



Release notes

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from <https://docs.netapp.com/us-en/storagegrid/release-notes/whats-new.html> on July 22, 2026. Always check docs.netapp.com for the latest.

Table of Contents

- Release notes 1
 - What's new in StorageGRID 12.1 1
 - Capacity 1
 - Control access 1
 - Federation 1
 - Manageability 1
 - S3 1
 - Security 2
 - Tenants 2
 - Upgrade 3
 - User interface 3
 - Removed or deprecated features and capabilities in StorageGRID 3
 - Definitions 4
 - StorageGRID end of feature support 4
 - Changes to the Grid Management API in StorageGRID 5
 - New endpoints for changing the BMC password and LAN IP settings 6
 - Changes to the Tenant Management API in StorageGRID 6
 - New API for object replication 6
 - Changes to StorageGRID S3 REST API support 6

Release notes

What's new in StorageGRID 12.1

StorageGRID 12.1 introduces the following features and functional changes.

For details about fixed issues and known issues in recent StorageGRID 12.1 releases, refer to the [StorageGRID 12.1 Release notes](#). You must sign in with your NetApp account or create an account to access the Release notes.

Capacity

EC rebalance now uses free space

EC rebalance now uses free space instead of used space. Refer to [Learn about EC rebalancing after expansion in StorageGRID](#).

Metadata allowed space

You can now increase the maximum allowed metadata value from 3.96 TB to 7.92 TB. Refer to [Allowed metadata space](#).

Control access

SSO using OIDC

You can now [set up single sign-on \(SSO\) in StorageGRID using OpenID Connect \(OIDC\)](#).

Federation

Global namespace

You can now set up a global namespace to allow tenants to access buckets across multiple StorageGRID systems. Refer to [Learn about global namespace](#).

Manageability

Auto-move ADC service

[When required to meet the ADC quorum](#), the ADC service will now be moved automatically when you're converting a Storage Node to a data-only node or decommissioning a Storage Node.

Primary Admin Node recovery

You can now recover any node from a non-primary Admin Node. Refer to [Recovering from primary Admin Node failures](#).

S3

Enable S3 Object Lock on existing buckets

When the allow S3 Object Lock for existing buckets setting is enabled, an S3 tenant account can now enable S3 Object Lock for an existing bucket. After an S3 tenant account enables S3 Object Lock for an existing bucket, it can't be disabled.

Replication allowed for S3 Object Lock-enabled buckets

You can now use CloudMirror to replicate objects in S3 Object Lock-enabled buckets. Refer to [Learn about platform services](#).

Enable cross-grid replication for non-empty buckets

You can now enable cross-grid replication for buckets that aren't empty. Refer to [Requirements for cross-grid replication](#).

S3 Batch operations (FPVR only)

You can use S3 batch operations to replicate existing objects in a versioning-enabled bucket that you plan to configure for cross-grid replication.

This feature requires FPVR approval for StorageGRID 12.1. To use this feature, contact your account representative.

Non-functional S3 REST API headers

The `If-Match` and `If-None-Match` headers are accepted but non-functional for the S3 REST API [PutObject](#), [CompleteMultipartUpload](#), [CopyObject](#), and [DeleteObject](#).

For additional information, refer to [Changes to StorageGRID S3 REST API support](#).

Support for pre-calculated checksum values

The S3 REST SPI now provides support for pre-calculated checksum values and the `x-amz-checksum-type` request header. Refer to [Updates to REST API support](#).

Security

Multi-admin verification

Multi-admin verification (MAV) helps prevent accidental or unauthorized changes to your StorageGRID system. Refer to [Learn about StorageGRID multi-admin verification](#).

Security policy updates for FIPS

The FIPS strict policy criteria have been updated. Refer to [Select a security policy in Manage the TLS and SSH policy](#).

Tenants

Account sync

The *account clone* feature now refers to a one-time clone of specific tenant account information.

Account sync is a new feature that allows you to automatically and continuously replicate tenant account, tenant groups, tenant users, and S3 access keys among the StorageGRID systems in one or more grid federation connections. Refer to [Learn about account sync in StorageGRID](#).

