TR-4907: Konfigurieren Sie StorageGRID mit Veritas Enterprise Vault

How to enable StorageGRID in your environment

NetApp
July 05, 2024

Inhalt

TR-4907: Konfigurieren Sie StorageGRID mit Veritas Enterprise Vault

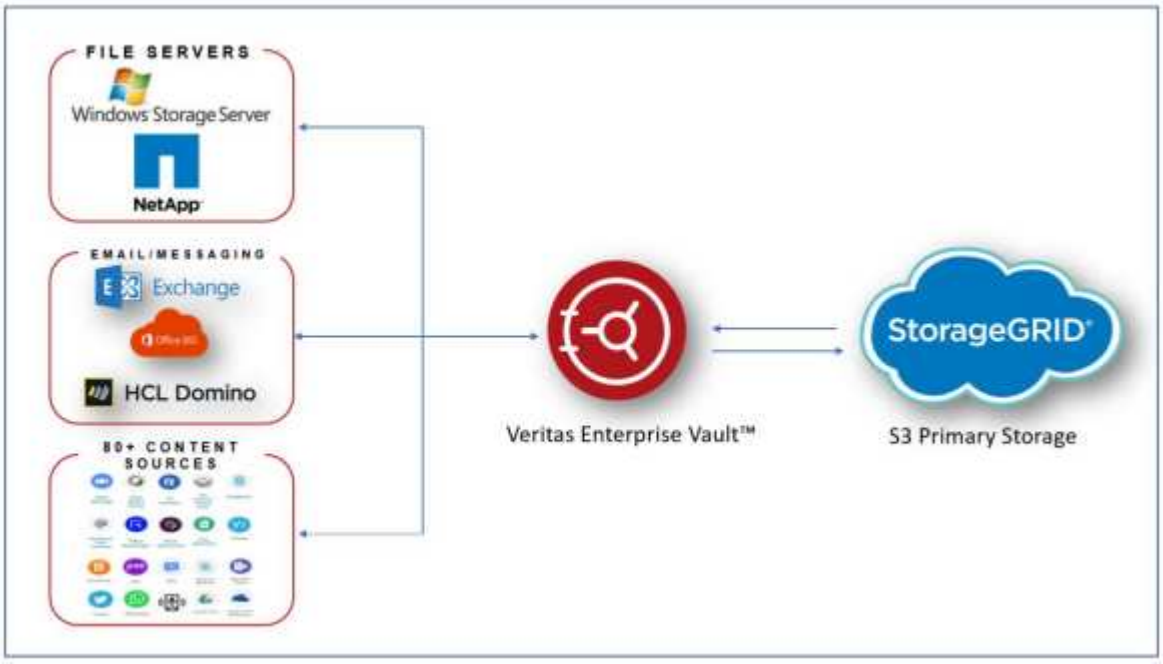
Einführung in die Konfiguration von StorageGRID für Site Failover

Erfahren Sie, wie Veritas Enterprise Vault StorageGRID als primäres Storage-Ziel für Disaster Recovery verwendet.

Diese Konfigurationsanleitung enthält die Schritte zur Konfiguration von NetApp® StorageGRID® als primäres Speicherziel mit Veritas Enterprise Vault. Es wird auch beschrieben, wie StorageGRID für ein Standort-Failover in einem Disaster Recovery-Szenario (DR) konfiguriert wird.

Referenzarchitektur von NetApp dar

StorageGRID bietet ein lokales, S3-kompatibles Cloud-Backup-Ziel für Veritas Enterprise Vault. Die folgende Abbildung zeigt die Architektur von Veritas Enterprise Vault und StorageGRID.



Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRID Dokumentations-Ressourcen https://www.netapp.com/data-storage/storagegrid/documentation/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Konfigurieren Sie StorageGRID und Veritas Enterprise Vault

Erfahren Sie, wie Sie grundlegende Konfigurationen für StorageGRID 11.5 oder höher und Veritas Enterprise Vault 14.1 oder höher implementieren.

Dieser Konfigurationsleitfaden basiert auf StorageGRID 11.5 und Enterprise Vault 14.1. Für WORM-Modus (Write Once, Read Many) wurde Storage mit S3 Object Lock, StorageGRID 11.6 und Enterprise Vault 14.2.2 verwendet. Weitere Details zu diesen Richtlinien finden Sie auf der "StorageGRID-Dokumentation" Seite oder bei einem StorageGRID Experten.

Voraussetzungen für die Konfiguration von StorageGRID und Veritas Enterprise Vault

- Bevor Sie StorageGRID mit Veritas Enterprise Vault konfigurieren, überprüfen Sie die folgenden Voraussetzungen:

> Für WORM Storage (Objektsperre) ist StorageGRID 11.6 oder höher erforderlich.

- Veritas Enterprise Vault 14.1 oder höher ist installiert.

> Für WORM Storage (Object Lock) ist Enterprise Vault ab Version 14.2.2 erforderlich.

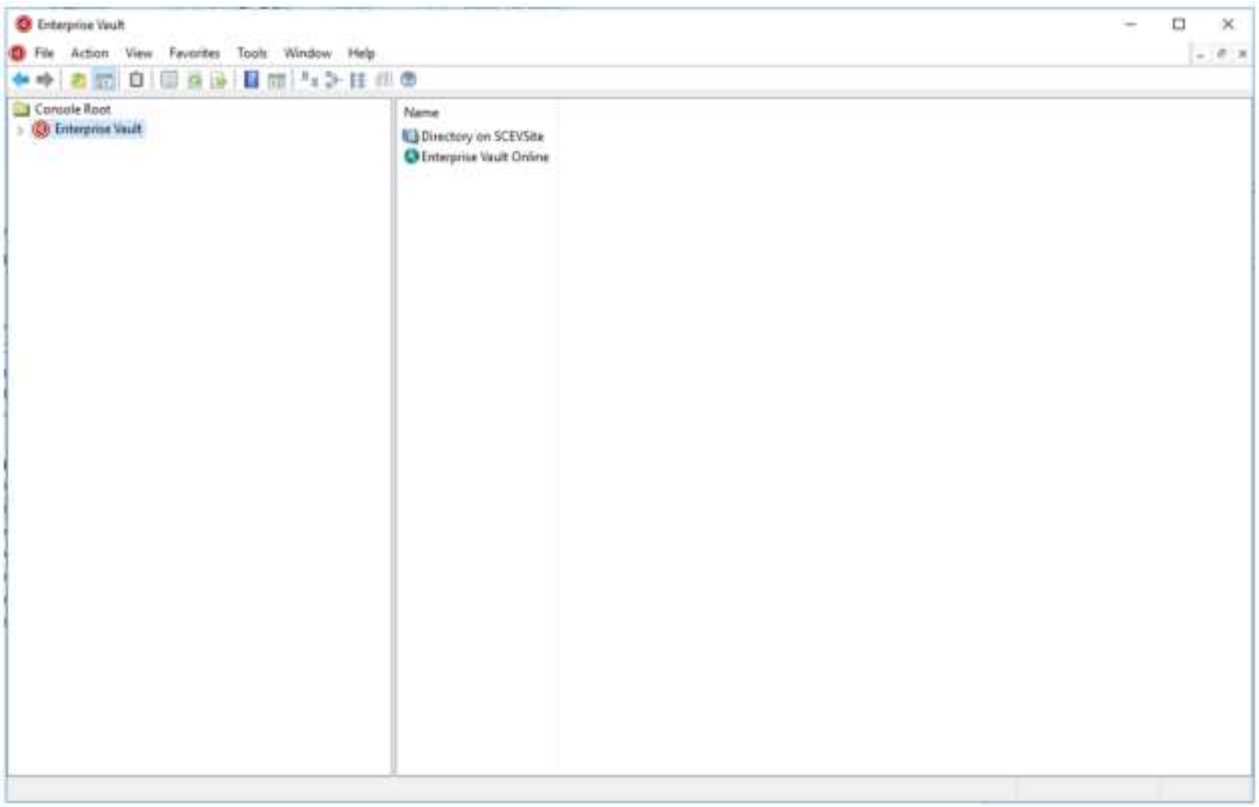
- Vault-Speichergruppen und ein Vault-Speicher wurden erstellt. Weitere Informationen finden Sie im Veritas Enterprise Vault Administration Guide.
- Ein StorageGRID-Mandant, Zugriffsschlüssel, geheimer Schlüssel und Bucket wurden erstellt.
- Ein StorageGRID-Load-Balancer-Endpunkt wurde erstellt (entweder HTTP oder HTTPS).
- Wenn Sie ein selbstsigniertes Zertifikat verwenden, fügen Sie das selbstsignierte StorageGRID-CA-Zertifikat zu den Enterprise Vault-Servern hinzu. Weitere Informationen finden Sie in diesem "Artikel der Veritas Knowledge Base".
- Aktualisieren Sie die aktuelle Enterprise Vault-Konfigurationsdatei, und wenden Sie sie an, um unterstützte Speicherlösungen wie NetApp StorageGRID zu ermöglichen. Weitere Informationen finden Sie in diesem "Artikel der Veritas Knowledge Base".

