Technical Report

NetApp StorageGRID with Veritas Enterprise Vault

Implementing NetApp StorageGRID as the primary storage for Enterprise Vault archives

Configuration guide

Jonathan Wong, NetApp
Rahul Patil, Veritas
July 2022 | TR-4907

In partnership with

VERITAS

Abstract

This configuration guide provides the steps to configure NetApp® StorageGRID® as a primary storage target with Veritas Enterprise Vault. It also describes how to configure StorageGRID for site failover in a disaster recovery (DR) scenario.

TABLE OF CONTENTS

Basic configuration 3

Prerequisites.....3

Configure StorageGRID with Veritas Enterprise Vault.....4

StorageGRID Object Lock configuration (optional) 9

Prerequisites.....9

Configure StorageGRID S3 Object Lock default bucket retention 9

Configure Enterprise Vault 13

StorageGRID site failover configuration (optional) 14

Prerequisites.....14

Configure StorageGRID site failover 14

Where to find additional information 16

Version history 17

LIST OF FIGURES

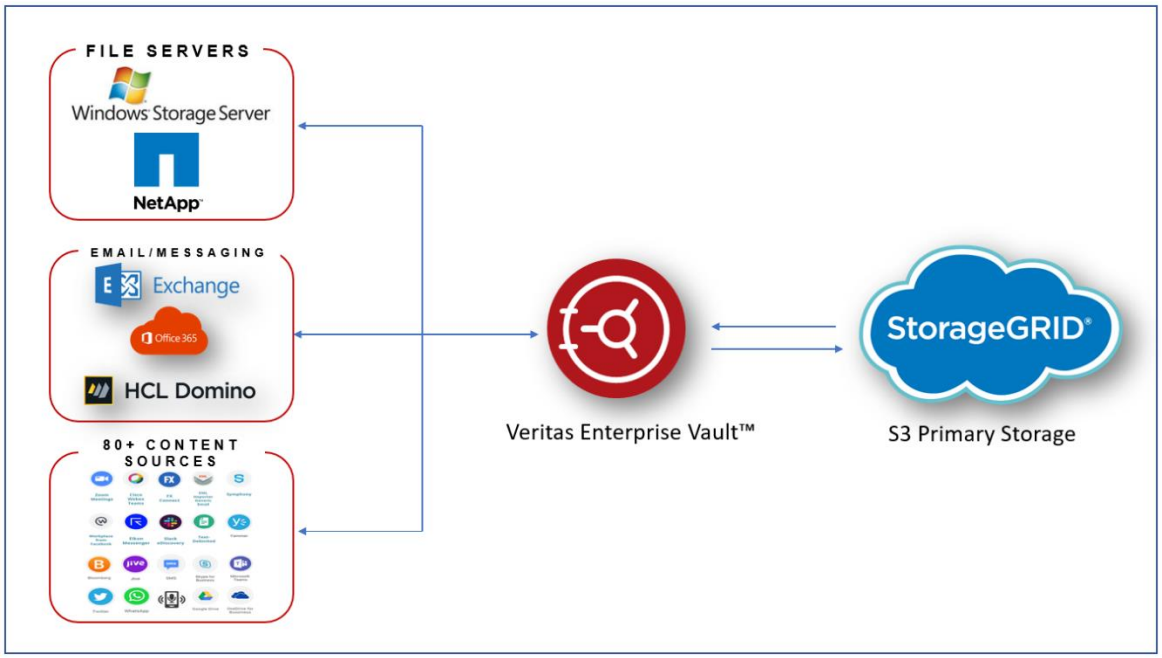
Figure 1) Veritas Enterprise Vault and StorageGRID architecture. 3

Reference architecture

StorageGRID provides an on-premises, S3-compatible cloud backup target for Veritas Enterprise Vault.

Figure 1 illustrates the Veritas Enterprise Vault and StorageGRID architecture.

Figure 1) Veritas Enterprise Vault and StorageGRID architecture.



Basic configuration

This configuration guide is based on StorageGRID 11.5 and Enterprise Vault 14.1. For write once, read many (WORM) mode storage using S3 Object Lock, StorageGRID 11.6 and Enterprise Vault 14.2.2 was used. For more detailed information about these guidelines, see the StorageGRID 11.6 Documentation page or contact a StorageGRID expert.

Prerequisites

Before you configure StorageGRID with Veritas Enterprise Vault, verify the following prerequisites:

- StorageGRID 11.5+ is installed.

  Note: For WORM storage (Object Lock), StorageGRID 11.6 is required.

- Veritas Enterprise Vault 14.1+ is installed.

  Note: For WORM storage (Object Lock), Enterprise Vault version 14.2.2 is required.

- Vault store groups and a vault store has been created.

  For more information, see the Veritas Enterprise Vault Administration Guide.

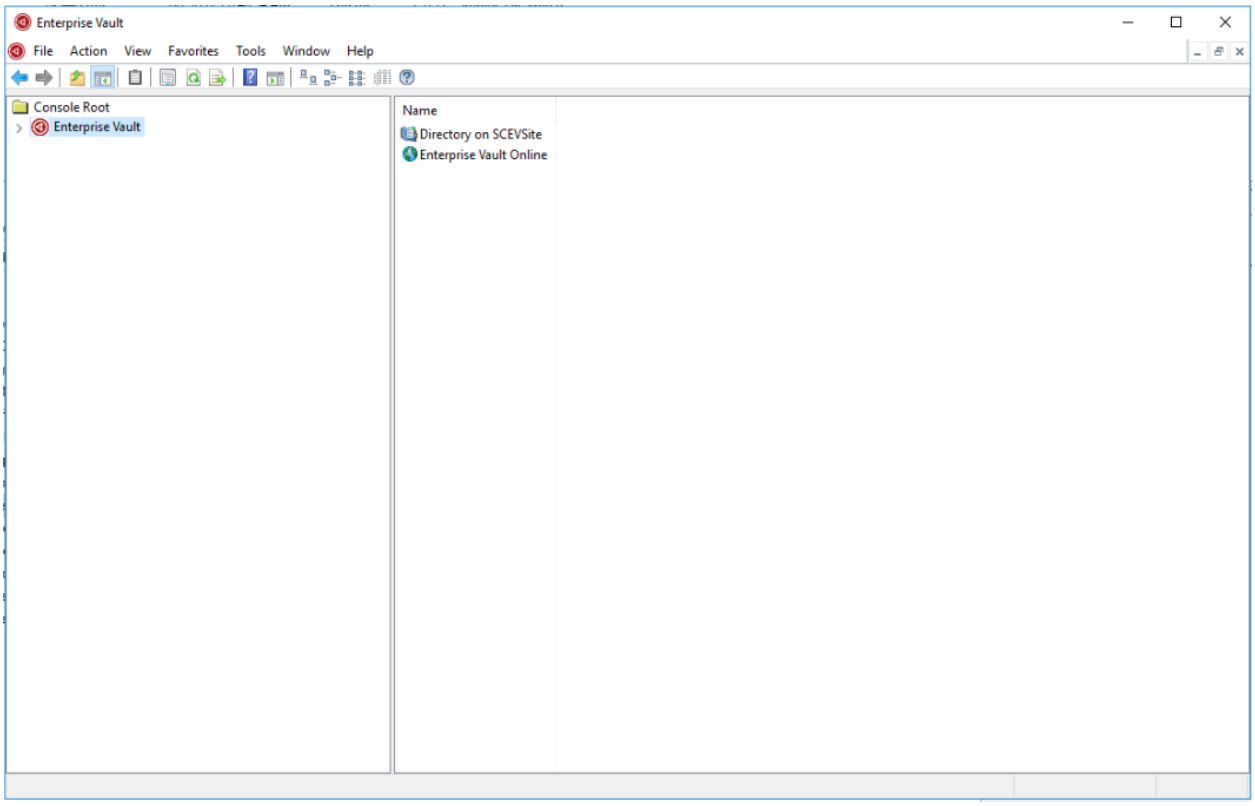
- A StorageGRID tenant, access key, secret key and bucket have been created.
- A StorageGRID load balancer endpoint has been created (either HTTP or HTTPS).
- If using a self-signed certificate, add the StorageGRID self-signed CA certificate to the Enterprise Vault Servers. For more information, see this Veritas Knowledge Base article.

