About StorageGRID 11.5

StorageGRID

NetApp
October 03, 2025

Table of Contents

About StorageGRID 11.5

Before starting an upgrade, review this section to learn about the new features and enhancements in StorageGRID 11.5, determine whether any features have been deprecated or removed, and find out about changes to StorageGRID APIs.

- What's new in StorageGRID 11.5
- Removed or deprecated features
- Changes to the Grid Management API
- Changes to the Tenant Management API

What's new in StorageGRID 11.5

StorageGRID 11.5 introduces S3 Object Lock, support for KMIP encryption of data, usability improvements to ILM, a redesigned Tenant Manager user interface, support for decommissioning a StorageGRID site, and an appliance node clone procedure.

S3 Object Lock for compliant data

The S3 Object Lock feature in StorageGRID 11.5 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 and legal hold settings for the objects in those buckets.

S3 Object Lock lets tenant users comply with regulations that require certain objects to be retained for a fixed amount of time or indefinitely.

Learn more

- Manage objects with ILM
- Use S3
- Use a tenant account

KMS encryption key management

You can now configure one or more external key management servers (KMS) in the Grid Manager 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. After the appliance volumes are encrypted, you cannot access any data on the appliance unless the node can communicate with the KMS.

> ⓘ If you want to use encryption key management, you must use the StorageGRID Appliance Installer to enable the **Node Encryption** setting for the appliance before you add the appliance to the grid.

Learn more

- Administer StorageGRID

Usability enhancements for information lifecycle management (ILM)

- You can now view the total capacity of a storage pool, including the amount of used and free space. You can also see which nodes are included in a storage pool and which ILM rules and Erasure Coding profiles use the storage pool.
- You can now design ILM rules that apply to more than one tenant account.
- When you create an ILM rule for erasure coding, you are now reminded to set the Object Size (MB) advanced filter to greater than 0.2 to ensure that very small objects are not erasure coded.
- The ILM policy interface now ensures that the default ILM rule will be always be used for any objects not matched by another rule. Starting in StorageGRID 11.5, the default rule cannot use any basic or advanced filters and is automatically placed as the last rule in the policy.

  > ⓘ If your current ILM policy does not conform to the new requirements, you can continue to use it after you upgrade to StorageGRID 11.5. However, if you attempt to clone a non-conforming policy after you upgrade, you are prompted to select a default rule that does not include filters and you are required to place the default rule at the end of the policy.

- The stock All Storage Nodes storage pool is no longer selected by default when you create a new ILM rule or a new Erasure Coding profile. In addition, you can now remove the All Storage Nodes storage pool as long as it not used in any rule.

  > ⓘ Using the All Storage Nodes storage pool is not recommended because this storage pool contains all sites. Multiple copies of an object might be placed on the same site if you use this storage pool with a StorageGRID system that includes more than one site.

- You can now remove the stock Make 2 Copies rule (which uses the All Storage Nodes storage pool) as long as it is not used in an active or proposed policy.
- Objects stored in a Cloud Storage Pool can now be deleted immediately (synchronous deletion).

Learn more

- Manage objects with ILM

Enhancements to the Grid Manager

- The redesigned Tenant Accounts page makes it easier to view tenant account usage. The tenant summary table now includes columns for Space Used, Quota Utilization, Quota, and Object Count. A new **View Details** button accesses an overview of each tenant as well as details about the account’s S3 buckets or Swift containers. In addition, you can now export two `.csv` files for tenant usage: one containing usage values for all tenants and one containing details about a tenant’s buckets or containers.

  Related to this change, three new Prometheus metrics were added to track tenant account usage:

  - `storagegrid_tenant_usage_data_bytes`
  - `storagegrid_tenant_usage_object_count`
  - `storagegrid_tenant_usage_quota_bytes`

- The new **Access Mode** field on the Admin Groups page (**Configuration** > **Access Control**) allows you to specify whether the management permissions for the group are read-write (default) or read-only. Users who belong to a group with read-write access mode can change settings and perform operations in the Grid Manager and the Grid Management API. Users who belong to a group with read-only access mode can only view the settings and features that are selected for the group.

> ⓘ When you upgrade to StorageGRID 11.5, the read-write access mode option is selected for all existing admin groups.

- The AutoSupport user interface was redesigned. You can now configure event-triggered, user-triggered, and weekly AutoSupport messages from a single page in the Grid Manager. You can also configure an additional destination for AutoSupport messages.

