



# 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』	1
サイトフェイルオーバーのためのStorageGRIDの設定の概要	1
StorageGRIDとVeritas Enterprise Vaultの設定	2
WORMストレージ用のStorageGRID S3オブジェクトロックの設定	7
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	11

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

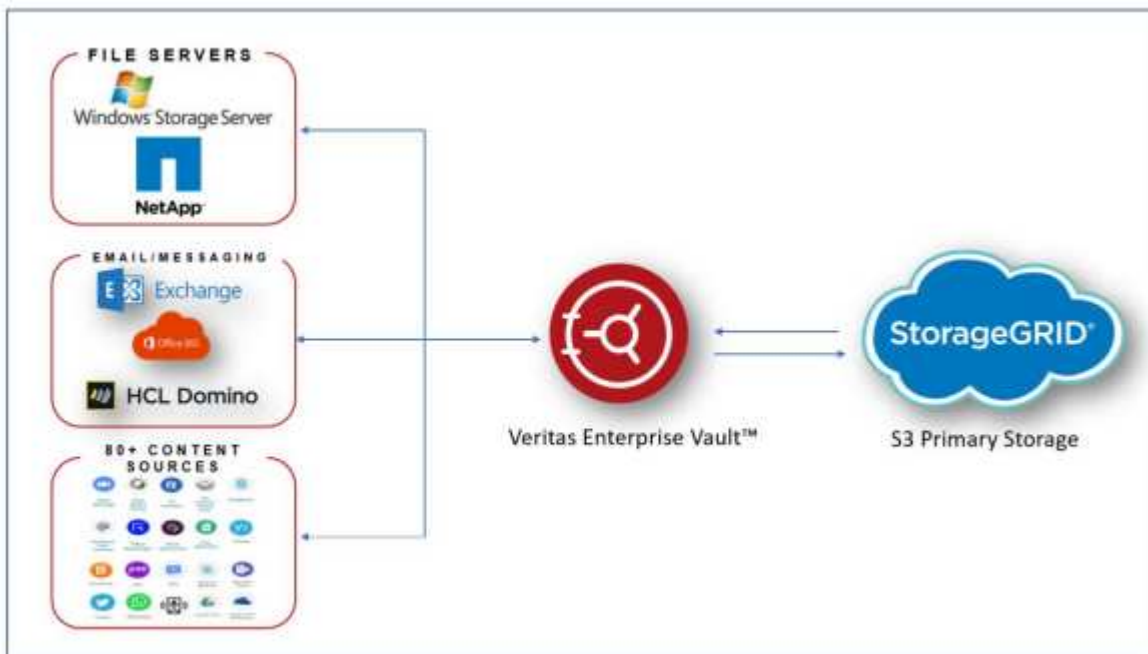
## サイトフェイルオーバーのためのStorageGRIDの設定の概要

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。

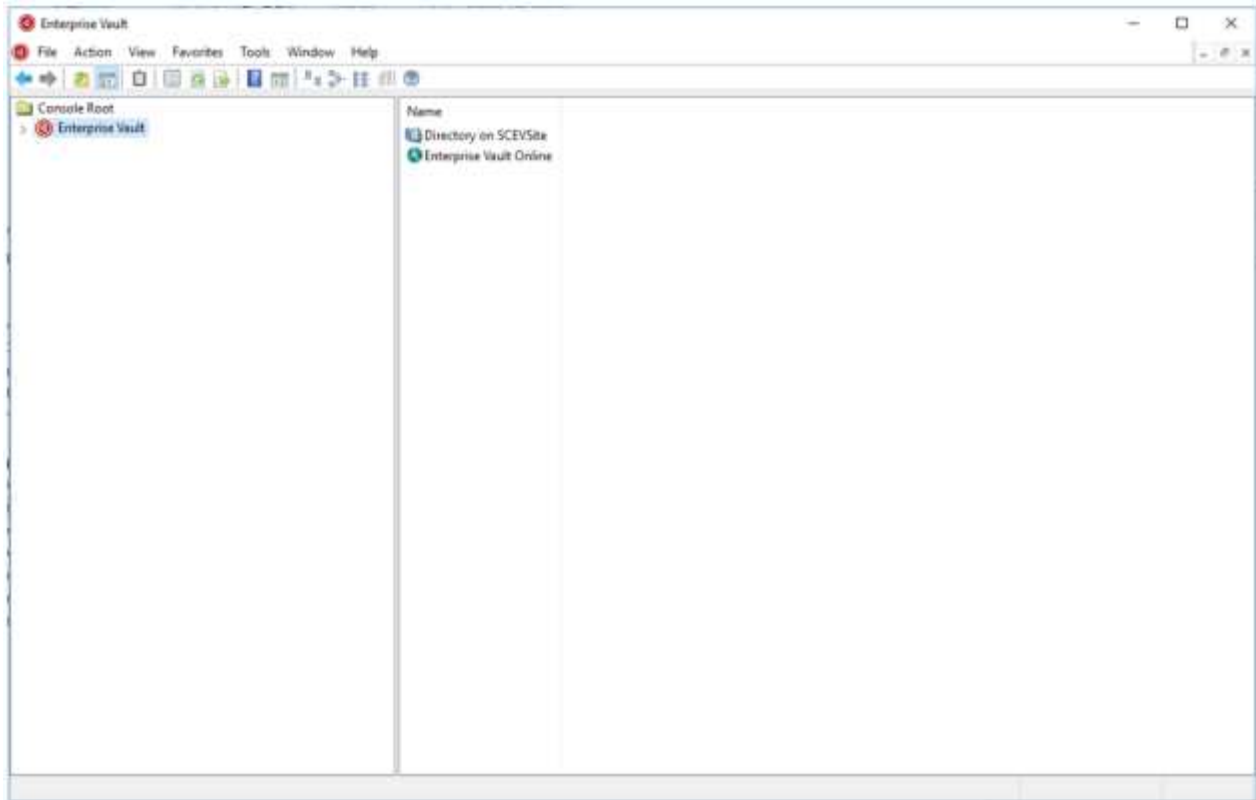
- ボールトストアグループとボールトストアが作成されました。詳細については、『Veritas Enterprise Vault Administration Guide』を参照してください。
- StorageGRIDテナント、アクセスキー、シークレットキー、およびバケットが作成されている。
