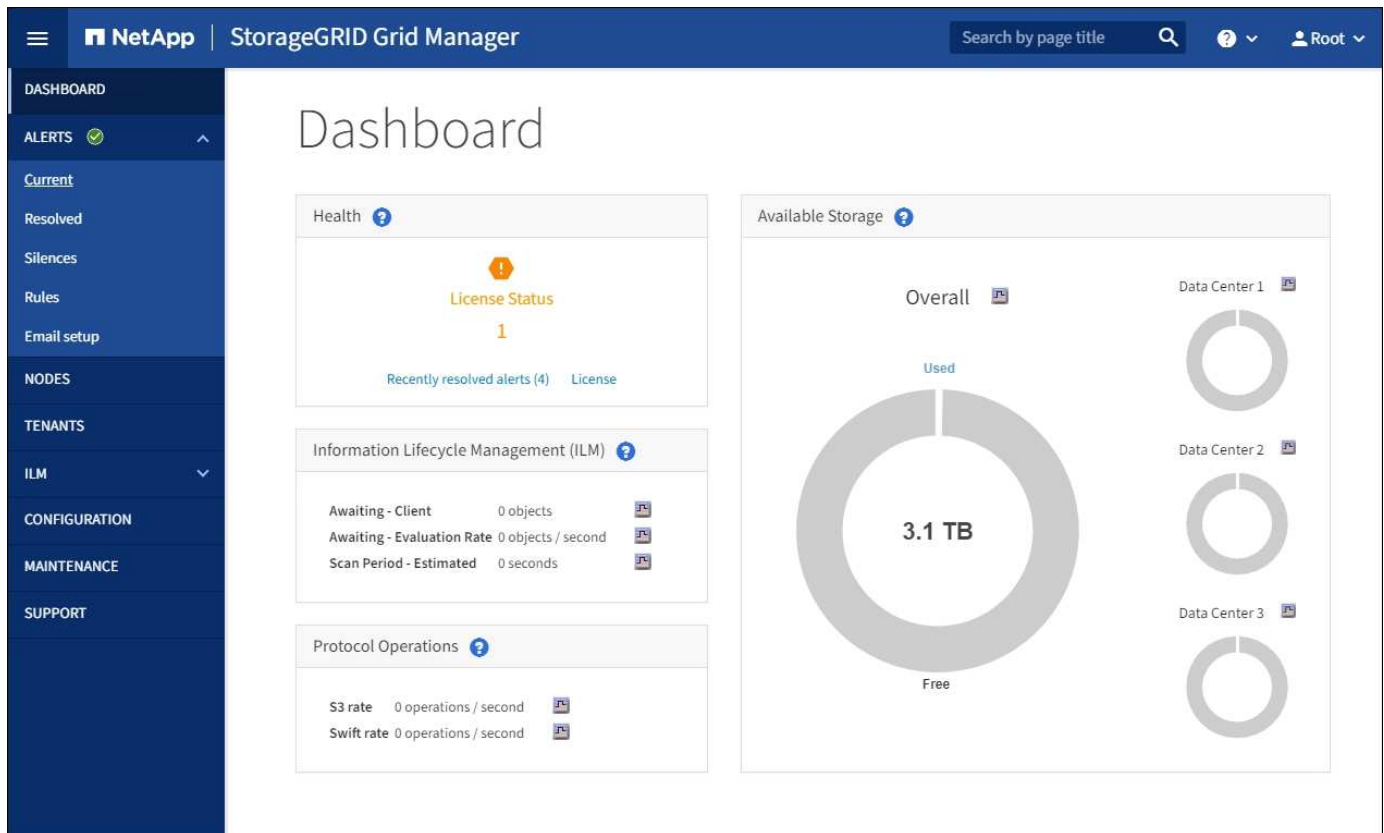
When you sign in to the Grid Manager, you are connecting to an Admin Node. Each StorageGRID system includes one primary Admin Node and any number of non-primary Admin Nodes. You can connect to any Admin Node, and each Admin Node displays a similar view of the StorageGRID system.

You can access the Grid Manager using a [supported web browser](#).

Grid Manager Dashboard

When you first sign in to the Grid Manager, you can use the Dashboard to monitor system activities at a glance.

The Dashboard includes summary information about system health, storage use, ILM processes, and S3 and Swift operations.



For an explanation of the information on each panel, click the help icon (?) for that panel.

Learn more

- [Monitor and troubleshoot](#)

Search field

The **Search** field in the header bar allows you to quickly navigate to a specific page within Grid Manager. For example, you can enter **km** to access the Key Management Server (KMS) page. You can use **Search** to find entries in the sidebar of the Grid Manager and on the Configuration, Maintenance, and Support menus.

Alerts menu

The Alerts menu provides an easy-to-use interface for detecting, evaluating, and resolving issues that might occur during StorageGRID operation.



From the Alerts menu, you can do the following:

- Review current alerts
- Review resolved alerts
- Configure silences to suppress alert notifications
- Define alert rules for conditions that trigger alerts
- Configure the email server for alert notifications

Learn more

- [Monitor and manage alerts](#)
- [Monitor and troubleshoot](#)

Nodes page

The Nodes page displays information about the entire grid, each site in the grid, and each node at a site.

The Nodes home page displays combined metrics for the entire grid. To view information for a particular site or node, select the site or node.

Learn more

- [Manage tenants and client connections](#)
- [Administer StorageGRID](#)
- [Use a tenant account](#)

ILM menu

The ILM menu allows you to configure the information lifecycle management (ILM) rules and policies that govern data durability and availability. You can also enter an object identifier to view the metadata for that object.



Learn more

- [Use information lifecycle management](#)
- [Manage objects with ILM](#)

Configuration menu

The Configuration menu allows you to specify network settings, security settings, system settings, monitoring options, and access control options.

Configuration

Configure your StorageGRID system.

| Network | Security | System | Monitoring | Access control |
|--|---|---------------------------------|---|-------------------------------------|
| Domain names | Certificates | Display options | Audit and syslog server | Admin groups |
| High availability groups | Key management server | Grid options | SNMP agent | Admin users |
| Link cost | Proxy settings | S3 Object Lock | | Grid passwords |
| Load balancer endpoints | Untrusted Client Networks | Storage options | | Identity federation |
| Traffic classification | | | | Single sign-on |
| VLAN interfaces | | | | |

Learn more

- [Configure network settings](#)
- [Manage tenants and client connections](#)
- [Review audit messages](#)
- [Control StorageGRID access](#)
- [Administer StorageGRID](#)
- [Monitor and troubleshoot](#)
- [Review audit logs](#)

Maintenance menu

The Maintenance menu allows you to perform maintenance tasks, system maintenance, and network maintenance.

Maintenance

Perform maintenance procedures on your StorageGRID system.

| Tasks | System | Network |
|--|----------------------------------|------------------------------|
| Decommission | License | DNS servers |
| Expansion | Recovery package | Grid Network |
| Recovery | Software update | NTP servers |
| Object existence check | | |

Tasks

Maintenance tasks include:

- Decommission operations to remove unused grid nodes and sites.
- Expansion operations to add new grid nodes and sites.
- Recovery operations to replace a failed node and restore data.
- Object existence check to verify the existence (although not the correctness) of object data.

System

System maintenance tasks you can perform include:

- Reviewing details for the current StorageGRID license or uploading a new license.
- Generating a Recovery Package.
- Performing StorageGRID software updates, including software upgrades, hotfixes, and updates to the SANtricity OS software on selected appliances.

Network

Network maintenance tasks you can perform include:

- Editing information about DNS servers.
- Configuring the subnets that are used on the Grid Network.
- Editing information about NTP servers.

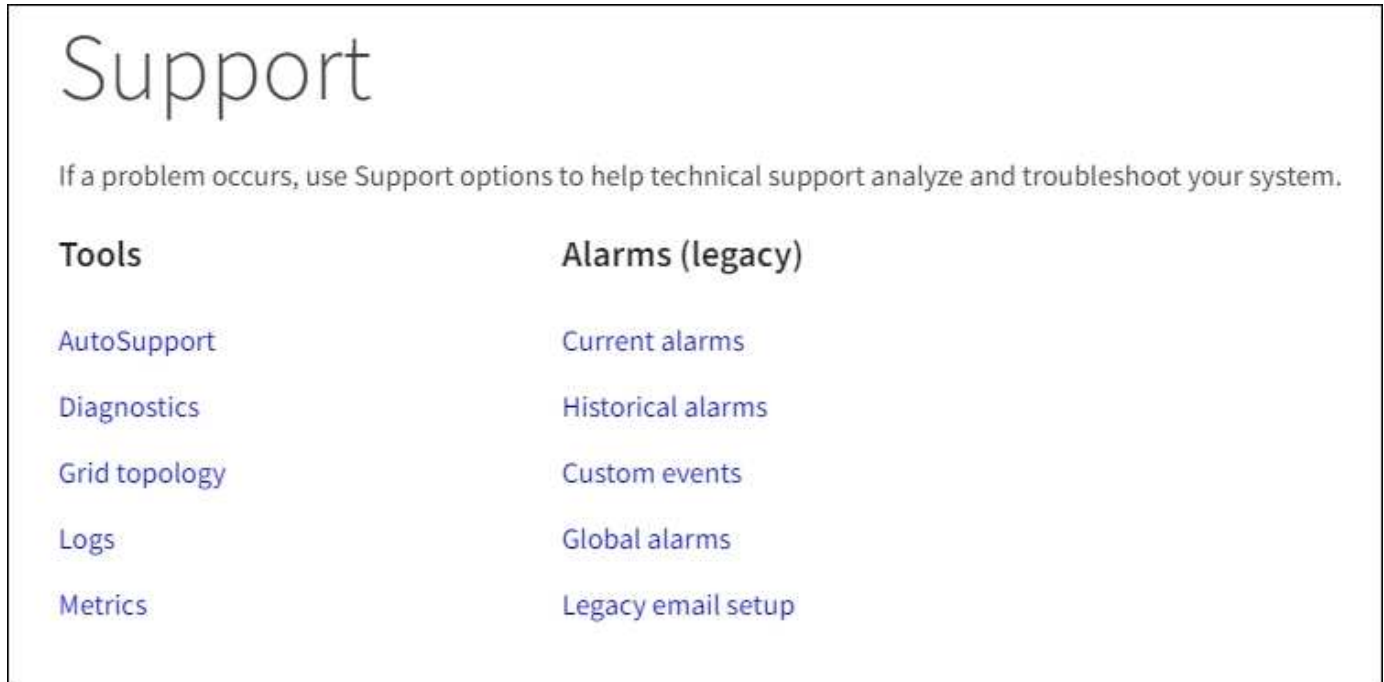
Learn more

- [Perform maintenance](#)
- [Download the Recovery Package](#)
- [Expand your grid](#)

- [Upgrade software](#)
- [Recover and maintain](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

Support menu

The Support menu provides options that help technical support analyze and troubleshoot your system. There are two parts to the Support menu: Tools and Alarms (legacy).



Tools

From the Tools section of the Support menu, you can:

- Enable AutoSupport.
- Perform a set of diagnostic checks on the current state of the grid.
- Access the grid topology tree to view detailed information about grid nodes, services, and attributes.
- Retrieve log files and system data.
- Review detailed metrics and charts.



The tools available from the **Metrics** option are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Alarms (legacy)

From the Alarms (legacy) section of the Support menu, you can review current, historical, and global alarms, set up custom events, and set up email notifications for legacy alarms and AutoSupport.



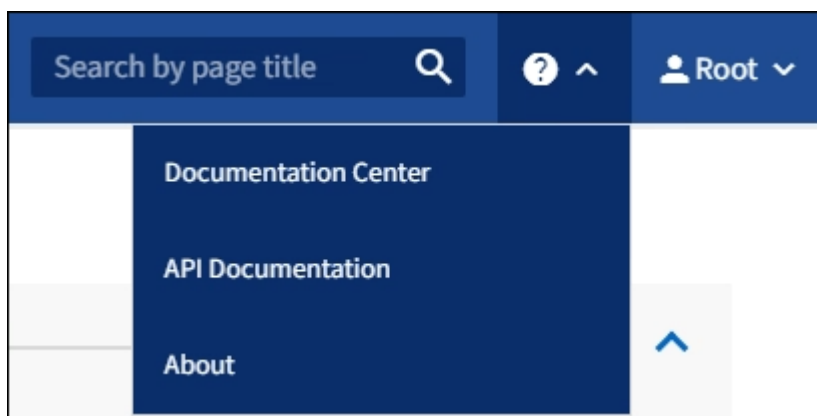
While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

Learn more

- [StorageGRID architecture and network topology](#)
- [StorageGRID attributes](#)
- [Use StorageGRID support options](#)
- [Administer StorageGRID](#)
- [Monitor and troubleshoot](#)

Help menu

The Help option provides access to the StorageGRID Documentation Center for the current release and to the API documentation. You can also determine which version of StorageGRID is currently installed.



Learn more

- [Administer StorageGRID](#)

Explore the Tenant Manager

The Tenant Manager is the browser-based graphical interface that tenant users access to configure, manage, and monitor their storage accounts.

When tenant users sign in to the Tenant Manager, they are connecting to an Admin Node.

Tenant Manager Dashboard

After a grid administrator creates a tenant account using the Grid Manager or the Grid Management API, tenant users can sign in to the Tenant Manager.

The Tenant Manager Dashboard allows tenant users to monitor storage usage at a glance. The Storage usage panel contains a list of the largest buckets (S3) or containers (Swift) for the tenant. The Space used value is the total amount of object data in the bucket or container. The bar chart represents the relative sizes of these buckets or containers.

The value shown above the bar chart is a sum of the space used for all of the tenant's buckets or containers. If the maximum number of gigabytes, terabytes, or petabytes available for the tenant was specified when the account was created, the amount of quota used and remaining are also shown.

Dashboard

16

Buckets

[View buckets](#)

2

Platform services endpoints

[View endpoints](#)

0

Groups

[View groups](#)

1

User

[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



| Bucket name | Space used | Number of objects |
|-----------------|------------|-------------------|
| Bucket-15 | 969.2 GB | 913,425 |
| Bucket-04 | 937.2 GB | 576,806 |
| Bucket-13 | 815.2 GB | 957,389 |
| Bucket-06 | 812.5 GB | 193,843 |
| Bucket-10 | 473.9 GB | 583,245 |
| Bucket-03 | 403.2 GB | 981,226 |
| Bucket-07 | 362.5 GB | 420,726 |
| Bucket-05 | 294.4 GB | 785,190 |
| 8 other buckets | 1.4 TB | 3,007,036 |

Total objects

8,418,886
objects

Tenant details [?](#)

Name: Tenant02

ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Storage menu (S3 tenants only)

The Storage menu is provided for S3 tenant accounts only. This menu allows S3 users to manage access keys, create and delete buckets, and manage platform service endpoints.



My access keys

S3 tenant users can manage access keys as follows:

- Users who have the Manage Your Own S3 Credentials permission can create or remove their own S3 access keys.
- Users who have the Root Access permission can manage the access keys for the S3 root account, their own account, and all other users. Root access keys also provide full access to the tenant's buckets and

objects unless explicitly disabled by a bucket policy.



Managing the access keys for other users takes place from the Access Management menu.

