TR-4907：『Configure StorageGRID with Veritas Enterprise Vault』

How to enable StorageGRID in your environment

NetApp
July 05, 2024

目次

TR-4907：『Configure StorageGRID with Veritas Enterprise Vault』

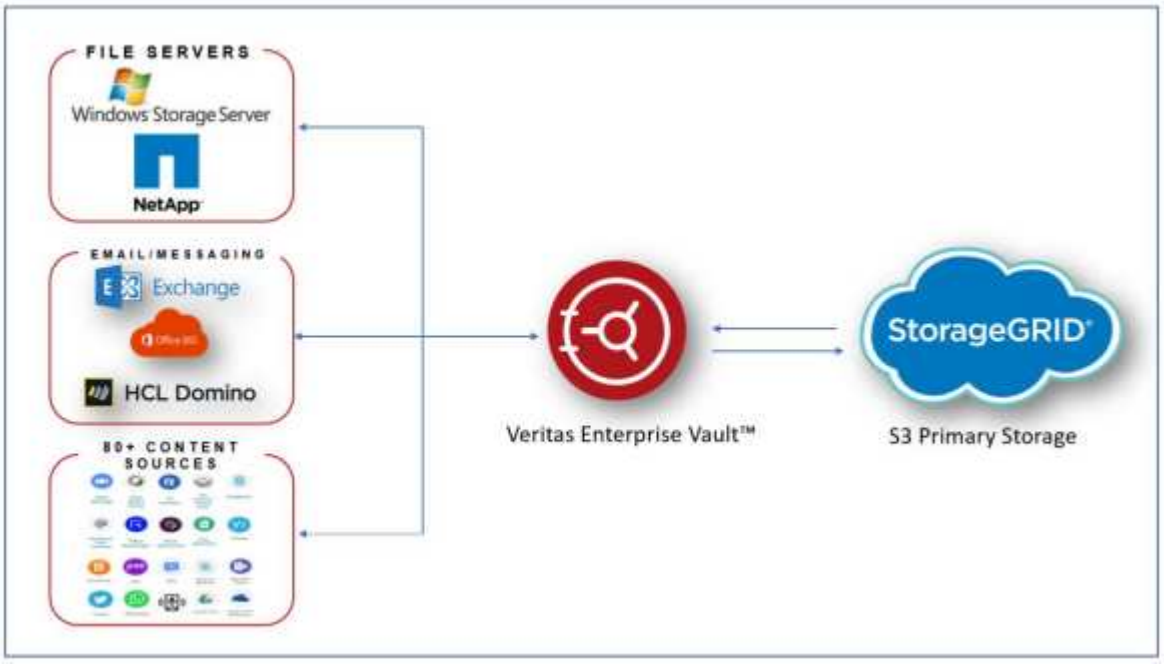
サイトフェイルオーバーのためのStorageGRIDの設定の概要

Veritas Enterprise Vaultでは、ディザスタリカバリのプライマリストレージターゲットとしてStorageGRIDを使用しています。

この構成ガイドでは、NetApp®StorageGRID®をVeritas Enterprise Vaultのプライマリストレージターゲットとして設定する手順を説明します。また、ディザスタリカバリ（DR）シナリオでサイトフェイルオーバー用にStorageGRIDを設定する方法についても説明します。

リファレンスアーキテクチャ

StorageGRIDは、Veritas Enterprise Vault向けにオンプレミスのS3互換クラウドバックアップターゲットを提供します。次の図は、Veritas Enterprise VaultとStorageGRIDのアーキテクチャを示しています。



追加情報の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- NetApp StorageGRIDドキュメントセンター https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRIDイネーブルメント https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRIDドキュメントリソースページ https://www.netapp.com/data-storage/storagegrid/documentation/
- NetApp製品ドキュメント https://www.netapp.com/support-and-training/documentation/

StorageGRIDとVeritas Enterprise Vaultの設定

StorageGRID 11.5以降およびVeritas Enterprise Vault 14.1以降の基本構成を実装する方法について説明します。

この構成ガイドは、StorageGRID 11.5およびEnterprise Vault 14.1に基づいています。Write Onceには、S3 Object Lock、StorageGRID 11.6、Enterprise Vault 14.2.2を使用したRead Many（WORM）モードのストレージを使用しました。これらのガイドラインの詳細については、ページを参照する "StorageGRID のドキュメント" か、StorageGRIDの専門家にお問い合わせください。

StorageGRIDとVeritas Enterprise Vaultを設定するための前提条件

- Veritas Enterprise VaultでStorageGRIDを設定する前に、次の前提条件を確認してください。

> WORMストレージ（オブジェクトロック）には、StorageGRID 11.6以降が必要です。

- Veritas Enterprise Vault 14.1以降がインストールされている。

> WORMストレージ（オブジェクトロック）の場合は、Enterprise Vaultバージョン14.2.2以降が必要です。

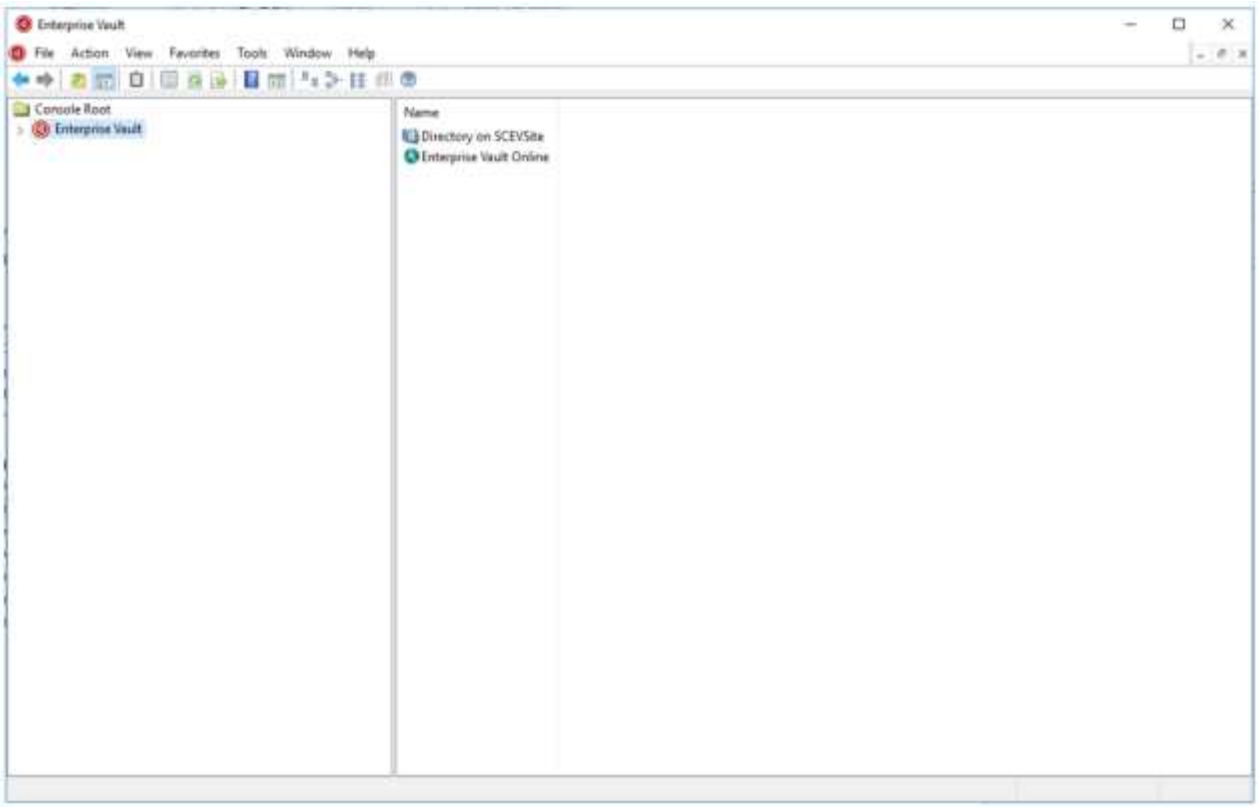
- ボールトストアグループとボールトストアが作成されました。詳細については、『Veritas Enterprise Vault Administration Guide』を参照してください。
- StorageGRIDテナント、アクセスキー、シークレットキー、およびバケットが作成されている。
- StorageGRIDロードバランサエンドポイント（HTTPまたはHTTPS）が作成されている。
- 自己署名証明書を使用する場合は、StorageGRID自己署名CA証明書をEnterprise Vaultサーバーに追加します。詳細については、こちらを参照して "Veritasナレッジベースの記事"ください。
- 最新のEnterprise Vault構成ファイルを更新して適用し、NetApp StorageGRIDなどのサポートされているストレージソリューションを有効にします。詳細については、こちらを参照して "Veritasナレッジベースの記事"ください。