Konfigurieren Sie StorageGRID mit Veritas Enterprise Vault

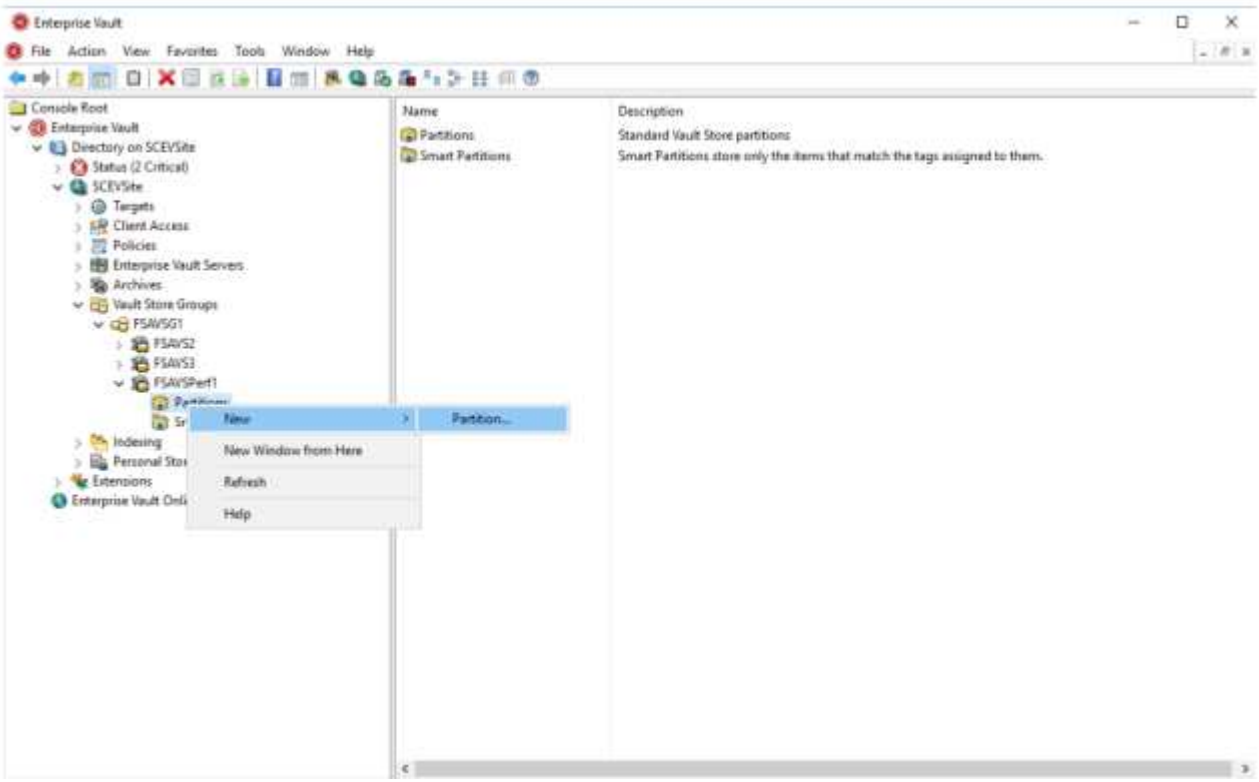
So konfigurieren Sie StorageGRID mit Veritas Enterprise Vault:

Schritte

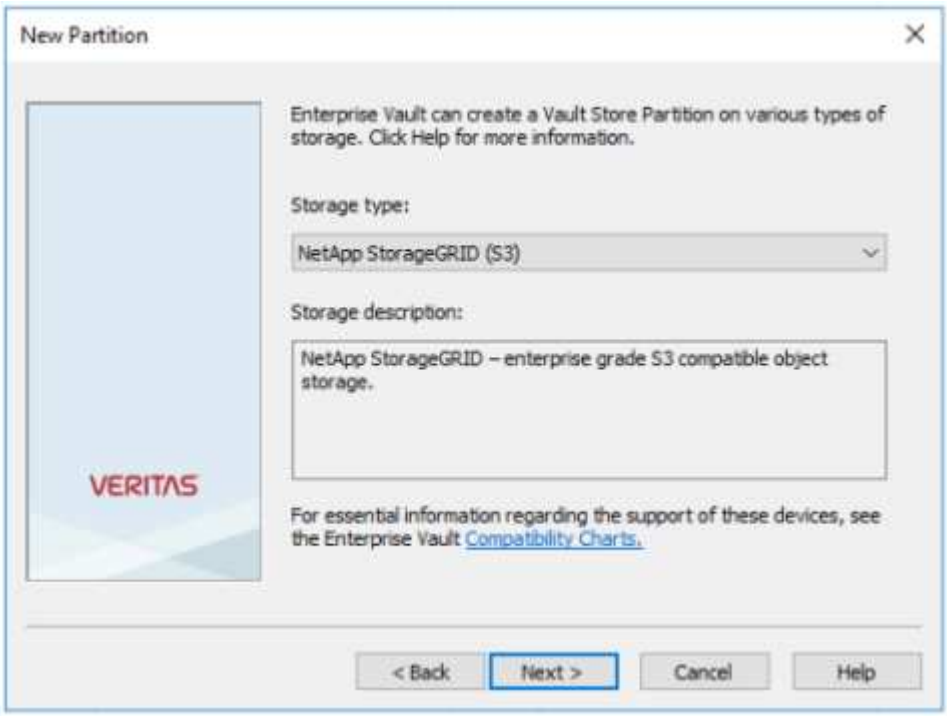
1. Starten Sie die Enterprise Vault Administration-Konsole.