Buckets

S3 tenant users with the appropriate permissions can perform the following tasks related to buckets:

- Create buckets
- Enable S3 Object Lock for a new bucket (assumes that S3 Object Lock is enabled for the StorageGRID system)
- Update consistency level settings
- Apply a default retention setting
- Configure cross-origin resource sharing (CORS)
- Enable and disable last access time update settings for the buckets belonging to the tenant
- Delete empty buckets
- Manage the objects in a bucket using the [experimental S3 Console](#)

If a grid administrator has enabled the use of platform services for the tenant account, an S3 tenant user with the appropriate permissions can also perform these tasks:

- Configure S3 event notifications, which can be sent to a destination service that supports the AWS Simple Notification Service™ (SNS).
- Configure CloudMirror replication, which enables the tenant to automatically replicate objects to an external S3 bucket.
- Configure search integration, which sends object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

Platform services endpoints

If a grid administrator has enabled the use of platform services for the tenant account, an S3 tenant user with the Manage Endpoints permission can configure a destination endpoint for each platform service.

Access Management menu

The Access Management menu allows StorageGRID tenants to import user groups from a federated identity source and assign management permissions. Tenants can also manage local tenant groups and users, unless single sign-on (SSO) is in effect for the entire StorageGRID system.



Related information

- [Explore the Grid Manager](#)
- [Use a tenant account](#)

Control StorageGRID access

You control who can access StorageGRID and which tasks users can perform by creating or importing groups and users and assigning permissions to each group. Optionally, you can enable single sign-on (SSO), create client certificates, and change grid passwords.

Control access to the Grid Manager

You determine who can access the Grid Manager and the Grid Management API by importing groups and users from an identity federation service or by setting up local groups and local users.

Using identity federation makes setting up groups and users faster, and it allows users to sign in to StorageGRID using familiar credentials. You can configure identity federation if you use Active Directory, OpenLDAP, or Oracle Directory Server.



Contact technical support if you want to use another LDAP v3 service.

You determine which tasks each user can perform by assigning different permissions to each group. For example, you might want users in one group to be able to manage ILM rules and users in another group to perform maintenance tasks. A user must belong to at least one group to access the system.

Optionally, you can configure a group to be read-only. Users in a read-only group can only view settings and features. They cannot make any changes or perform any operations in the Grid Manager or Grid Management API.

Enable single sign-on

The StorageGRID system supports single sign-on (SSO) using the Security Assertion Markup Language 2.0 (SAML 2.0) standard. When SSO is enabled, all users must be authenticated by an external identity provider before they can access the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API. Local users cannot sign in to StorageGRID.

When SSO is enabled and users sign in to StorageGRID, they are redirected to your organization's SSO page to validate their credentials. When users sign out of one Admin Node, they are automatically signed out of all

Admin Nodes.

Change grid passwords

The provisioning passphrase is required for many installation and maintenance procedures, and for downloading the StorageGRID Recovery Package. The passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. You can change this passphrase as required.

Related information

- [Administer StorageGRID](#)
- [Use a tenant account](#)

Manage tenants and client connections

As a grid administrator, you create and manage the tenant accounts that S3 and Swift clients use to store and retrieve objects, and manage the configuration options that control how clients connect to your StorageGRID system.

Tenant accounts

A tenant account allows you to specify who can use your StorageGRID system to store and retrieve objects, and which functionality is available to them. Tenant accounts allow client applications that support the S3 REST API or the Swift REST API to store and retrieve objects on StorageGRID. Each tenant account uses either the S3 client protocol or the Swift client protocol.

You must create at least one tenant account for each client protocol that will be used to store objects on your StorageGRID system. Optionally, you can create additional tenant accounts if you want to segregate the objects stored on your system by different entities. Each tenant account has its own federated or local groups and users, and its own buckets (containers for Swift) and objects.

You can use the Grid Manager or the Grid Management API to create tenant accounts. When creating a tenant account, you specify the following information:

- Display name for the tenant (the tenant's account ID is assigned automatically and cannot be changed).
- Whether the tenant account will use the S3 or Swift.
- For S3 tenant accounts: Whether the tenant account is allowed to use platform services. If the use of platform services is allowed, the grid must be configured to support their use.
- Optionally, a storage quota for the tenant account—the maximum number of gigabytes, terabytes, or petabytes available for the tenant's objects. A tenant's storage quota represents a logical amount (object size), not a physical amount (size on disk).
- If identity federation is enabled for the StorageGRID system, which federated group has Root Access permission to configure the tenant account.
- If single sign-on (SSO) is not in use for the StorageGRID system, whether the tenant account will use its own identity source or share the grid's identity source, and the initial password for the tenant's local root user.

If S3 tenant accounts need to comply with regulatory requirements, grid administrators can enable the global S3 Object Lock setting for the StorageGRID system. When S3 Object Lock is enabled for the system, all S3 tenant accounts can create buckets with S3 Object Lock enabled and then specify retention and legal hold settings for the object versions in that bucket.

After a tenant account is created, tenant users can sign in to the Tenant Manager.

Client connections to StorageGRID nodes

Before tenant users can use S3 or Swift clients to store and retrieve data in StorageGRID, you must decide how these clients will connect to StorageGRID nodes.

Client applications can store or retrieve objects by connecting to any of the following:

- The Load Balancer service on Admin Nodes or Gateway Nodes. This is the recommended connection.
- The CLB service on Gateway Nodes.



The CLB service is deprecated.

- Storage Nodes, with or without an external load balancer.

When configuring StorageGRID so that clients can use the Load Balancer service, you perform the following steps:

1. Optionally configure high availability (HA) groups. If you create an HA group, the interfaces of multiple Admin Nodes and Gateway Nodes are placed into an active-backup configuration. Client connections are made using the virtual IP address of the HA group.
2. Configure endpoints for the Load Balancer service. The Load Balancer service on Admin Nodes or Gateway Nodes distributes incoming network connections from client applications to Storage Nodes. When creating a load balancer endpoint, you specify a port number, whether the endpoint accepts HTTP or HTTPS connections, the type of client (S3 or Swift) that will use the endpoint, and the certificate to be used for HTTPS connections (if applicable).
3. Optionally specify that a node's Client Network is untrusted to ensure that all connections to the node's Client Network occur on the load balancer endpoints.

Related information

- [Administer StorageGRID](#)
- [Use a tenant account](#)
- [Use S3](#)
- [Use Swift](#)
- [Explore the Tenant Manager](#)
- [Configure network settings](#)

Configure network settings

You can configure various network settings from the Grid Manager to fine tune the operation of your StorageGRID system.

Domain names

If you plan to support S3 virtual hosted-style requests, you must configure the list of endpoint domain names that S3 clients connect to. Examples include `s3.example.com`, `s3.example.co.uk`, and `s3-east.example.com`.

The configured server certificates must match the endpoint domain names.

High availability groups

You can use high availability (HA) groups to provide highly available data connections for S3 and Swift clients or to provide highly available connections to the Grid Manager and the Tenant Manager.

When you create an HA group, you select a network interface for one or more nodes. Each HA group provides access to the shared services on the selected nodes.

- HA groups that include interfaces on Gateway Nodes, Admin Nodes, or both provide highly available data connections for S3 and Swift clients.
- HA groups that include interfaces on Admin Nodes only provide highly available connections to the Grid Manager and the Tenant Manager.

The interfaces can belong to the Grid Network (eth0), the Client Network (eth2), or a VLAN network.

You can assign up to 10 virtual IP (VIP) addresses to each HA group. You specify one interface to be the Primary interface and rank any other interfaces in priority order. The Primary interface is the active interface unless a failure occurs. If the active interface fails, the VIP addresses move to the first backup interface in the priority order. If that interface fails, the VIP addresses move to the next backup interface, and so on.

Link costs

You can adjust link costs to reflect the latency between sites. When two or more data center sites exist, link costs prioritize which data center site should provide a requested service.

Load balancer endpoints

You can use a load balancer to handle ingest and retrieval workloads from S3 and Swift clients. Load balancing maximizes speed and connection capacity by distributing the workloads and connections across multiple Storage Nodes.

If you want to use the StorageGRID load balancer service, which is included on Admin Nodes and Gateway Nodes, you must configure one or more load balancer endpoints. Each endpoint defines a Gateway Node or Admin Node port for S3 and Swift requests to Storage Nodes.

Traffic classification

You can create traffic classification policies to identify and handle different types of network traffic, including traffic related to specific buckets, tenants, client subnets, or load balancer endpoints. These policies can assist with traffic limiting and monitoring.

VLAN interfaces

You can create virtual LAN (VLAN) interfaces to isolate and partition traffic for security, flexibility, and performance. Each VLAN interface is associated with one or more parent interfaces on Admin Nodes and Gateway Nodes. You can use VLAN interfaces in HA groups and in load balancer endpoints to segregate client or admin traffic by application or tenant.

For example, your network might use VLAN 100 for FabricPool traffic and VLAN 200 for an archive application.

Related information

- [Administer StorageGRID](#)
- [Manage tenants and client connections](#)

Configure security settings

You can configure various security settings from the Grid Manager to help secure your StorageGRID system.

Certificates

StorageGRID uses two types of security certificates:

- Server certificates are required when you use HTTPS connections. Server certificates are used to establish secure connections between clients and servers, authenticating the identity of a server to its clients and providing a secure communication path for data. The server and the client each have a copy of the certificate.
- Client certificates authenticate a client or user identity to the server, providing more secure authentication than passwords alone. Client certificates do not encrypt data.

You can view all StorageGRID certificates on the **CONFIGURATION > Security > Certificates** page.

Key management servers

You can configure one or more external key management servers (KMS) to provide encryption keys to StorageGRID services and storage appliances. Each KMS or KMS cluster uses the Key Management Interoperability Protocol (KMIP) to provide an encryption key to the appliance nodes at the associated StorageGRID site. Using key management servers lets you protect StorageGRID data even if an appliance is removed from the data center. After the appliance volumes are encrypted, you cannot access any data on the appliance unless the node can communicate with the KMS.



To use encryption key management, you must enable the **Node Encryption** setting for each appliance during installation, before the appliance is added to the grid.

Proxy settings

If you are using S3 platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints. If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

| Proxy Settings |
|----------------|
| Storage |
| Admin |

Untrusted Client Networks

If you are using a Client Network, you can help secure StorageGRID from hostile attacks by specifying that the Client Network on each node be untrusted. If a node's Client Network is untrusted, the node only accepts inbound connections on ports explicitly configured as load balancer endpoints.

For example, you might want a Gateway Node to refuse all inbound traffic on the Client Network except for HTTPS S3 requests. Or, you might want to enable outbound S3 platform service traffic from a Storage Node, while preventing any inbound connections to that Storage Node on the Client Network.

Related information

- [Administer StorageGRID](#)
- [Manage tenants and client connections](#)

Configure system settings

You can configure various system settings from the Grid Manager to fine tune the operation of your StorageGRID system.

Display options

Display options allow you to specify the timeout period for user sessions and to suppress email notifications for legacy alarms and event-triggered AutoSupport messages.

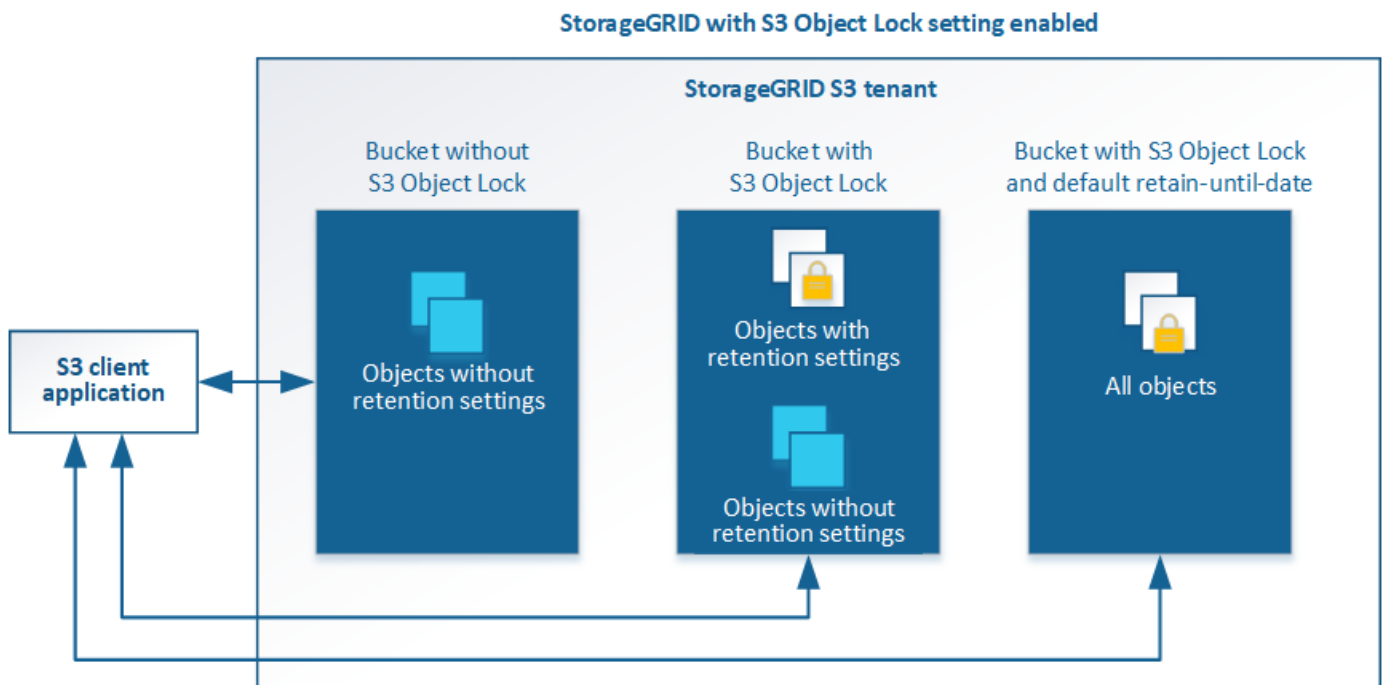
Grid options

You can use Grid Options to configure the settings for all of the objects stored in your StorageGRID system, including stored object compression, stored object encryption, and stored object hashing.

You can also use these options to specify global settings for S3 and Swift client operations.

S3 Object Lock

The StorageGRID S3 Object Lock feature is an object-protection solution that is equivalent to S3 Object Lock in Amazon Simple Storage Service (Amazon S3). You can enable the global S3 Object Lock setting for a StorageGRID system to allow S3 tenant accounts to create buckets with S3 Object Lock enabled. The tenant can then use an S3 client application to optionally specify retention settings (retain until date, legal hold, or both) for the objects in those buckets. In addition, each bucket that has S3 Object Lock enabled can optionally have a default retention mode and retention period, which apply if objects are added to the bucket without their own retention settings.



Storage options

Storage options allow you to control object segmentation and to override storage volume watermark settings to manage a Storage Node's usable storage space.

Use information lifecycle management

You use information lifecycle management (ILM) to control the placement, duration, and data protection for all objects in your StorageGRID system. ILM rules determine how StorageGRID stores objects over time. You configure one or more ILM rules and then add them to an ILM policy.