Veritas Enterprise Vaultを使用したStorageGRIDの設定

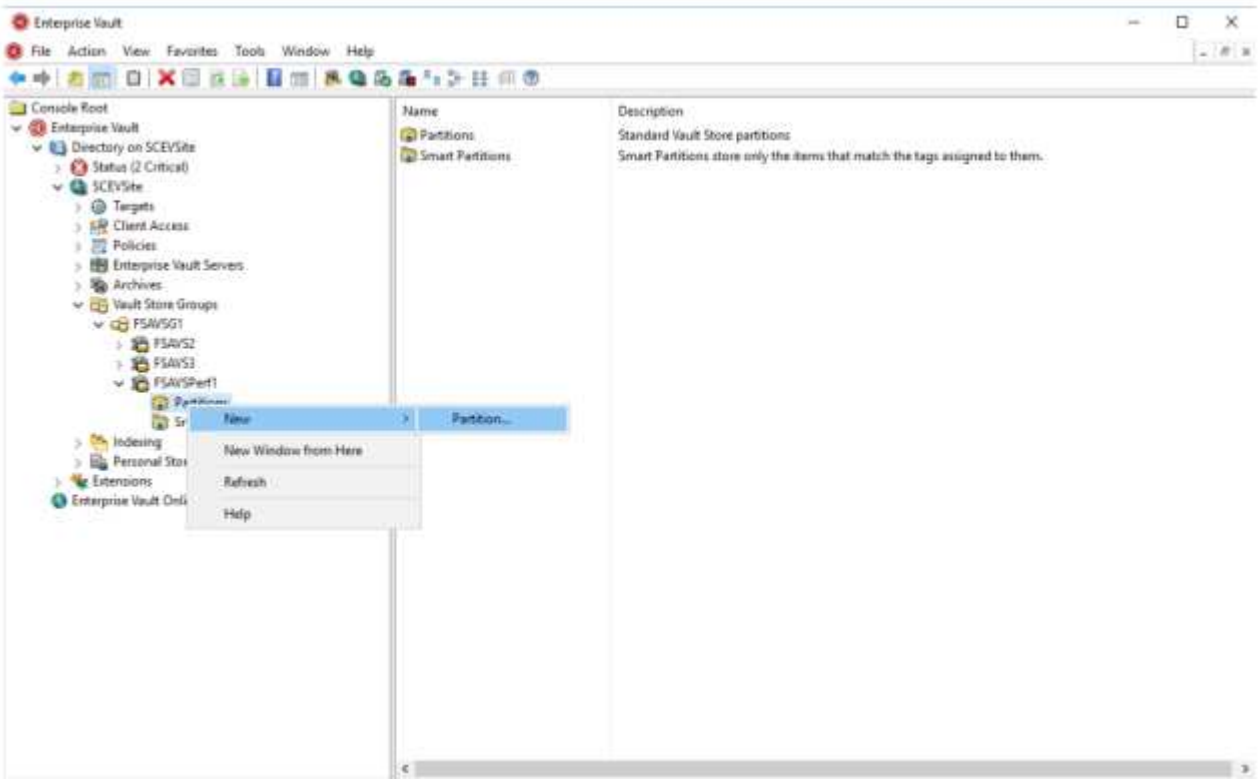
Veritas Enterprise Vaultを使用してStorageGRIDを設定するには、次の手順を実行します。