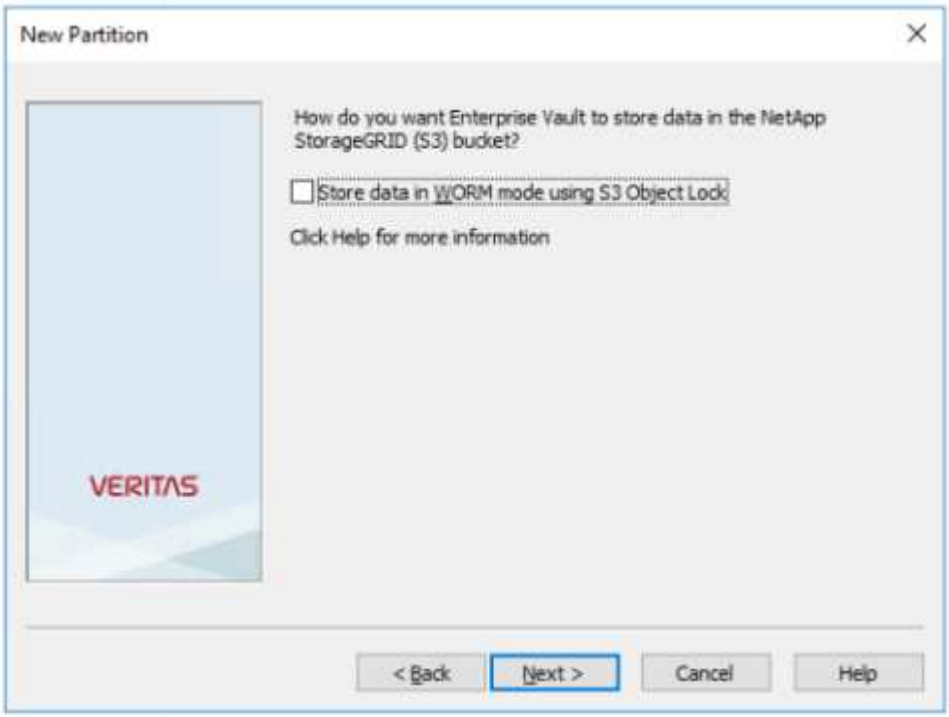
2. Erstellen Sie eine neue Vault-Speicherpartition im entsprechenden Vault-Speicher. Erweitern Sie den Ordner Vault Store Groups und anschließend den entsprechenden Vault-Speicher. Klicken Sie mit der rechten Maustaste auf Partition, und wählen Sie MENU:New[Partition].



3. Folgen Sie dem Assistenten zum Erstellen neuer Partitionen. Wählen Sie aus dem Dropdown-Menü Speichertyp die Option NetApp StorageGRID (S3) aus. Klicken Sie Auf Weiter.

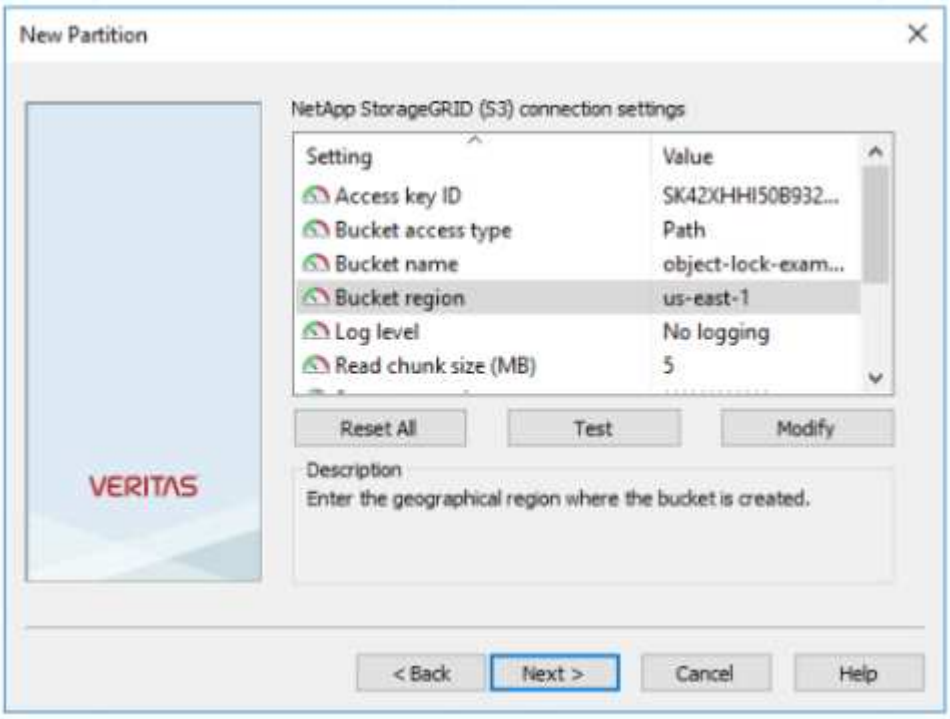


4. Lassen Sie die Option Daten im WORM-Modus mit S3 Objektsperre speichern deaktiviert. Klicken Sie Auf Weiter.

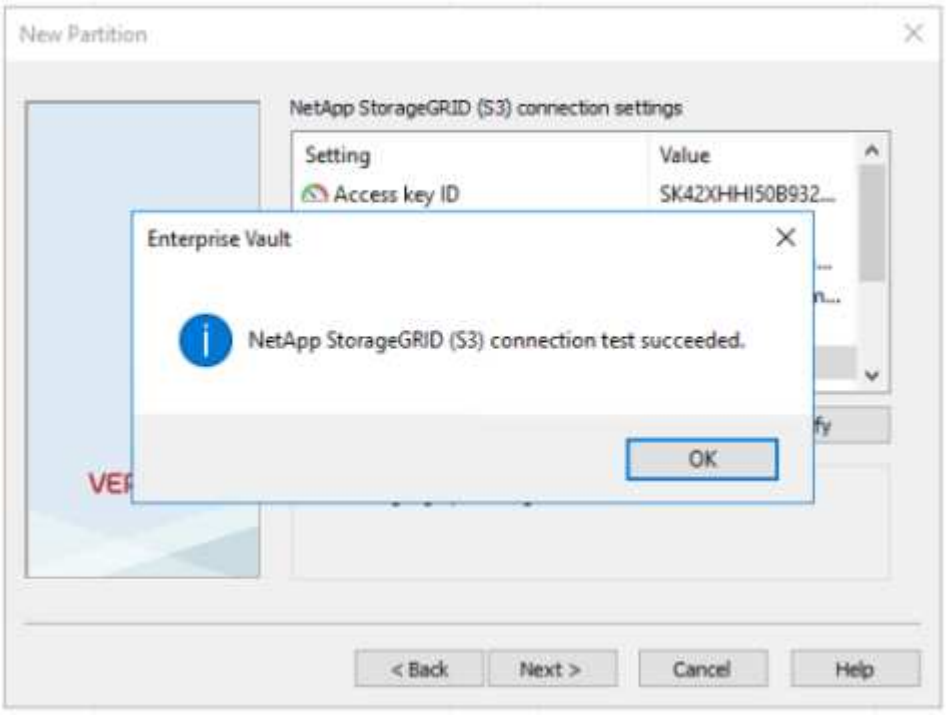


5. Geben Sie auf der Seite Verbindungseinstellungen folgende Informationen ein:
   - Zugriffsschlüssel-ID
   - Geheimer Zugriffsschlüssel
   - Service-Host-Name: Stellen Sie sicher, dass der in StorageGRID konfigurierte Load Balancer-Endpunkt (LBE)-Port (z. B. https://<hostname>:<LBE_port>) einbezogen wird.

- Bucket-Name: Name des bereits erstellten Ziel-Buckets. Veritas Enterprise Vault erstellt den Bucket nicht.
- Bucket-Region: `us-east-1` Ist der Standardwert.