ILM rules define:

- Which objects should be stored. A rule can apply to all objects, or you can specify filters to identify which objects a rule applies to. For example, a rule can apply only to objects associated with certain tenant accounts, specific S3 buckets or Swift containers, or specific metadata values.
- The storage type and location. Objects can be stored on Storage Nodes, in Cloud Storage Pools, or on Archive Nodes.
- The type of object copies made. Copies can be replicated or erasure coded.
- For replicated copies, the number of copies made.
- For erasure coded copies, the erasure-coding scheme used.
- The changes over time to an object's storage location and type of copies.
- How object data is protected as objects are ingested into the grid (synchronous placement or dual commit).

Note that object metadata is not managed by ILM rules. Instead, object metadata is stored in a Cassandra database in what is known as a metadata store. Three copies of object metadata are automatically maintained at each site to protect the data from loss. The copies are evenly distributed across all Storage Nodes.

Example ILM rule

This example ILM rule applies to the objects belonging to Tenant A. It makes two replicated copies of those objects and stores each copy at a different site. The two copies are retained "forever," which means that StorageGRID will not automatically delete them. Instead, StorageGRID will retain these objects until they are deleted by a client delete request or by the expiration of a bucket lifecycle.

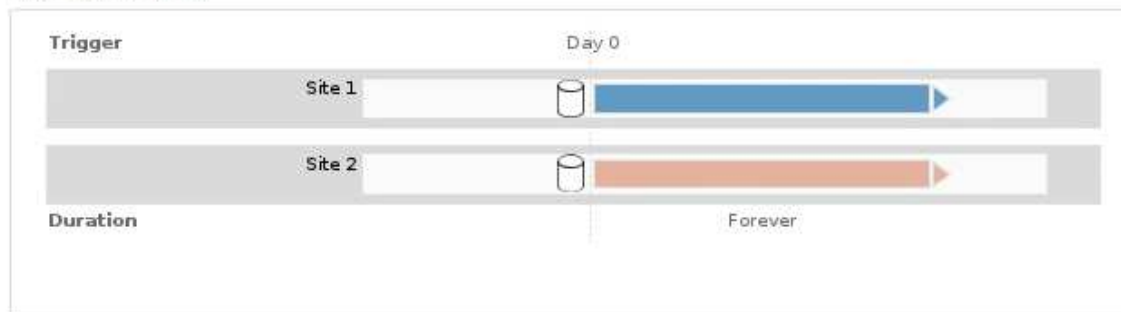
This rule uses the Balanced option for ingest behavior: the two-site placement instruction is applied as soon as Tenant A saves an object to StorageGRID, unless it is not possible to immediately make both required copies. For example, if Site 2 is unreachable when Tenant A saves an object, StorageGRID will make two interim copies on Storage Nodes at Site 1. As soon as Site 2 becomes available, StorageGRID will make the required copy at that site.

Two copies at two sites for Tenant A

Description: Applies only to Tenant A
Ingest Behavior: Balanced
Tenant Accounts: Tenant A (34176783492629515782)
Reference Time: Ingest Time
Filtering Criteria:

Matches all objects.

Retention Diagram:



How an ILM policy evaluates objects

The active ILM policy for your StorageGRID system controls the placement, duration, and data protection of all objects.

When clients save objects to StorageGRID, the objects are evaluated against the ordered set of ILM rules in the active policy, as follows:

1. If the filters for the first rule in the policy match an object, the object is ingested according to that rule's ingest behavior and stored according to that rule's placement instructions.
2. If the filters for the first rule do not match the object, the object is evaluated against each subsequent rule in the policy until a match is made.
3. If no rules match an object, the ingest behavior and placement instructions for the default rule in the policy are applied. The default rule is the last rule in a policy and cannot use any filters. It must apply to all tenants, all buckets, and all object versions.

Example ILM policy

This example ILM policy uses three ILM rules.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name Example ILM policy

Reason for change New policy

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

| | Default | Rule Name | Tenant Account | Actions |
|---|---------|--|---------------------------------|---------|
| + | | Rule 1: 3 replicated copies for Tenant A | Tenant A (58889986524346589742) | ✕ |
| + | | Rule 2: Erasure coding for objects greater than 1 MB | — | ✕ |
| | ✓ | Rule 3: 2 copies 2 data centers (default) | — | ✕ |

Cancel

Save

In this example, Rule 1 matches all objects belonging to Tenant A. These objects are stored as three replicated copies at three sites. Objects belonging to other tenants are not matched by Rule 1, so they are evaluated against Rule 2.

Rule 2 matches all objects from other tenants but only if they are greater than 1 MB. These larger objects are stored using 6+3 erasure coding at three sites. Rule 2 does not match objects 1 MB or smaller, so these objects are evaluated against Rule 3.

Rule 3 is the last and default rule in the policy, and it does not use filters. Rule 3 makes two replicated copies of all objects not matched by Rule 1 or Rule 2 (objects not belonging to Tenant A that are 1 MB or smaller).



Related information

- [Manage objects with ILM](#)

Monitor operations


View the [Nodes](#) page

When you need more detailed information about your StorageGRID system than the Dashboard provides, you can use the Nodes page to view metrics for the entire grid, each site in the grid, and each node at a site.

| Name | Type | Object data used | Object metadata used | CPU usage |
|---------------------------------|--------------------|------------------|----------------------|-----------|
| StorageGRID Webscale Deployment | Grid | 0% | 0% | — |
| DC1 | Site | 0% | 0% | — |
| DC1-ADM1 | Primary Admin Node | — | — | 6% |
| DC1-ARC1 | Archive Node | — | — | 1% |
| DC1-G1 | Gateway Node | — | — | 3% |
| DC1-S1 | Storage Node | 0% | 0% | 6% |
| DC1-S2 | Storage Node | 0% | 0% | 8% |
| DC1-S3 | Storage Node | 0% | 0% | 4% |
| DC2 | Site | 0% | 0% | — |


The Nodes table lists all the sites and nodes in your StorageGRID system. Summary information is displayed for each node. If a node has an active alert, an icon appears next to the node name. If the node is connected and has no active alerts, no icon is shown.

Connection state icons

- Not connected - Unknown** : The node is not connected to the grid for an unknown reason. For example, the network connection between nodes has been lost or the power is down. The **Unable to communicate with node** alert might also be triggered. Other alerts might be active as well. This situation requires immediate attention.




A node might appear as Unknown during managed shutdown operations. You can ignore the Unknown state in these cases.

- Not connected - Administratively down** : The node is not connected to the grid for an expected reason. For example, the node, or services on the node, has been gracefully shut down, the node is rebooting, or the software is being upgraded. One or more alerts might also be active.

If a node is disconnected from the grid, it might have an underlying alert, but only the “Not connected” icon appears. To see the active alerts for a node, select the node.

Alert icons

If there is an active alert for a node, one of the following icons appears next to the node name:

- Critical** : An abnormal condition exists that has stopped the normal operations of a StorageGRID node

or service. You must address the underlying issue immediately. Service disruption and loss of data might result if the issue is not resolved.

- **Major** : An abnormal condition exists that is either affecting current operations or approaching the threshold for a critical alert. You should investigate major alerts and address any underlying issues to ensure that the abnormal condition does not stop the normal operation of a StorageGRID node or service.
- **Minor** : The system is operating normally, but an abnormal condition exists that could affect the system's ability to operate if it continues. You should monitor and resolve minor alerts that do not clear on their own to ensure they do not result in a more serious problem.

Details for a system, site, or node

To view the available information, select the name of the grid, site, or node as follows:

- Select the grid name to see an aggregate summary of the statistics for your entire StorageGRID system. (The screenshot shows a system named StorageGRID Deployment.)
- Select a specific data center site to see an aggregate summary of the statistics for all nodes at that site.
- Select a specific node to view detailed information for that node.

Tabs for the Nodes page

The tabs at the top of the Nodes page are based on what you select from the tree at the left.

| Tab name | Description | Included for |
|----------|---|---|
| Overview | <ul style="list-style-type: none">• Provides basic information about each node.• Shows any active alerts affecting the node. | All nodes |
| Hardware | <ul style="list-style-type: none">• Displays CPU utilization and memory usage for each node• For appliance nodes, provides additional hardware information. | All nodes |
| Network | Displays a graph showing the network traffic received and sent across the network interfaces. The view for a single node shows additional information for the node. | All nodes, each site, and the entire grid |
| Storage | <ul style="list-style-type: none">• Provides details for the disk devices and volumes on each node.• For Storage Nodes, each site, and the entire grid, includes graphs showing object data storage and metadata storage used over time. | All nodes, each site, and the entire grid |
| Objects | <ul style="list-style-type: none">• Provides information about S3 and Swift ingest and retrieve rates.• For Storage Nodes, provides object counts and information about metadata store queries and background verification. | Storage Nodes, each site, and the entire grid |

| Tab name | Description | Included for |
|---------------------------|--|--|
| ILM | <p>Provides information about Information Lifecycle Management (ILM) operations.</p> <ul style="list-style-type: none"> • For Storage Nodes, provides details about ILM evaluation and background verification for erasure coded objects. • For each site and the entire grid, shows a graph of the ILM queue over time. • For the entire grid, provides the estimated time to complete a full ILM scan of all objects. | Storage Nodes, each site, and the entire grid |
| Load balancer | <p>Includes performance and diagnostic graphs related to the Load Balancer service.</p> <ul style="list-style-type: none"> • For each site, provides an aggregate summary of the statistics for all nodes at that site. • For the entire grid, provides an aggregate summary of the statistics for all sites. | Admin Nodes and Gateway Nodes, each site, and the entire grid |
| Platform services | Provides information about any S3 platform service operations at a site. | Each site |
| SANtricity System Manager | Provides access to SANtricity System Manager. From SANtricity System Manager, you can review hardware diagnostic and environmental information for the storage controller, as well as issues related to the drives. | <p>Storage appliance nodes</p> <p>Note: The SANtricity System Manager tab will not appear if the controller firmware on the storage appliance is earlier than 8.70.</p> |

Prometheus metrics

The Prometheus service on Admin Nodes collects time series metrics from the services on all nodes.

The metrics collected by Prometheus are used in a number of places in the Grid Manager:

- **Nodes page:** The graphs and charts on the tabs available from the Nodes page use the Grafana visualization tool to display the time-series metrics collected by Prometheus. Grafana displays time-series data in graph and chart formats, while Prometheus serves as the backend data source.



- **Alerts:** Alerts are triggered at specific severity levels when alert rule conditions that use Prometheus metrics evaluate as true.
- **Grid Management API:** You can use Prometheus metrics in custom alert rules or with external automation tools to monitor your StorageGRID system. A complete list of Prometheus metrics is available from the Grid Management API. (From the top of the Grid Manager, select the help icon and select **API Documentation > metrics**.) While more than a thousand metrics are available, only a relatively small number are required to monitor the most critical StorageGRID operations.



Metrics that include *private* in their names are intended for internal use only and are subject to change between StorageGRID releases without notice.

- The **SUPPORT > Tools > Diagnostics** page and the **SUPPORT > Tools > Metrics** page: These pages, which are primarily intended for use by technical support, provide a number of tools and charts that use the values of Prometheus metrics.



Some features and menu items within the Metrics page are intentionally non-functional and are subject to change.

StorageGRID attributes

Attributes report values and statuses for many of the functions of the StorageGRID system. Attribute values are available for each grid node, each site, and the entire grid.

StorageGRID attributes are used in a number of places in the Grid Manager:

- **Nodes page:** Many of the values shown on the Nodes page are StorageGRID attributes. (Prometheus metrics are also shown on the Nodes pages.)
- **Alarms:** When attributes reach defined threshold values, StorageGRID alarms (legacy system) are triggered at specific severity levels.
- **Grid Topology tree:** Attribute values are shown in the Grid Topology tree (**SUPPORT > Tools > Grid topology**).
- **Events:** System events occur when certain attributes record an error or fault condition for a node, including errors such as network errors.

Attribute values

Attributes are reported on a best-effort basis and are approximately correct. Attribute updates can be lost under some circumstances, such as the crash of a service or the failure and rebuild of a grid node.

In addition, propagation delays might slow the reporting of attributes. Updated values for most attributes are sent to the StorageGRID system at fixed intervals. It can take several minutes before an update is visible in the system, and two attributes that change more or less simultaneously can be reported at slightly different times.

Related information

- [Monitor and troubleshoot](#)
- [Monitor and manage alerts](#)
- [Use StorageGRID support options](#)

Monitor and manage alerts

The alert system provides an easy-to-use interface for detecting, evaluating, and resolving the issues that can occur during StorageGRID operation.

The alert system is designed to be your primary tool for monitoring any issues that might occur in your StorageGRID system.

- The alert system focuses on actionable problems in the system. Alerts are triggered for events that require your immediate attention, not for events that can safely be ignored.
- The Current Alerts and Resolved Alerts pages provide a user friendly interface for viewing current and historical problems. You can sort the listing by individual alerts and alert groups. For example, you might want to sort all alerts by node/site to see which alerts are affecting a specific node. Or, you might want to sort the alerts in a group by time triggered to find the most recent instance of a specific alert.
- Multiple alerts of the same type are grouped into one email to reduce the number of notifications. In addition, multiple alerts of the same type are shown as a group on the Current Alerts and Resolved Alerts pages. You can expand and collapse alert groups to show or hide the individual alerts. For example, if several nodes are reporting the **Unable to communicate with node** alert, only one email is sent and the alert is shown as a group on the Current Alerts page.

Current Alerts [Learn more](#)

View the current alerts affecting your StorageGRID system.

| | | | | | | | <input checked="" type="checkbox"/> Group alerts | Active ▾ |
|--|------------|---|--------------------------------|----------|---|--|--|----------|
| Name | Severity | Time triggered | Site / Node | Status | Current values | | | |
| ▼ Unable to communicate with node One or more services are unresponsive or cannot be reached by the metrics collection job. | 2 Major | 9 minutes ago (newest) 19 minutes ago (oldest) | | 2 Active | | | | |
| Low root disk capacity The space available on the root disk is low. | Minor | 25 minutes ago | Data Center 1 / DC1-S1-99-51 | Active | Disk space available: 2.00 GB Total disk space: 21.00 GB | | | |
| Expiration of server certificate for Storage API Endpoints The server certificate used for the storage API endpoints is about to expire. | Major | 31 minutes ago | Data Center 1 / DC1-ADM1-99-49 | Active | Days remaining: 14 | | | |
| Expiration of server certificate for Management Interface The server certificate used for the management interface is about to expire. | Minor | 31 minutes ago | Data Center 1 / DC1-ADM1-99-49 | Active | Days remaining: 30 | | | |
| ▼ Low installed node memory The amount of installed memory on a node is low. | 8 Critical | a day ago (newest) a day ago (oldest) | | 8 Active | | | | |

- Alerts use intuitive names and descriptions to help you understand more quickly what the problem is. Alert notifications include details about the node and site affected, the alert severity, the time when the alert rule was triggered, and the current value of metrics related to the alert.

- Alert email notifications and the alert listings on the Current Alerts and Resolved Alerts pages provide recommended actions for resolving an alert. These recommended actions often include direct links to StorageGRID documentation to make it easier to find and access more detailed troubleshooting procedures.