- Update and apply the latest Enterprise Vault configuration file to enable supported storage solutions such as NetApp StorageGRID. For more information, see this Veritas Knowledge Base article.

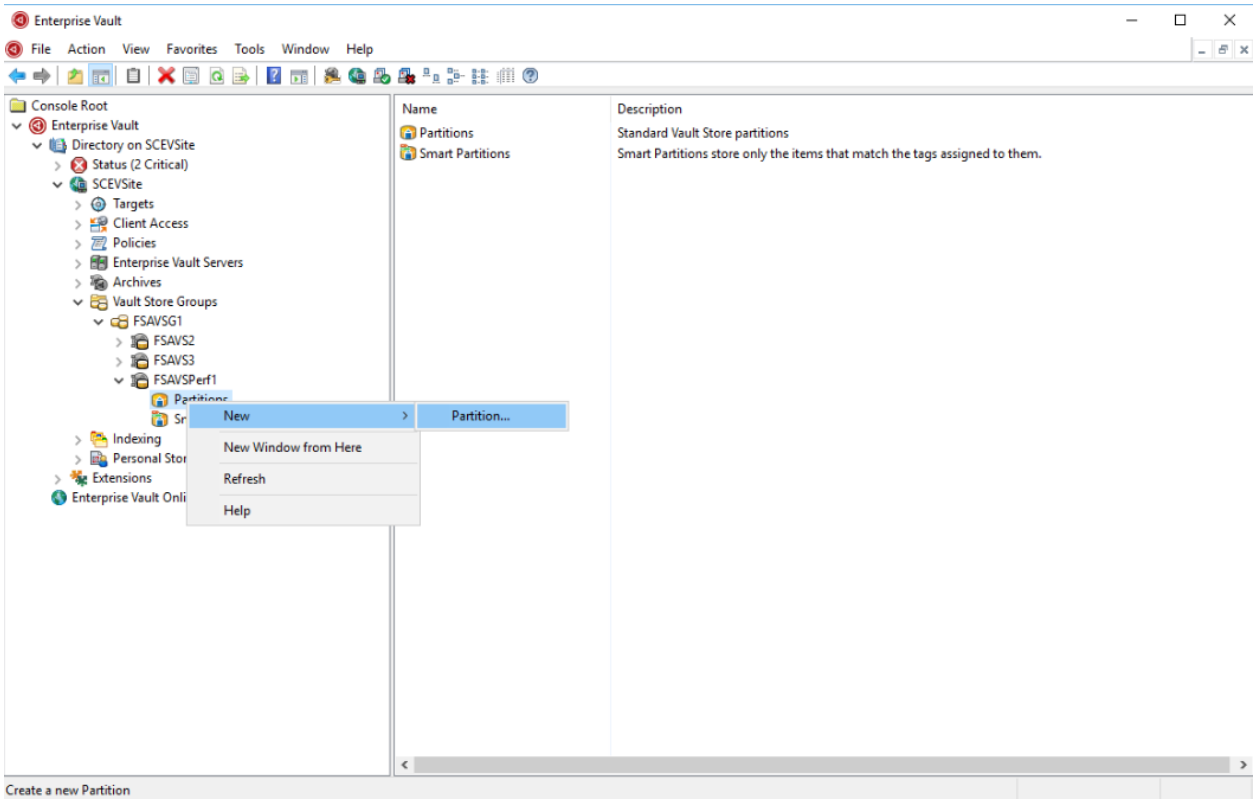
Configure StorageGRID with Veritas Enterprise Vault

To configure StorageGRID with Veritas Enterprise Vault, compete the following steps:

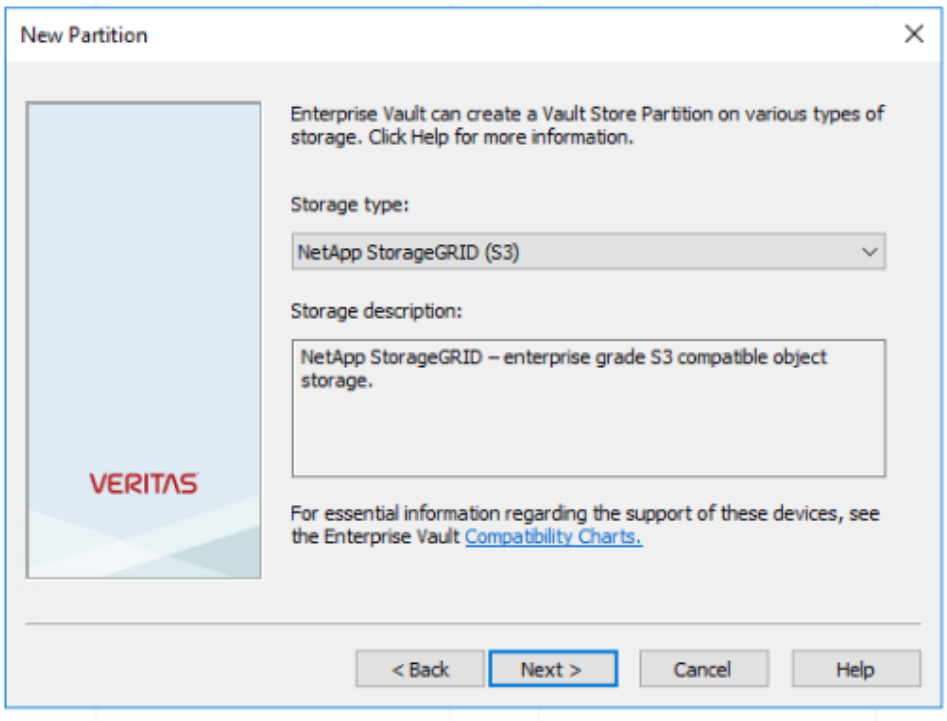
1. Launch the Enterprise Vault Administration console.