- StorageGRIDロードバランサエンドポイント（HTTPまたはHTTPS）が作成されている。
- 自己署名証明書を使用する場合は、StorageGRID自己署名CA証明書をEnterprise Vaultサーバーに追加します。詳細については、こちらを参照して "[Veritasナレッジベースの記事](#)" 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

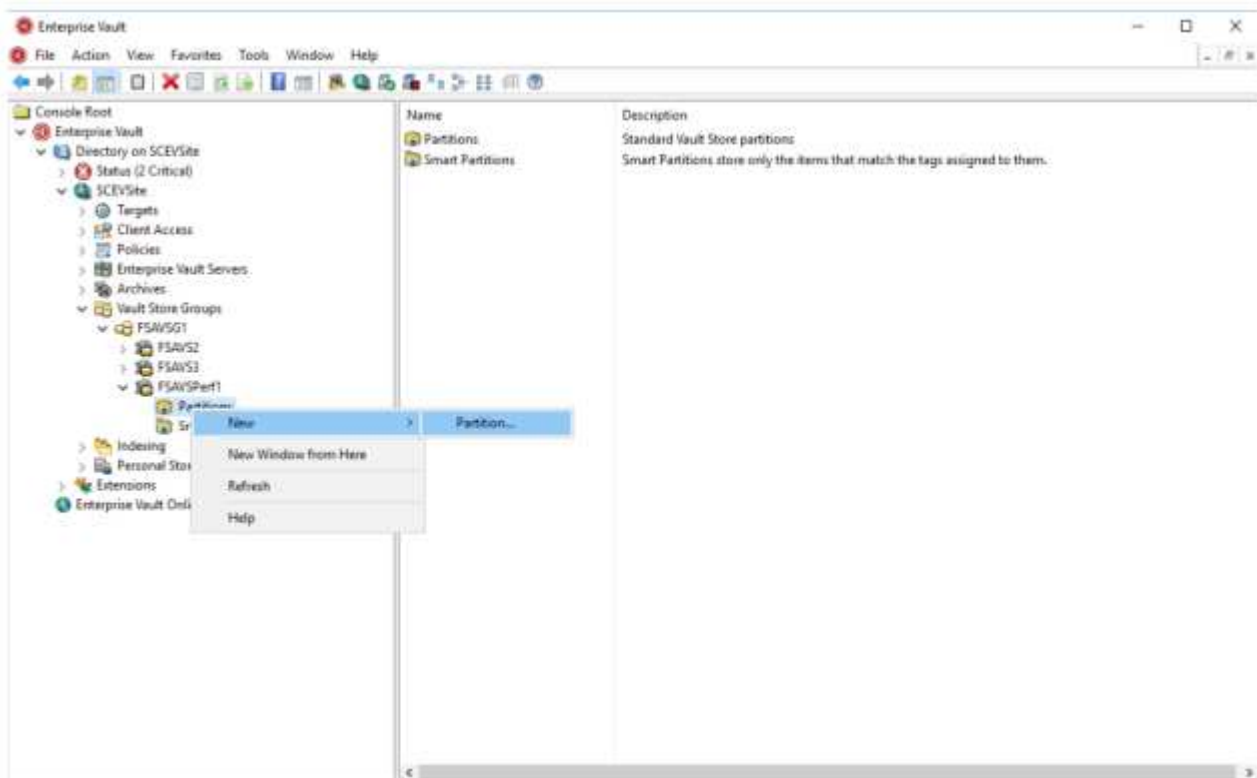
Veritas Enterprise Vaultを使用してStorageGRIDを設定するには、次の手順を実行します。