Low installed node memory

The amount of installed memory on a node is low.

Recommended actions

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Time triggered

2019-07-15 17:07:41 MDT (2019-07-15 23:07:41 UTC)

Status

Active ([silence this alert](#) )

Site / Node

Data Center 2 / DC2-S1-99-56

Severity

 Critical

Total RAM size

8.38 GB

Condition

[View conditions](#) | [Edit rule](#) 

Close



The legacy alarm system is deprecated. The user interface and APIs for the legacy alarm system will be removed in a future release. The alert system offers significant benefits and is easier to use.

Manage alerts

All StorageGRID users can view alerts. If you have the Root Access or Manage Alerts permission, you can also manage alerts, as follows:

- If you need to temporarily suppress the notifications for an alert at one or more severity levels, you can easily silence a specific alert rule for a specified duration. You can silence an alert rule for the entire grid, a single site, or a single node.
- You can edit the default alert rules as required. You can disable an alert rule completely, or change its trigger conditions and duration.
- You can create custom alert rules to target the specific conditions that are relevant to your situation and to provide your own recommended actions. To define the conditions for a custom alert, you create expressions using the Prometheus metrics available from the Metrics section of the Grid Management API.

For example, this expression causes an alert to be triggered if the amount of installed RAM for a node is less than 24,000,000,000 bytes (24 GB).

```
node_memory_MemTotal < 24000000000
```

Related information

Use SNMP monitoring

If you want to monitor StorageGRID using the Simple Network Management Protocol (SNMP), you can use the Grid Manager to configure the SNMP agent.

Each StorageGRID node runs an SNMP agent, or daemon, that provides a management information base (MIB). The StorageGRID MIB contains table and notification definitions for alerts and alarms. Each StorageGRID node also supports a subset of MIB-II objects.

Initially, SNMP is disabled on all nodes. When you configure the SNMP agent, all StorageGRID nodes receive the same configuration.

The StorageGRID SNMP agent supports all three versions of the SNMP protocol. The agent provides read-only MIB access for queries, and it can send two types of event-driven notifications to a management system:

- **Traps** are notifications sent by the SNMP agent that do not require acknowledgment by the management system. Traps serve to notify the management system that something has happened within StorageGRID, such as an alert being triggered. Traps are supported in all three versions of SNMP.
- **Informs** are similar to traps, but they require acknowledgment by the management system. If the SNMP agent does not receive an acknowledgment within a certain amount of time, it resends the inform until an acknowledgment is received or the maximum retry value has been reached. Informes are supported in SNMPv2c and SNMPv3.

Trap and inform notifications are sent in the following cases:

- A default or custom alert is triggered at any severity level. To suppress SNMP notifications for an alert, you must configure a silence for the alert. Alert notifications are sent by whichever Admin Node is configured to be the preferred sender.
- Certain alarms (legacy system) are triggered at specified severity levels or higher.



SNMP notifications are not sent for every alarm or every alarm severity.

Related information

- [Monitor and troubleshoot](#)

Review audit messages

Audit messages can help you get a better understanding of the detailed operations of your StorageGRID system. You can use audit logs to troubleshoot issues and to evaluate performance.

During normal system operation, all StorageGRID services generate audit messages, as follows:

- System audit messages are related to the auditing system itself, grid node states, system-wide task activity, and service backup operations.
- Object storage audit messages are related to the storage and management of objects within StorageGRID, including object storage and retrievals, grid-node to grid-node transfers, and verifications.
- Client read and write audit messages are logged when an S3 or Swift client application makes a request to

create, modify, or retrieve an object.

- Management audit messages log user requests to the Management API.

Each Admin Node stores audit messages in text files. The audit share contains the active file (audit.log) as well as compressed audit logs from previous days. Additionally, each node in your grid stores a limited amount of audit messages in a local log file (localaudit.log).

For easy access to audit logs, you can configure client access to the audit share for both NFS and CIFS (CIFS is deprecated). You can also access audit log files directly from the command line of the Admin Node.

Optionally, you can send audit information stored on Admin Nodes and local nodes to an external syslog server. Using an external syslog server can make it easier to manage your audit information and reduce network traffic. See [Configure audit messages and log destinations](#) for more information.

For details on the audit log file, the format of audit messages, the types of audit messages, and the tools available to analyze audit messages, see the [instructions for audit messages](#). To learn how to configure audit client access, see [Configure audit client access](#).

Related information

- [Review audit logs](#)
- [Administer StorageGRID](#)

Perform maintenance

You perform various maintenance procedures to keep your StorageGRID system up-to-date and to ensure it is performing efficiently. The Grid Manager provides tools and options to facilitate the process of performing maintenance tasks.

Software updates

You can perform three types of software updates from the Software Update page in the Grid Manager:

- StorageGRID software upgrade
- StorageGRID hotfix
- SANtricity OS upgrade

StorageGRID software upgrades

When a new StorageGRID feature release is available, the Software Upgrade page guides you through the process of uploading the required file and upgrading your StorageGRID system. You must upgrade all grid nodes for all data center sites from the primary Admin Node.

During a StorageGRID software upgrade, client applications can continue to ingest and retrieve object data.

Hotfixes

If issues with the software are detected and resolved between feature releases, you might need to apply a hotfix to your StorageGRID system.

StorageGRID hotfixes contain software changes that are made available outside of a feature or patch release. The same changes are included in a future release.

The StorageGRID Hotfix page, shown below, allows you to upload a hotfix file.

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available.

When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Passphrase

Provisioning Passphrase ?

The hotfix is applied first to the primary Admin Node. Then, you must approve the application of the hotfix to other grid nodes until all nodes in your StorageGRID system are running the same software version. You can customize the approval sequence by selecting to approve individual grid nodes, groups of grid nodes, or all grid nodes.



While all grid nodes are updated with the new hotfix version, the actual changes in a hotfix might only affect specific services on specific types of nodes. For example, a hotfix might only affect the LDR service on Storage Nodes.

SANtricity OS upgrades

You might need to upgrade the SANtricity OS Software on the storage controllers of your storage appliances, if the controllers are not functioning optimally. You can upload the SANtricity OS file to the primary Admin Node in your StorageGRID system and apply the upgrade from the Grid Manager.

The SANtricity page, shown below, allows you to upload the SANtricity OS upgrade file.

SANtricity OS

Use this procedure to upgrade the SANtricity OS software (controller firmware) on the storage controllers in your storage appliances.

1. Download the SANtricity OS version that is compatible with the storage controllers. If you use different appliance models, repeat these steps for each model.
2. Confirm the storage controllers are Nominal (**NODES > appliance node > Hardware**) and ready to upgrade.
3. Start the upgrade and approve the nodes you want to upgrade. Nodes are upgraded one at a time.
During the upgrade, a health check is performed and valid NVSRAM is installed. When the upgrade is complete, the appliance is rebooted. The upgrade can take up to 30 minutes for each appliance.
4. Select **Skip Nodes and Finish** if you only want to apply this upgrade to some nodes or if you want to upgrade some nodes later.

SANtricity OS Upgrade File

SANtricity OS Upgrade File ?

Browse

Passphrase

Provisioning Passphrase ?

Start

After you upload the file, you can approve the upgrade on individual Storage Nodes or all nodes. The ability to selectively approve nodes makes it easier for you to schedule the upgrade. After you approve a node for upgrade, the system performs a health check and installs the upgrade if it is applicable to the node.

Expansion procedures

You can expand a StorageGRID system by adding storage volumes to Storage Nodes, adding new grid nodes to an existing site, or adding a new data center site. If you have Storage Nodes that use the SG6060 storage appliance, you can add one or two expansion shelves to double or triple the storage capacity of the node.

You can perform expansions without interrupting the operation of your current system. When you add nodes or a site, you first deploy the new nodes and then perform the expansion procedure from the Grid Expansion page.

Grid Expansion

i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

Expansion Progress


Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing Grid Nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

| | | | | | | Search  |
|--------------|--------|---------------------------|------------------------|--------------------------------------|--|--|
| Name | Site | Grid Network IPv4 Address | Progress | Stage | | |
| DC2-ADM1-184 | Site A | 172.17.3.184/21 | <div><div></div></div> | Waiting for NTP to synchronize | | |
| DC2-S1-185 | Site A | 172.17.3.185/21 | <div><div></div></div> | Waiting for Dynamic IP Service peers | | |
| DC2-S2-186 | Site A | 172.17.3.186/21 | <div><div></div></div> | Waiting for NTP to synchronize | | |
| DC2-S3-187 | Site A | 172.17.3.187/21 | <div><div></div></div> | Waiting for NTP to synchronize | | |
| DC2-S4-188 | Site A | 172.17.3.188/21 | <div><div></div></div> | Waiting for Dynamic IP Service peers | | |
| DC2-ARC1-189 | Site A | 172.17.3.189/21 | <div><div></div></div> | Waiting for NTP to synchronize | | |

2. Initial Configuration

Pending

3. Distributing the new grid node's certificates to the StorageGRID system.

Pending

4. Starting services on the new grid nodes

Pending

5. Cleaning up unused Cassandra keys

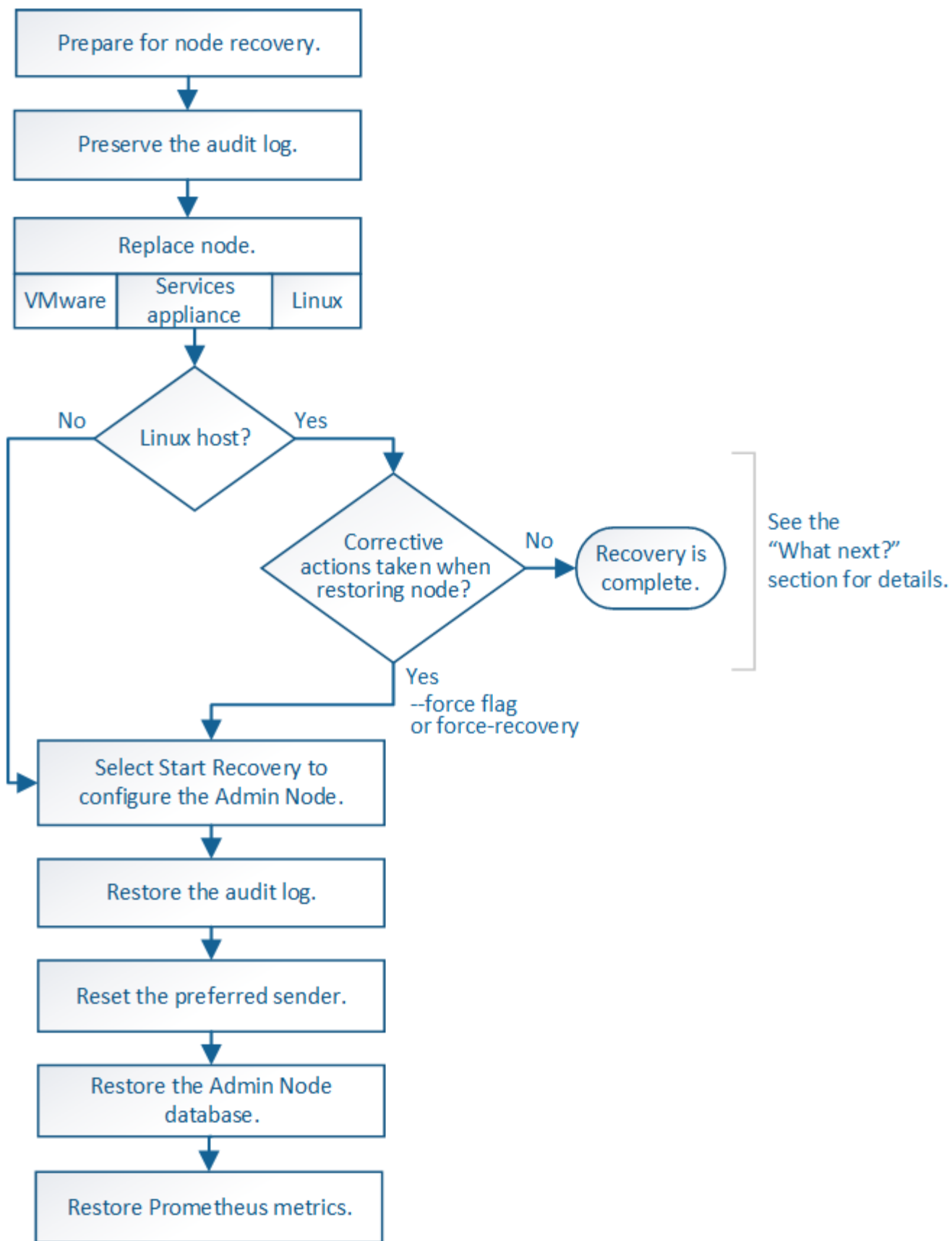
Pending

Node recovery procedures

Grid nodes can fail if a hardware, virtualization, operating system, or software fault renders the node inoperable or unreliable.

The steps to recover a grid node depend on the platform where the grid node is hosted and on the type of grid node. Each type of grid node has a specific recovery procedure, which you must follow exactly. Generally, you try to preserve data from the failed grid node where possible, repair or replace the failed node, use the Recovery page to configure the replacement node, and restore the node's data.

For example, this flowchart shows the recovery procedure if an Admin Node has failed.



Decommission procedures

You might want to permanently remove grid nodes or an entire data center site from your StorageGRID system.

For example, you might want to decommission one or more grid nodes in these cases:

- You have added a larger Storage Node to the system and you want to remove one or more smaller Storage Nodes, while at the same time preserving objects.
- You require less total storage.
- You no longer require a Gateway Node or a non-primary Admin Node.
- Your grid includes a disconnected node that you cannot recover or bring back online.

You can use the Decommission Nodes page in the Grid Manager to remove the following types of grid nodes:

- Storage Nodes, unless not enough nodes would remain at the site to support certain requirements
- Gateway Nodes
- Non-primary Admin Nodes

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

| Name | Site | Type | Has ADC | Health | Decommission Possible |
|-----------------------------------|---------------|------------------|---------|--------|---|
| DC1-ADM1 | Data Center 1 | Admin Node | - | ✓ | No, primary Admin Node decommissioning is not supported. |
| DC1-ARC1 | Data Center 1 | Archive Node | - | ✓ | No, Archive Nodes decommissioning is not supported. |
| <input type="checkbox"/> DC1-G1 | Data Center 1 | API Gateway Node | - | ✓ | ✓ |
| DC1-S1 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| DC1-S2 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| DC1-S3 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| <input type="checkbox"/> DC1-S4 | Data Center 1 | Storage Node | No | ✓ | ✓ |
| <input type="checkbox"/> DC2-ADM1 | Data Center 2 | Admin Node | - | ✓ | ✓ |
| DC2-S1 | Data Center 2 | Storage Node | Yes | ✓ | No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services. |

You can use the Decommission Site page in the Grid Manager to remove a site. A connected site decommission removes an operational site and preserves data. A disconnected site decommission removes a failed site but does not preserve data. The Decommission Site wizard guides you through the process of selecting the site, viewing site details, revising the ILM policy, removing site references from ILM rules, and resolving any node conflicts.