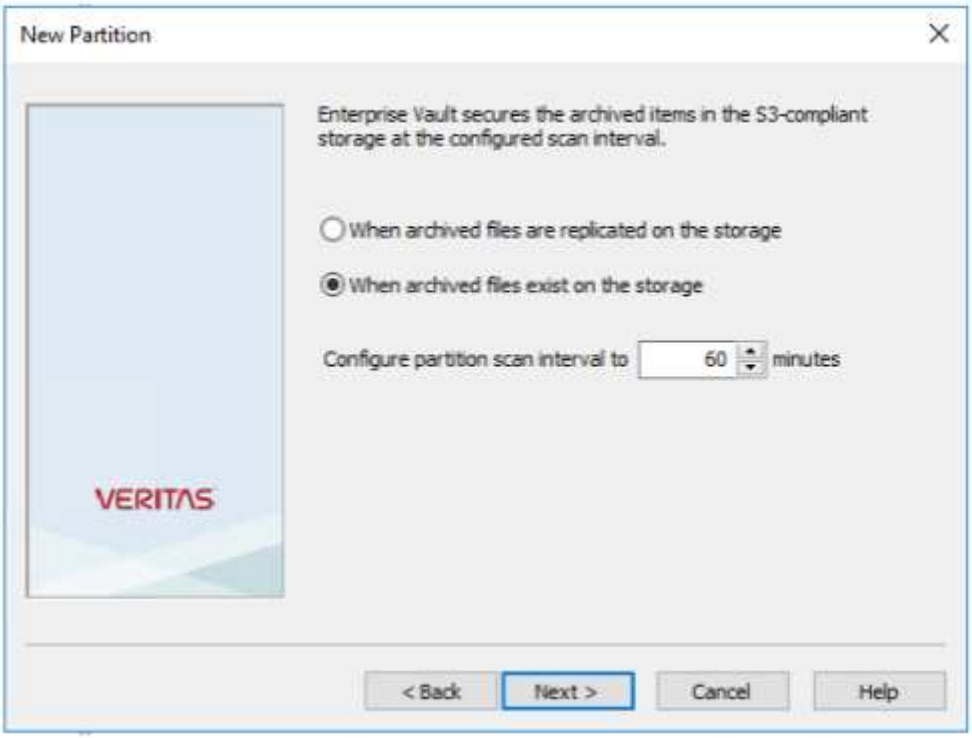


6. Um die Verbindung zum StorageGRID-Bucket zu überprüfen, klicken Sie auf Test. Überprüfen Sie, ob der Verbindungstest erfolgreich war. Klicken Sie auf OK und dann auf Weiter.

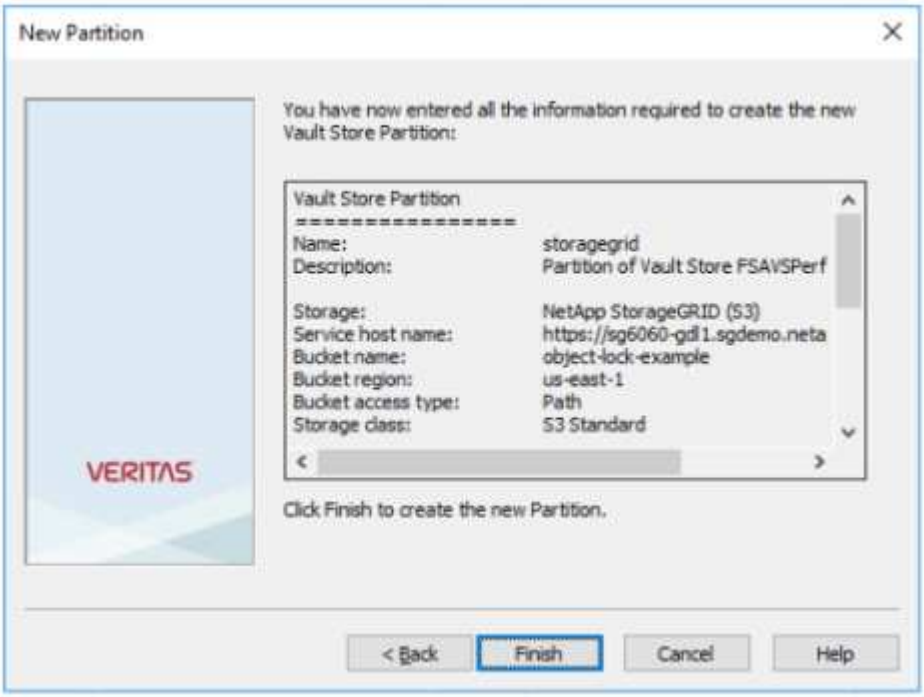


7. StorageGRID unterstützt den S3-Replizierungsparameter nicht. Zum Schutz Ihrer Objekte verwendet StorageGRID Regeln für Information Lifecycle Management (ILM), um Datensicherungsschemata festzulegen – mehrere Kopien oder Erasure Coding. Wählen Sie die Option Wenn archivierte Dateien im

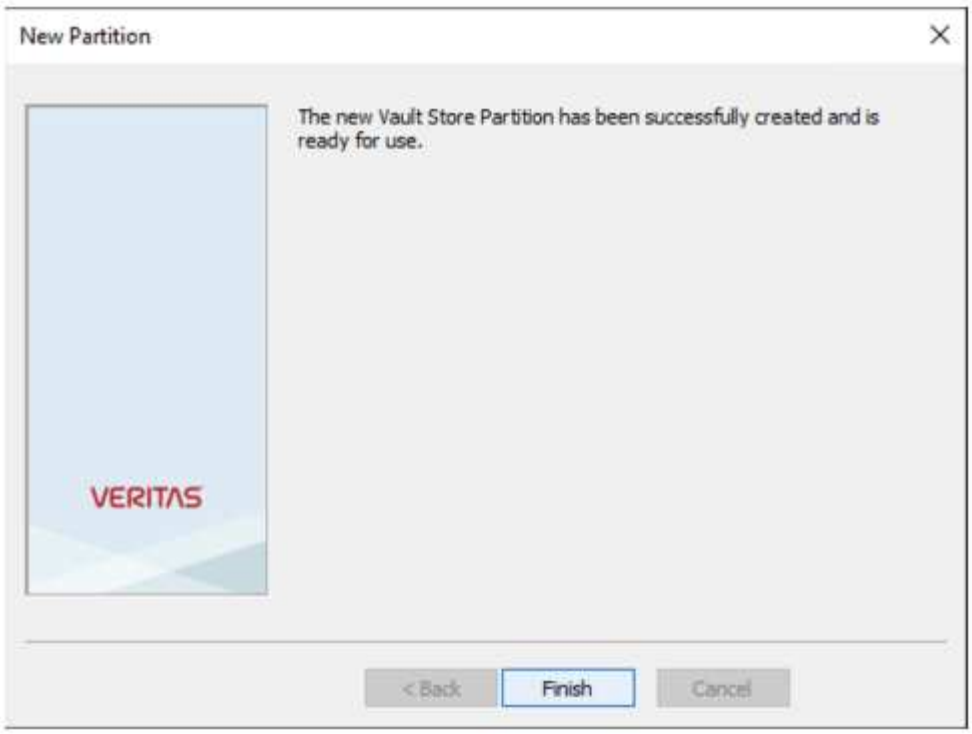
Speicher vorhanden sind aus, und klicken Sie auf Weiter.



8. Überprüfen Sie die Informationen auf der Übersichtsseite, und klicken Sie auf Fertig stellen.



9. Nachdem die neue Vault-Speicherpartition erfolgreich erstellt wurde, können Sie Daten in Enterprise Vault mit StorageGRID als primärem Speicher archivieren, wiederherstellen und suchen.