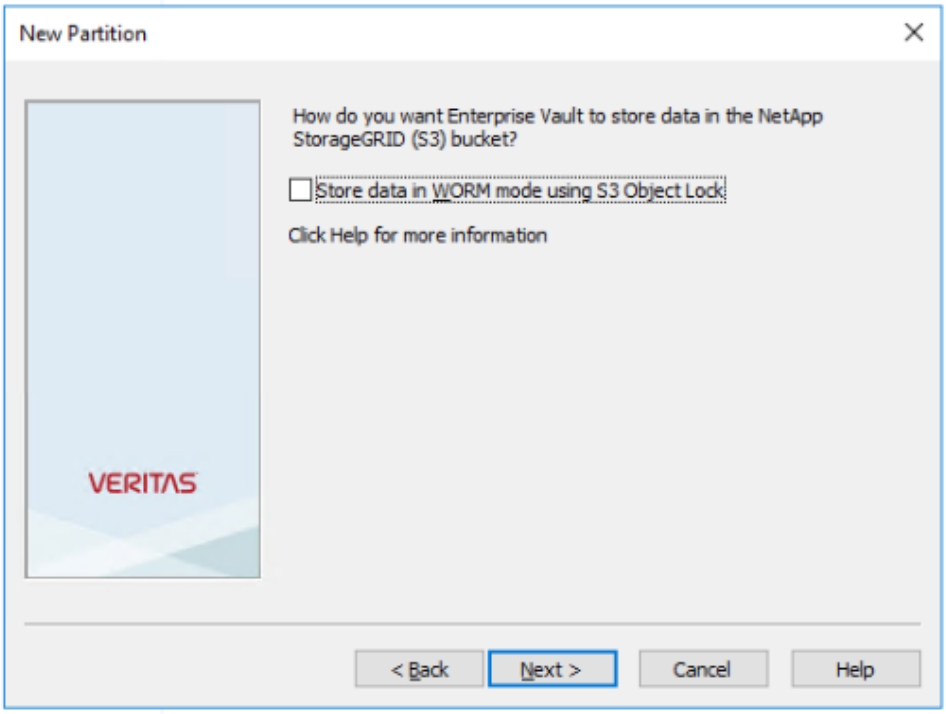
2. Create a new vault store partition in the appropriate vault store. Expand the Vault Store Groups folder and then the appropriate vault store. Right-click Partition and select New > Partition.



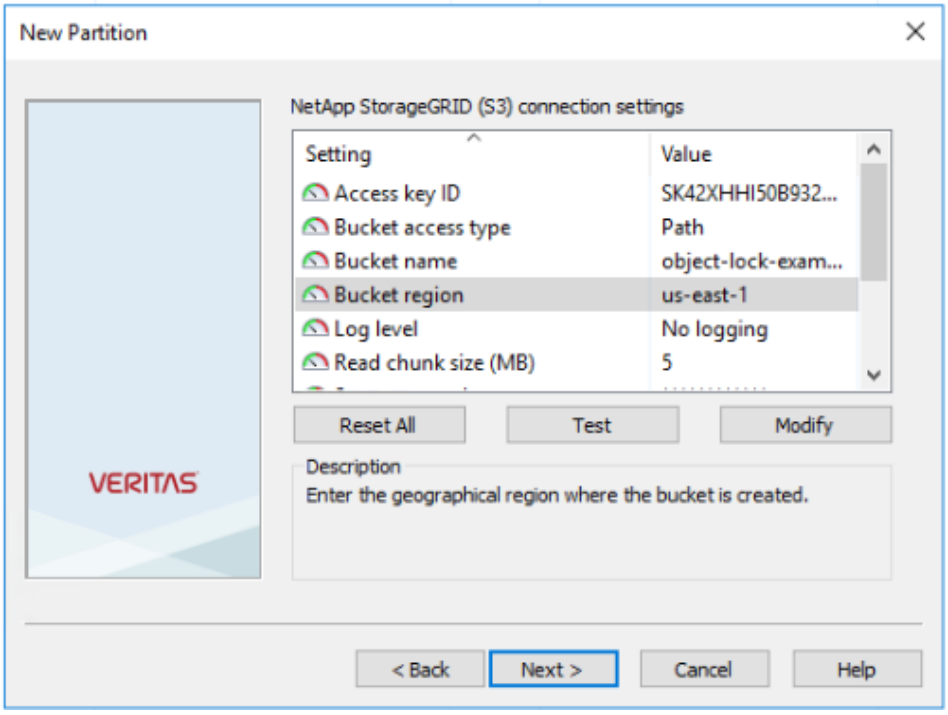
3. Follow the New Partition creation wizard. From the Storage Type drop-down menu, select NetApp StorageGRID (S3). Click Next.



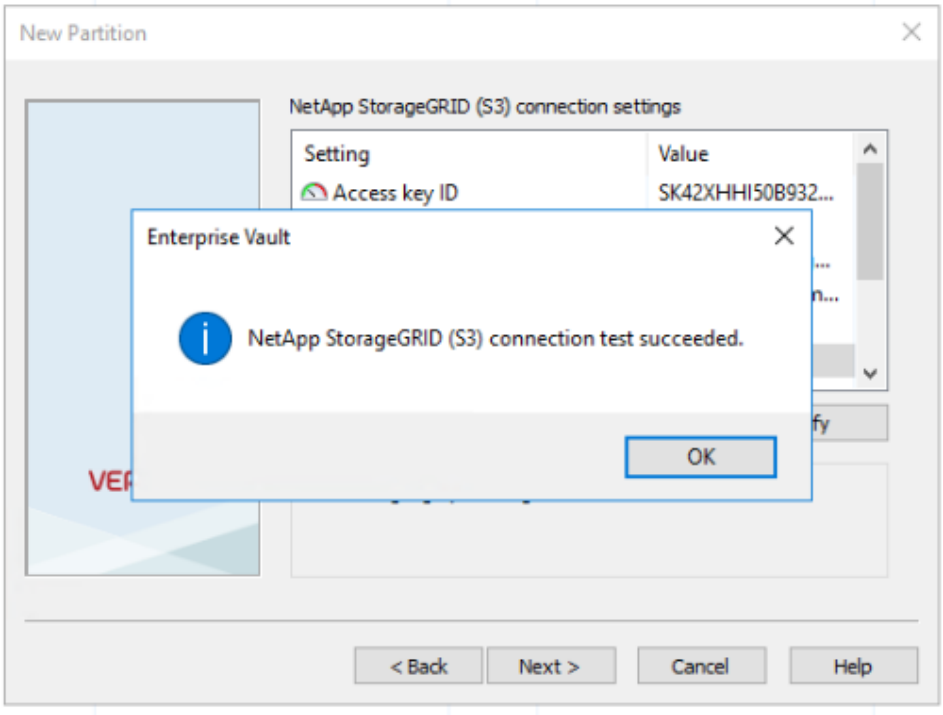
4. Leave the Store Data in WORM Mode Using S3 Object Lock option unchecked. Click Next.