手順

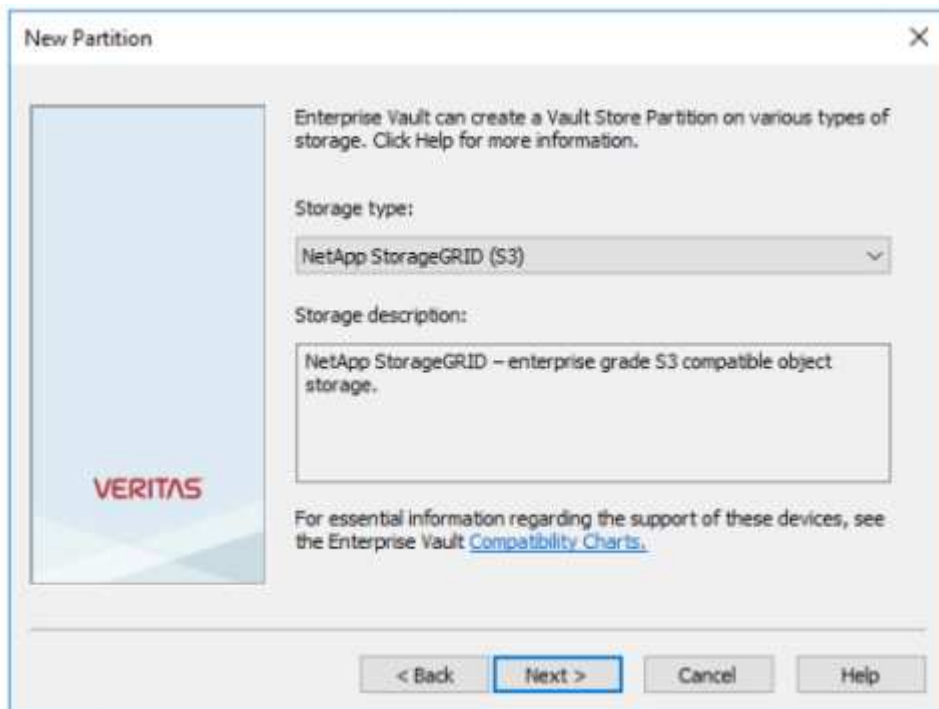
1. Enterprise Vault管理コンソールを起動します。



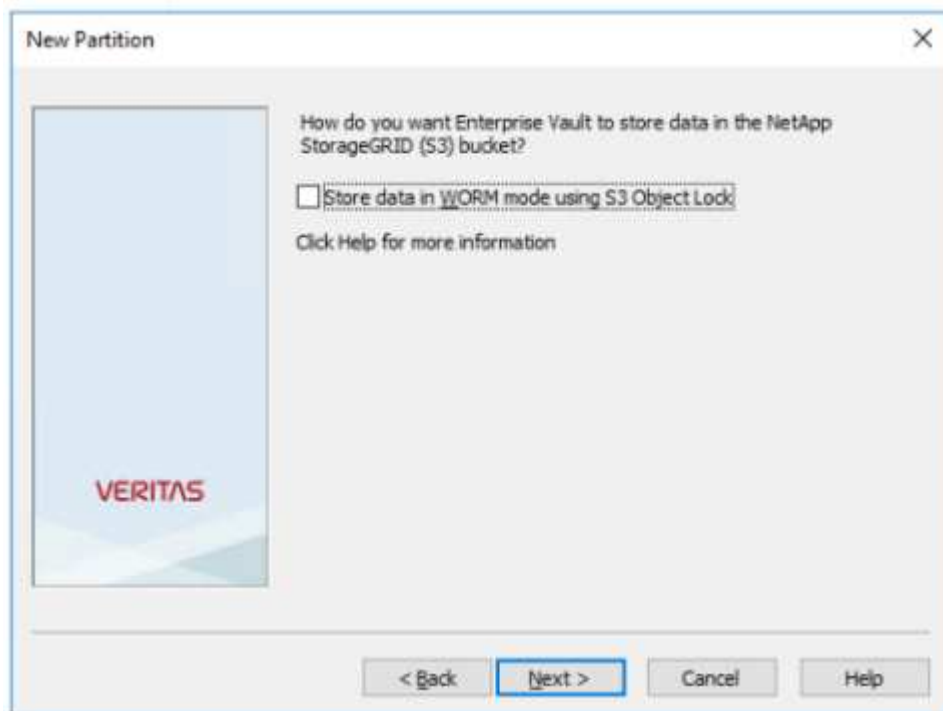
2. 適切なポールドストアに新しいポールドストアパーティションを作成します。ポールドストアグループ (Vault Store Groups) フォルダを展開し、適切なポールドストアを展開します。「パーティション」を右クリックし、メニュー「新規パーティション」を選択します。