> ⓘ If AutoSupport has not been enabled, a reminder message now appears on the Grid ManagerDashboard.

- When viewing the **Storage Used - Object Data** chart on the Nodes page, you can now see estimates for the amount of replicated object data and the amount of erasure-coded data on the grid, site, or Storage Node (**Nodes** > ***grid/site/Storage Node*** > **Storage**).
- Grid Manager menu options were reorganized to make options easier to find. For example, a new **Network Settings** submenu was added to the **Configuration** menu and options in the **Maintenance** and **Support** menus are now listed in alphabetic order.

Learn more

- Administer StorageGRID

Enhancements to the Tenant Manager

- The appearance and organization of the Tenant Manager user interface has been completely redesigned to improve the user experience.
- The new Tenant Manager dashboard provides a high-level summary of each account: it provides bucket details and shows the number of buckets or containers, groups, users, and platform services endpoints (if configured).

Learn more

- Use a tenant account

Client certificates for Prometheus metrics export

You can now upload or generate client certificates (**Configuration** > **Access Control** > **Client Certificates**), which can be used to provide secure, authenticated access to the StorageGRID Prometheus database. For example, you can use client certificates if you need to monitor StorageGRID externally using Grafana.

Learn more

- Administer StorageGRID

Load balancer enhancements

- When handling routing requests at a site, the Load Balancer service now performs load aware routing: it considers the CPU availability of the Storage Nodes at the same site. In some cases, information about CPU availability is limited to the site where the Load Balancer service is located.

> ⓘ CPU awareness will be not enabled until at least two-thirds of the Storage Nodes at a site have been upgraded to StorageGRID 11.5 and are reporting CPU statistics.

- For added security, you can now specify a binding mode for each load balancer endpoint. Endpoint pinning lets you restrict the accessibility of each endpoint to specific high availability groups or node interfaces.

Learn more

- Administer StorageGRID

Object metadata changes

- **New Actual reserved space metric**: To help you understand and monitor object metadata space usage on each Storage Node, a new Prometheus metric is shown on the Storage Used - Object Metadata graph for a Storage Node (**Nodes** > ***Storage Node*** > **Storage**).

  ```
  storagegrid_storage_utilization_metadata_reserved
  ```

  The **Actual reserved space** metric indicates how much space StorageGRID has reserved for object metadata on a specific Storage Node.

- **Metadata space increased for installations with larger Storage Nodes**: The system-wide Metadata Reserved Space setting has been increased for StorageGRID systems containing Storage Nodes with 128 GB or more of RAM, as follows:
  - **8 TB for new installations**: If you are installing a new StorageGRID 11.5 system and each Storage Node in the grid has 128 GB or more of RAM, the system-wide Metadata Reserved Space setting is now set to 8 TB instead of 3 TB.
  - **4 TB for upgrades**: If you are upgrading to StorageGRID 11.5 and each Storage Node at any one site has 128 GB or more of RAM, the system-wide Metadata Reserved Space setting is now set to 4 TB instead of 3 TB.

    The new values for the Metadata Reserved Space setting increase the allowed metadata space for these larger Storage Nodes, up to 2.64 TB, and ensure that adequate metadata space is reserved for future hardware and software versions.

    > ⓘ If your Storage Nodes have enough RAM and sufficient space on volume 0, you can manually increase the Metadata Reserved Space setting up to 8 TB after you upgrade. Reserving additional metadata space after the StorageGRID 11.5 upgrade will simplify future hardware and software upgrades.
    >
    > Increasing the Metadata Reserved Space setting

    > ⓘ If your StorageGRID system stores (or is expected to store) more than 2.64 TB of metadata on any Storage Node, the allowed metadata space can be increased in some cases. If your Storage Nodes each have available free space on storage volume 0 and more than 128 GB of RAM, contact your NetApp account representative. NetApp will review your requirements and increase the allowed metadata space for each Storage Node, if possible.

- **Automatic cleanup of deleted metadata**: When 20% or more of the metadata stored on a Storage Node is ready to be removed (because the corresponding objects were deleted), StorageGRID can now perform an automatic compaction on that Storage Node. This background process only runs if the load on the system is low—that is, when there is available CPU, disk space, and memory. The new compaction process removes metadata for deleted objects sooner than in previous releases and helps to free up space for new objects to be stored.