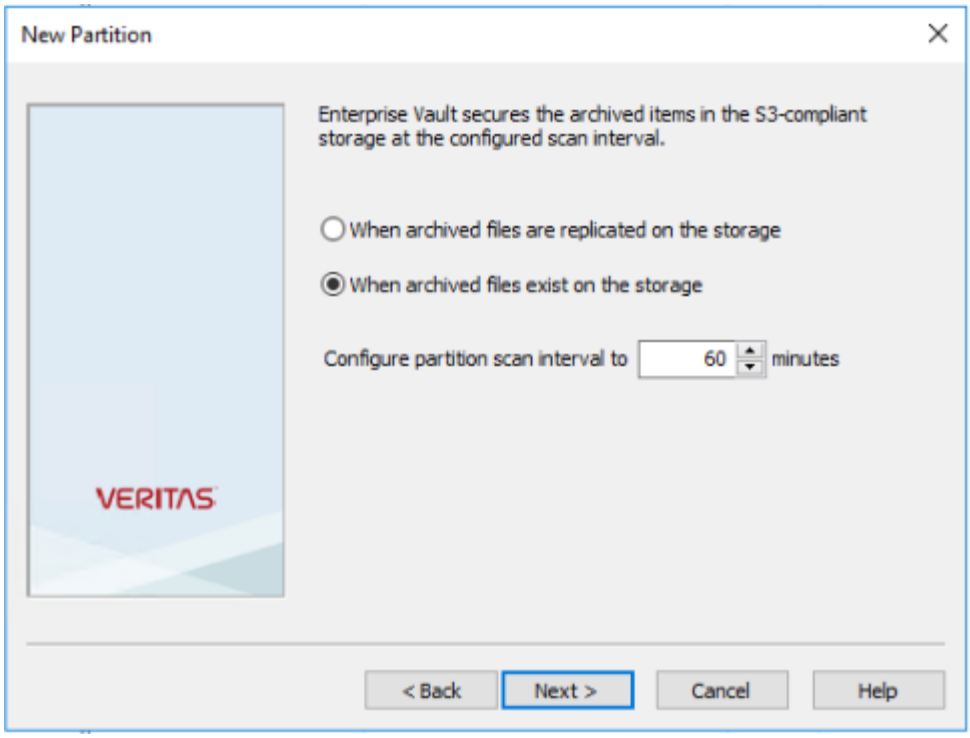
5. On the connection settings page, provide the following information:
   - Access key ID
   - Secret access key
   - Service host name: Ensure to include the load balancer endpoint (LBE) port configured in StorageGRID (such as https://<hostname>:<LBE_port>).
   - Bucket name: Name of the precreated target bucket. Veritas Enterprise Vault does not create the bucket.
   - Bucket region: `us-east-1` is the default value.



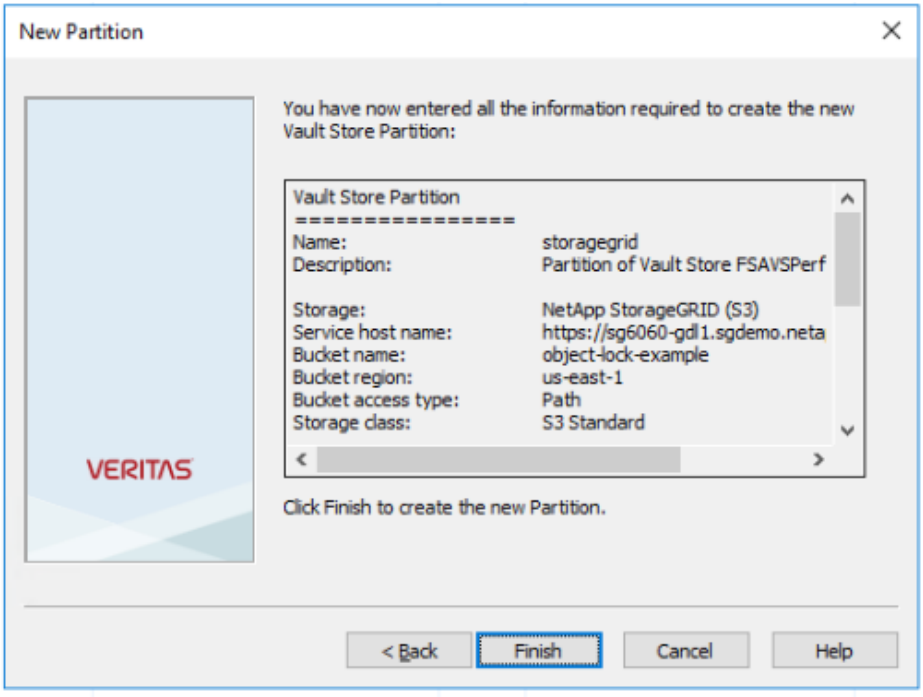
6. To verify the connection to the StorageGRID bucket, click Test. Verify that the connection test was successful. Click OK and then Next.



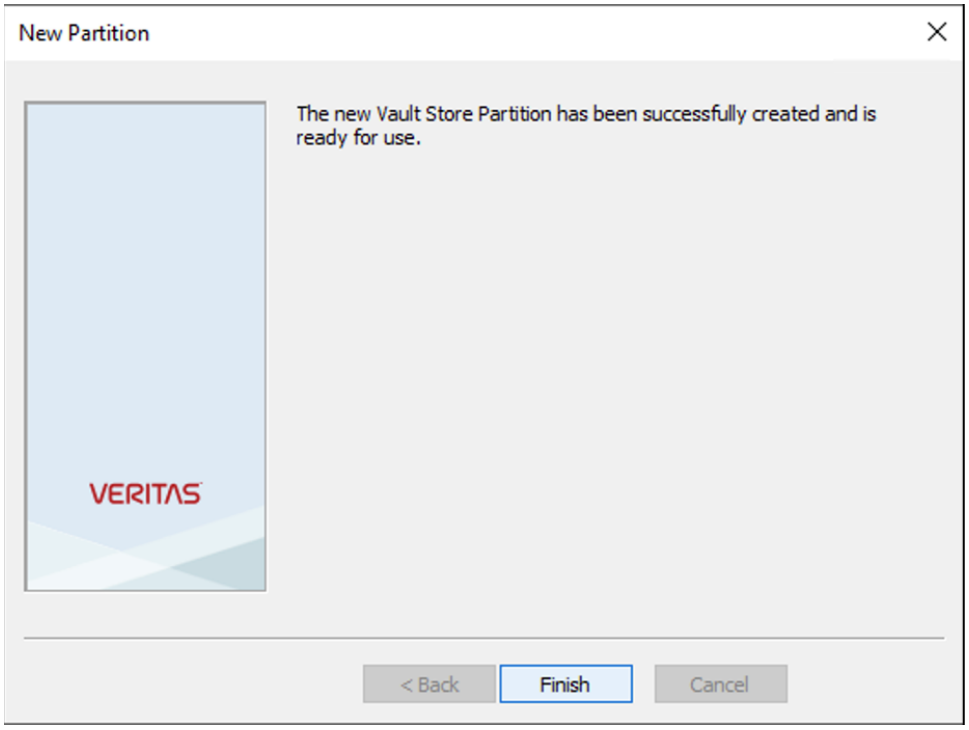
7. StorageGRID does not support the S3 replication parameter. To protect your objects, StorageGRID uses Information Lifecycle Management (ILM) rules to specify data protection schemes – multiple copies or erasure coding. Select the When Archived Files Exist on the Storage Option and click Next.



8. Verify the information on the summary page and click Finish.



9. After the new vault store partition has been successfully created, you can archive, restore, and search data in Enterprise Vault with StorageGRID as the primary storage.