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。

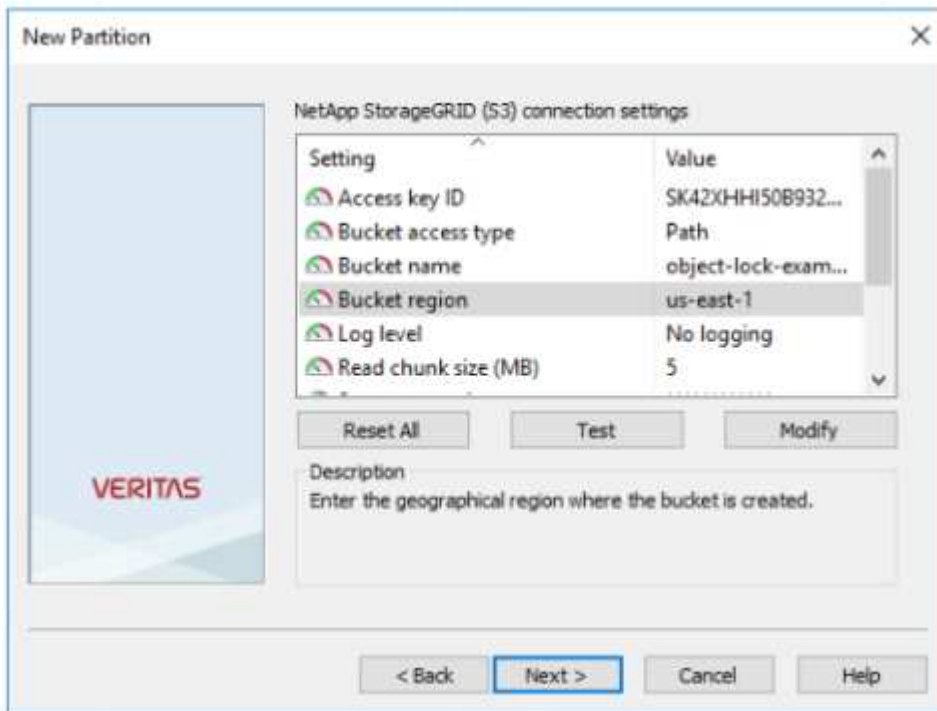


4. [Store Data in WORM Mode using S3 Object Lock]オプションはオフのままにします。[Next]をクリックします。

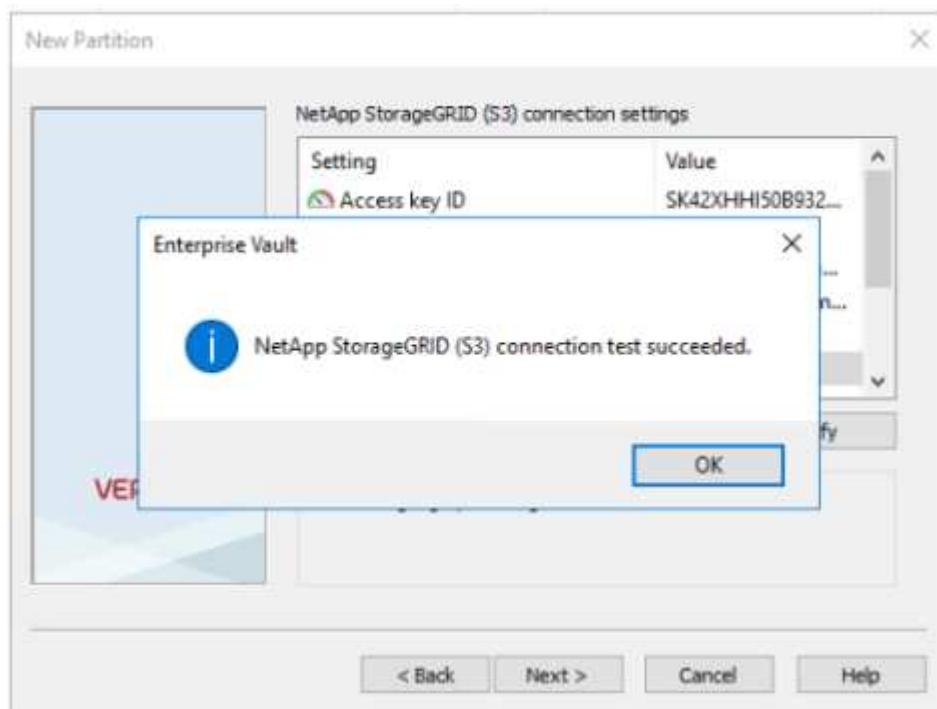


5. 接続設定ページで、次の情報を入力します。
- アクセスキーID
  - シークレットアクセスキー
  - サービスホスト名：StorageGRIDで設定されたロードバランサエンドポイント（LBE）ポート（https://<hostname>:<LBE\_port>など）を含めるようにしてください。