Learn more

- Administer StorageGRID

Changes to S3 REST API support

- You can now use the S3 REST API to specify S3 Object Lock settings:
  - To create a bucket with S3 Object Lock enabled, use a PUT Bucket request with the `x-amz-bucket-object-lock-enabled` header.
  - To determine if S3 Object Lock is enabled for a bucket, use a GET Object Lock Configuration request.
  - When adding an object version to a bucket with S3 Object Lock enabled, use the following request headers to specify the retention and legal hold settings: `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, and `x-amz-object-lock-legal-hold`.
- You can now use DELETE Multiple Objects on a versioned bucket.
- You can now use PUT, GET, and DELETE Bucket encryption requests to manage encryption for an existing S3 bucket.
- A minor change was made to a field name for the `Expiration` parameter. This parameter is included in the response to a PUT Object, HEAD Object, or GET Object request if an expiration rule in the lifecycle configuration applies to a specific object. The field that indicates which expiration rule was matched was previously named `rule_id`. This field was renamed to `rule-id` to match the AWS implementation.
- By default, the S3 GET Storage Usage request now attempts to retrieve the storage used by a tenant account and its buckets using strong-global consistency. If strong-global consistency cannot be achieved, StorageGRID attempts to retrieve the usage information using strong-site consistency.
- The `Content-MD5` request header is now correctly supported.

Learn more

- Use S3

Maximum size for CloudMirror objects increased to 5 TB

The maximum size for objects that can be replicated to a destination bucket by the CloudMirror replication service was increased to 5 TB, which is the maximum object size supported by StorageGRID.

Learn more

- Use S3
- Use Swift

New alerts added

The following new alerts were added for StorageGRID 11.5:

- Appliance BMC communication error
- Appliance Fibre Channel fault detected
- Appliance Fibre Channel HBA port failure
- Appliance LACP port missing

- Cassandra auto-compactor error
- Cassandra auto-compactor metrics out of date
- Cassandra compactions overloaded
- Disk I/O is very slow
- KMS CA certificate expiration
- KMS client certificate expiration
- KMS configuration failed to load
- KMS connectivity error
- KMS encryption key name not found
- KMS encryption key rotation failed
- KMS is not configured
- KMS key failed to decrypt an appliance volume
- KMS server certificate expiration
- Low free space for storage pool
- Node network reception frame error
- Services appliance storage connectivity degraded
- Storage appliance storage connectivity degraded (previously named Appliance storage connectivity degraded)
- Tenant quota usage high
- Unexpected node reboot

Learn more

- Monitor & troubleshoot

TCP support for SNMP traps

You can now select Transmission Control Protocol (TCP) as the protocol for SNMP trap destinations. Previously, only the User Datagram Protocol (UDP) protocol was supported.

Learn more

- Monitor & troubleshoot

Installation and networking enhancements

- **MAC address cloning**: You can now use MAC address cloning to enhance the security of certain environments. MAC address cloning enables you to use a dedicated virtual NIC for the Grid Network, Admin Network, and Client Network. Having the Docker container use the MAC address of the dedicated NIC on the host allows you to avoid using promiscuous mode network configurations. Three new MAC address cloning keys were added to the node configuration file for Linux-based (bare metal) nodes.
- **Automatic discovery of DNS and NTP host routes**: Previously, there were restrictions on which network your NTP and DNS servers had to connect to, such as the requirement that you could not have all of your NTP and DNS servers on the Client Network. Now, those restrictions are removed.

Learn more

- Install Red Hat Enterprise Linux or CentOS
- Install Ubuntu or Debian

Support for rebalancing erasure-coded (EC) data after Storage Node expansion

The EC rebalance procedure is a new command-line script that might be required after you add new Storage Nodes. When you perform the procedure, StorageGRID redistributes erasure-coded fragments among the existing and the newly expanded Storage Nodes at a site.

> ⓘ You should only perform the EC rebalance procedure in limited cases. For example, if you cannot add the recommended number of Storage Nodes in an expansion, you can use the EC rebalance procedure to allow additional erasure-coded objects to be stored.