手順

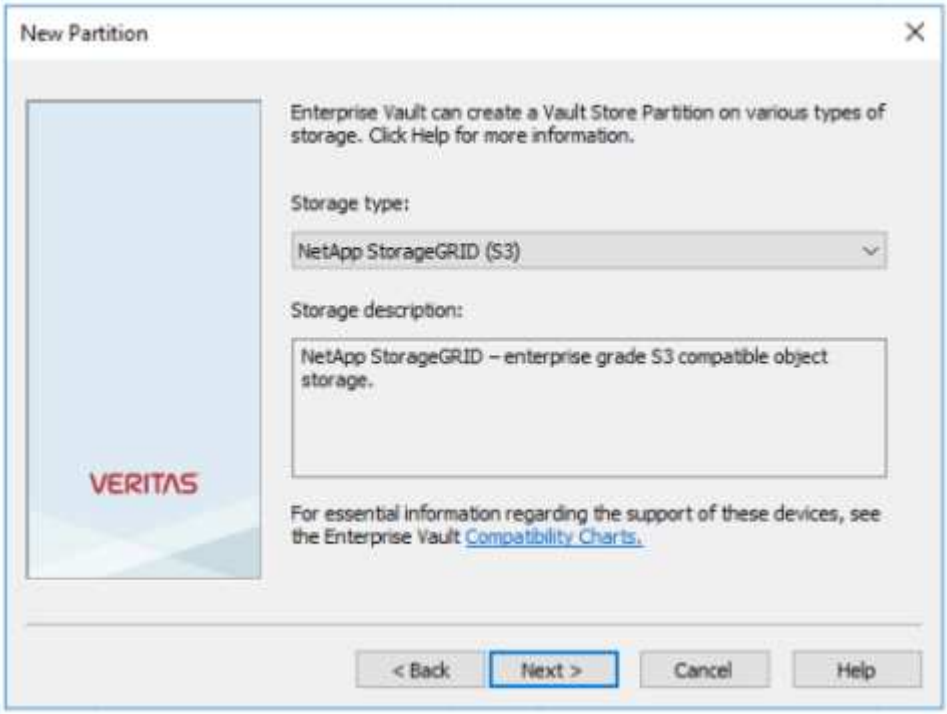
1. Enterprise Vault管理コンソールを起動します。



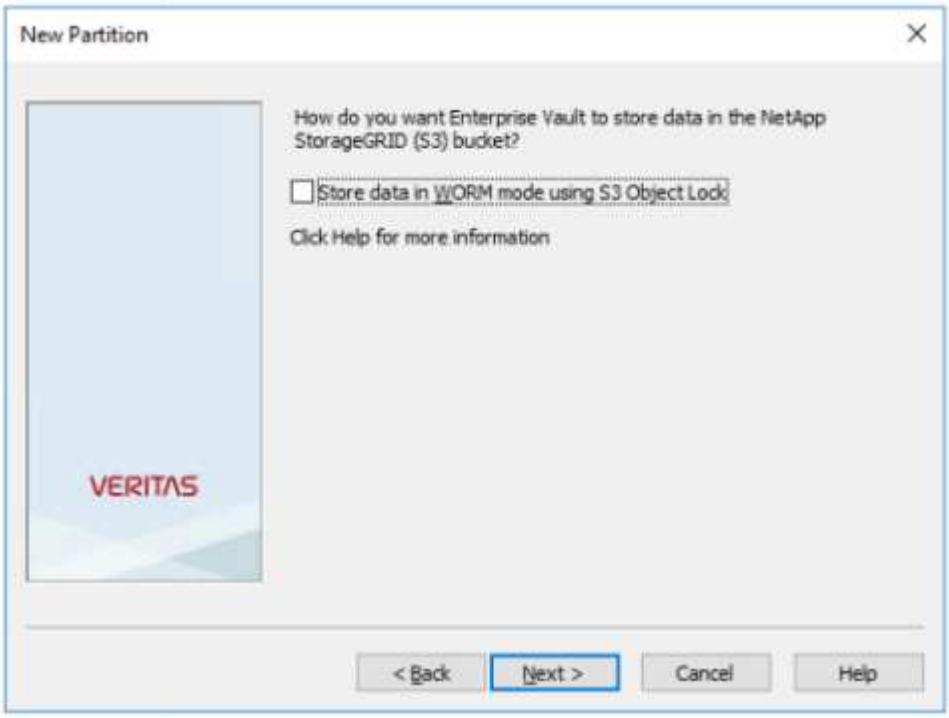
2. 適切なボールトストアに新しいボールトストアパーティションを作成します。ボールトストアグループ（Vault Store Groups）フォルダを展開し、適切なボールトストアを展開します。「パーティション」を右クリックし、メニュー「新規パーティション」を選択します。



3. 新しいパーティションの作成ウィザードに従います。[Storage Type]ドロップダウンメニューから、NetApp StorageGRID（S3）を選択します。[Next]をクリックします。

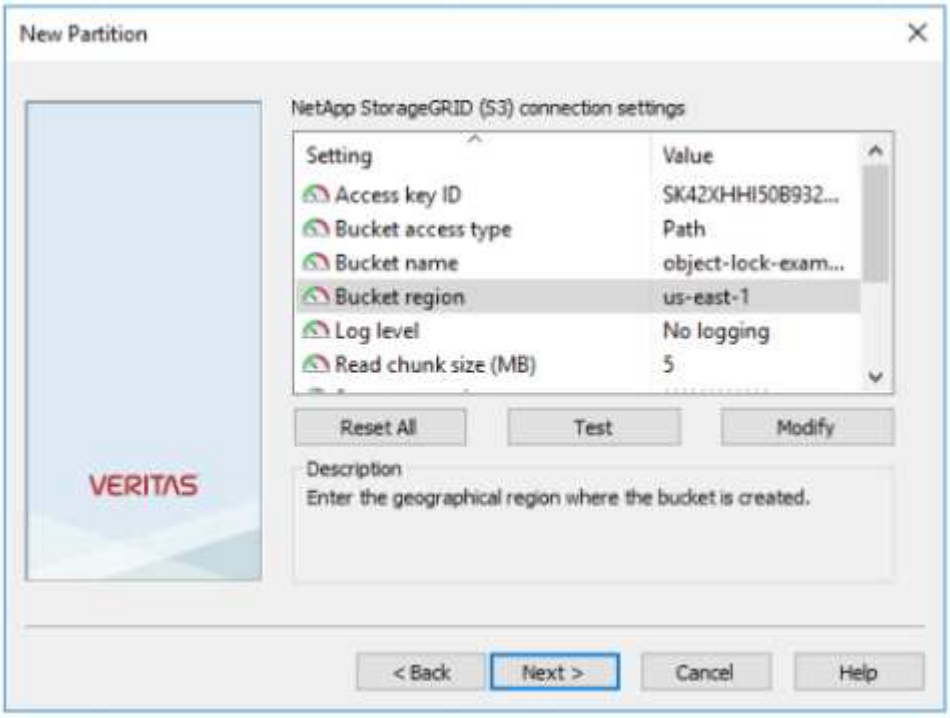


4. [Store Data in WORM Mode using S3 Object Lock]オプションはオフのままにします。[Next]をクリックします。

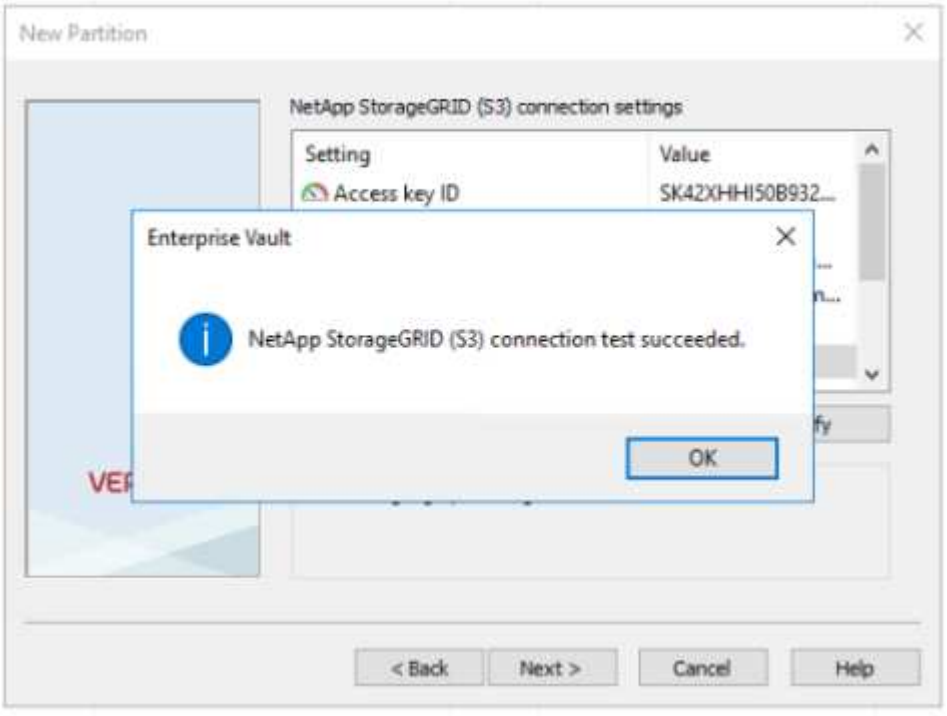


5. 接続設定ページで、次の情報を入力します。
   - アクセスキーID
   - シークレットアクセスキー
   - サービスホスト名：StorageGRIDで設定されたロードバランサエンドポイント（LBE）ポート（\https：//<hostname>：<LBE_port>など）を含めるようにしてください。