StorageGRID Object Lock configuration (optional)

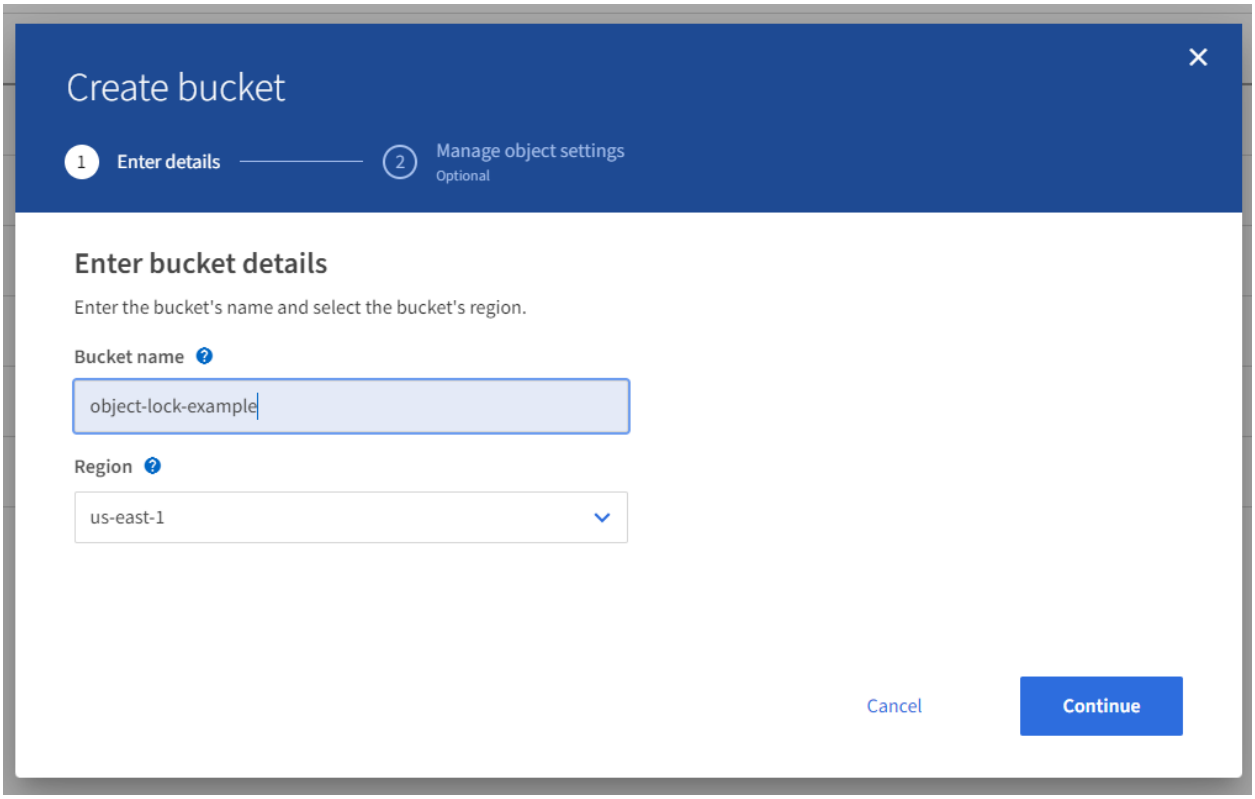
Prerequisites

For WORM storage, StorageGRID uses S3 Object Lock to retain objects for compliance. This requires StorageGRID 11.6, where S3 Object Lock default bucket retention was introduced. Enterprise Vault also requires version 14.2.2

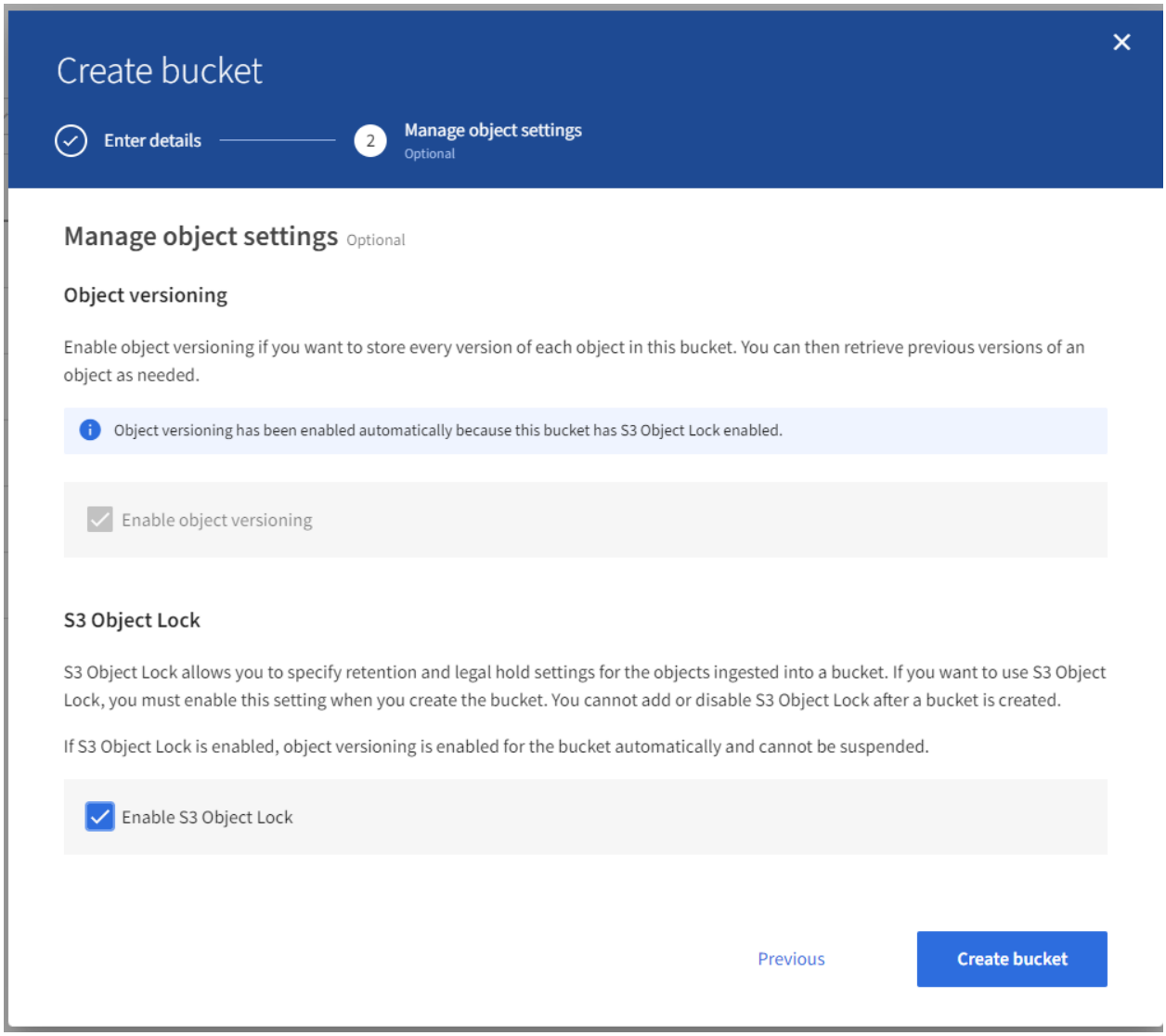
Configure StorageGRID S3 Object Lock default bucket retention