Learn more

- Expand your grid

New and revised maintenance procedures

- **Site decommission**: You can now remove an operational site from your StorageGRID system. The connected site decommission procedure removes an operational site and preserves data. The new Decommission Site wizard guides you through the process (**Maintenance** > **Decommission** > **Decommission Site**).
- **Appliance node cloning**: You can now clone an existing appliance node to upgrade the node to a new appliance model. For example, you can clone a smaller-capacity appliance node to a larger-capacity appliance. You can also clone an appliance node to implement new functionality, such as the new **Node Encryption** setting that is required for the KMS encryption.
- **Ability to change the provisioning passphrase**: You can now change the provisioning passphrase (**Configuration** > **Access Control** > **Grid Passwords**). The passphrase is required for recovery, expansion, and maintenance procedures.
- **Enhanced SSH password behavior**: To enhance the security of StorageGRID appliances, the SSH password is no longer changed when you place an appliance into maintenance mode. In addition, new SSH host certificates and host keys are generated when you upgrade a node to StorageGRID 11.5.

  > ⓘ If you use SSH to log in to a node after upgrading to StorageGRID 11.5, you will receive a warning that the host key has changed. This behavior is expected and you can safely approve the new key.

Learn more

- Maintain & recover

Changes to StorageGRID appliances

- **Direct access to SANtricity System Manager for storage appliances**: You can now access the E-Series SANtricity System Manager user interface from the StorageGRID Appliance Installer and from the Grid Manager. Using these new methods enables access to SANtricity System Manager without using the management port on the appliance. Users who need to access SANtricity System Manager from the Grid Manager must have the new Storage Appliance Administrator permission.
- **Node encryption**: As part of the new KMS encryption feature, a new **Node Encryption** setting was added to the StorageGRID Appliance Installer. If you want to use encryption key management to protect appliance

data, you must enable this setting during the hardware configuration stage of appliance installation.

- **UDP port connectivity**: You can now test the network connectivity of a StorageGRID appliance to UDP ports, such as those used for an external NFS or DNS server. From the StorageGRID Appliance Installer, select **Configure Networking** > **Port Connectivity Test (nmap)**.
- **Automating installation and configuration**: A new JSON configuration upload page was added to the StorageGRID Appliance Installer (**Advanced** > **Update Appliance Configuration**). This page enables you to use one file to configure multiple appliances in large grids. Additionally, the `configure-sga.py` Python script has been updated to match the capabilities of the StorageGRID Appliance Installer.

Learn more

- SG100 & SG1000 services appliances
- SG6000 storage appliances
- SG5700 storage appliances
- SG5600 storage appliances

Changes to audit messages

- **Automatic cleanup of overwritten objects**: Previously, objects that were overwritten were not removed from disk in specific cases, which resulted in additional space consumption. These overwritten objects, which are inaccessible to users, are now automatically removed to save storage space. Refer to the LKCU audit message for more information.
- **New audit codes for S3 Object Lock**: Four new audit codes were added to the SPUT audit message to include S3 Object Lock request headers:
  - LKEN: Object Lock Enabled
  - LKLH: Object Lock Legal Hold
  - LKMD: Object Lock Retention Mode
  - LKRU: Object Lock Retain Until Date
- **New fields for Last Modified Time and Previous Object Size**: You can now track when an object was overwritten as well as the original object size.
  - The MTME (Last Modified Time) field was added to the following audit messages:
    - SDEL (S3 DELETE)
    - SPUT (S3 PUT)
    - WDEL (Swift DELETE)
    - WPUT (Swift PUT)
  - The CSIZ (Previous Object Size) field was added to the OVWR (Object Overwrite) audit message.

Learn more

- Review audit logs

New nms.requestlog file

A new log file, `/var/local/log/nms.requestlog`, is maintained on all Admin Nodes. This file contains information about outgoing connections from the Management API to internal StorageGRID services.

Learn more

- Monitor & troubleshoot

StorageGRID documentation changes

- To make networking information and requirements easier to find and to clarify that the information also applies to StorageGRID appliance nodes, the networking documentation was moved from the software-based installation guides (RedHat Enterprise Linux/CentOS, Ubuntu/Debian, and VMware) to a new networking guide.

  Network guidelines

- To make ILM-related instructions and examples easier to find, the documentation for managing objects with information lifecycle management was moved from the *Administrator Guide* to a new ILM guide.

  Manage objects with ILM

- A new FabricPool guide provides an overview of configuring StorageGRID as a NetApp FabricPool cloud tier and describes the best practices for configuring ILM and other StorageGRID options for a FabricPool workload.