Decommission Site



When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

| | Site Name | Used Storage Capacity ? | Decommission Possible |
|-----------------------|-----------|-------------------------|--|
| <input type="radio"/> | Raleigh | 3.93 MB | ✓ |
| <input type="radio"/> | Sunnyvale | 3.97 MB | ✓ |
| <input type="radio"/> | Vancouver | 3.90 MB | No. This site contains the primary Admin Node. |

Next

Network maintenance procedures

Some of the network maintenance procedures you might need to perform include the following:

- Updating the subnets on the Grid Network
- Using the Change IP tool to change the networking configuration that was initially set during grid deployment
- Adding, removing, or updating domain name system (DNS) servers
- Adding, removing, or updating network time protocol (NTP) servers to ensure that data is synchronized accurately between grid nodes
- Restoring network connectivity to nodes that might have become isolated from the rest of the grid

Host-level and middleware procedures

Some maintenance procedures are specific to StorageGRID nodes that are deployed on Linux or VMware, or are specific to other components of the StorageGRID solution. For example, you might want to migrate a grid node to a different Linux host or perform maintenance on an Archive Node that is connected to Tivoli Storage Manager (TSM).

Appliance node cloning

Appliance node cloning lets you easily replace an existing appliance node in your grid with an appliance of newer design or increased capabilities that is part of the same logical StorageGRID site. The process transfers all data to the new appliance, placing it in service to replace the old appliance node and leaving the old appliance in a pre-install state. Cloning provides a hardware-upgrade process that is easy to perform, and provides an alternate method for replacing appliances.

Grid node procedures

You might need to perform certain procedures on a specific grid node. For example, you might need to reboot a grid node or manually stop and restart a specific grid node service. Some grid node procedures can be performed from the Grid Manager; others require you to log in to the grid node and use the node's command line.

Related information

- [Administer StorageGRID](#)
- [Upgrade software](#)
- [Expand your grid](#)
- [Recover and maintain](#)

Download the Recovery Package

The Recovery Package is a downloadable .zip file that contains deployment-specific files and software needed to install, expand, upgrade, and maintain a StorageGRID system.

The Recovery Package file also contains system-specific configuration and integration information, including server hostnames and IP addresses, and highly confidential passwords needed during system maintenance, upgrade, and expansion. The Recovery Package is required to recover from the failure of the primary Admin Node.

When installing a StorageGRID system, you are required to download the Recovery Package file and to confirm that you can successfully access the contents of this file. You should also download the file each time the grid topology of the StorageGRID system changes because of maintenance or upgrade procedures.

Recovery Package

Enter your provisioning passphrase and click Start Download to save a copy of the Recovery Package file. Download the file each time the grid topology of the StorageGRID system changes because of maintenance or upgrade procedures, so that you can restore the grid if a failure occurs.

When the download completes, copy the Recovery Package file to two safe, secure, and separate locations.

Important: The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

Provisioning Passphrase

Start Download

After downloading the Recovery Package file and confirming you can extract the contents, copy the Recovery Package file to two safe, secure, and separate locations.



The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

Related information

- [Upgrade software](#)
- [Expand your grid](#)
- [Recover and maintain](#)

Use StorageGRID support options

The Grid Manager provides options to help you work with technical support if an issue arises with your StorageGRID system.

Configure AutoSupport

The AutoSupport feature enables your StorageGRID system to send health and status messages to technical support. Using AutoSupport can significantly speed problem determination and resolution. Technical support can also monitor the storage needs of your system and help you determine if you need to add new nodes or sites. Optionally, you can configure AutoSupport messages to be sent to one additional destination.

You configure AutoSupport using the Grid Manager (**SUPPORT > Tools > AutoSupport**). The **AutoSupport** page has two tabs: **Settings** and **Results**.


AutoSupport


The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.


Settings

Results


Protocol Details


Protocol  ☒ HTTPS ☐ HTTP ☐ SMTP


NetApp Support Certificate Validation 

Use NetApp support certificate 


AutoSupport Details

Enable Weekly AutoSupport  ☒


Enable Event-Triggered AutoSupport  ☒

Enable AutoSupport on Demand  ☐

Software Updates

Check for software updates  ☒

Additional AutoSupport Destination

Enable Additional AutoSupport Destination  ☐

Save

Send User-Triggered AutoSupport

Information included in AutoSupport messages

AutoSupport messages include information such as the following:

- StorageGRID software version
- Operating system version
- System-level and location-level attribute information
- Recent alerts and alarms (legacy system)

- Current status of all grid tasks, including historical data
- Admin Node database usage
- Number of lost or missing objects
- Grid configuration settings
- NMS entities
- Active ILM policy
- Provisioned grid specification file
- Diagnostic metrics

You can enable the AutoSupport feature and the individual AutoSupport options when you first install StorageGRID, or you can enable them later. If AutoSupport is not enabled, a message appears on the Grid Manager Dashboard. The message includes a link to the AutoSupport configuration page.

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



If you close the message, it will not appear again until your browser cache is cleared, even if AutoSupport remains disabled.

Use Active IQ

Active IQ is a cloud-based digital advisor that leverages predictive analytics and community wisdom from NetApp's installed base. Its continuous risk assessments, predictive alerts, prescriptive guidance, and automated actions help you prevent problems before they occur, leading to improved system health and higher system availability.

You must enable AutoSupport if you want to use the Active IQ dashboards and functionality on the NetApp Support site.

[Active IQ Digital Advisor Documentation](#)

Collect StorageGRID logs

To help troubleshoot a problem, you might need to collect log files and forward them to technical support.

StorageGRID uses log files to capture events, diagnostic messages, and error conditions. The bycast.log file is maintained for every grid node and is the primary troubleshooting file. StorageGRID also creates log files for individual StorageGRID services, log files related to deployment and maintenance activities, and log files related to third-party applications.

Users who have the appropriate permissions and who know the provisioning passphrase for your StorageGRID system can use the Logs page in the Grid Manager to gather log files, system data, and configuration data. When you collect logs, you select a node or nodes and specify a time period. Data is collected and archived in a `.tar.gz` file, which you can download to a local computer. Inside this file, there is one log file archive for each grid node.

StorageGRID

- DC1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3
 - DC1-S4
- DC2
 - DC2-ADM1
 - DC2-G1
 - DC2-S1
 - DC2-S2
 - DC2-S3
 - DC2-S4

Log Start Time: 2021-12-03 06 : 31 AM MST

Log End Time: 2021-12-03 10 : 31 AM MST

Log Types:
 ☒ Application Logs
 ☐ Network Trace
 ☐ Audit Logs
 ☐ Prometheus Database

Notes:

Provisioning Passphrase:

Collect Logs

Use metrics and run diagnostics

When troubleshooting an issue, you can work with technical support to review detailed metrics and charts for your StorageGRID system. You can also run pre-constructed diagnostic queries to proactively assess key values for your StorageGRID system.

Metrics page

The Metrics page provides access to the Prometheus and Grafana user interfaces. Prometheus is open-source software for collecting metrics. Grafana is open-source software for metrics visualization.



The tools available on the Metrics page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional and are subject to change.

Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- <https://storagegrid.sagegate.com/metrics/graph>

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

| | | |
|---|---|---|
| ADE | Grid | S3 - Node |
| Account Service Overview | ILM | S3 Overview |
| Alertmanager | Identity Service Overview | S3 Select |
| Audit Overview | Ingests | Site |
| Cassandra Cluster Overview | Node | Support |
| Cassandra Network Overview | Node (Internal Use) | Traces |
| Cassandra Node Overview | OSL - AsyncIO | Traffic Classification Policy |
| Cloud Storage Pool Overview | Platform Services Commits | Usage Processing |
| EC - ADE | Platform Services Overview | Virtual Memory (vmstat) |
| EC - Chunk Service | Platform Services Processing | |
| EC Overview | Replicated Read Path Overview | |

The link in the Prometheus section of the Metrics page allows you to query the current values of StorageGRID metrics and to view graphs of the values over time.

PrometheusAlertsGraphStatus ▾Help

☐ Enable query history

Expression (press Shift+Enter for newlines)

Execute

- insert metric at cursor - ▾

Graph

Console

| Element | Value |
|---------|-------|
| no data | |

Remove Graph

Add Graph



Metrics that include *private* in their names are intended for internal use only and are subject to change between StorageGRID releases without notice.

The links in the Grafana section of the Metrics page allow you to access pre-constructed dashboards containing graphs of StorageGRID metrics over time.



Diagnostics page

The Diagnostics page performs a set of pre-constructed diagnostic checks on the current state of the grid. In the example, all diagnostics have a Normal status.

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- ✓ **Normal:** All values are within the normal range.
- ⚠ **Attention:** One or more of the values are outside of the normal range.
- ✖ **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

✓ **Cassandra blocked task queue too large**

✓ **Cassandra commit log latency**

✓ **Cassandra commit log queue depth**

✓ **Cassandra compaction queue too large**

Clicking a specific diagnostic lets you see details about the diagnostic and its current results.

In this example, the current CPU utilization for every node in a StorageGRID system is shown. All node values are below the Attention and Caution thresholds, so the overall status of the diagnostic is Normal.

✓ CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status ✓ Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`

[View in Prometheus](#)

Thresholds
⚠ Attention >= 75%
✖ Caution >= 95%

| Status | Instance | CPU Utilization |
|--------|----------|-----------------|
| ✓ | DC1-ADM1 | 2.598% |
| ✓ | DC1-ARC1 | 0.937% |
| ✓ | DC1-G1 | 2.119% |
| ✓ | DC1-S1 | 8.708% |
| ✓ | DC1-S2 | 8.142% |
| ✓ | DC1-S3 | 9.669% |
| ✓ | DC2-ADM1 | 2.515% |
| ✓ | DC2-ARC1 | 1.152% |
| ✓ | DC2-S1 | 8.204% |
| ✓ | DC2-S2 | 5.000% |
| ✓ | DC2-S3 | 10.469% |

Related information

- [Administer StorageGRID](#)
- [Configure network settings](#)

Networking guidelines

Networking guidelines: Overview

Use these guidelines to learn about StorageGRID architecture and networking topologies and to learn the requirements for network configuration and provisioning.

About these instructions

These guidelines provide information you can use to create the StorageGRID networking infrastructure before deploying and configuring StorageGRID nodes. Use these guidelines to help ensure that communication can occur among all the nodes in the grid and between the grid and external clients and services.

External clients and external services need to connect to StorageGRID networks to perform functions such as the following:

- Store and retrieve object data
- Receive email notifications
- Access the StorageGRID management interface (the Grid Manager and Tenant Manager)
- Access the audit share (optional)
- Provide services such as:
 - Network Time Protocol (NTP)
 - Domain Name System (DNS)
 - Key Management Server (KMS)

StorageGRID networking must be configured appropriately to handle the traffic for these functions and more.

Before you begin

Configuring the networking for a StorageGRID system requires a high level of experience with Ethernet switching, TCP/IP networking, subnets, network routing, and firewalls.

Before you configure networking, become familiar with StorageGRID architecture as described in the [Grid primer](#).

After you determine which StorageGRID networks you want to use and how those networks will be configured, you can install and configure the StorageGRID nodes by following the appropriate instructions.

Install software-based nodes

- [Install Red Hat Enterprise Linux or CentOS](#)
- [Install Ubuntu or Debian](#)
- [Install VMware](#)

Install appliance nodes

- [SG100 and SG1000 services appliances](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

Configure and administer StorageGRID software

- [Administer StorageGRID](#)
- [Release notes](#)

StorageGRID network types

The grid nodes in a StorageGRID system process *grid traffic*, *admin traffic*, and *client traffic*. You must configure the networking appropriately to manage these three types of traffic and to provide control and security.

Traffic types

| Traffic type | Description | Network type |
|----------------|--|---|
| Grid traffic | The internal StorageGRID traffic that travels between all nodes in the grid. All grid nodes must be able to communicate with all other grid nodes over this network. | Grid Network (required) |
| Admin traffic | The traffic used for system administration and maintenance. | Admin Network (optional), VLAN network (optional) |
| Client traffic | The traffic that travels between external client applications and the grid, including all object storage requests from S3 and Swift clients. | Client Network (optional), VLAN network (optional) |

You can configure networking in the following ways:

- Grid Network only
- Grid and Admin Networks
- Grid and Client Networks
- Grid, Admin, and Client Networks

The Grid Network is mandatory and can manage all grid traffic. The Admin and Client Networks can be included at the time of installation or added later to adapt to changes in requirements. Although the Admin Network and Client Network are optional, when you use these networks to handle administrative and client traffic, the Grid Network can be made isolated and secure.

Internal ports are only accessible over the Grid Network. External ports are accessible from all network types. This flexibility provides multiple options for designing a StorageGRID deployment and setting up external IP and port filtering in switches and firewalls. See [internal grid node communications](#) and [external communications](#).

Network interfaces

StorageGRID nodes are connected to each network using the following specific interfaces:

| Network | Interface name |
|---------------------------|----------------|
| Grid Network (required) | eth0 |
| Admin Network (optional) | eth1 |
| Client Network (optional) | eth2 |

For details about mapping virtual or physical ports to node network interfaces, see the installation instructions:

Software-based nodes

- [Install Red Hat Enterprise Linux or CentOS](#)
- [Install Ubuntu or Debian](#)
- [Install VMware](#)

Appliance nodes

- [SG100 and SG1000 services appliances](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

Network information for each node

You must configure the following for each network you enable on a node:

- IP address
- Subnet mask
- Gateway IP address

You can only configure one IP address/mask/gateway combination for each of the three networks on each grid node. If you do not want to configure a gateway for a network, you should use the IP address as the gateway address.

High availability groups

High availability (HA) groups provide the ability to add virtual IP (VIP) addresses to the Grid or Client Network interface. For more information, see [Manage high availability groups](#).

Grid Network

The Grid Network is required. It is used for all internal StorageGRID traffic. The Grid Network provides connectivity among all nodes in the grid, across all sites and subnets. All nodes on the Grid Network must be able to communicate with all other nodes. The Grid Network can consist of multiple subnets. Networks containing critical grid services, such as NTP, can also be added as grid subnets.



StorageGRID does not support network address translation (NAT) between nodes.

The Grid Network can be used for all admin traffic and all client traffic, even if the Admin Network and Client Network are configured. The Grid Network gateway is the node default gateway unless the node has the Client Network configured.



When configuring the Grid Network, you must ensure that the network is secured from untrusted clients, such as those on the open internet.

Note the following requirements and details for the Grid Network gateway:

- The Grid Network gateway must be configured if there are multiple grid subnets.
- The Grid Network gateway is the node default gateway until grid configuration is complete.
- Static routes are generated automatically for all nodes to all subnets configured in the global Grid Network Subnet List.
- If a Client Network is added, the default gateway switches from the Grid Network gateway to the Client Network gateway when grid configuration is complete.

Admin Network

The Admin Network is optional. When configured, it can be used for system administration and maintenance traffic. The Admin Network is typically a private network and does not need to be routable between nodes.

You can choose which grid nodes should have the Admin Network enabled on them.

When you use the Admin Network, administrative and maintenance traffic does not need to travel across the Grid Network. Typical uses of the Admin Network include the following:

- Access to the Grid Manager and Tenant Manager user interfaces.
- Access to critical services such as NTP servers, DNS servers, external key management servers (KMS), and Lightweight Directory Access Protocol (LDAP) servers.
- Access to audit logs on Admin Nodes.
- Secure Shell Protocol (SSH) access for maintenance and support.