To configure the StorageGRID S3 Object Lock default bucket retention, complete the following steps:

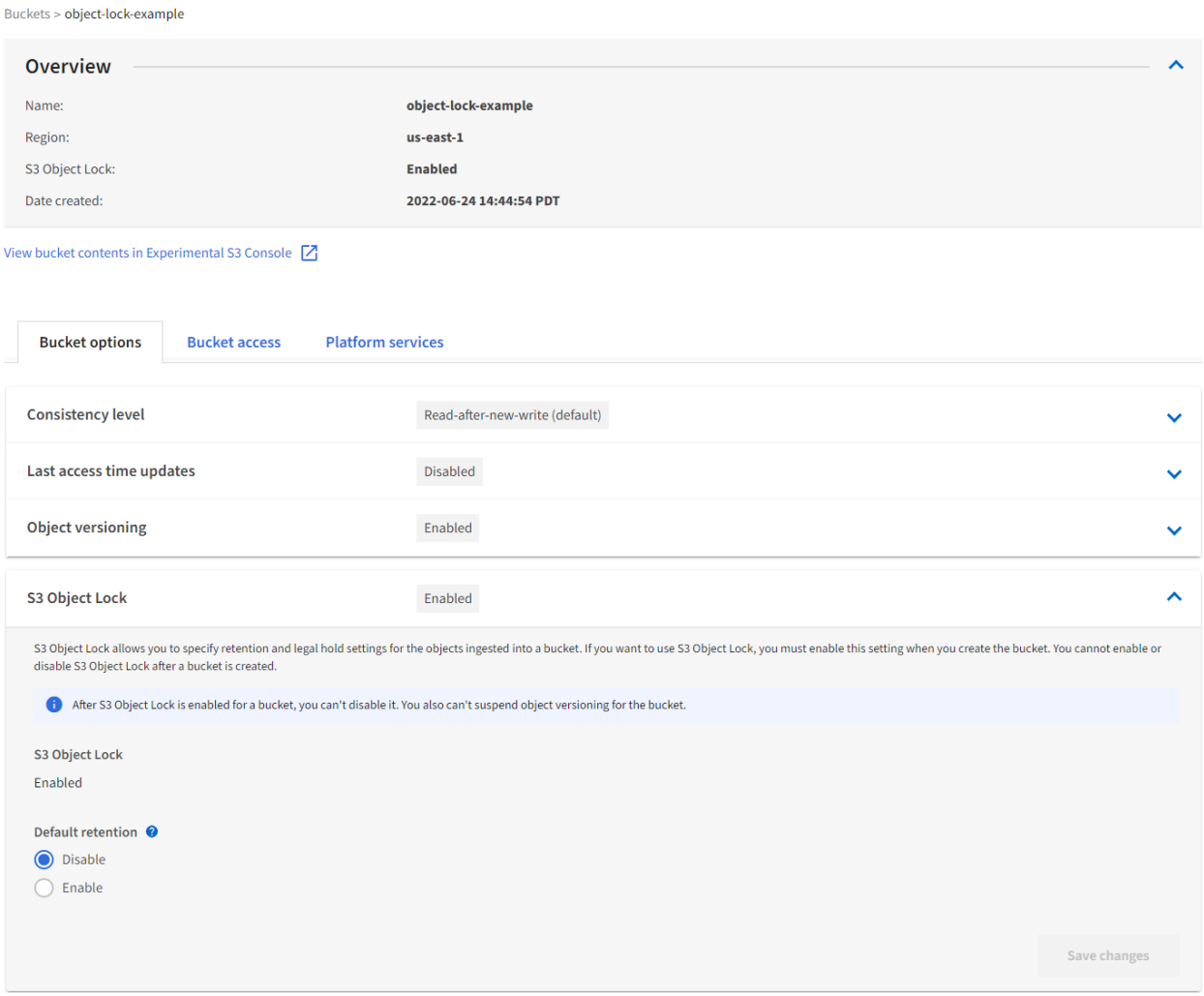
1. In StorageGRID Tenant Manager, create a bucket and click Continue



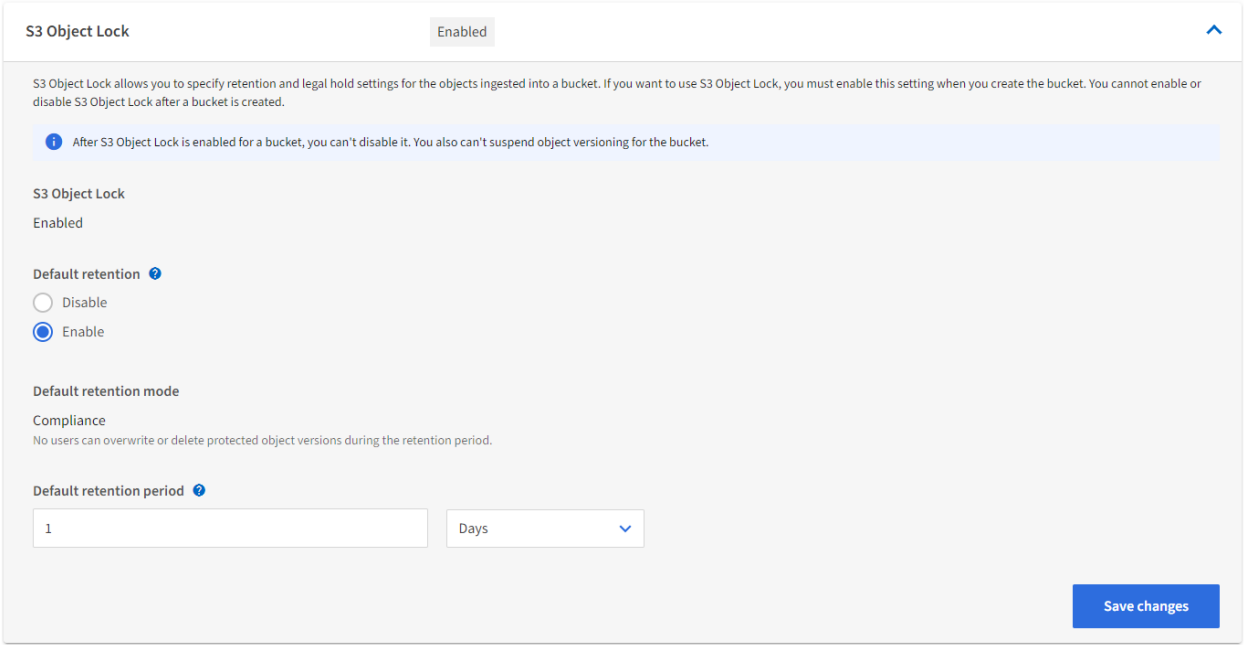
2. Select the Enable S3 Object Lock option and click Create Bucket.



3. After the bucket is created, select the bucket to view the bucket options. Expand the S3 Object Lock drop-down option.