  Configure StorageGRID for FabricPool

- You can now access several instructional videos from the Grid Manager. The current videos provide instructions for managing alerts, custom alerts, ILM rules, and ILM policies.

Removed or deprecated features

Some features were removed or deprecated in StorageGRID 11.5. You must review these items to understand whether you need to update client applications or modify your configuration before you upgrade.

Weak consistency control removed

The Weak consistency control was removed for StorageGRID 11.5. After you upgrade, the following behaviors will apply:

- Requests to set Weak consistency for an S3 bucket or Swift container will succeed, but the consistency level will actually be set to Available.
- Existing buckets and containers that use Weak consistency will be silently updated to use Available consistency.
- Requests that have a Weak consistency-control header will actually use Available consistency, if applicable.

The Available consistency control behaves the same as the “read-after-new-write” consistency level, but only provides eventual consistency for HEAD operations. The Available consistency control offers higher availability for HEAD operations than “read-after-new-write” if Storage Nodes are unavailable.

Alarm for grid health deprecated

The `/grid/health/topology` API, which checks for active *alarms* on nodes, is deprecated. In its place, a new `/grid/node-health` endpoint was added. This API returns the current status of each node by checking for active *alerts* on nodes.

Compliance feature deprecated

The S3 Object Lock feature in StorageGRID 11.5 replaces the Compliance feature that was available in previous StorageGRID versions. Because the new S3 Object Lock feature conforms to Amazon S3 requirements, it deprecates the proprietary StorageGRID Compliance feature, which is now referred to as “legacy Compliance.”

If you previously enabled the global Compliance setting, the new global S3 Object Lock setting is enabled automatically when you upgrade to StorageGRID 11.5. Tenant users will no longer be able to create new buckets with Compliance enabled in StorageGRID; however, as required, tenant users can continue to use and manage any existing legacy Compliant buckets.

In the Tenant Manager, a shield icon 🛡 indicates a legacy Compliant bucket. Legacy Compliant buckets might also have a hold badge HOLD to indicate that the bucket is under a legal hold.

KB: How to manage legacy Compliant buckets in StorageGRID 11.5

Manage objects with ILM

“S3 multipart part too small” alert removed

The **S3 multipart part too small** alert was removed. Previous, this alert was triggered if an S3 client attempted to complete a multipart upload with parts that did not meet Amazon S3 size limits. After the upgrade to StorageGRID 11.5, any multipart upload requests that do not meet the following size limits will fail:

- Each part in a multipart upload must be between 5 MiB (5,242,880 bytes) and 5 GiB (5,368,709,120 bytes).
- The last part can be smaller than 5 MiB (5,242,880 bytes).
- In general, part sizes should be as large as possible. For example, use part sizes of 5 GiB for a 100 GiB object. Since each part is considered a unique object, using large part sizes reduces StorageGRID metadata overhead.
- For objects smaller than 5 GiB, consider using non-multipart upload instead.

"Appliance link down on Grid Network" alerts removed

The following alerts were removed. If the Grid Network is down, the metrics that would trigger these alerts are not accessible:

- Services appliance link down on Grid Network
- Storage appliance link down on Grid Network

Support for fully qualified domain name removed from SNMP configuration

When configuring an SNMP server in the baseboard management controller (BMC) for the SG6000, SG100, or SG1000, you must now specify an IP address instead of a fully qualified domain name. If a fully qualified domain name was previously configured, change it to an IP address before upgrading to StorageGRID 11.5.

Legacy attributes removed

The following legacy attributes were removed. As applicable, equivalent information is provided by Prometheus metrics:

Legacy attribute	Equivalent Prometheus metric
BREC	storagegrid_service_network_received_bytes
BTRA	storagegrid_service_network_transmitted_bytes
CQST	storagegrid_metadata_queries_average_latency_milliseconds
HAIS	storagegrid_http_sessions_incoming_attempted
HCCS	storagegrid_http_sessions_incoming_currently_established
HEIS	storagegrid_http_sessions_incoming_failed
HISC	storagegrid_http_sessions_incoming_successful
LHAC	*none*
NREC	*none*
NTSO (Chosen Time Source Offset)	storagegrid_ntp_chosen_time_source_offset_milliseconds
NTRA	*none*
SLOD	storagegrid_service_load
SMEM	storagegrid_service_memory_usage_bytes
SUTM	storagegrid_service_cpu_seconds
SVUT	storagegrid_service_uptime_seconds
TRBS (Total bits per second received)	*none*
TRXB	storagegrid_network_received_bytes
TTBS (Total bits per second transmitted)	*none*
TTXB	storagegrid_network_transmitted_bytes

The following related changes were also made:

- The `network_received_bytes` and `network_transmitted_bytes` Prometheus metrics were changed from gauges to counters because the values of these metrics only increase. If you are currently using these metrics in Prometheus queries, you should start using the `increase()` function in the query.