The Admin Network is never used for internal grid traffic. An Admin Network gateway is provided and allows the Admin Network to communicate with multiple external subnets. However, the Admin Network gateway is never used as the node default gateway.

Note the following requirements and details for the Admin Network gateway:

- The Admin Network gateway is required if connections will be made from outside of the Admin Network subnet or if multiple Admin Network subnets are configured.
- Static routes are created for each subnet configured in the node's Admin Network Subnet List.

Client Network

The Client Network is optional. When configured, it is used to provide access to grid services for client applications such as S3 and Swift. If you plan to make StorageGRID data accessible to an external resource (for example, a Cloud Storage Pool or the StorageGRID CloudMirror replication service), the external resource can also use the Client Network. Grid nodes can communicate with any subnet reachable through the Client Network gateway.

You can choose which grid nodes should have the Client Network enabled on them. All nodes do not have to be on the same Client Network, and nodes will never communicate with each other over the Client Network. The Client Network does not become operational until grid installation is complete.

For added security, you can specify that a node's Client Network interface be untrusted so that the Client Network will be more restrictive of which connections are allowed. If a node's Client Network interface is untrusted, the interface accepts outbound connections such as those used by CloudMirror replication, but only accepts inbound connections on ports that have been explicitly configured as load balancer endpoints. See [Manage untrusted Client Networks](#) and [Configure load balancer endpoints](#).

When you use a Client Network, client traffic does not need to travel across the Grid Network. Grid Network traffic can be separated onto a secure, non-routable network. The following node types are often configured with a Client Network:

- Gateway Nodes, because these nodes provide access to the StorageGRID Load Balancer service and S3 and Swift client access to the grid.
- Storage Nodes, because these nodes provide access to the S3 and Swift protocols and to Cloud Storage Pools and the CloudMirror replication service.
- Admin Nodes, to ensure that tenant users can connect to the Tenant Manager without needing to use the Admin Network.

Note the following for the Client Network gateway:

- The Client Network gateway is required if the Client Network is configured.
- The Client Network gateway becomes the default route for the grid node when grid configuration is complete.

Optional VLAN networks

As required, you can optionally use virtual LAN (VLAN) networks for client traffic and for some types of admin traffic. Grid traffic, however, cannot use a VLAN interface. The internal StorageGRID traffic between nodes must always use the Grid Network on eth0.

To support the use VLANs, you must configure one or more interfaces on a node as trunk interfaces at the switch. You can configure the Grid Network interface (eth0) or the Client Network interface (eth2) to be a trunk, or you can add additional trunk interfaces to the node.

If eth0 is configured as a trunk, Grid Network traffic flows over the trunk native interface, as configured on the switch. Similarly, if eth2 is configured as a trunk, and the Client Network is also configured on the same node, the Client Network uses the trunk port's native VLAN as configured on the switch.

Only inbound admin traffic, such as used for SSH, Grid Manager, or Tenant Manager traffic, is supported over VLAN networks. Outbound traffic, such as used for NTP, DNS, LDAP, KMS, and Cloud Storage Pools, is not supported over VLAN networks.



VLAN interfaces can be added to Admin Nodes and Gateway Nodes only. You cannot use a VLAN interface for client or admin access to Storage Nodes or Archive Nodes.

See [Configure VLAN interfaces](#) for instructions and guidelines.

VLAN interfaces are only used in HA groups and are assigned VIP addresses on the active node. See [Manage high availability groups](#) for instructions and guidelines.

Related information

- [Networking requirements](#)

Network topology examples

Grid Network topology

The simplest network topology is created by configuring the Grid Network only.

When you configure the Grid Network, you establish the host IP address, subnet mask, and Gateway IP address for the eth0 interface for each grid node.

During configuration, you must add all Grid Network subnets to the Grid Network Subnet List (GNSL). This list includes all subnets for all sites, and might also include external subnets that provide access to critical services such as NTP, DNS, or LDAP.

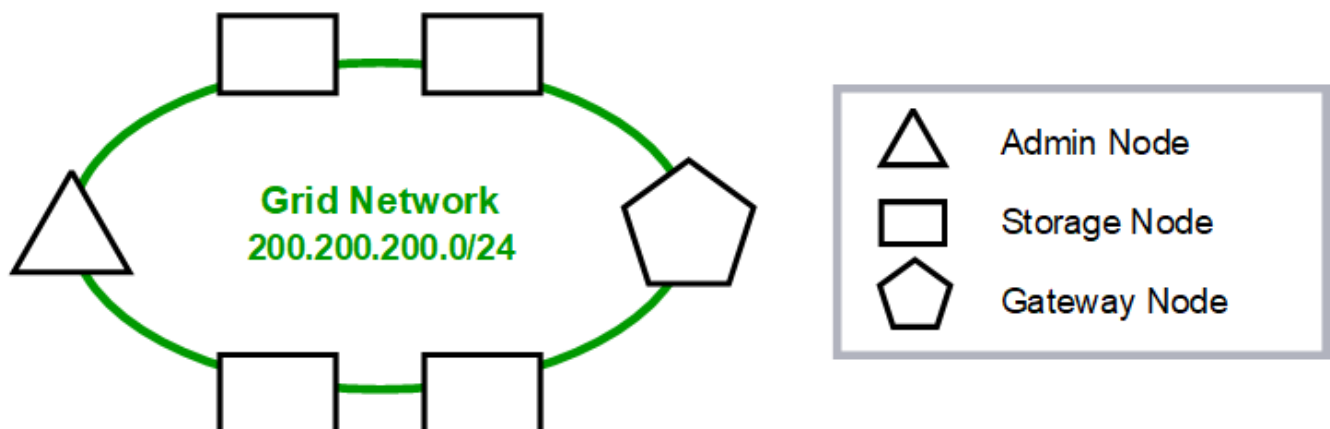
At installation, the Grid Network interface applies static routes for all subnets in the GNSL and sets the node's default route to the Grid Network gateway if one is configured. The GNSL is not required if there is no Client Network and the Grid Network gateway is the node's default route. Host routes to all other nodes in the grid are also generated.

In this example, all traffic shares the same network, including traffic related to S3 and Swift client requests and administrative and maintenance functions.



This topology is appropriate for single-site deployments that are not externally available, proof-of-concept or test deployments, or when a third-party load balancer acts as the client access boundary. When possible, the Grid Network should be used exclusively for internal traffic. Both the Admin Network and the Client Network have additional firewall restrictions that block external traffic to internal services. Using the Grid Network for external client traffic is supported, but this use offers fewer layers of protection.

Topology example: Grid Network only



*Provisioned***GNSL → 200.200.200.0/24**

| Grid Network | | |
|---------------------|-------------------|----------------|
| Nodes | IP/mask | Gateway |
| Admin | 200.200.200.32/24 | 200.200.200.1 |
| Storage | 200.200.200.33/24 | 200.200.200.1 |
| Storage | 200.200.200.34/24 | 200.200.200.1 |
| Storage | 200.200.200.35/24 | 200.200.200.1 |
| Storage | 200.200.200.36/24 | 200.200.200.1 |
| Gateway | 200.200.200.37/24 | 200.200.200.1 |

System Generated

| Nodes | Routes | Type | From |
|--------------|---------------------------|-------------|----------------------|
| All | 0.0.0.0/0 → 200.200.200.1 | Default | Grid Network gateway |
| | 200.200.200.0/24 → eth0 | Link | Interface IP/mask |

Admin Network topology

Having an Admin Network is optional. One way that you can use an Admin Network and a Grid Network is to configure a routable Grid Network and a bounded Admin Network for each node.

When you configure the Admin Network, you establish the host IP address, subnet mask, and Gateway IP address for the eth1 interface for each grid node.

The Admin Network can be unique to each node and can consist of multiple subnets. Each node can be configured with an Admin External Subnet List (AESL). The AESL lists the subnets reachable over the Admin Network for each node. The AESL must also include the subnets of any services the grid will access over the Admin Network, such as NTP, DNS, KMS, and LDAP. Static routes are applied for each subnet in the AESL.

In this example, the Grid Network is used for traffic related to S3 and Swift client requests and object management. while the Admin Network is used for administrative functions.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

| Nodes | Grid Network | | Admin Network | |
|-----------|------------------|--------------|---------------|-----------|
| | IP/mask | Gateway | IP/mask | Gateway |
| Admin | 172.16.200.32/24 | 172.16.200.1 | 10.10.1.10/24 | 10.10.1.1 |
| Storage 1 | 172.16.200.33/24 | 172.16.200.1 | 10.10.1.11/24 | 10.10.1.1 |
| Storage 2 | 172.16.200.34/24 | 172.16.200.1 | 10.10.3.65/24 | 10.10.3.1 |
| Storage 3 | 172.16.200.35/24 | 172.16.200.1 | 10.10.1.12/24 | 10.10.1.1 |
| Storage 4 | 172.16.200.36/24 | 172.16.200.1 | 10.10.1.13/24 | 10.10.1.1 |
| Gateway | 172.16.200.37/24 | 172.16.200.1 | 10.10.3.66/24 | 10.10.3.1 |

| System Generated | | | | | |
|----------------------------------|---------------|---|--------------|---------|----------------------|
| Nodes | Routes | | | Type | From |
| All | 0.0.0.0/0 | → | 172.16.200.1 | Default | Grid Network gateway |
| Admin, Storage 1, 3, and 4 | 172.16.0.0/16 | → | eth0 | Static | GNSL |
| | 10.10.1.0/24 | → | eth1 | Link | Interface IP/mask |
| | 10.10.2.0/24 | → | 10.10.1.1 | Static | AESL |
| | 10.10.3.0/24 | → | 10.10.1.1 | Static | AESL |
| Storage 2, Gateway | 172.16.0.0/16 | → | eth0 | Static | GNSL |
| | 10.10.1.0/24 | → | 10.10.3.1 | Static | AESL |
| | 10.10.2.0/24 | → | 10.10.3.1 | Static | AESL |
| | 10.10.3.0/24 | → | eth1 | Link | Interface IP/mask |

Client Network topology

Having a Client Network is optional. Using a Client Network allows client network traffic (for example, S3 and Swift) to be separated from grid internal traffic, which allows grid networking to be more secure. Administrative traffic can be handled by either the Client or Grid Network when the Admin Network is not configured.

When you configure the Client Network, you establish the host IP address, subnet mask, and Gateway IP address for the eth2 interface for the configured node. Each node's Client Network can be independent of the Client Network on any other node.

If you configure a Client Network for a node during installation, the node's default gateway switches from the Grid Network gateway to the Client Network gateway when installation is complete. If a Client Network is added later, the node's default gateway switches in the same way.

In this example, the Client Network is used for S3 and Swift client requests and for administrative functions, while the Grid Network is dedicated to internal object management operations.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

| Nodes | Grid Network | Client Network | |
|---------|------------------|----------------|----------|
| | IP/mask | IP/mask | Gateway |
| Admin | 172.16.200.32/24 | 37.5.5.10/24 | 37.5.5.1 |
| Storage | 172.16.200.33/24 | 37.5.5.11/24 | 37.5.5.1 |
| Storage | 172.16.200.34/24 | 37.5.5.12/24 | 37.5.5.1 |
| Storage | 172.16.200.35/24 | 37.5.5.13/24 | 37.5.5.1 |
| Storage | 172.16.200.36/24 | 37.5.5.14/24 | 37.5.5.1 |
| Gateway | 172.16.200.37/24 | 37.5.5.15/24 | 37.5.5.1 |

System Generated

| Nodes | Routes | | Type | From |
|-------|---------------|------------|---------|------------------------|
| All | 0.0.0.0/0 | → 37.5.5.1 | Default | Client Network gateway |
| | 172.16.0.0/16 | → eth0 | Link | Interface IP/mask |
| | 37.5.5.0/24 | → eth2 | Link | Interface IP/mask |

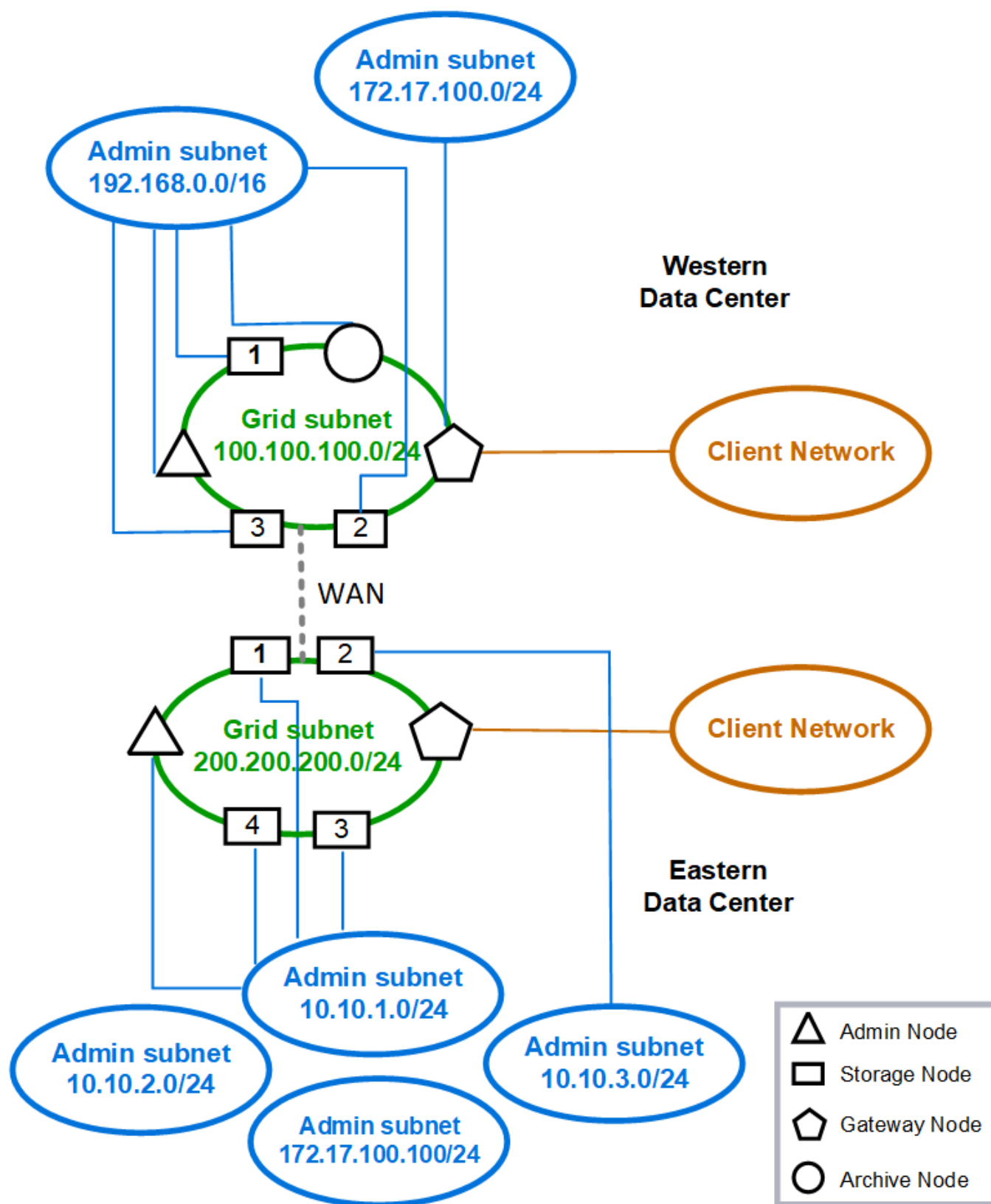
Topology for all three networks

You can configure all three networks into a network topology consisting of a private Grid Network, bounded site-specific Admin Networks, and open Client Networks. Using load balancer endpoints and untrusted Client Networks can provide additional security if needed.