- Bucket name：事前に作成されたターゲットバケットの名前。Veritas Enterprise Vaultはバケットを作成しません。
- Bucket region： `us-east-1` デフォルト値。

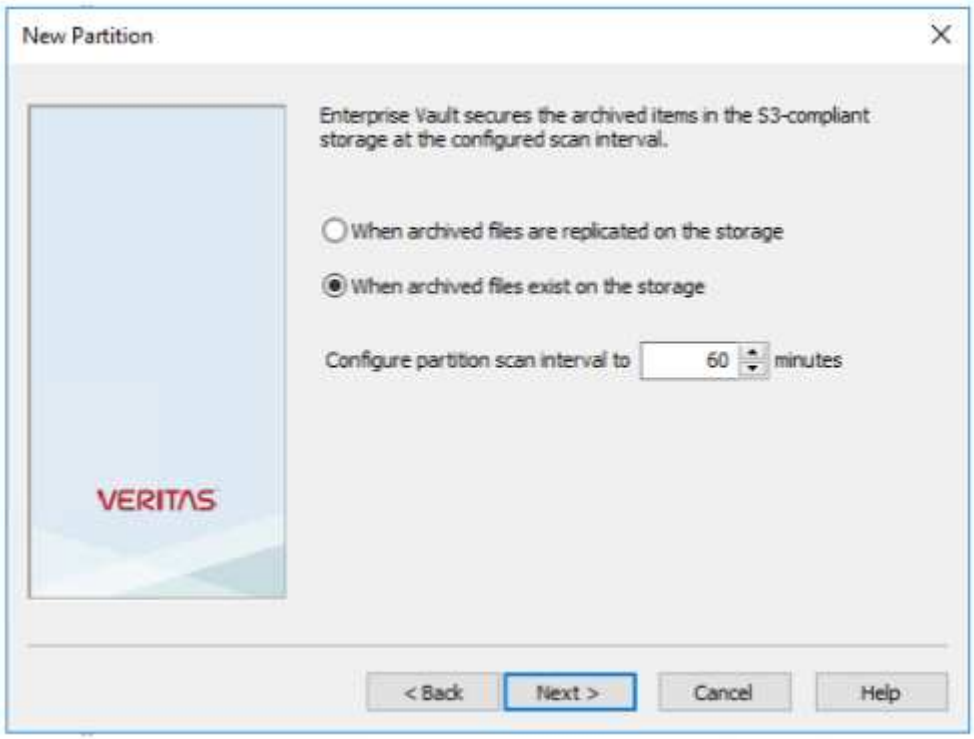


6. StorageGRIDバケットへの接続を確認するには、[Test]をクリックします。接続テストが成功したことを確認します。[OK]をクリックし、[Next]をクリックします。

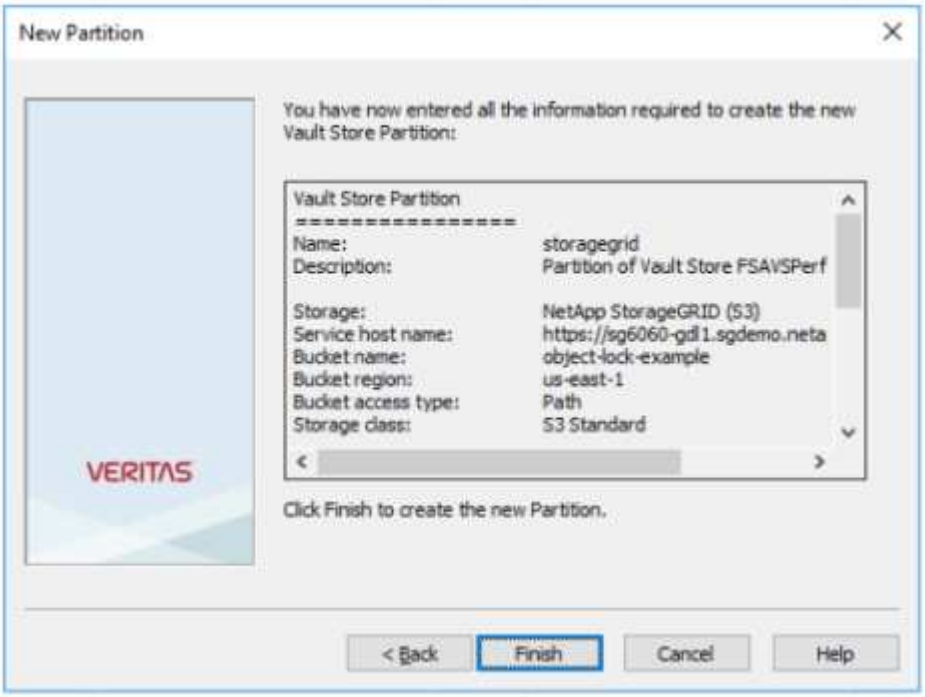


7. StorageGRIDでは、S3レプリケーションパラメータがサポートされません。StorageGRIDでは、オブジェクトを保護するために、情報ライフサイクル管理（ILM）ルールを使用してデータ保護スキーム（複数の

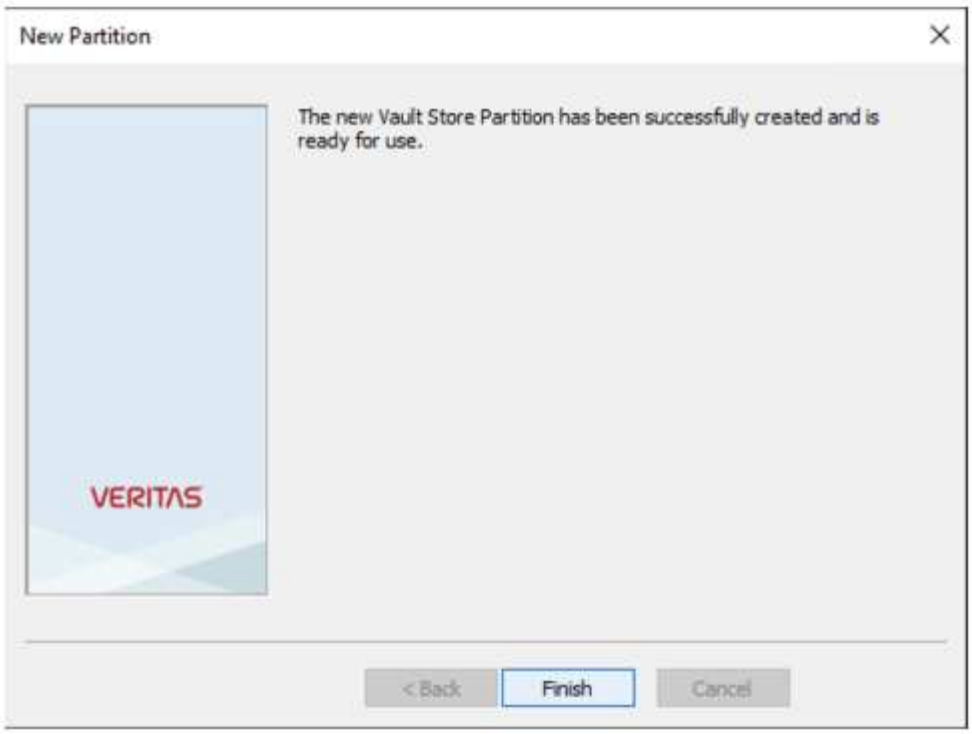
コピーまたはイレイジャーコーディング）を指定します。[When Archived Files Exist on the Storage]オプションを選択し、[Next]をクリックします。