- 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。

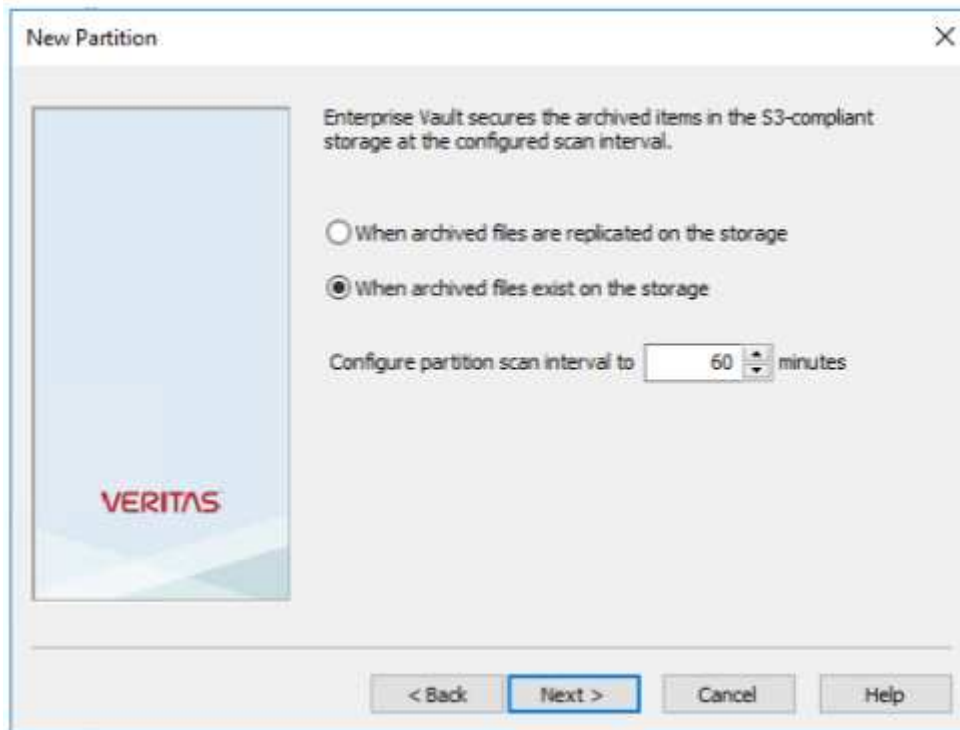


6. StorageGRIDバケットへの接続を確認するには、[Test]をクリックします。接続テストが成功したことを確認します。[OK]をクリックし、[Next]をクリックします。

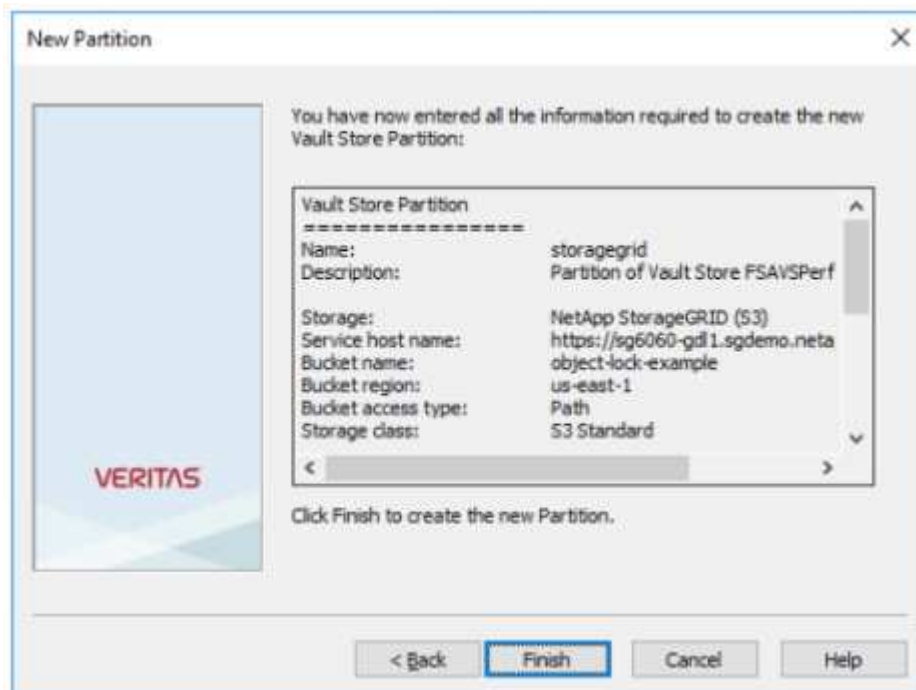


7. StorageGRIDでは、S3レプリケーションパラメータがサポートされません。StorageGRIDでは、オブジェクトを保護するために、情報ライフサイクル管理 (ILM) ルールを使用してデータ保護スキーム (複数の

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。

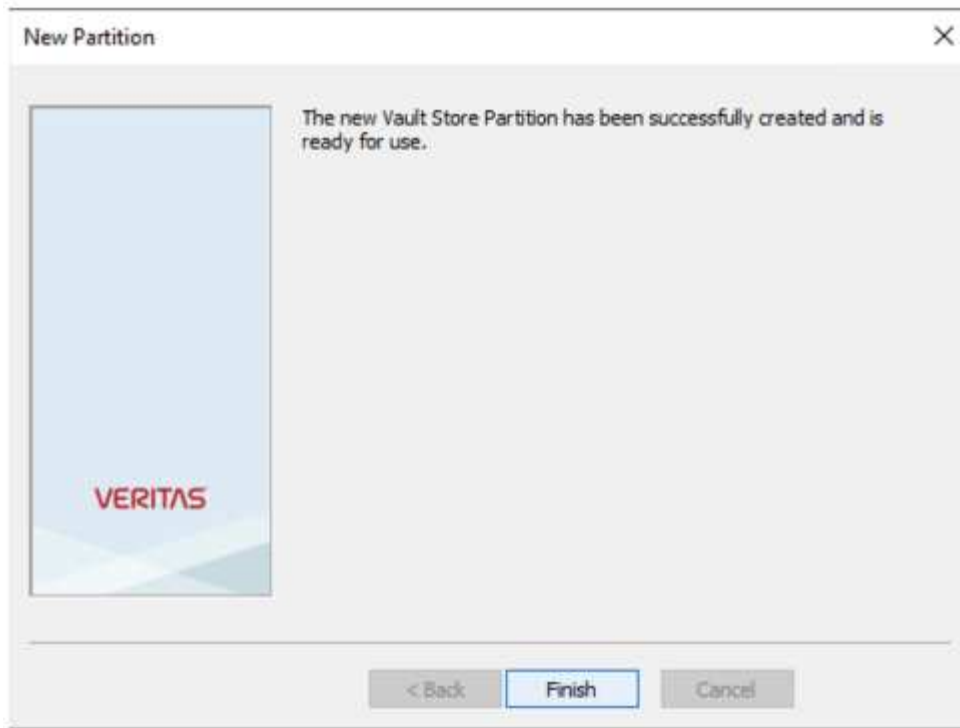


8. 概要ページの情報を確認し、[Finish]をクリックします。



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。

**Create bucket**

1 Enter details ————— 2 Manage object settings  
Optional

**Enter bucket details**

Enter the bucket's name and select the bucket's region.

Bucket name ⓘ

object-lock-example

Region ⓘ

us-east-1

Cancel Continue

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

# Create bucket

1 Enter details ————— 2 Manage object settings Optional

## Manage object settings Optional

### Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

**i** Object versioning has been enabled automatically because this bucket has S3 Object Lock enabled.

Enable object versioning

### S3 Object Lock

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot add or disable S3 Object Lock after a bucket is created.

If S3 Object Lock is enabled, object versioning is enabled for the bucket automatically and cannot be suspended.

Enable S3 Object Lock

[Previous](#) [Create bucket](#)

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。

**Overview**

Name: **object-lock-example**  
Region: **us-east-1**  
S3 Object Lock: **Enabled**  
Date created: **2022-06-24 14:44:54 PDT**

[View bucket contents in Experimental S3 Console](#)

**Bucket options** | **Bucket access** | **Platform services**

Consistency level: Read-after-new-write (default) ▼

Last access time updates: Disabled ▼

Object versioning: Enabled ▼

**S3 Object Lock** Enabled ▲

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot enable or disable S3 Object Lock after a bucket is created.

After S3 Object Lock is enabled for a bucket, you can't disable it. You also can't suspend object versioning for the bucket.

S3 Object Lock: Enabled

Default retention ?

Disable

Enable

[Save changes](#)

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。

**S3 Object Lock** Enabled ▲

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot enable or disable S3 Object Lock after a bucket is created.

After S3 Object Lock is enabled for a bucket, you can't disable it. You also can't suspend object versioning for the bucket.

S3 Object Lock: Enabled

Default retention ?

Disable

Enable

Default retention mode

Compliance

No users can overwrite or delete protected object versions during the retention period.

Default retention period ?