In this example:

- The Grid Network is used for network traffic related to internal object management operations.
- The Admin Network is used for traffic related to administrative functions.
- The Client Network is used for traffic related to S3 and Swift client requests.

Topology example: Grid, Admin, and Client Networks



Networking requirements

You must verify that the current networking infrastructure and configuration can support the planned StorageGRID network design.

General networking requirements

All StorageGRID deployments must be able to support the following connections.

These connections can occur through the Grid, Admin, or Client Networks, or the combinations of these networks as illustrated in the network topology examples.

- **Management connections:** Inbound connections from an administrator to the node, usually through SSH. Web browser access to the Grid Manager, the Tenant Manager, and the StorageGRID Appliance Installer.
- **NTP server connections:** Outbound UDP connection that receives an inbound UDP response.

At least one NTP server must be reachable by the primary Admin Node.

- **DNS server connections:** Outbound UDP connection that receives an inbound UDP response.
- **LDAP/Active Directory server connections:** Outbound TCP connection from the Identity service on Storage Nodes.
- **AutoSupport:** Outbound TCP connection from the Admin Nodes to either `support.netapp.com` or a customer-configured proxy.
- **External key management server:** Outbound TCP connection from each appliance node with node encryption enabled.
- Inbound TCP connections from S3 and Swift clients.
- Outbound requests from StorageGRID platform services such as CloudMirror replication or from Cloud Storage Pools.

If StorageGRID is unable to make contact with any of the provisioned NTP or DNS servers using the default routing rules, it will automatically attempt contact on all networks (Grid, Admin, and Client) as long as the IP addresses of the DNS and NTP servers are specified. If the NTP or DNS servers can be reached on any network, StorageGRID will automatically create additional routing rules to ensure that network is used for all future attempts to connect to it.



Although you can use these automatically discovered host routes, in general you should manually configure the DNS and NTP routes to ensure connectivity in case automatic discovery fails.

If you are not ready to configure the optional Admin and Client Networks during deployment, you can configure these networks when you approve grid nodes during the configuration steps. Additionally, you can configure these networks after installation, using the Change IP tool (see [Configure IP addresses](#)).

Only S3 and Swift client connections and SSH, Grid Manager, and Tenant Manager administrative connections are supported over VLAN interfaces. Outbound connections, such as to NTP, DNS, LDAP, AutoSupport, and KMS servers, must go over the Client, Admin, or Grid Network interfaces directly. If the interface is configured as a trunk to support VLAN interfaces, this traffic will flow over the interface's native VLAN, as configured at the switch.

Wide Area Networks (WANs) for multiple sites

When configuring a StorageGRID system with multiple sites, the WAN connection between sites must have a minimum bandwidth of 25 Mbit/second in each direction before accounting for client traffic. Data replication or erasure coding between sites, node or site expansion, node recovery, and other operations or configurations will require additional bandwidth.

Connections for Admin Nodes and Gateway Nodes

Admin Nodes must always be secured from untrusted clients, such as those on the open internet. You must ensure that no untrusted client can access any Admin Node on the Grid Network, the Admin Network, or the Client Network.

Admin Nodes and Gateway Nodes that you plan to add to high availability groups must be configured with a static IP address. For more information, see [Manage high availability groups](#).

Using network address translation (NAT)

Do not use network address translation (NAT) on the Grid Network between grid nodes or between StorageGRID sites. When you use private IPv4 addresses for the Grid Network, those addresses must be directly routable from every grid node at every site. As required, however, you can use NAT between external clients and grid nodes, such as to provide a public IP address for a Gateway Node. Using NAT to bridge a public network segment is supported only when you employ a tunneling application that is transparent to all nodes in the grid, meaning the grid nodes require no knowledge of public IP addresses.

Network-specific requirements

Follow the requirements for each StorageGRID network type.

Network gateways and routers

- If set, the gateway for a given network must be within the specific network's subnet.
- If you configure an interface using static addressing, you must specify a gateway address other than 0.0.0.0.
- If you do not have a gateway, the best practice is to set the gateway address to be the IP address of the network interface.

Subnets



Each network must be connected to its own subnet that does not overlap with any other network on the node.

The following restrictions are enforced by the Grid Manager during deployment. They are provided here to assist in pre-deployment network planning.

- The subnet mask for any network IP address cannot be 255.255.255.254 or 255.255.255.255 (/31 or /32 in CIDR notation).
- The subnet defined by a network interface IP address and subnet mask (CIDR) cannot overlap the subnet of any other interface configured on the same node.
- The Grid Network subnet for each node must be included in the GNSL.
- The Admin Network subnet cannot overlap the Grid Network subnet, the Client Network subnet, or any

subnet in the GNSL.

- The subnets in the AESL cannot overlap with any subnets in the GNSL.
- The Client Network subnet cannot overlap the Grid Network subnet, the Admin Network subnet, any subnet in the GNSL, or any subnet in the AESL.

Grid Network

- At deployment time, each grid node must be attached to the Grid Network and must be able to communicate with the primary Admin Node using the networking configuration you specify when deploying the node.
- During normal grid operations, each grid node must be able to communicate with all other grid nodes over the Grid Network.



The Grid Network must be directly routable between each node. Network address translation (NAT) between nodes is not supported.

- If the Grid Network consists of multiple subnets, add them to the Grid Network Subnet List (GNSL). Static routes are created on all nodes for each subnet in the GNSL.
- If the Grid Network interface is configured as a trunk to support VLAN interfaces, the trunk native VLAN must be the VLAN used for Grid Network traffic. All grid nodes must be accessible over the trunk native VLAN.

Admin Network

The Admin Network is optional. If you plan to configure an Admin Network, follow these requirements and guidelines.

Typical uses of the Admin Network include management connections, AutoSupport, KMS, and connections to critical servers such as NTP, DNS, and LDAP if these connections are not provided through the Grid Network or Client Network.



The Admin Network and AESL can be unique to each node, as long as the desired network services and clients are reachable.



You must define at least one subnet on the Admin Network to enable inbound connections from external subnets. Static routes are automatically generated on each node for each subnet in the AESL.

Client Network

The Client Network is optional. If you plan to configure a Client Network, note the following considerations.

- The Client Network is designed to support traffic from S3 and Swift clients. If configured, the Client Network gateway becomes the node's default gateway.
- If you use a Client Network, you can help secure StorageGRID from hostile attacks by accepting inbound client traffic only on explicitly configured load balancer endpoints. See [Configure load balancer endpoints](#).
- If the Client Network interface is configured as a trunk to support VLAN interfaces, consider whether configuring the Client Network interface (eth2) is necessary. If configured, Client Network traffic will flow over the trunk native VLAN, as configured in the switch.

Deployment-specific networking considerations

Linux deployments

For efficiency, reliability, and security, the StorageGRID system runs on Linux as a collection of container engines. Container engine-related network configuration is not required in a StorageGRID system.

Use a non-bond device, such as a VLAN or virtual Ethernet (veth) pair, for the container network interface. Specify this device as the network interface in the node configuration file.



Do not use bond or bridge devices directly as the container network interface. Doing so could prevent node start-up because of a kernel issue with the use of macvlan with bond and bridge devices in the container namespace.

See the installation instructions for [Red Hat Enterprise Linux or CentOS](#) or [Ubuntu or Debian](#) deployments.

Host network configuration for container engine deployments

Before starting your StorageGRID deployment on a container engine platform, determine which networks (Grid, Admin, Client) each node will use. You must ensure that each node's network interface is configured on the correct virtual or physical host interface, and that each network has sufficient bandwidth.

Physical hosts

If you are using physical hosts to support grid nodes:

- Make sure all hosts use the same host interface for each node interface. This strategy simplifies host configuration and enables future node migration.
- Obtain an IP address for the physical host itself.



A physical interface on the host can be used by the host itself and one or more nodes running on the host. Any IP addresses assigned to the host or nodes using this interface must be unique. The host and the node cannot share IP addresses.

- Open the required ports to the host.
- If you intend to use VLAN interfaces in StorageGRID, the host must have one or more trunk interfaces that provide access to the desired VLANs. These interfaces can be passed into the node container as eth0, eth2, or as additional interfaces. To add trunk or access interfaces, see the following:
 - **RHEL or CentOS (before installing the node):** [Create node configuration files](#)
 - **Ubuntu or Debian (before installing the node):** [Create node configuration files](#)
 - **RHEL, CentOS, Ubuntu, or Debian (after installing the node):** [Linux: Add trunk or access interfaces to a node](#)

Minimum bandwidth recommendations

The following table provides the minimum bandwidth recommendations for each type of StorageGRID node and each type of network. You must provision each physical or virtual host with sufficient network bandwidth to meet the aggregate minimum bandwidth requirements for the total number and type of StorageGRID nodes you plan to run on that host.

| Type of node | Type of network | | |
|--------------|-----------------|--------|---------|
| | Grid | Admin | Client |
| Admin | 10 Gbps | 1 Gbps | 1 Gbps |
| Gateway | 10 Gbps | 1 Gbps | 10 Gbps |
| Storage | 10 Gbps | 1 Gbps | 10 Gbps |
| Archive | 10 Gbps | 1 Gbps | 10 Gbps |



This table does not include SAN bandwidth, which is required for access to shared storage. If you are using shared storage accessed over Ethernet (iSCSI or FCoE), you should provision separate physical interfaces on each host to provide sufficient SAN bandwidth. To avoid introducing a bottleneck, SAN bandwidth for a given host should roughly match the aggregate Storage Node network bandwidth for all Storage Nodes running on that host.

Use the table to determine the minimum number of network interfaces to provision on each host, based on the number and type of StorageGRID nodes you plan to run on that host.

For example, to run one Admin Node, one Gateway Node, and one Storage Node on a single host:

- Connect the Grid and Admin Networks on the Admin Node (requires $10 + 1 = 11$ Gbps)
- Connect the Grid and Client Networks on the Gateway Node (requires $10 + 10 = 20$ Gbps)
- Connect the Grid Network on the Storage Node (requires 10 Gbps)

In this scenario, you should provide a minimum of $11 + 20 + 10 = 41$ Gbps of network bandwidth, which could be met by two 40 Gbps interfaces or five 10 Gbps interfaces, potentially aggregated into trunks and then shared by the three or more VLANs carrying the Grid, Admin, and Client subnets local to the physical data center containing the host.

For some recommended ways of configuring physical and network resources on the hosts in your StorageGRID cluster to prepare for your StorageGRID deployment, see the following:

- [Configure the host network \(Red Hat Enterprise Linux or CentOS\)](#)
- [Configure the host network \(Ubuntu or Debian\)](#)

Networking and ports for platform services and Cloud Storage Pools

If you plan to use StorageGRID platform services or Cloud Storage Pools, you must configure grid networking and firewalls to ensure that the destination endpoints can be reached.

Networking for platform services

As described in [Manage platform services for tenants](#) and [What are platform services](#), platform services include external services that provide search integration, event notification, and CloudMirror replication.

Platform services require access from Storage Nodes that host the StorageGRID ADC service to the external

service endpoints. Examples for providing access include:

- On the Storage Nodes with ADC services, configure unique Admin Networks with AESL entries that route to the target endpoints.
- Rely on the default route provided by a Client Network. If you use the default route, you can use the [untrusted Client Network feature](#) to restrict inbound connections.

Networking for Cloud Storage Pools

Cloud Storage Pools also require access from Storage Nodes to the endpoints provided by the external service used, such as Amazon S3 Glacier or Microsoft Azure Blob storage. For information, see [What a Cloud Storage Pool is](#).

Ports for platform services and Cloud Storage Pools

By default, platform services and Cloud Storage Pool communications use the following ports:

- **80**: For endpoint URIs that begin with `http`
- **443**: For endpoint URIs that begin with `https`

A different port can be specified when the endpoint is created or edited. See [Network port reference](#).

If you use a non-transparent proxy server, you must also [configure storage proxy settings](#) to allow messages to be sent to external endpoints, such as an endpoint on the internet.

VLANs and platform services and Cloud Storage Pools

You cannot use VLAN networks for platform services or Cloud Storage Pools. The destination endpoints must be reachable over the Grid, Admin, or Client Network.

Appliance nodes

You can configure the network ports on StorageGRID appliances to use the port bond modes that meet your requirements for throughput, redundancy, and failover.

The 10/25-GbE ports on the StorageGRID appliances can be configured in Fixed or Aggregate bond mode for connections to the Grid Network and Client Network.

The 1-GbE Admin Network ports can be configured in Independent or Active-Backup mode for connections to the Admin Network.

See the information about port bond modes in the installation and maintenance instructions for your appliance:

- [SG100 and SG1000 services appliances](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

Network installation and provisioning

You must understand how the Grid Network and the optional Admin and Client Networks are used during node deployment and grid configuration.

Initial deployment of a node

When you first deploy a node, you must attach the node to the Grid Network and ensure it has access to the primary Admin Node. If the Grid Network is isolated, you can configure the Admin Network on the primary Admin Node for configuration and installation access from outside the Grid Network.

A Grid Network with a gateway configured becomes the default gateway for a node during deployment. The default gateway allows grid nodes on separate subnets to communicate with the primary Admin Node before the grid has been configured.

If necessary, subnets containing NTP servers or requiring access to the Grid Manager or API can also be configured as grid subnets.

Automatic node registration with primary Admin Node

After the nodes are deployed, they register themselves with the primary Admin Node using the Grid Network. You can then use the Grid Manager, the `configure-storagegrid.py` Python script, or the Installation API to configure the grid and approve the registered nodes. During grid configuration, you can configure multiple grid subnets. Static routes to these subnets through the Grid Network gateway will be created on each node when you complete grid configuration.

Disabling the Admin Network or Client Network

If you want to disable the Admin Network or Client Network, you can remove the configuration from them during the node approval process, or you can use the Change IP tool after installation is complete (see [Configure IP addresses](#)).

Post-installation guidelines

After completing grid node deployment and configuration, follow these guidelines for DHCP addressing and network configuration changes.

- If DHCP was used to assign IP addresses, configure a DHCP reservation for each IP address on the networks being used.

You can only set up DHCP during the deployment phase. You cannot set up DHCP during configuration.



Nodes reboot when their IP addresses change, which can cause outages if a DHCP address change affects multiple nodes at the same time.

- You must use the Change IP procedures if you want to change IP addresses, subnet masks, and default gateways for a grid node. See [Configure IP addresses](#).
- If you make networking configuration changes, including routing and gateway changes, client connectivity to the primary Admin Node and other grid nodes might be lost. Depending on the networking changes applied, you might need to re-establish these connections.