8. 概要ページの情報を確認し、[Finish]をクリックします。



9. 新しいヴォールトストアパーティションが正常に作成されたら、StorageGRIDをプライマリストレージとして使用するEnterprise Vaultでデータをアーカイブ、リストア、および検索できます。



WORMストレージ用のStorageGRID S3オブジェクトロックの設定

S3オブジェクトロックを使用してWORMストレージ用にStorageGRIDを設定する方法について説明します。

WORMストレージ用にStorageGRIDを設定するための前提条件

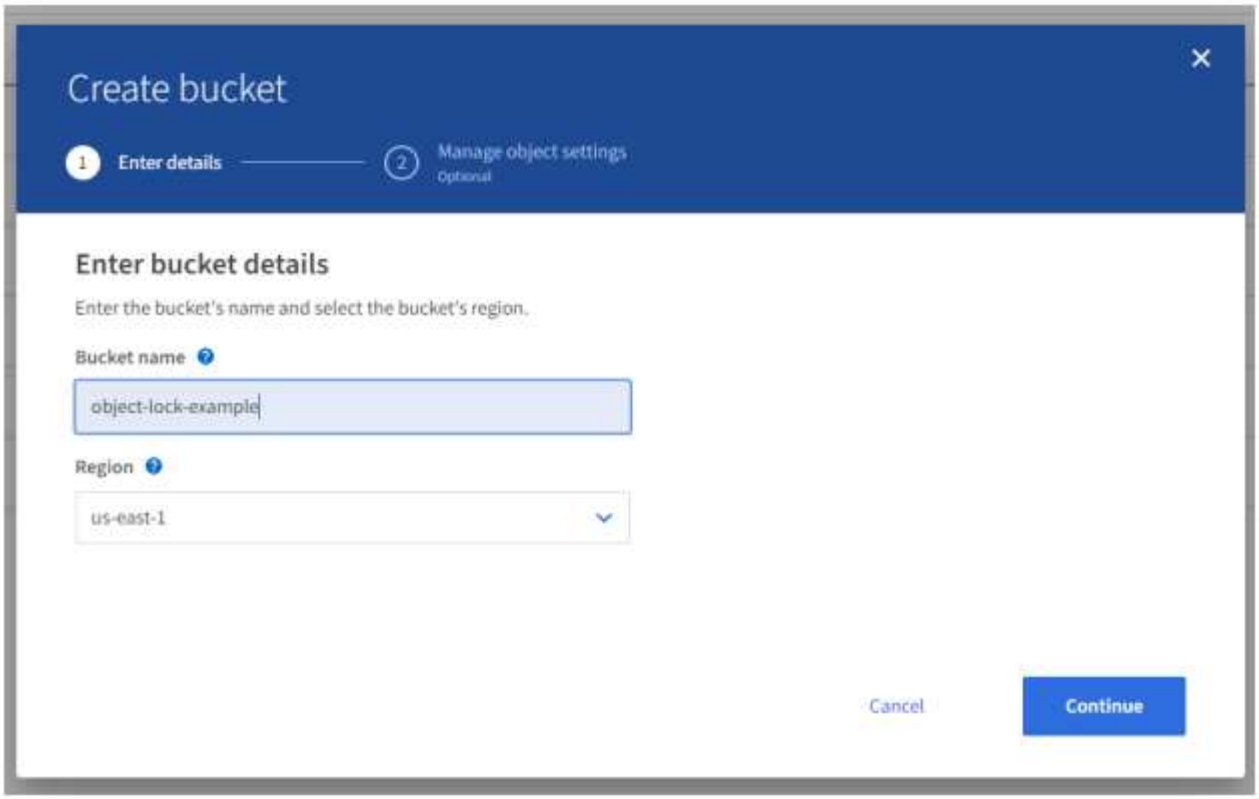
WORMストレージでは、StorageGRIDはS3オブジェクトロックを使用してオブジェクトを保持し、コンプライアンスを確保します。これには、S3オブジェクトロックのデフォルトバケット保持機能が導入されたStorageGRID 11.6以降が必要です。Enterprise Vaultにはバージョン14.2.2以降も必要です。

StorageGRID S3オブジェクトロックのデフォルトバケット保持の設定

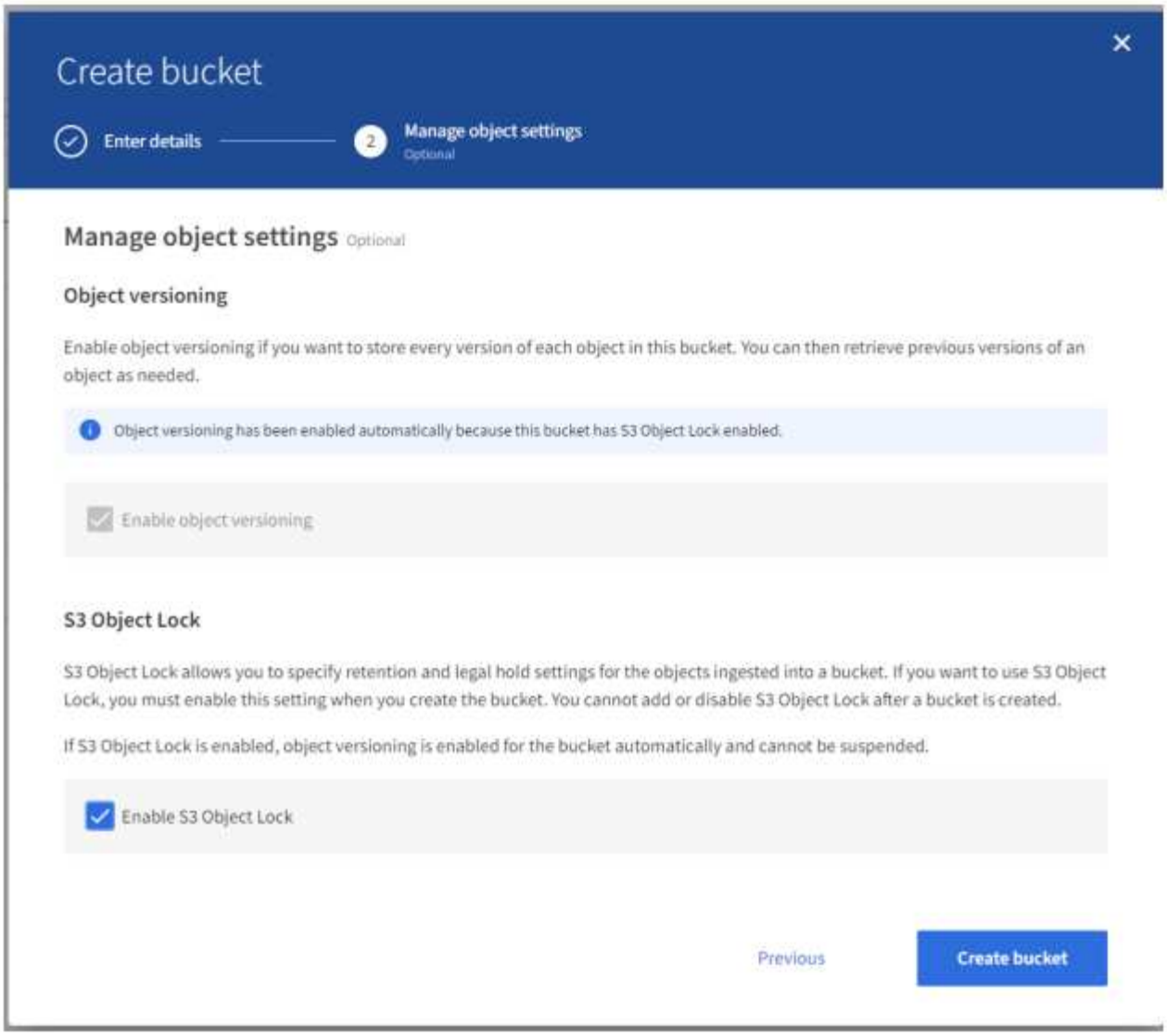
StorageGRID S3オブジェクトロックのデフォルトバケット保持を設定するには、次の手順を実行します。