Konfigurieren Sie die StorageGRID S3 Objektsperre für WORM Storage

Erfahren Sie, wie Sie StorageGRID für WORM-Storage mit S3 Object Lock konfigurieren.

Voraussetzungen für die Konfiguration von StorageGRID für WORM Storage

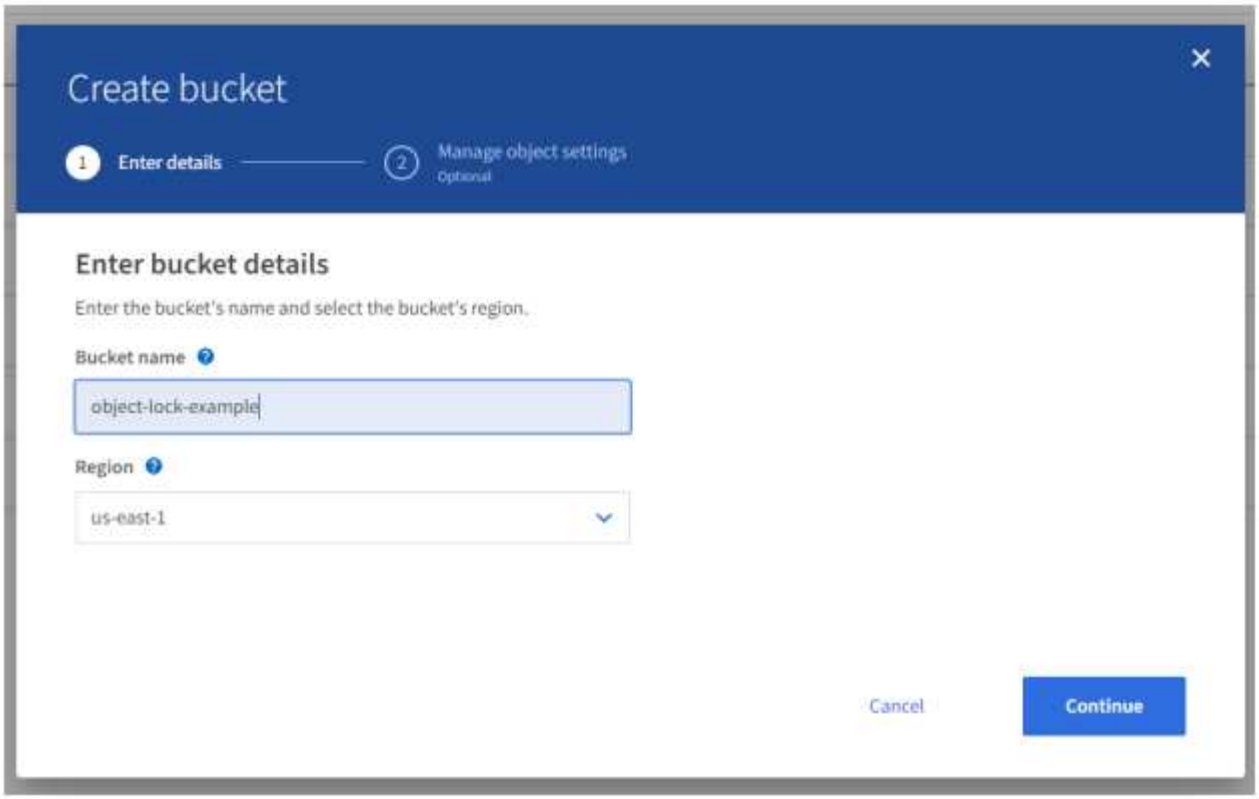
Bei WORM-Storage verwendet StorageGRID S3 Objektsperre, um Objekte zwecks Compliance aufzubewahren. Dies erfordert StorageGRID 11.6 oder höher. Dabei wurde die standardmäßige S3 Object Lock Bucket-Aufbewahrung eingeführt. Enterprise Vault erfordert außerdem Version 14.2.2 oder höher.

Konfigurieren Sie die standardmäßige Bucket-Aufbewahrung von StorageGRID S3 Object Lock

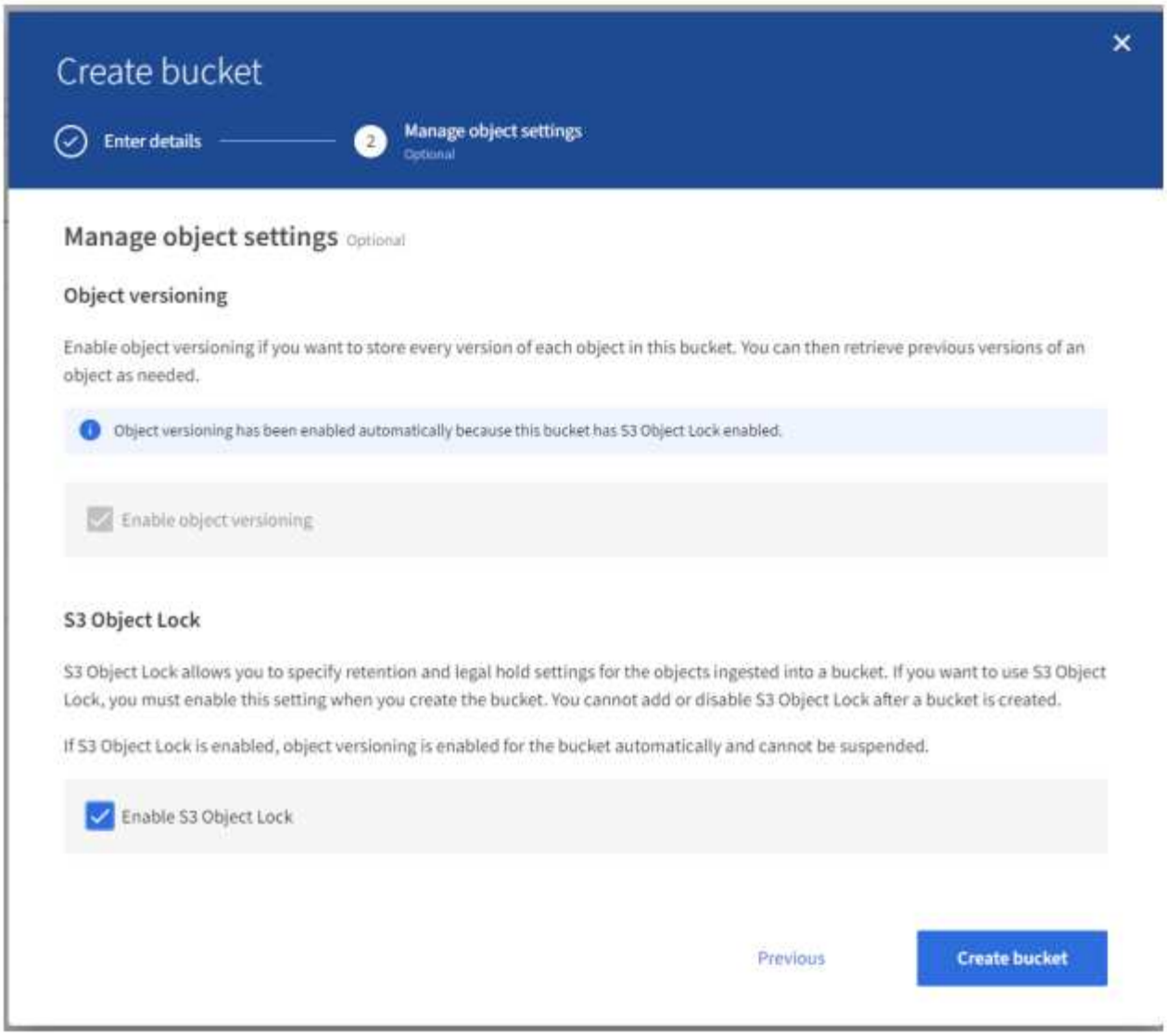
Führen Sie die folgenden Schritte aus, um die standardmäßige Bucket-Aufbewahrung von StorageGRID S3 Object Lock zu konfigurieren:

Schritte

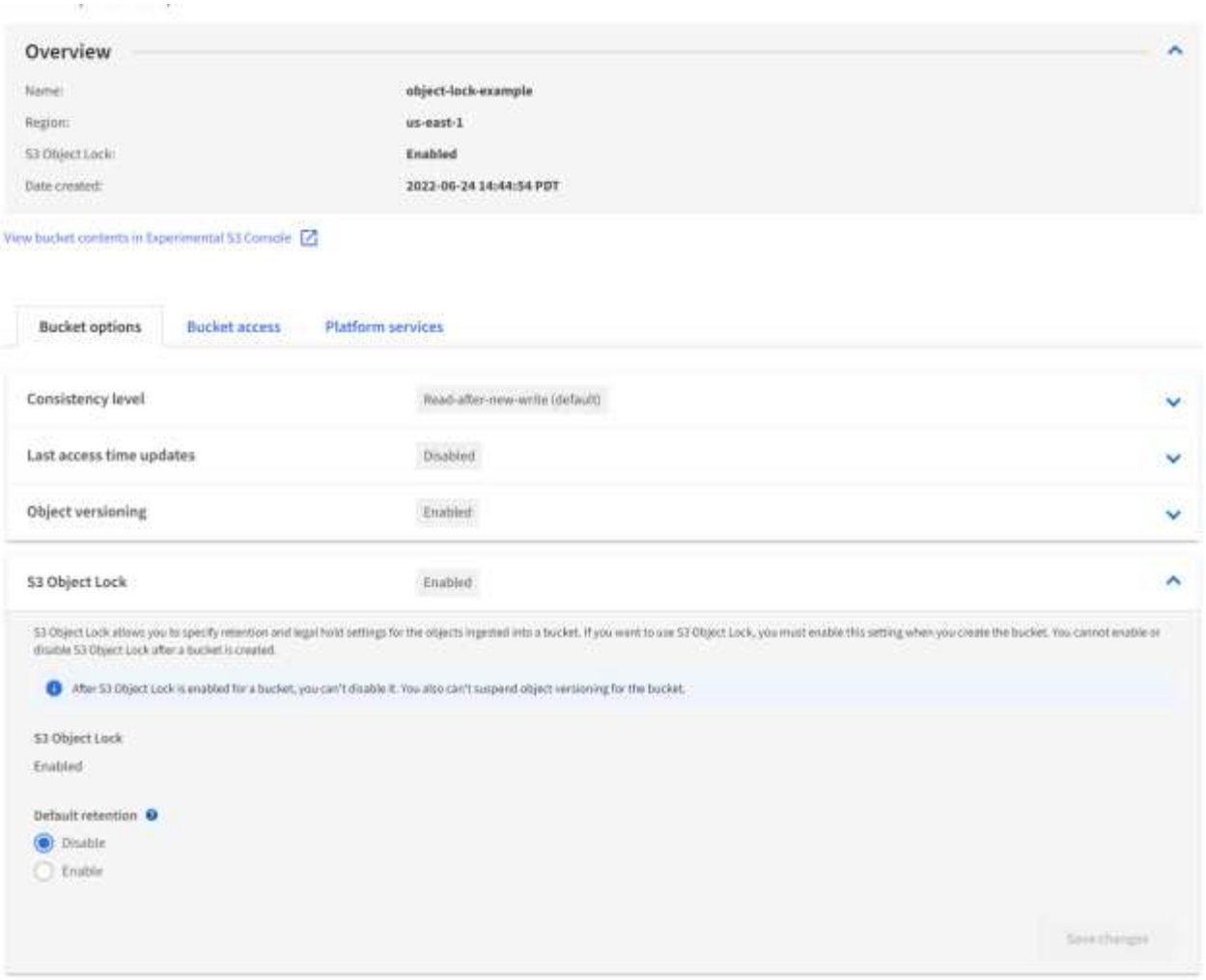
1. Erstellen Sie in StorageGRID-Mandantenmanager einen Bucket, und klicken Sie auf Fortfahren



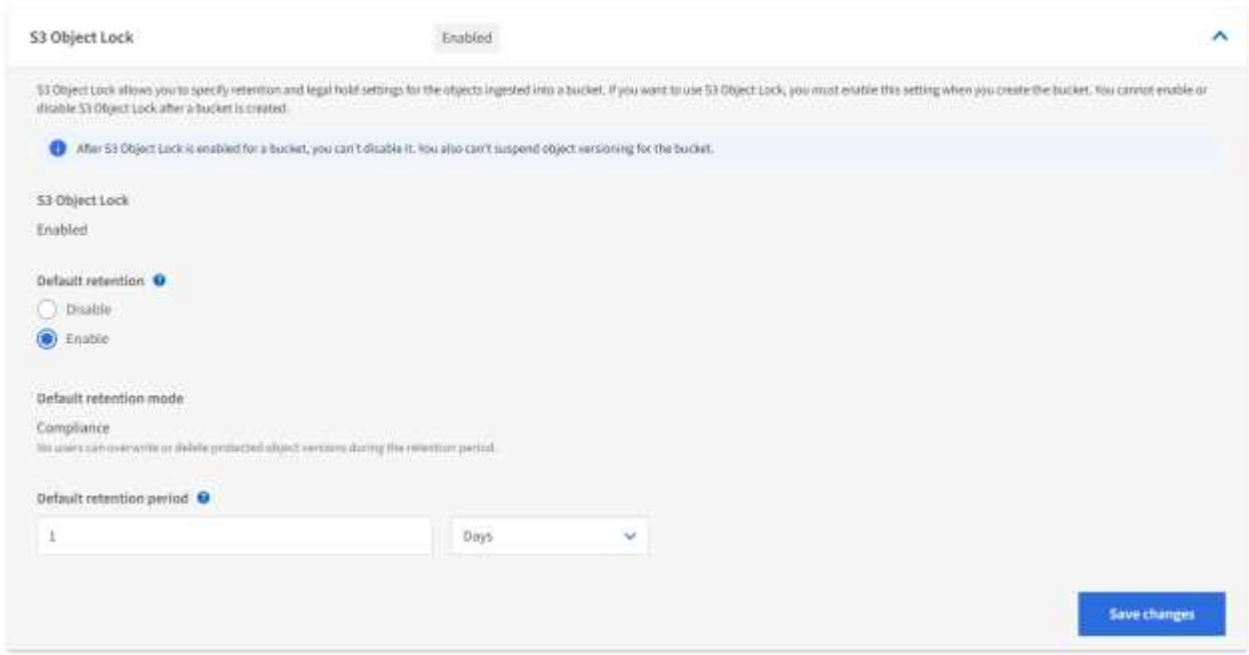
2. Wählen Sie die Option S3-Objektsperre aktivieren aus, und klicken Sie auf Bucket erstellen.



3. Nachdem der Bucket erstellt wurde, wählen Sie den Bucket aus, um die Bucket-Optionen anzuzeigen. Erweitern Sie die Dropdown-Option S3 Object Lock.



4. Wählen Sie unter Standardaufbewahrung die Option Aktivieren aus, und legen Sie eine Standardaufbewahrungsfrist von 1 Tag fest. Klicken Sie Auf Änderungen Speichern.



