StorageGRIDのソリューションとリソース

StorageGRID solutions and resources

NetApp
December 12, 2025

目次

StorageGRIDのソリューションとリソース

StorageGRID評価ソフトウェアへのアクセス手順

この手順は、NetAppと連携しているNetAppの営業担当者、パートナー様、見込み客を対象としています。

アカウントに登録します

1. お勤め先のEメールアドレスを使用して、でアカウントを登録し "NetAppサポートサイト" ます。
   a. 新しく作成したアカウントでサインインしていないことを確認します。
   b. すでにアカウントをお持ちの場合は、サインインしていないことを確認し、次の手順に進みます。
2. テクニカル以外のサポートケースを作成して、アクセスレベルを「見込み客」に引き上げます。これを行うには、Webサイトのフッターにある「リンク」をクリックして ""問題を報告する"ください。
3. フィードバックカテゴリとして「登録の問題」を選択します。
4. コメント欄に「私のアカウントのメールアドレスは_あなたの-メールアドレス_です。見込み顧客にStorageGRID評価ソフトウェアをダウンロードしてもらいたいのですが」
   a. 見込み客へのアクセスリクエストを提案したNetApp社内担当者の名前を記入します。

StorageGRIDのダウンロード

1. サポートケースの確認と承認が完了すると、NetAppサポートからお客様のアカウントに見込み客へのアクセス権が付与されたことがEメールで通知されます。
2. をダウンロードします "StorageGRID評価用ソフトウェア"。

Evalライセンスファイルはzipファイル内にあります。解凍した時点では、StorageGRID Webscale -<version>\ vsphere \ NLF000000.txtです。

ソフトウェアのダウンロードは、法的要件を遵守するための貿易コンプライアンス措置を含むプロセスです。コンプライアンスを確保するには、アクセスする前にアカウントを作成し、サポートケースをオープンする必要があります。このプロセスは、適切な管理と文書化を維持しながら、見込み客に必要な本番環境対応ソフトウェアを提供するのに役立ちます。

StorageGRIDの「本番環境対応」バージョンを提供しています。これは、オープンソースまたは代替バージョンではありません。お客様が本番環境のライセンスにアップグレードしない限り、サポートは提供されません。

上記の手順で問題が発生した場合は、StorageGRID.Feedback@netapp.comまでお問い合わせください。

検証済みのサードパーティソリューション

検証済みのサードパーティソリューション：概要

ネットアップはパートナー様と協力して、これらのソリューションをStorageGRID で使用できるように検証しました。このセクションの情報を参照して、検証済みのソリューションを確認し、必要に応じて追加の手順を入手してください。

ネットアップの業界最高水準のテスト済みソリューションを構築すると、力を合わせてネットアップのポートフォリオを強化し、市場認知度を高め、売上を拡大できます。 "今すぐアライアンスパートナーになりましょう"。

StorageGRID 12.0 検証済みサードパーティソリューション

次のサードパーティ ソリューションは、 StorageGRID 12.0 での使用が検証されています。 + 探しているソリューションがリストにない場合は、 NetApp のアカウント担当者にお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- アルクシオ
- Apache Kafka です
- AWSマウントポイント
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Collibra（Collibra Data Qualityの最小バージョン2024.02）
- Commvault 11.
- カウチベース エンタープライズ アナリティクス 2.0
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Diskoverデータ
- デレミオ
- Elasticsearch Snapshot（フローズン階層を含む）

- eMAM
- FUJIFILMオブジェクトアーカイブ
- GitHubエンタープライズサーバ
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- Interica
- Komprise
- Microsoft SQL Server Big Data Clustersの略
- モデル9.
- Modzy
- Moonwalk Universalの略
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- PixitMedia ngenea.
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706以上
- Rubrik CDMの略
- s3a
- シグニエント
- 雪の結晶
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- スターバースト
- ストレージが簡単になりました
- トリノ
- ニスエンタープライズ6.0.4
- Veeam 12

- Veritas Enterprise Vault 15.1.
- Veritas NetBackup 10.1.1以降
- Vertica 10.x
- ビディズパイン
- Virtalica StorageFabricの詳細を参照してください
- Weka v3.10以降

StorageGRID で検証済みの、オブジェクトロック機能を備えたサードパーティ製ソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- CommVault 11 Feature Release 26
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15.1.
- Veritas NetBackup 10.1.1以降

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- Gitlab
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン

- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRIDでサポートされるキー管理ツール

これらのソリューションはテスト済みです。

- Entrust 暗号化セキュリティ プラットフォーム v10.4.5
- Entrust KeyControl 10.2
- ハシコープ ボールト 1.20.2
- タレス CipherTrust マネージャー 2.20