手順

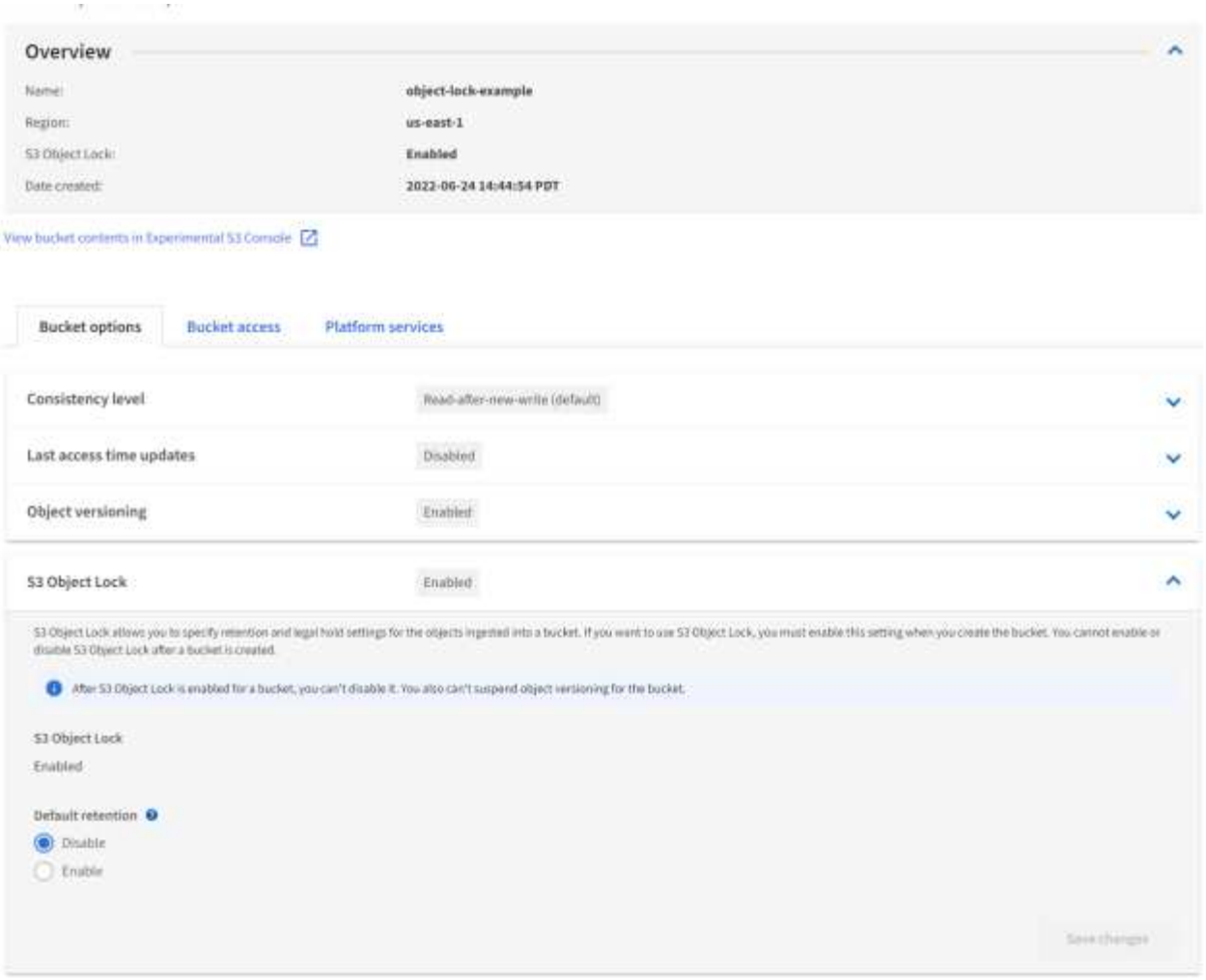
1. StorageGRIDテナントマネージャでバケットを作成し、[Continue]をクリックします。



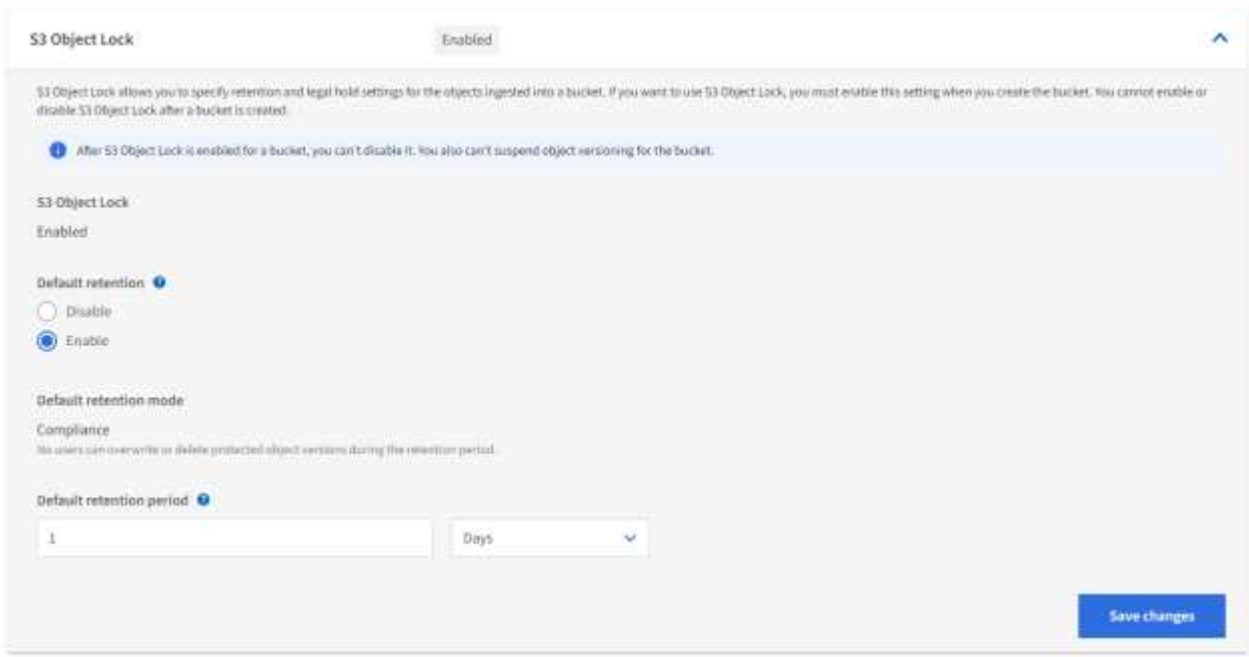
2. [Enable S3 Object Lock]オプションを選択し、[Create Bucket]をクリックします。