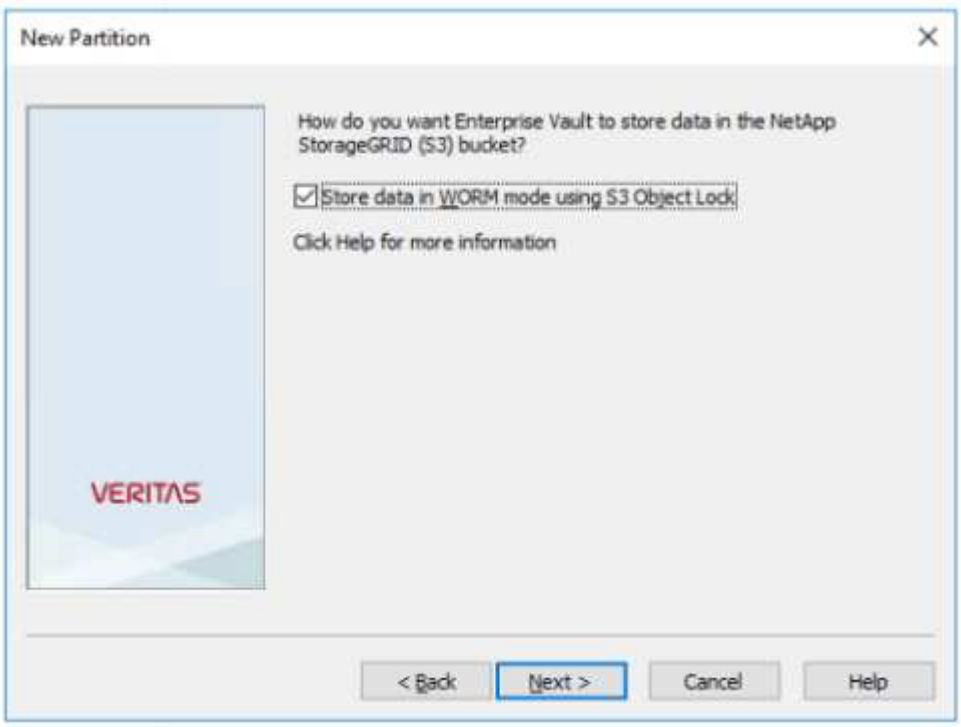
Der Bucket kann jetzt von Enterprise Vault zur Speicherung von WORM-Daten verwendet werden.

Enterprise Vault Konfigurieren

Gehen Sie wie folgt vor, um Enterprise Vault zu konfigurieren:

Schritte

1. Wiederholen Sie die Schritte 1-3 im "Basiskonfiguration" Abschnitt, wählen Sie jedoch diesmal die Option Daten im WORM-Modus mit S3 Objektsperre speichern. Klicken Sie Auf Weiter.



2. Stellen Sie bei der Eingabe der S3 Bucket-Verbindungseinstellungen sicher, dass Sie den Namen eines S3-Buckets eingeben, für den die S3 Object Lock Default Retention aktiviert ist.
3. Testen Sie die Verbindung, um die Einstellungen zu überprüfen.

Konfigurieren Sie StorageGRID-Standort-Failover für Disaster Recovery

Erfahren Sie, wie Sie ein StorageGRID-Standort-Failover in einem Disaster-Recovery-Szenario konfigurieren.

Eine Implementierung einer StorageGRID-Architektur hat gemein mehrere Standorte. Standorte können entweder aktiv/aktiv oder aktiv/Passiv für DR sein. Stellen Sie in einem DR-Szenario sicher, dass Veritas Enterprise Vault die Verbindung zu seinem primären Speicher (StorageGRID) aufrechterhalten kann und bei einem Standortausfall weiterhin Daten aufnehmen und abrufen kann. Dieser Abschnitt enthält allgemeine Konfigurationsanleitungen für eine aktiv/Passiv-Bereitstellung an zwei Standorten. Detaillierte Informationen zu diesen Richtlinien finden Sie auf der "StorageGRID-Dokumentation" Seite oder bei einem StorageGRID Experten.

Voraussetzungen für die Konfiguration von StorageGRID mit Veritas Enterprise Vault

Überprüfen Sie vor dem Konfigurieren des StorageGRID-Standort-Failover die folgenden Voraussetzungen:

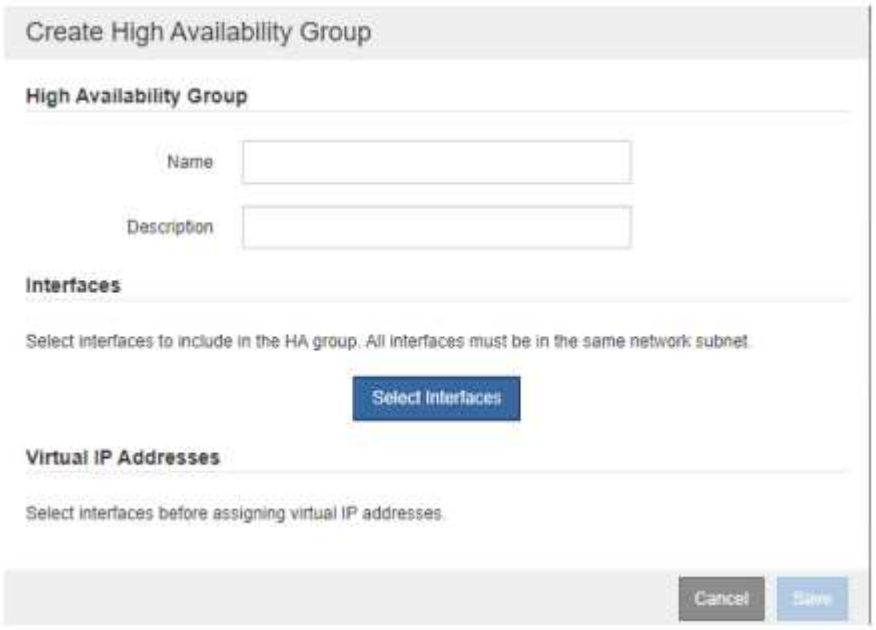
- Es gibt eine StorageGRID-Bereitstellung an zwei Standorten, z. B. Standort 1 und STANDORT 2.
- Es wurde an jedem Standort ein Admin-Node erstellt, auf dem der Load Balancer ausgeführt wird, oder ein Gateway-Node zum Lastausgleich.
- Ein Endpunkt des StorageGRID Load Balancer wurde erstellt.