1  Days ▼

[Save changes](#)

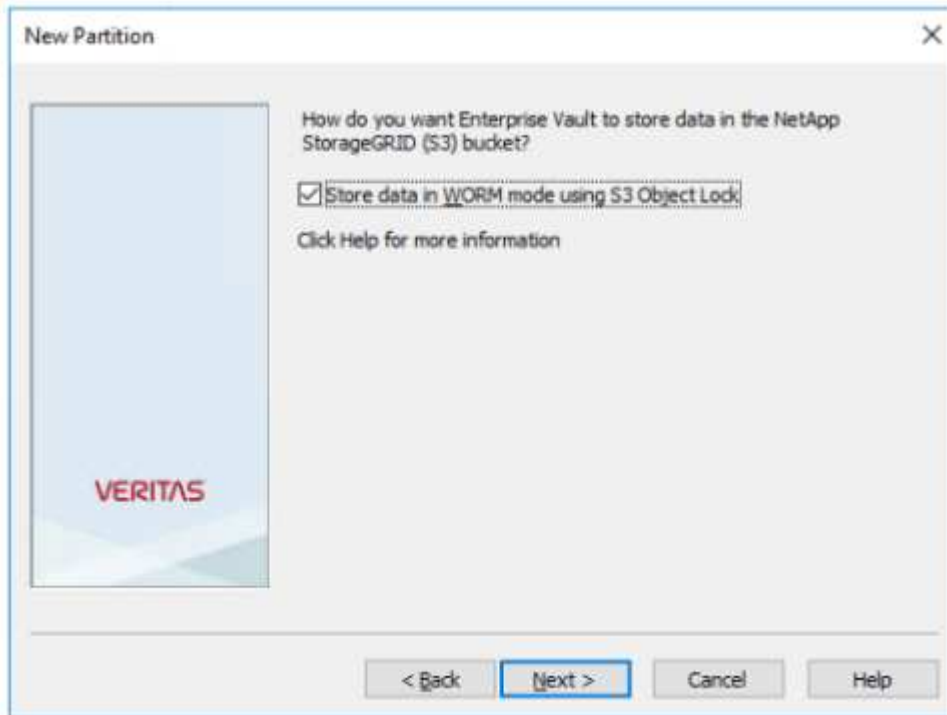
これで、バケットをEnterprise VaultでWORMデータの格納に使用できるようになりました。

## 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**" ですが、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サイトのフェイ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。

The screenshot shows a web form titled "Create High Availability Group". It is divided into three main sections: "High Availability Group", "Interfaces", and "Virtual IP Addresses".

- High Availability Group:** Contains two input fields: "Name" and "Description".
- Interfaces:** Includes the instruction "Select interfaces to include in the HA group. All interfaces must be in the same network subnet." and a blue button labeled "Select Interfaces".
- Virtual IP Addresses:** Includes the instruction "Select interfaces before assigning virtual IP addresses."

At the bottom right of the form, there are two buttons: "Cancel" and "Save".

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。

### Edit High Availability Group 'site1-HA'

**High Availability Group**

Name:

Description:

**Interfaces**

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
SITE1-ADM1	eth2	193.205.0/24	<input checked="" type="radio"/>
SITE2-ADM1	eth2	193.205.0/24	<input type="radio"/>

Displaying 2 interfaces.

**Virtual IP Addresses**

Virtual IP Subnet: 10.193.205.0/24. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1:  +

Cancel Save

- 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。
- 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

#### Storage Pool Details - site1

Nodes Included: [ILM Usage](#)

Number of Nodes: 4  
Storage Grade: All Storage Nodes

Node Name	Site Name	Used (%)
SITE1-S3	SITE1	0.448%
SITE1-S4	SITE1	0.401%
SITE1-S2	SITE1	0.383%
SITE1-S1	SITE1	0.312%

Close

Storage Pool Details - site2

Nodes Included **ILM Usage**

Number of Nodes: 4  
Storage Grade: All Storage Nodes

Node Name	Site Name	Used (%)
SITE2-S2	SITE2	0.382%
SITE2-S1	SITE2	0.417%
SITE2-S3	SITE2	0.434%
SITE2-S4	SITE2	0.323%

Close

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。

1 copy per site

Description: 1 copy per site  
Ingest Behavior: Balanced  
Retention: Ingest Time

Filtering Criteria:  
Matches all objects

Retention Diagram:  
Trigger: ILM  
Retention: ILM  
Expiration: Expiration

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rchive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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。