3. バケットの作成後、バケットを選択してバケットのオプションを表示します。[S3 Object Lock]ドロップダウンオプションを展開します。



4. [Default Retention]で[Enable]を選択し、デフォルトの保持期間を1日に設定します。[Save Changes]をクリックします。



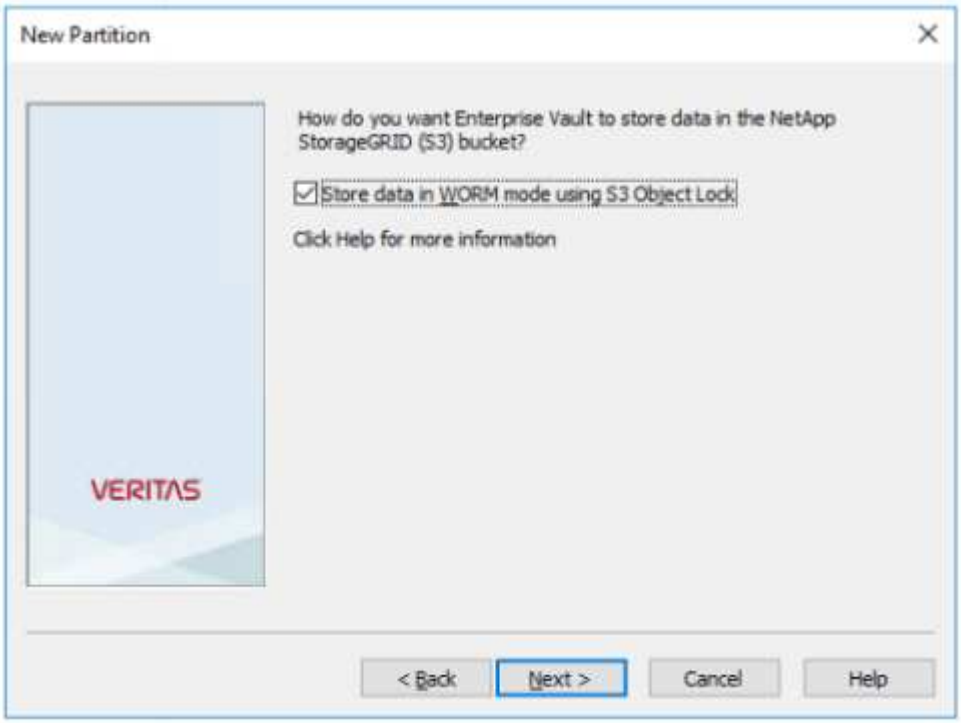
これで、バケットをEnterprise VaultでWORMデータの格納に使用できるようになりました。

Enterprise Vaultの設定

Enterprise Vaultを設定するには、次の手順を実行します。

手順

1. セクションの手順1~3を繰り返し "キホンセツ" ますが、今回は[Store data in WORM Mode using S3 Object Lock]オプションを選択します。[Next]をクリックします。



2. S3バケット接続設定を入力するときは、S3オブジェクトロックのデフォルトの保持が有効になっているS3バケットの名前を入力します。
3. 接続をテストして設定を確認します。

ディザスタリカバリ用のStorageGRIDサイトフェイルオーバーの設定

ディザスタリカバリシナリオでStorageGRIDサイトのフェイルオーバーを設定する方法について説明します。

StorageGRIDアーキテクチャをマルチサイトに導入するのは一般的です。サイトは、DRのアクティブ/アクティブまたはアクティブ/パッシブにすることができます。DRシナリオでは、Veritas Enterprise Vaultがプライマリストレージ（StorageGRID）への接続を維持し、サイト障害が発生してもデータの取り込みと読み出しを継続できることを確認します。この項では、2サイトのアクティブ/パッシブ配置の概要を説明します。 これらのガイドラインの詳細については、ページを参照する "StorageGRID のドキュメント" か、StorageGRIDの専門家にお問い合わせください。

Veritas Enterprise VaultでStorageGRIDを設定するための前提条件

StorageGRIDサイトのフェイルオーバーを設定する前に、次の前提条件を確認してください。

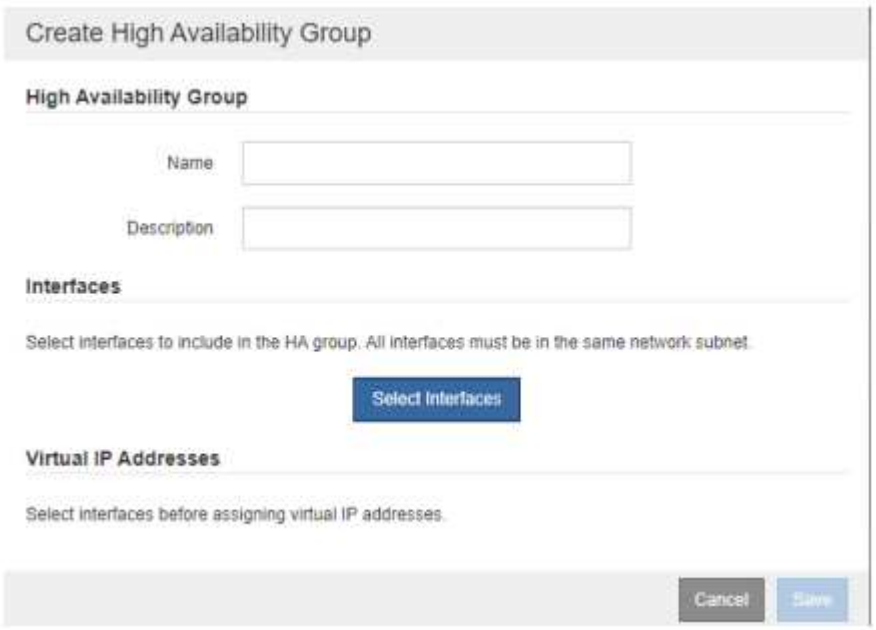
- 2サイトのStorageGRID環境（たとえば、Site1とSite2）があります。
- ロードバランササービスを実行する管理ノード、またはロードバランシングのためのゲートウェイノードが各サイトに作成されている。
- StorageGRIDロードバランサエンドポイントが作成されている。