StorageGRID 11.9検証済みのサードパーティソリューション

以下のサードパーティソリューションは、StorageGRID 11.9での使用が検証済みです。+お探しの解決策 が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- アルクシオ
- Apache Kafka です
- AWSマウントポイント
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Collibra（Collibra Data Qualityの最小バージョン2024.02）
- Commvault 11.
- カウチベース エンタープライズ アナリティクス 2.0
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Diskoverデータ

- デレミオ
- Elasticsearch Snapshot（フローズン階層を含む）
- eMAM
- FUJIFILMオブジェクトアーカイブ
- GitHubエンタープライズサーバ
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- Interica
- Komprise
- Microsoft SQL Server Big Data Clustersの略
- モデル9.
- Modzy
- Moonwalk Universalの略
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- PixitMedia ngenea.
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706以上
- Rubrik CDMの略
- s3a
- シグニエント
- 雪の結晶
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- スターバースト
- ストレージが簡単になりました
- トリノ

- ニスエンタープライズ6.0.4
- Veeam 12
- Veritas Enterprise Vault 15.1.
- Veritas NetBackup 10.1.1以降
- Vertica 10.x
- ビディズパイン
- Virtalica StorageFabricの詳細を参照してください
- Weka v3.10以降

StorageGRID で検証済みの、オブジェクトロック機能を備えたサードパーティ製ソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- CommVault 11 Feature Release 26
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15.1.
- Veritas NetBackup 10.1.1以降

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- Gitlab
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム

- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRIDでサポートされるキー管理ツール

これらのソリューションはテスト済みです。

- Entrust 暗号化セキュリティ プラットフォーム v10.4.5
- Entrust KeyControl 10.2
- Hashicorp Vault 1.15.0
- タレスCipherTrust Manager 2.0
- タレスCipherTrust Manager 2.1
- タレスCipherTrust Manager 2.2
- タレスCipherTrust Manager 2.3
- タレスCipherTrust Manager 2.4
- タレスCipherTrust Manager 2.8
- タレスCipherTrust Manager 2.9
- タレスCipherTrust Manager 2.10
- タレスCipherTrust Manager 2.11
- タレスCipherTrust Manager 2.12
- タレスCipherTrust Manager 2.13
- タレスCipherTrust Manager 2.14
- タレス CipherTrust マネージャー 2.15
- タレス CipherTrust マネージャー 2.16
- タレス CipherTrust マネージャー 2.20

StorageGRID 11.8検証済みのサードパーティソリューション

以下のサードパーティソリューションは、StorageGRID 11.8での使用が検証済みです。[+]
お探しの解決策が表示されない場合は、NetAppのアカウント担当者にお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- アルクシオ
- Apache Kafka です
- AWSマウントポイント
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Collibra（Collibra Data Qualityの最小バージョン2024.02）
- Commvault 11.
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Diskoverデータ
- デレミオ
- Elasticsearch Snapshot（フローズン階層を含む）
- eMAM
- FUJIFILMオブジェクトアーカイブ
- GitHubエンタープライズサーバ
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- Interica
- Komprise
- Microsoft SQL Server Big Data Clustersの略
- モデル9.
- Modzy
- Moonwalk Universalの略
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4

- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- PixitMedia ngenea.
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706以上
- Rubrik CDMの略
- s3a
- シグニエント
- 雪の結晶
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- スターバースト
- ストレージが簡単になりました
- トリノ
- ニスエンタープライズ6.0.4
- Veeam 12
- Veritas Enterprise Vault 15.1.
- Veritas NetBackup 10.1.1以降
- Vertica 10.x
- ビディズパイン
- Virtalica StorageFabricの詳細を参照してください
- Weka v3.10以降

StorageGRID で検証済みの、オブジェクトロック機能を備えたサードパーティ製ソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- CommVault 11 Feature Release 26
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- OpenText Documentum 21.4
- Rubrik
- Veeam 12

- Veritas Enterprise Vault 15.1.
- Veritas NetBackup 10.1.1以降

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- Gitlab
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRIDでサポートされるキー管理ツール

これらのソリューションはテスト済みです。

- Entrust KeyControl 10.2
- Hashicorp Vault 1.15.0
- タレスCipherTrust Manager 2.0
- タレスCipherTrust Manager 2.1
- タレスCipherTrust Manager 2.2
- タレスCipherTrust Manager 2.3
- タレスCipherTrust Manager 2.4
- タレスCipherTrust Manager 2.8
- タレスCipherTrust Manager 2.9

- タレスCipherTrust Manager 2.10
- タレスCipherTrust Manager 2.11
- タレスCipherTrust Manager 2.12
- タレスCipherTrust Manager 2.13
- タレスCipherTrust Manager 2.14