Konfigurieren Sie das StorageGRID Site Failover

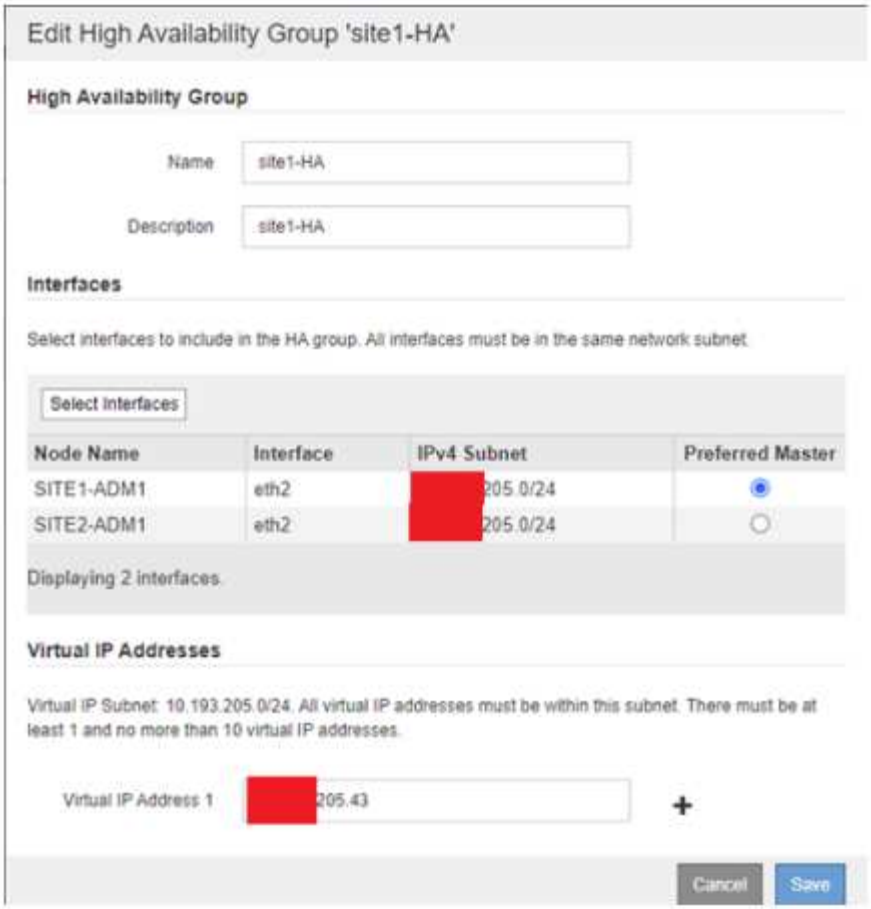
Führen Sie zum Konfigurieren des StorageGRID-Standort-Failover die folgenden Schritte aus:

Schritte

1. Konfigurieren Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit), um die Verbindung zu StorageGRID bei Standortausfällen sicherzustellen. Klicken Sie in der StorageGRID-Grid-Manager-Oberfläche (GMI) auf Konfiguration, Hochverfügbarkeitsgruppen und + Erstellen.



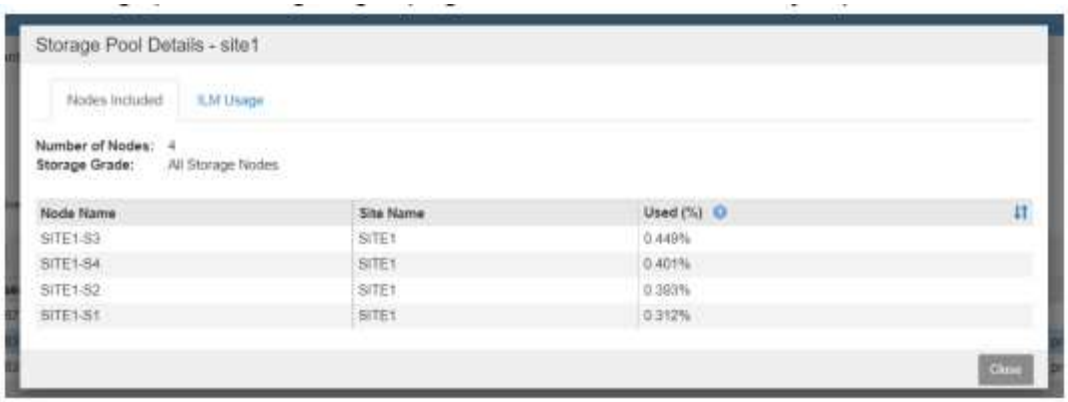
2. Geben Sie die erforderlichen Informationen ein. Klicken Sie auf Schnittstellen auswählen und schließen Sie sowohl die Netzwerkschnittstellen von SITE 1 als auch von SITE2 ein, wobei SITE 1 (der primäre Standort) der bevorzugte Master ist. Weisen Sie eine virtuelle IP-Adresse innerhalb desselben Subnetzes zu. Klicken Sie auf Speichern .

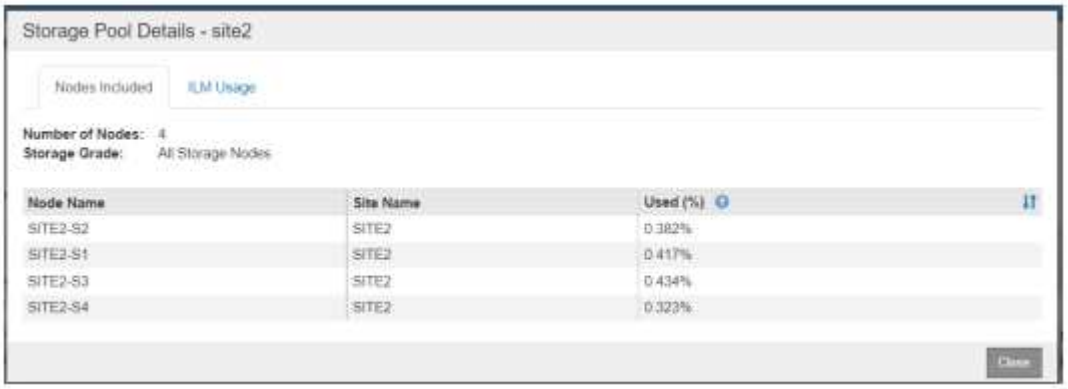


3. Diese virtuelle IP (VIP)-Adresse sollte dem S3-Hostnamen zugeordnet werden, der während der Partitionskonfiguration von Veritas Enterprise Vault verwendet wird. Die VIP-Adresse löst Datenverkehr an STANDORT 1 auf. Während STANDORT 1-Fehler leitet die VIP-Adresse den Datenverkehr transparent an STANDORT 2 um.
4. Stellen Sie sicher, dass die Daten sowohl an STANDORT 1 als auch an STANDORT 2 repliziert werden. So sind die Objektdaten auch bei Ausfall von STANDORT 1 von SITE2 aus verfügbar. Dazu müssen zunächst die Speicherpools konfiguriert werden.

   Klicken Sie in StorageGRID GMI auf ILM, Speicherpools und dann auf Erstellen. Folgen Sie dem Assistenten, um zwei Speicherpools zu erstellen: Einen für STANDORT 1 und einen anderen für STANDORT 2.

   Storage-Pools sind logische Gruppen von Nodes, die zur Definition der Objektplatzierung verwendet werden





5. Klicken Sie in StorageGRID GMI auf ILM, Regeln und dann auf + Erstellen. Befolgen Sie den Assistenten, um eine ILM-Regel zu erstellen, die eine Kopie angibt, die pro Standort mit einem ausgewogenen Aufnahmeverhalten gespeichert werden soll.

6. Fügen Sie die ILM-Regel einer ILM-Richtlinie hinzu und aktivieren Sie die Richtlinie.

Diese Konfiguration hat das folgende Ergebnis:

- Eine virtuelle S3-Endpunkt-IP, wobei STANDORT 1 der primäre und STANDORT 2 der sekundäre Endpunkt ist. Wenn STANDORT 1 ausfällt, erfolgt ein Failover der VIP auf STANDORT 2.
- Wenn archivierte Daten von Veritas Enterprise Vault gesendet werden, stellt StorageGRID sicher, dass eine Kopie auf SITE 1 gespeichert wird und eine andere DR-Kopie in SITE2 gespeichert wird. Wenn STANDORT 1 ausfällt, wird Enterprise Vault weiterhin von STANDORT 2 aufgenommen und abgerufen.

Beide Konfigurationen sind für Veritas Enterprise Vault transparent. Der S3-Endpunkt, der Bucket-Name, die Zugriffsschlüssel usw. sind identisch. Es ist nicht notwendig, die S3-Verbindungseinstellungen auf der Veritas Enterprise Vault-Partition neu zu konfigurieren.