StorageGRIDサイトのフェイルオーバーの設定

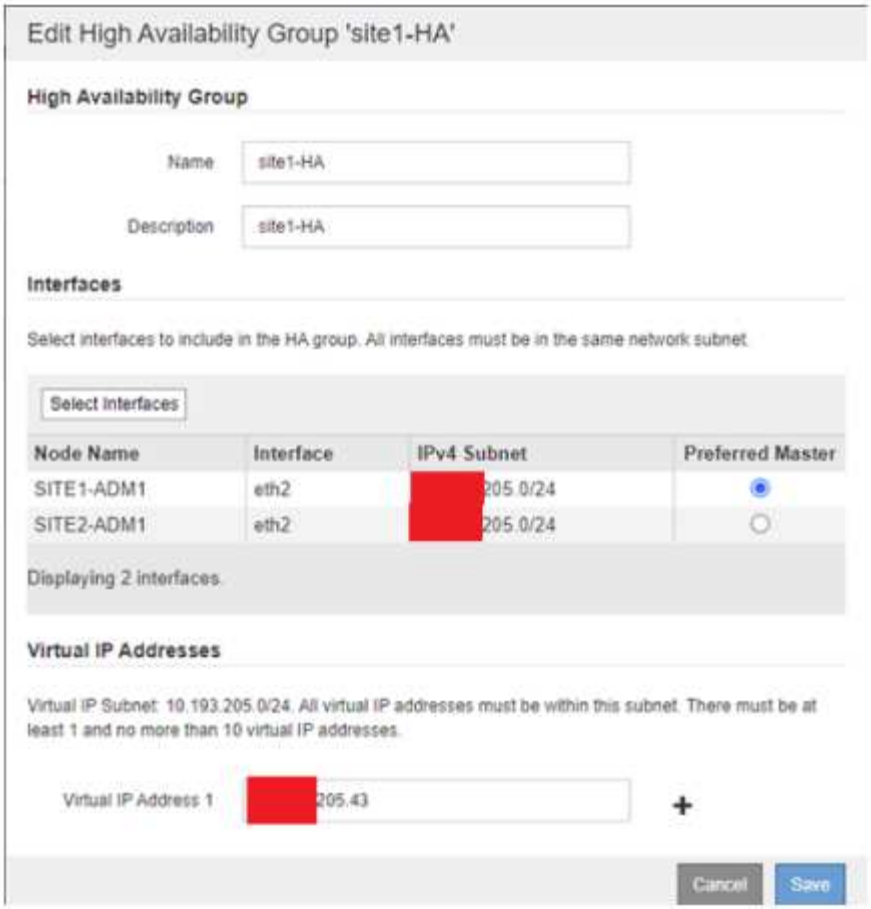
StorageGRIDサイトのフェールオーバーを設定するには、次の手順を実行します。

手順

1. サイト障害時にStorageGRIDへの接続を確保するには、ハイアベイラビリティ（HA）グループを設定します。StorageGRIDのGrid Managerインターフェイス（GMI）で、[Configuration]、[High Availability Groups]、[+Create]の順にクリックします。



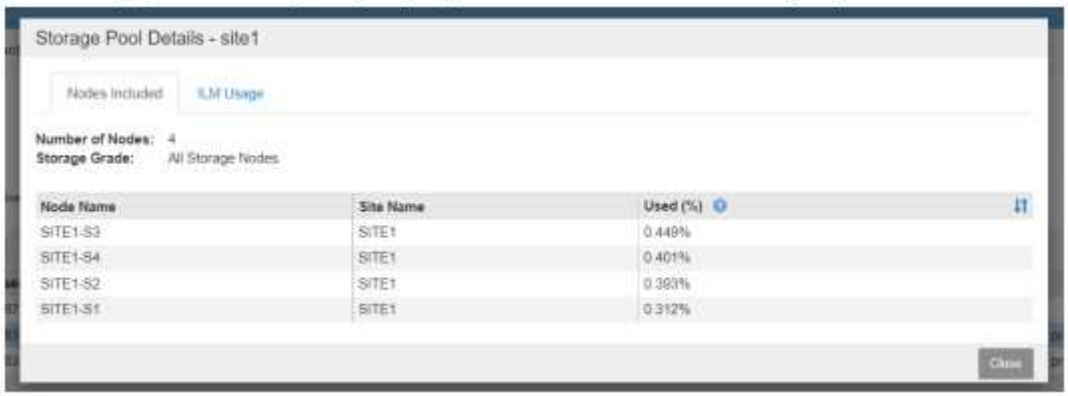
2. 必要な情報を入力します。[Select Interfaces]をクリックし、Site1（プライマリサイト）が優先マスターであるSite2のネットワークインターフェイスを含めます。同じサブネット内の仮想IPアドレスを割り当てます。保存をクリックします。

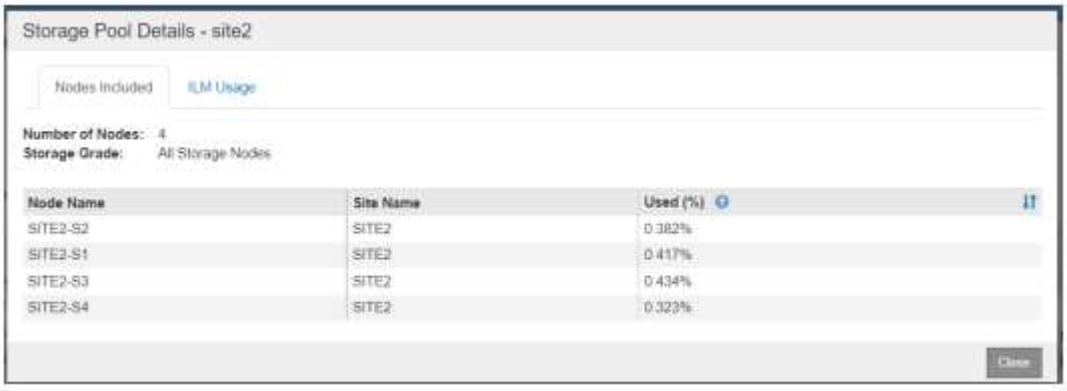


3. この仮想IP（VIP）アドレスは、Veritas Enterprise Vaultのパーティション設定時に使用されるS3ホスト名に関連付ける必要があります。VIPアドレスはトラフィックをSite1に解決します。Site1に障害が発生すると、VIPアドレスはトラフィックをSite2に透過的に再ルーティングします。
4. データがSite1とSite2の両方にレプリケートされていることを確認します。これにより、Site1に障害が発生しても、Site2からオブジェクトデータを引き続き使用できます。そのためには、まずストレージプールを構成します。

   StorageGRID GMIで、[ILM]、[Storage Pools]の順にクリックし、[+Create]をクリックします。ウィザードに従って、Site1用とSite2用の2つのストレージプールを作成します。

   ストレージプールは、オブジェクトの配置を定義するために使用されるノードを論理的にグループ化したもの





5. StorageGRID GMIで、[ILM]、[Rules]、[+Create]の順にクリックします。ウィザードの指示に従って、サイトごとに1つのコピーを格納し、取り込み動作はBalancedでILMルールを作成します。

6. ILMポリシーにILMルールを追加し、ポリシーをアクティブ化します。

この構成では、次の結果が得られます。

- 仮想S3エンドポイントIP。Site1がプライマリエンドポイント、Site2がセカンダリエンドポイントです。Site1に障害が発生すると、VIPはSite2にフェイルオーバーします。
- アーカイブデータがVeritas Enterprise Vaultから送信されると、StorageGRIDは1つのコピーがサイト1に格納され、もう1つのDRコピーがサイト2に格納されることを確認します。Site1に障害が発生した場合、Enterprise VaultはSite2からの取り込みと読み出しを続行します。

これらの構成はどちらもVeritas Enterprise Vaultでは透過的です。S3エンドポイント、バケット名、アクセスキーなどは同じです。Veritas Enterprise Vaultパーティションで S3接続設定を再設定する必要はありません。

著作権に関する情報

商標に関する情報