Network port reference

You must ensure the network infrastructure can provide internal and external communication between nodes within the grid and to external clients and services. You might need access across internal and external firewalls, switching systems, and routing systems.

Use the details provided for [Internal grid node communications](#) and [External communications](#) to determine how to configure each required port.

Internal grid node communications

The StorageGRID internal firewall only allows incoming connections to specific ports on the Grid Network, with the exception of ports 22, 80, 123, and 443 (see the information about external communications). Connections are also accepted on ports defined by load balancer endpoints.



NetApp recommends that you enable Internet Control Message Protocol (ICMP) traffic between grid nodes. Allowing ICMP traffic can improve failover performance when a grid node cannot be reached.

In addition to ICMP and the ports listed in the table, StorageGRID uses the Virtual Router Redundancy Protocol (VRRP). VRRP is an internet protocol that uses IP protocol number 112. StorageGRID uses VRRP in unicast mode only. VRRP is required only if [high availability groups](#) are configured.

Guidelines for Linux-based nodes

If enterprise networking policies restrict access to any of these ports, you can remap ports at deployment time using a deployment configuration parameter. For more information about port remapping and deployment configuration parameters, see:

- [Install Red Hat Enterprise Linux or CentOS](#)
- [Install Ubuntu or Debian](#)

Guidelines for VMware-based nodes

Configure the following ports only if you need to define firewall restrictions that are external to VMware networking.

If enterprise networking policies restrict access to any of these ports, you can remap ports when you deploy nodes using the VMware vSphere Web Client, or by using a configuration file setting when automating grid node deployment. For more information about port remapping and deployment configuration parameters, see [Install VMware](#).

Guidelines for appliance nodes

If enterprise networking policies restrict access to any of these ports, you can remap ports using the StorageGRID Appliance Installer. For more information about port remapping for appliances, see:

- [SG100 and SG1000 services appliances](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

StorageGRID internal ports

| Port | TCP or UDP | From | To | Details |
|------|------------|------|----|---------|
|------|------------|------|----|---------|

| | | | | |
|------|-----|--------------------|------------------------|--|
| 22 | TCP | Primary Admin Node | All nodes | For maintenance procedures, the primary Admin Node must be able to communicate with all other nodes using SSH on port 22. Allowing SSH traffic from other nodes is optional. |
| 80 | TCP | Appliances | Primary Admin Node | Used by StorageGRID appliances to communicate with the primary Admin Node to start the installation. |
| 123 | UDP | All nodes | All nodes | Network time protocol service. Every node synchronizes its time with every other node using NTP. |
| 443 | TCP | All nodes | Primary Admin Node | Used for communicating status to the primary Admin Node during installation and other maintenance procedures. |
| 1139 | TCP | Storage Nodes | Storage Nodes | Internal traffic between Storage Nodes. |
| 1501 | TCP | All nodes | Storage Nodes with ADC | Reporting, auditing, and configuration internal traffic. |
| 1502 | TCP | All nodes | Storage Nodes | S3- and Swift-related internal traffic. |
| 1504 | TCP | All nodes | Admin Nodes | NMS service reporting and configuration internal traffic. |

| | | | | |
|------|-----|---------------|--------------------|---|
| 1505 | TCP | All nodes | Admin Nodes | AMS service internal traffic. |
| 1506 | TCP | All nodes | All nodes | Server status internal traffic. |
| 1507 | TCP | All nodes | Gateway Nodes | Load balancer internal traffic. |
| 1508 | TCP | All nodes | Primary Admin Node | Configuration management internal traffic. |
| 1509 | TCP | All nodes | Archive Nodes | Archive Node internal traffic. |
| 1511 | TCP | All nodes | Storage Nodes | Metadata internal traffic. |
| 5353 | UDP | All nodes | All nodes | Optionally used for full-grid IP changes and for primary Admin Node discovery during installation, expansion, and recovery. |
| 7001 | TCP | Storage Nodes | Storage Nodes | Cassandra TLS inter-node cluster communication. |
| 7443 | TCP | All Nodes | Admin Nodes | Internal traffic for maintenance procedures and error reporting. |
| 9042 | TCP | Storage Nodes | Storage Nodes | Cassandra client port. |
| 9999 | TCP | All nodes | All nodes | Internal traffic for multiple services. Includes maintenance procedures, metrics, and networking updates. |

| | | | | |
|-------|-----|-----------------------|------------------------|---|
| 10226 | TCP | Storage Nodes | Primary Admin Node | Used by StorageGRID appliances for forwarding AutoSupport messages from E-Series SANtricity System Manager to the primary Admin Node. |
| 11139 | TCP | Archive/Storage Nodes | Archive/Storage Nodes | Internal traffic between Storage Nodes and Archive Nodes. |
| 18000 | TCP | Admin/Storage Nodes | Storage Nodes with ADC | Account service internal traffic. |
| 18001 | TCP | Admin/Storage Nodes | Storage Nodes with ADC | Identity Federation internal traffic. |
| 18002 | TCP | Admin/Storage Nodes | Storage Nodes | Internal API traffic related to object protocols. |
| 18003 | TCP | Admin/Storage Nodes | Storage Nodes with ADC | Platform services internal traffic. |
| 18017 | TCP | Admin/Storage Nodes | Storage Nodes | Data Mover service internal traffic for Cloud Storage Pools. |
| 18019 | TCP | Storage Nodes | Storage Nodes | Chunk service internal traffic for erasure coding. |
| 18082 | TCP | Admin/Storage Nodes | Storage Nodes | S3-related internal traffic. |
| 18083 | TCP | All nodes | Storage Nodes | Swift-related internal traffic. |
| 18200 | TCP | Admin/Storage Nodes | Storage Nodes | Additional statistics about client requests. |

| | | | | |
|-------|-----|---------------------|------------------------|------------------------------------|
| 19000 | TCP | Admin/Storage Nodes | Storage Nodes with ADC | Keystone service internal traffic. |
|-------|-----|---------------------|------------------------|------------------------------------|

Related information

[External communications](#)

External communications

Clients need to communicate with grid nodes to ingest and retrieve content. The ports used depends on the object storage protocols chosen. These ports need to be accessible to the client.

Restricted access to ports

If enterprise networking policies restrict access to any of the ports, you can use [load balancer endpoints](#) to allow access on user-defined ports. You can then use [untrusted Client Networks](#) to allow access only on load balancer endpoint ports.

Port remapping

To use systems and protocols such as SMTP, DNS, SSH, or DHCP, you must remap ports when deploying nodes. However, you should not remap load balancer endpoints. For information about port remapping, see the installation instructions for your platform:

Software-based nodes

- [Install Red Hat Enterprise Linux or CentOS](#)
- [Install Ubuntu or Debian](#)
- [Install VMware](#)

Appliance nodes

- [SG100 and SG1000 services appliances](#)
- [SG6000 storage appliances](#)
- [SG5700 storage appliances](#)
- [SG5600 storage appliances](#)

Ports used for external communications

The following table shows the ports used for traffic into the nodes.



This list does not include ports that might be configured as [load balancer endpoints](#).

| Port | TCP or UDP | Protocol | From | To | Details |
|------|------------|----------|------------------------|--------------|---|
| 22 | TCP | SSH | Service laptop | All nodes | SSH or console access is required for procedures with console steps. Optionally, you can use port 2022 instead of 22. |
| 25 | TCP | SMTP | Admin Nodes | Email server | Used for alerts and email-based AutoSupport. You can override the default port setting of 25 using the Email Servers page. |
| 53 | TCP/ UDP | DNS | All nodes | DNS servers | Used for domain name system. |
| 67 | UDP | DHCP | All nodes | DHCP service | Optionally used to support DHCP-based network configuration. The dhclient service does not run for statically-configured grids. |
| 68 | UDP | DHCP | DHCP service | All nodes | Optionally used to support DHCP-based network configuration. The dhclient service does not run for grids that use static IP addresses. |
| 80 | TCP | HTTP | Browser | Admin Nodes | Port 80 redirects to port 443 for the Admin Node user interface. |
| 80 | TCP | HTTP | Browser | Appliances | Port 80 redirects to port 8443 for the StorageGRID Appliance Installer. |
| 80 | TCP | HTTP | Storage Nodes with ADC | AWS | Used for platform services messages sent to AWS or other external services that use HTTP. Tenants can override the default HTTP port setting of 80 when creating an endpoint. |

| Port | TCP or UDP | Protocol | From | To | Details |
|------|------------|----------|-------------------|--------------|---|
| 80 | TCP | HTTP | Storage Nodes | AWS | Cloud Storage Pools requests sent to AWS targets that use HTTP. Grid administrators can override the default HTTP port setting of 80 when configuring a Cloud Storage Pool. |
| 111 | TCP/ UDP | RPCBind | NFS client | Admin Nodes | Used by NFS-based audit export (portmap). Note: This port is required only if NFS-based audit export is enabled. |
| 123 | UDP | NTP | Primary NTP nodes | External NTP | Network time protocol service. Nodes selected as primary NTP sources also synchronize clock times with the external NTP time sources. |
| 137 | UDP | NetBIOS | SMB client | Admin Nodes | Used by SMB-based audit export for clients that require NetBIOS support. Note: This port is required only if SMB-based audit export is enabled. |
| 138 | UDP | NetBIOS | SMB client | Admin Nodes | Used by SMB-based audit export for clients that require NetBIOS support. Note: This port is required only if SMB-based audit export is enabled. |
| 139 | TCP | SMB | SMB client | Admin Nodes | Used by SMB-based audit export for clients that require NetBIOS support. Note: This port is required only if SMB-based audit export is enabled. |

| Port | TCP or UDP | Protocol | From | To | Details |
|------|------------|--------------------|------------------------|---------------------------|---|
| 161 | TCP/ UDP | SNMP | SNMP client | All nodes | <p>Used for SNMP polling. All nodes provide basic information; Admin Nodes also provide alert and alarm data. Defaults to UDP port 161 when configured.</p> <p>Note: This port is only required, and is only opened on the node firewall if SNMP is configured. If you plan to use SNMP, you can configure alternate ports.</p> <p>Note: For information about using SNMP with StorageGRID, contact your NetApp account representative.</p> |
| 162 | TCP/ UDP | SNMP Notifications | All nodes | Notification destinations | <p>Outbound SNMP notifications and traps default to UDP port 162.</p> <p>Note: This port is only required if SNMP is enabled and notification destinations are configured. If you plan to use SNMP, you can configure alternate ports.</p> <p>Note: For information about using SNMP with StorageGRID, contact your NetApp account representative.</p> |
| 389 | TCP/ UDP | LDAP | Storage Nodes with ADC | Active Directory/LDAP | Used for connecting to an Active Directory or LDAP server for Identity Federation. |
| 443 | TCP | HTTPS | Browser | Admin Nodes | Used by web browsers and management API clients for accessing the Grid Manager and Tenant Manager. |
| 443 | TCP | HTTPS | Admin Nodes | Active Directory | Used by Admin Nodes connecting to Active Directory if single sign-on (SSO) is enabled. |

| Port | TCP or UDP | Protocol | From | To | Details |
|------|------------|----------|------------------------|-------------|---|
| 443 | TCP | HTTPS | Archive Nodes | Amazon S3 | Used for accessing Amazon S3 from Archive Nodes. |
| 443 | TCP | HTTPS | Storage Nodes with ADC | AWS | Used for platform services messages sent to AWS or other external services that use HTTPS. Tenants can override the default HTTP port setting of 443 when creating an endpoint. |
| 443 | TCP | HTTPS | Storage Nodes | AWS | Cloud Storage Pools requests sent to AWS targets that use HTTPS. Grid administrators can override the default HTTPS port setting of 443 when configuring a Cloud Storage Pool. |
| 445 | TCP | SMB | SMB client | Admin Nodes | Used by SMB-based audit export. Note: This port is required only if SMB-based audit export is enabled. |
| 903 | TCP | NFS | NFS client | Admin Nodes | Used by NFS-based audit export (<code>rpc.mountd</code>). Note: This port is required only if NFS-based audit export is enabled. |
| 2022 | TCP | SSH | Service laptop | All nodes | SSH or console access is required for procedures with console steps. Optionally, you can use port 22 instead of 2022. |
| 2049 | TCP | NFS | NFS client | Admin Nodes | Used by NFS-based audit export (<code>nfs</code>). Note: This port is required only if NFS-based audit export is enabled. |

| Port | TCP or UDP | Protocol | From | To | Details |
|------|------------|----------|----------------|---------------|--|
| 5696 | TCP | KMIP | Appliance | KMS | Key Management Interoperability Protocol (KMIP) external traffic from appliances configured for node encryption to the Key Management Server (KMS), unless a different port is specified on the KMS configuration page of the StorageGRID Appliance Installer. |
| 8022 | TCP | SSH | Service laptop | All nodes | SSH on port 8022 grants access to the base operating system on appliance and virtual node platforms for support and troubleshooting. This port is not used for Linux-based (bare metal) nodes and is not required to be accessible between grid nodes or during normal operations. |
| 8082 | TCP | HTTPS | S3 clients | Gateway Nodes | S3 client traffic to the deprecated CLB service on Gateway Nodes (HTTPS). |
| 8083 | TCP | HTTPS | Swift clients | Gateway Nodes | Swift client traffic to the deprecated CLB service on Gateway Nodes (HTTPS). |
| 8084 | TCP | HTTP | S3 clients | Gateway Nodes | S3 client traffic to the deprecated CLB service on Gateway Nodes (HTTP). |
| 8085 | TCP | HTTP | Swift clients | Gateway Nodes | Swift client traffic to the deprecated CLB service on Gateway Nodes (HTTP). |
| 8443 | TCP | HTTPS | Browser | Admin Nodes | Optional. Used by web browsers and management API clients for accessing the Grid Manager. Can be used to separate Grid Manager and Tenant Manager communications. |

| Port | TCP or UDP | Protocol | From | To | Details |
|-------|------------|----------|--------------------------|---------------|---|
| 9022 | TCP | SSH | Service laptop | Appliances | Grants access to StorageGRID appliances in pre-configuration mode for support and troubleshooting. This port is not required to be accessible between grid nodes or during normal operations. |
| 9091 | TCP | HTTPS | External Grafana service | Admin Nodes | Used by external Grafana services for secure access to the StorageGRID Prometheus service. Note: This port is required only if certificate-based Prometheus access is enabled. |
| 9443 | TCP | HTTPS | Browser | Admin Nodes | Optional. Used by web browsers and management API clients for accessing the Tenant Manager. Can be used to separate Grid Manager and Tenant Manager communications. |
| 18082 | TCP | HTTPS | S3 clients | Storage Nodes | S3 client traffic directly to Storage Nodes (HTTPS). |
| 18083 | TCP | HTTPS | Swift clients | Storage Nodes | Swift client traffic directly to Storage Nodes (HTTPS). |
| 18084 | TCP | HTTP | S3 clients | Storage Nodes | S3 client traffic directly to Storage Nodes (HTTP). |
| 18085 | TCP | HTTP | Swift clients | Storage Nodes | Swift client traffic directly to Storage Nodes (HTTP). |

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.