Kafka endpoints and mTLS authentication

Mutual Transport Layer Security (mTLS) is now supported for Kafka endpoints. Refer to [Configure platform services endpoints](#).

Maximum number of buckets

A StorageGRID system now supports a maximum of 20,000 buckets for each S3 tenant account.

Upgrade

Time to enable features is increased

During StorageGRID upgrade to version 12.1, the time to enable features has increased from under five minutes to an hour. Refer to [Estimate the time to complete a StorageGRID upgrade](#).

User interface

BMC settings page

A new BMC Settings tab has been added to the Nodes page in Grid Manager to allow BMC password reset and changes to the BMC LAN IP settings. Refer to [Change appliance BMC password](#) and [Change appliance node BMC LAN IP settings](#). New API endpoints have also been added to support these functions. Refer to [New endpoints for changing the BMC password and LAN IP settings](#).

Email notifications

The Grid Manager now has a common email page to configure and manage email notifications for alerts, AutoSupport, and multi-admin verification (MAV). Refer to [Configure email server](#).

Link cost page update

StorageGRID 12.1 provides more detailed Link cost information and settings. Refer to [Manage link costs](#).

USB port control

You can now enable or disable USB ports through Grid Manager. Refer to [Control remote access through USB ports](#).

Removed or deprecated features and capabilities in StorageGRID

Learn about features and capabilities that have been removed or deprecated in StorageGRID 12.1.0. Before you upgrade, check whether any removed or deprecated features affect your client applications or grid configuration.

Definitions

Deprecated

You **should not** use the feature in new production environments. Existing production environments can continue using the feature.

End of Life

Last shipped version that supports the feature. In some cases, documentation for the feature might be removed at this stage.

Removed

First version that **does not** support the feature.

StorageGRID end of feature support

Deprecated features will be removed in N+2 major versions. For example, if a feature is deprecated in version N (for example, 6.3), the last version where the feature will exist is N+1 (for example, 6.4). Version N+2 (for example, 6.5) is the first release when the feature doesn't exist in the product.

See the [Software Version Support page](#) for additional information.



In certain situations, NetApp might end support for particular features sooner than indicated.

Feature	Deprecated	End of Life	Removed	Links to earlier documentation
Global SSE setting for AES-128 encryption	12.1	12.2	12.3	Beginning with StorageGRID 12.1.0, support for AES-128 encryption of new stored object data at rest is deprecated. Support continues for retrieval of stored objects that were originally encrypted with AES-128.
Alarms, legacy (<i>not Alerts</i>)	11.7	11.8	11.9	Alarms reference (StorageGRID 11.8)
Archive Node support	11.7	11.8	11.9	Considerations for decommissioning Archive Nodes (StorageGRID 11.8) Note: Before starting your upgrade, you must: - Decommission all Archive Nodes. Refer to Grid node decommissioning (StorageGRID 11.8 doc site). - Remove all Archive Node references from storage pools and ILM policies. Refer to NetApp Knowledge Base: StorageGRID 11.9 software upgrade resolution guide.

Feature	Deprecated	End of Life	Removed	Links to earlier documentation
Audit export through CIFS/Samba	11.1	11.6	11.7	
CLB service	11.4	11.6	11.7	
Docker container engine	11.8	11.9	TBD	Support for Docker as the container engine for software-only deployments is deprecated. Docker will be replaced with another container engine in a future release. Refer to the software requirements for software-based nodes for a list of Docker versions currently supported.
Email setup (legacy)	11.9	12.0	12.1	Configure notifications for alarms (legacy system) (StorageGRID 11.8)
NFS audit export	11.8	11.9	12.0	Configure audit client access for NFS (StorageGRID 11.8)
Port remap	12.0	12.1	12.2	
Swift API support	11.7	11.9	12.0	Use Swift REST API (StorageGRID 11.8)
RHEL 8.8	11.9	11.9	12.0	
RHEL 9.0	11.9	11.9	12.0	
RHEL 9.2	11.9	11.9	12.0	
Ubuntu 18.04	11.9	11.9	12.0	
Ubuntu 20.04	11.9	11.9	12.0	
Debian 11	11.9	11.9	12.0	

Also refer to:

- [Changes to the Grid Management API](#)
- [Changes to the Tenant Management API](#)

Changes to the Grid Management API in StorageGRID

StorageGRID 12.1 uses version 4 of the Grid Management API. Version 4 deprecates

version 3; however, versions 1, 2, and 3 are still supported.