- The Network Resources table was removed from the Resources tab for StorageGRID services. (Select **Support** > **Tools** > **Grid Topology**.Then, select ***node*** > ***service*** > **Resources**.)
- The HTTP Sessions page was removed for Storage Nodes. Previously, you could access this page by selecting **Support** > **Tools** > **Grid Topology** and then selecting ***Storage Node*** > **LDR** > **HTTP**.
- The HCCS (Currently Established Incoming Sessions) alarm was removed.
- The NTSO (Chosen Time Source Offset) alarm was removed.

Changes to the Grid Management API

StorageGRID 11.5 uses version 3 of the Grid Management API. Version 3 deprecates version 2; however, version 1 and version 2 are still supported.

> You can continue to use version 1 and version 2 of the management API with StorageGRID 11.5; however, support for these versions of the API will be removed in a future release of StorageGRID. After upgrading to StorageGRID 11.5, the deprecated v1 and v2 APIs can be deactivated using the `PUT /grid/config/management` API.

New client-certificates section

The new section, `/grid/client-certificates`, allows you to configure client certificates to provide secure, authenticated access to the StorageGRID Prometheus database. For example, you can monitor StorageGRID externally using Grafana.

Legacy compliance endpoints moved to new s3-object-lock section

With the introduction of StorageGRID S3 Object Lock, the APIs used to manage the legacy compliance settings for the grid were moved to a new section of the Swagger user interface. The **s3-object-lock** section includes the two `/grid/compliance-global` API endpoints, which now control the global S3 Object Lock setting. The endpoint URIs remain unchanged for compatibility with existing applications.

Swift-admin-password Accounts endpoint removed

The following Accounts API endpoint, which was deprecated in StorageGRID 10.4, has now been removed:

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

New grid-passwords section

The **grid-passwords** section enables operations for grid password management. The section includes two `/grid/change-provisioning-passphrase` API endpoints. The endpoints allow users to change the StorageGRID provisioning passphrase and retrieve the status of the passphrase change.

storageAdmin permission added to Groups API

The `/grid/groups` API now includes the storageAdmin permission.

New parameter for Storage Usage API

The `GET /grid/accounts/{id}/usage` API now has a `strictConsistency` parameter. To enforce a strong-global consistency when retrieving storage usage information across Storage Nodes, set this parameter to `true`. When this parameter is set to `false` (default), StorageGRID attempts to retrieve usage information using strong-global consistency, but falls back to strong-site consistency if strong-global consistency cannot be met.

New Node Health API

A new `/grid/node-health` endpoint was added. This API returns the current status of each node by checking for active *alerts* on the nodes. The `/grid/health/topology` API, which checks for active *alarms* on nodes, is deprecated.

Change to "ApplianceStorageShelvesPowerSupplyDegraded" alert rule ID

The alert rule ID "ApplianceStorageShelvesPowerSupplyDegraded" has been renamed to "ApplianceStorageShelvesDegraded" to better reflect the alert’s actual behavior.

Related information

Administer StorageGRID

Changes to the Tenant Management API

StorageGRID 11.5 uses version 3 of the Tenant Management API. Version 3 deprecates version 2; however, version 1 and version 2 are still supported.

> You can continue to use version 1 and version 2 of the management API with StorageGRID 11.5; however, support for these versions of the API will be removed in a future release of StorageGRID. After upgrading to StorageGRID 11.5, the deprecated v1 and v2 APIs can be deactivated using the `PUT /grid/config/management` API.

New parameter for tenant Storage Usage API

The `GET /org/usage` API now has a `strictConsistency` parameter. To enforce a strong-global consistency when retrieving storage usage information across Storage Nodes, set this parameter to `true`. When this parameter is set to `false` (default), StorageGRID attempts to retrieve usage information using strong-global consistency, but falls back to strong-site consistency if strong-global consistency cannot be met.

Related information

Use S3

Use a tenant account