4. Under Default Retention, select Enable and set a default retention period of 1 day. Click Save Changes.

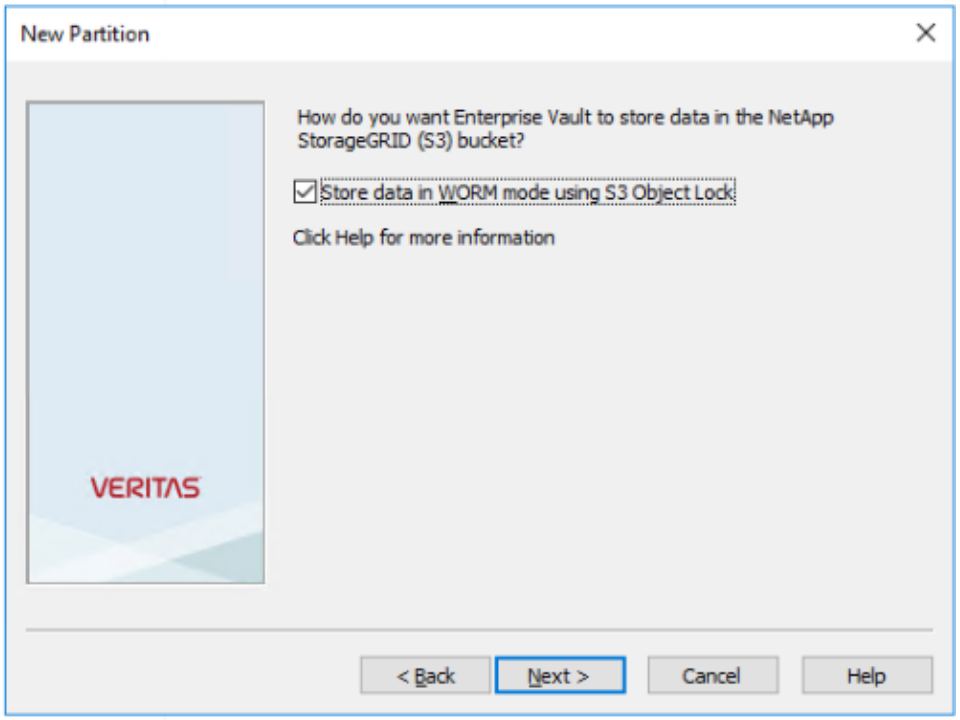


The bucket is now ready to be used by Enterprise Vault to store WORM data.

Configure Enterprise Vault

To configure Enterprise Vault, complete the following steps:

1. Repeat steps 1–3 in the “Basic configuration” section, but this time select the Store data in WORM Mode Using S3 Object Lock option. Click Next.



2. When entering your S3 Bucket connection settings, make sure you are entering the name of an S3 bucket that has the S3 Object Lock Default retention enabled.
3. Test the connection to verify the settings.

StorageGRID site failover configuration (optional)

It is a common for a StorageGRID architecture deployment to be multisite. Sites can either be active-active or active-passive for DR. In a DR scenario, make sure that Veritas Enterprise Vault can maintain connection to its primary storage (StorageGRID) and continue to ingest and retrieve data during a site failure. This section provides high-level configuration guidance for a two-site, active-passive deployment. For detailed information about these guidelines, see the StorageGRID 11.6 Documentation page or contact a StorageGRID expert.

Prerequisites

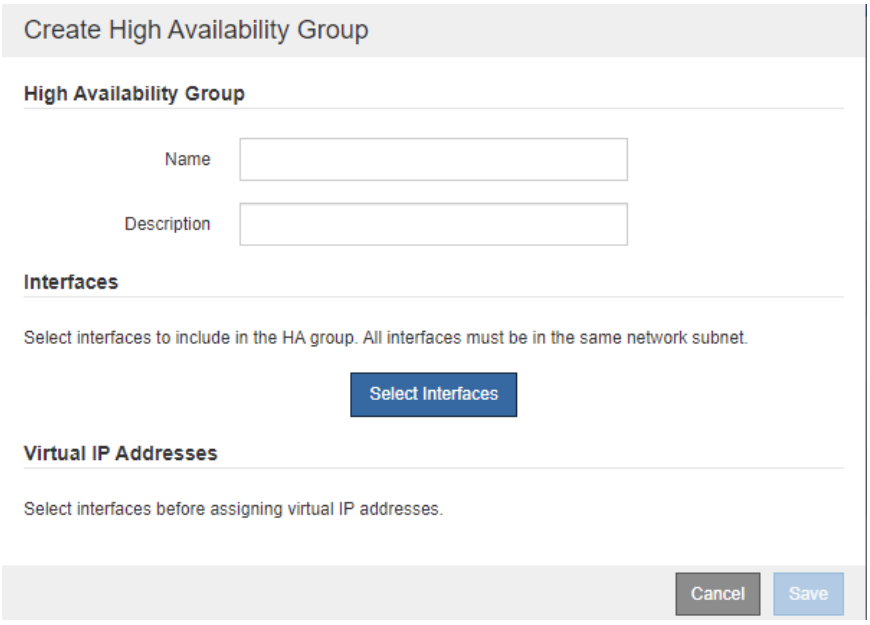
Before you configure StorageGRID site failover, verify the following prerequisites:

- There is a two-site StorageGRID deployment; for example, SITE1 and SITE2.
- An admin node running the load balancer service or a gateway node, at each site, for load balancing has been created.
- A StorageGRID load balancer endpoint has been created.

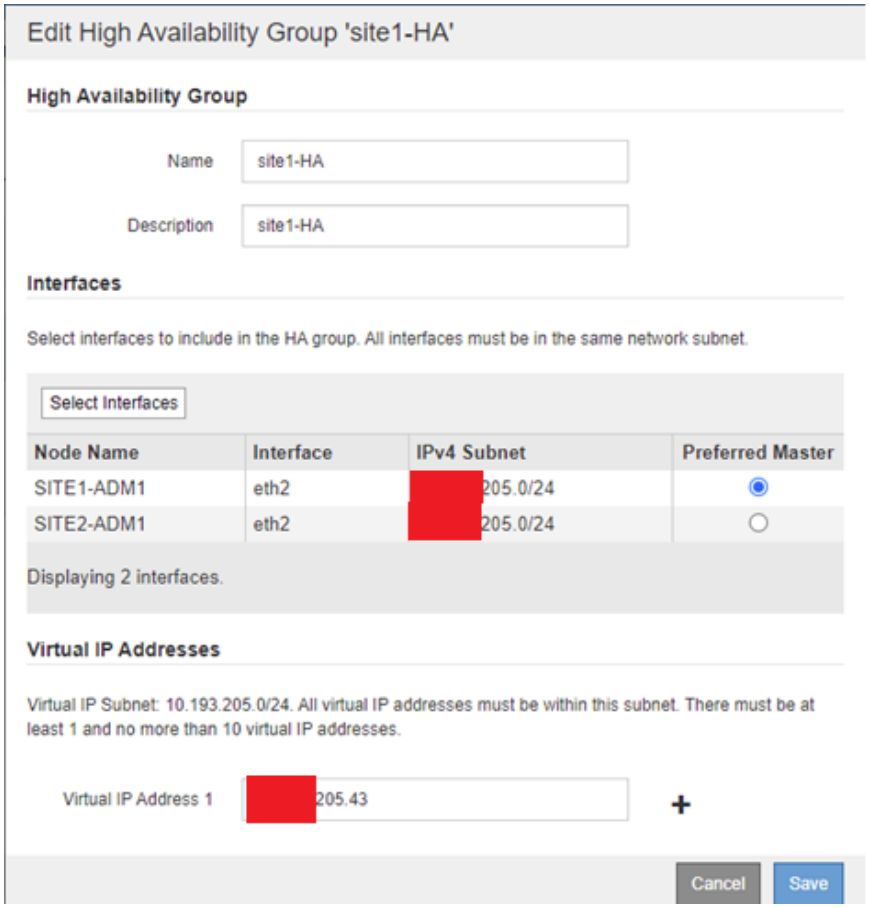
Configure StorageGRID site failover

To configure StorageGRID site failover, complete the followings steps:

1. To ensure connectivity to StorageGRID during site failures, configure a high-availability (HA) group. From StorageGRID Grid Manager Interface (GMI), click Configuration, High Availability Groups, and + Create.