You can continue to use deprecated versions of the management API with StorageGRID; however, support for these versions of the API will be removed in a future release of StorageGRID. After upgrading to StorageGRID 12.0 or later, you can deactivate the deprecated APIs by using the `PUT /grid/config/management` API.

To learn more, go to [Use the Grid Management API](#).

New endpoints for changing the BMC password and LAN IP settings

The following endpoint has been added to allow you to [change an appliance BMC password](#).

```
PUT /bmc-configuration/root-password
```

The following endpoints have been added to allow you to [change or view the BMC LAN IP settings](#).

```
PUT /grid/bmc/{node-id}/lan-ip-config
```

```
GET /grid/bmc/{node-id}/lan-ip-config
```

Changes to the Tenant Management API in StorageGRID

StorageGRID 12.1 uses version 4 of the Tenant Management API. Version 4 deprecates version 3; however, versions 1, 2, and 3 are still supported.



You can continue to use deprecated versions of the Tenant Management API with StorageGRID; however, support for these versions of the API will be removed in a future release of StorageGRID. After upgrading to StorageGRID 12.0 or later, you can deactivate the deprecated APIs by using the `PUT /grid/config/management` API.

To learn more, go to [Understand the Tenant Management API](#).

New API for object replication

You can use the `/org/cross-grid-replication/{versionId}/replicate` API to manually replicate objects on an existing bucket that has cross-grid replication newly configured.

Changes to StorageGRID S3 REST API support

The S3 REST API used by StorageGRID is updated regularly.

Release	Comments
12.1.0	• <code>If-Match</code> The <code>If-Match</code> header behaves differently depending on your StorageGRID configuration. Providing this header might return an error message (501 Not Implemented). If the <code>If-Match</code> header is accepted but non-functional, an alert might trigger with instructions about enabling the stricter 501 Not Implemented error behavior. • <code>If-None-Match</code> The <code>If-None-Match</code> header behaves differently depending on your StorageGRID configuration. Providing this header might return an error message (501 Not Implemented). If the <code>If-None-Match</code> header is accepted but non-functional, an alert might trigger with instructions about enabling the stricter 501 Not Implemented error behavior. • Added support for pre-calculated checksum values for the following requests and supported headers: ◦ <code>CompleteMultipartUpload</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, and <code>x-amz-checksum-crc64nvme</code> ◦ <code>CreateMultipartUpload</code>: <code>CRC32</code>, <code>CRC32C</code>, and <code>CRC64NVME</code> for <code>x-amz-checksum-algorithm</code> ◦ <code>CopyObject</code>: <code>CRC32</code>, <code>CRC32C</code>, <code>CRC64NVME</code>, and <code>SHA256</code> for <code>x-amz-checksum-algorithm</code> ◦ <code>PutObject</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, and <code>x-amz-checksum-crc64nvme</code> ◦ <code>UploadPart</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, and <code>x-amz-checksum-crc64nvme</code> • Added support for <code>x-amz-checksum-type</code> for <code>CreateMultipartUpload</code> and <code>CompleteMultipartUpload</code>. • Added support for the <code>s3:x-amz-copy-source</code> policy condition key. • Allow S3 Object Lock to be enabled on existing buckets.
12.0	• Added support for cross-origin resource sharing (CORS) for a management interface, which allows another domain to access data in StorageGRID using management APIs. Learn more. • Added support for STS AssumeRole and session policy. See an example of a session policy. You can set up AssumeRole under tenant groups.