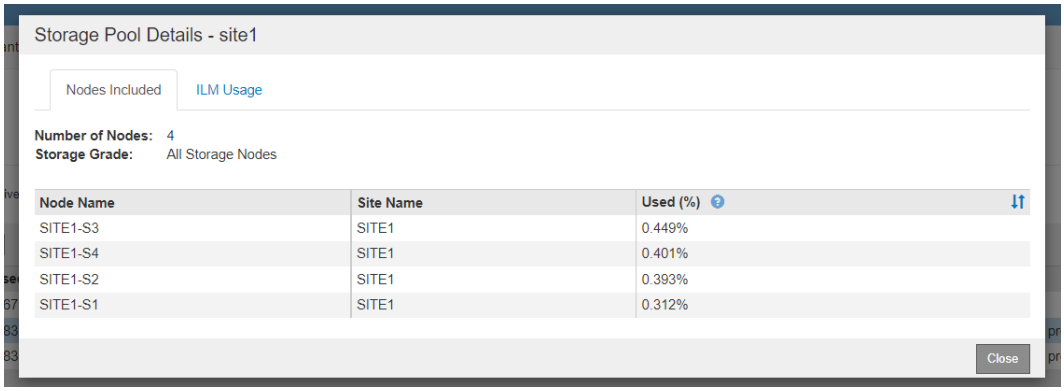
2. Enter the required information. Click Select Interfaces and include both SITE1 and SITE2's network interfaces where SITE1 (the primary site) is the preferred master. Assign a virtual IP address within the same subnet. Click Save.

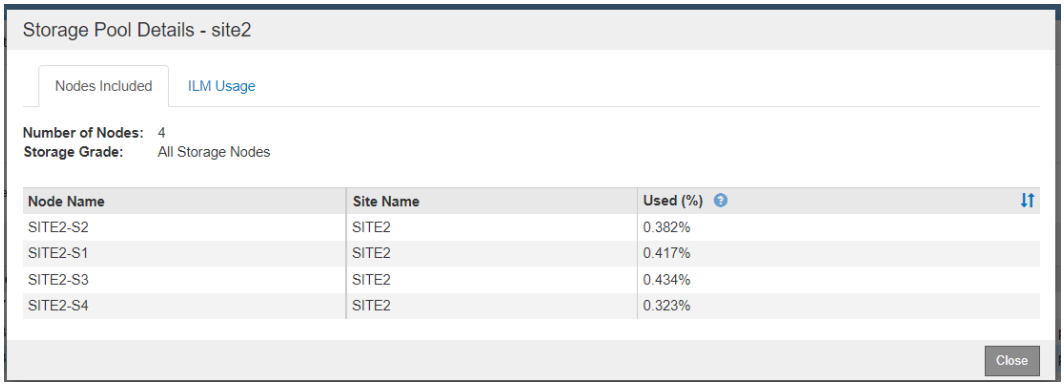


3. This virtual IP (VIP) address should be associated to the S3 host name used during Veritas Enterprise Vault 's partition configuration. The VIP address resolves traffic to SITE1—and during SITE1 failure, the VIP address transparently reroutes traffic to SITE2.
4. Make sure the data is replicated to both SITE1 and SITE2. That way if SITE1 fails, the object data is still available from SITE2. This is done by first configuring the storage pools.

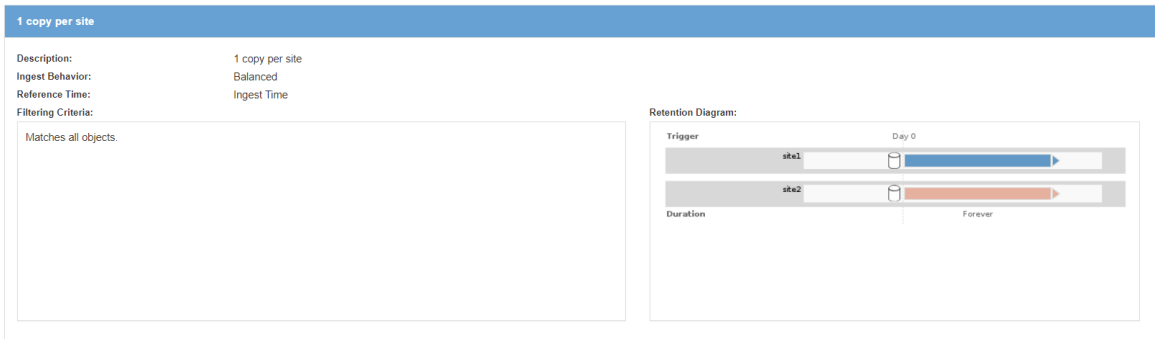
   From StorageGRID GMI, click ILM, Storage Pools, and then + Create. Follow the wizard to create two storage pools: one for SITE1 and another for SITE2.

   Storage pools are logical groupings of nodes used to define object placement





5. From StorageGRID GMI, click ILM, Rules, and then + Create. Follow the wizard to create an ILM rule specifying one copy to be stored per site with an ingest behavior of Balanced.



6. Add the ILM rule into an ILM policy and activate the policy.

   This configuration results in the following outcome:

   a. A virtual S3 endpoint IP where SITE1 is the primary and SITE2 is the secondary endpoint. If SITE1 fails, the VIP fails over to SITE2.

   b. When archived data is sent from Veritas Enterprise Vault, StorageGRID ensures one copy is stored in SITE1 and another DR copy is stored in SITE2. If SITE1 fails, Enterprise Vault continues to ingest and retrieve from SITE2.

   Note: Both of these configurations are transparent to Veritas Enterprise Vault. The S3 endpoint, bucket name, access keys, and so on are the same. There is no need to reconfigure the S3 connection settings on the Veritas Enterprise Vault partition.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp StorageGRID Product Documentation
  https://docs.netapp.com/us-en/storagegrid-116/
- StorageGRID documentation resources
  https://www.netapp.com/data-storage/storagegrid/documentation/
- Veritas Enterprise Vault Product Documentation
  https://www.veritas.com/support/en_US/article.100049763

Version history

Version	Date	Document version history
Version 1.0	September 2021	Initial release.
Version 1.1	December 2021	Added a KB article pertaining to self-signed certificates.
Version 1.2	July 2022	Added the Object Lock configuration for WORM storage.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Trademark information

TR-4907-0722

NetApp