Release	Comments
11.9	• Added support for pre-calculated SHA-256 checksum values for the following requests and supported headers. You can use this feature to verify the integrity of uploaded objects: ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ HeadObject: x-amz-checksum-mode ◦ ListParts ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • Added the ability for the grid administrator to control tenant-level retention and Compliance settings. These settings affect S3 Object Lock settings. ◦ Bucket default retention mode and object retention mode: Governance or Compliance, if allowed by the grid administrator. ◦ Bucket default retention period and object Retain Until Date: Must be less than or equal to what is allowed by the maximum retention period set by grid administrator. • Improved support for aws-chunked content encoding and streaming x-amz-content-sha256 values. Limitations: ◦ If present, chunk-signature is optional and not validated ◦ If present, x-amz-trailer content is ignored
11.8	Updated the names of S3 operations to match the names used in the Amazon Web Services (AWS) Documentation: Amazon Simple Storage Service API Reference .
11.7	• Added Quick reference: Supported S3 API requests. • Added support for using GOVERNANCE mode with S3 Object Lock. • Added support for the StorageGRID-specific x-ntap-sg-cgr-replication-status response header for GET Object and HEAD Object requests. This header provides an object's replication status for cross-grid replication. • SelectObjectContent requests now support Parquet objects.

Release	Comments
11.6	• Added support for using the <code>partNumber</code> request parameter in GET Object and HEAD Object requests. • Added support for a default retention mode and a default retention period at the bucket level for S3 Object Lock. • Added support for the <code>s3:object-lock-remaining-retention-days</code> policy condition key to set the range of allowable retention periods for your objects. • Changed the maximum <i>recommended</i> size for a single PUT Object operation to 5 GiB (5,368,709,120 bytes). If you have objects that are larger than 5 GiB, use multipart upload instead.
11.5	• Added support for managing bucket encryption. • Added support for S3 Object Lock and deprecated legacy Compliance requests. • Added support for using DELETE Multiple Objects on versioned buckets. • The <code>Content-MD5</code> request header is now correctly supported.
11.4	• Added support for DELETE Bucket tagging, GET Bucket tagging, and PUT Bucket tagging. Cost allocation tags aren't supported. • For buckets created in StorageGRID 11.4, restricting object key names to meet performance best practices is no longer required. • Added support for bucket notifications on the <code>s3:ObjectRestore:Post</code> event type. • AWS size limits for multipart parts are now enforced. Each part in a multipart upload must be between 5 MiB and 5 GiB. The last part can be smaller than 5 MiB. • Added support for TLS 1.3
11.3	• Added support for server-side encryption of object data with customer-provided keys (SSE-C). • Added support for DELETE, GET, and PUT Bucket lifecycle operations (Expiration action only) and for the <code>x-amz-expiration</code> response header. • Updated PUT Object, PUT Object - Copy, and Multipart Upload to describe the impact of ILM rules that use synchronous placement at ingest. • TLS 1.1 ciphers are no longer supported.
11.2	Added support for POST Object restore for use with Cloud Storage Pools. Added support for using the AWS syntax for ARN, policy condition keys, and policy variables in group and bucket policies. Existing group and bucket policies that use the StorageGRID syntax will continue to be supported. Note: Uses of ARN/URN in other configuration JSON/XML, including those used in custom StorageGRID features, have not changed.
11.1	Added support for cross-origin resource sharing (CORS), HTTP for S3 client connections to grid nodes, and compliance settings on buckets.

Release	Comments
11.0	Added support for configuring platform services (CloudMirror replication, notifications, and Elasticsearch search integration) for buckets. Also added support for object tagging location constraints for buckets, and the Available consistency.
10.4	Added support for ILM scanning changes to versioning, Endpoint Domain Names page updates, conditions and variables in policies, policy examples, and the PutOverwriteObject permission.
10.3	Added support for versioning.
10.2	Added support for group and bucket access policies, and for multipart copy (Upload Part - Copy).
10.1	Added support for multipart upload, virtual-hosted-style requests, and v4 authentication.
10.0	Initial support of the S3 REST API by the StorageGRID system. The currently supported version of the <i>Simple Storage Service API Reference</i> is 2006-03-01.

Refer to [S3 REST API supported versions and updates](#) for more information.

Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.