StorageGRID 11.7で検証済みのサードパーティソリューション

以下のサードパーティソリューションは、StorageGRID 11.7での使用が検証済みです。+お探しの解決策 が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- アルクシオ
- Apache Kafka です
- AWSマウントポイント
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Collibra（Collibra Data Qualityの最小バージョン2024.02）
- Commvault 11.
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Diskoverデータ
- デレミオ
- Elasticsearch Snapshot（フローズン階層を含む）
- eMAM
- FUJIFILMオブジェクトアーカイブ
- GitHubエンタープライズサーバ
- IBM FileNetの順にクリックします
- IBM Spectrum Protect Plusのサポート

- IBM ストレージ保護
- Interica
- Komprise
- Microsoft SQL Server Big Data Clustersの略
- モデル9.
- Modzy
- Moonwalk Universalの略
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- PixitMedia ngenea.
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706以上
- Rubrik CDMの略
- s3a
- シグニエント
- 雪の結晶
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- ストレージが簡単になりました
- トリノ
- ニスエンタープライズ6.0.4
- Veeam 12
- Veritas Enterprise Vault 14.
- Veritas NetBackup 10.1.1以降
- Vertica 10.x
- ビディズパイン
- Virtalica StorageFabricの詳細を参照してください
- Weka v3.10以降

StorageGRID で検証済みの、オブジェクトロック機能を備えたサードパーティ製ソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- CommVault 11 Feature Release 26
- IBM FileNetの順にクリックします
- IBM ストレージ保護
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1以降

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- Gitlab
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRIDでサポートされるキー管理ツール

これらのソリューションはテスト済みです。

- タレスCipherTrust Manager 2.0
- タレスCipherTrust Manager 2.1
- タレスCipherTrust Manager 2.2
- タレスCipherTrust Manager 2.3
- タレスCipherTrust Manager 2.4
- タレスCipherTrust Manager 2.8
- タレスCipherTrust Manager 2.9

StorageGRID 11.6検証済みのサードパーティソリューション

StorageGRID 11.6では、以下のサードパーティソリューションの使用が検証されています。+お探しの解決策 が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- アルクシオ
- Apache Kafka です
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Commvault 11.
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Diskoverデータ
- デレミオ
- eMAM
- FUJIFILMオブジェクトアーカイブ
- GitHubエンタープライズサーバ
- IBM FileNetの順にクリックします
- IBM Spectrum Protect Plusのサポート
- Interica

- Komprise
- Microsoft SQL Server Big Data Clustersの略
- モデル9.
- Modzy
- Moonwalk Universalの略
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- PixitMedia ngenea.
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Reveille v10 build 220706以上
- Rubrik CDMの略
- s3a
- シグニエント
- 雪の結晶
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- ストレージが簡単になりました
- トリノ
- ニスエンタープライズ6.0.4
- Veeam 12
- Veritas Enterprise Vault 14.
- Veritas NetBackup 8.0
- Vertica 10.x
- ビディズパイン
- Virtalica StorageFabricの詳細を参照してください
- Weka v3.10以降

StorageGRID で検証済みの、オブジェクトロック機能を備えたサードパーティ製ソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- CommVault 11 Feature Release 26
- IBM FileNetの順にクリックします
- OpenText Documentum 21.4
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1以降

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- Gitlab
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRID 11.5で検証済みのサードパーティソリューション

次の他社製ソリューションは、StorageGRID 11.5で使用することが検証されています。+お探しの解決策 が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- アルクシオ
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Commvault 11.
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Interica
- Komprise
- Moonwalk Universalの略
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Rubrik CDMの略
- s3a
- シグニエント
- Splunk Smartstore
- トリノ
- ニスエンタープライズ6.0.4
- Veeam 11の統合によって
- Veritas Enterprise Vault 11.

- Veritas Enterprise Vault 12.
- Veritas NetBackup 8.0
- Vertica 10.x
- ビディズパイン
- Virtalica StorageFabricの詳細を参照してください

StorageGRID で検証済みの、オブジェクトロック機能を備えたサードパーティ製ソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- OpenText Documentum 21.4
- Veeam 11の統合によって

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- Gitlab
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRID 11.4検証済みのサードパーティソリューション

次のサードパーティソリューションは、StorageGRID 11.4で使用することが検証されて

います。+お探しの解決策 が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Commvault 11.
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Interica
- Komprise
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- Rubrik CDMの略
- シグニエント
- Splunk Smartstore
- ニスエンタープライズ6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11.
- Veritas Enterprise Vault 12.
- Veritas NetBackup 8.0
- Vertica 10.x

- ビディズパイン

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRID 11.3は、検証済みのサードパーティソリューションです

StorageGRID 11.3では、次のサードパーティソリューションが検証されています。+お探しの解決策 が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Commvault 11.

- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Interica
- Komprise
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura
- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- RUBRIK CDM 5.0.1 p1-1342
- シグニエント
- Splunk Smartstore
- ニスエンタープライズ6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11.
- Veritas Enterprise Vault 12.
- Veritas NetBackup 8.0
- ビディズパイン

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ

- GE Centricity Enterprise Archiveの略
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

StorageGRID 11.2で検証済みのサードパーティ製ソリューション

以下の他社製ソリューションは、StorageGRID 11.2で検証済みです。+お探しの解決策が表示されない場合は、ネットアップの担当者までお問い合わせください。

StorageGRID で検証済みのサードパーティソリューション

これらのソリューションは、それぞれのパートナーと協力してテストされています。

- Actifio
- ブリッジストール
- カンテモ
- Citrixコンテンツコラボレーション
- Commvault 11.
- CTERAポータル6.
- ダレト
- ダタドビ
- Data Dynamics StorageXのように入力します
- DefendX
- Interica
- Komprise
- 良いですね
- Nasuni
- OpenText Documentum 16.4
- CyanGate Cloudを使用したOpenText Media Management 16.5
- Panzura

- Point Archival Gateway 2.0の場合
- Point Storage Manager 6.4
- プリミティブストリーム
- Quantum StorNext 5.4.0.1
- RUBRIK CDM 5.0.1 p1-1342
- シグニエント
- Splunk Smartstore
- ニスエンタープライズ6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11.
- Veritas Enterprise Vault 12.
- Veritas NetBackup 8.0
- ビディズパイン

StorageGRIDでサポートされているサードパーティソリューション

これらのソリューションはテスト済みです。

- アーチウェア
- アクシスコミュニケーションズ
- コングルーシティ360
- DataFrameworksの略
- EcoDigital DIVAプラットフォーム
- Encoding.com
- FUJIFILMオブジェクトアーカイブ
- GE Centricity Enterprise Archiveの略
- ハイランド・アクオ
- IBM Aspera
- マイルストーンシステム
- ONSSI
- REACHエンジン
- SilverTrak
- SoftNAS
- QSTAR
- ベラシア

製品機能ガイド

『Achieving zero RPO with StorageGRID - A Comprehensive Guide to Multi-Site Replication』

この技術レポートでは、サイト障害発生時に復旧ポイント目標 (RPO) ゼロを達成するためのStorageGRIDレプリケーション戦略の実装に関する包括的なガイドを提供します。このドキュメントでは、マルチサイト同期レプリケーションやマルチグリッド非同期レプリケーションなど、 StorageGRIDのさまざまな展開オプションについて詳しく説明します。複数の場所にわたってデータの耐久性と可用性を確保するために、 StorageGRID情報ライフサイクル管理 (ILM) ポリシーを構成する方法について説明します。さらに、レポートでは、中断のないクライアント操作を維持するためのパフォーマンスに関する考慮事項、障害シナリオ、および回復プロセスについても説明します。このドキュメントの目的は、同期レプリケーション技術と非同期レプリケーション技術の両方を活用して、サイト全体の障害が発生した場合でも、データがアクセス可能で一貫性が保たれるようにするための情報を提供することです。

StorageGRIDの概要

NetApp StorageGRIDは、業界標準のAmazon Simple Storage Service（Amazon S3）APIをサポートするオブジェクトベースのストレージシステムです。

StorageGRIDは、情報ライフサイクル管理ポリシー（ILM）に基づくさまざまなサービスレベルで、複数の場所にわたって単一のネームスペースを提供します。これらのライフサイクル ポリシーを使用すると、ライフサイクル全体にわたってデータが存在する場所を最適化できます。

StorageGRIDを使用すると、ローカルソリューションや地理的に分散したソリューションで、データの保持方法と可用性を設定できます。データがオンプレミスにあるかパブリッククラウドにあるかに関係なく、統合ハイブリッドクラウドワークフローにより、Amazon Simple Notification Service (Amazon SNS)、Google Cloud、Microsoft Azure Blob、Amazon S3 Glacier、Elasticsearch などのクラウドサービスをビジネスで活用できます。

StorageGRIDスケール

最小限のStorageGRID展開は、単一サイト内の管理ノードと 3 つのストレージ ノードで構成されます。1 つのグリッドは最大 220 ノードまで拡張できます。StorageGRID は、単一のサイトとして展開することも、16 サイトに拡張することもできます。

管理ノードには、メトリックとログの中心点となる管理インターフェイスが含まれており、 StorageGRIDコンポーネントの構成を維持します。管理ノードには、S3 API アクセス用の統合ロードバランサーも含まれています。

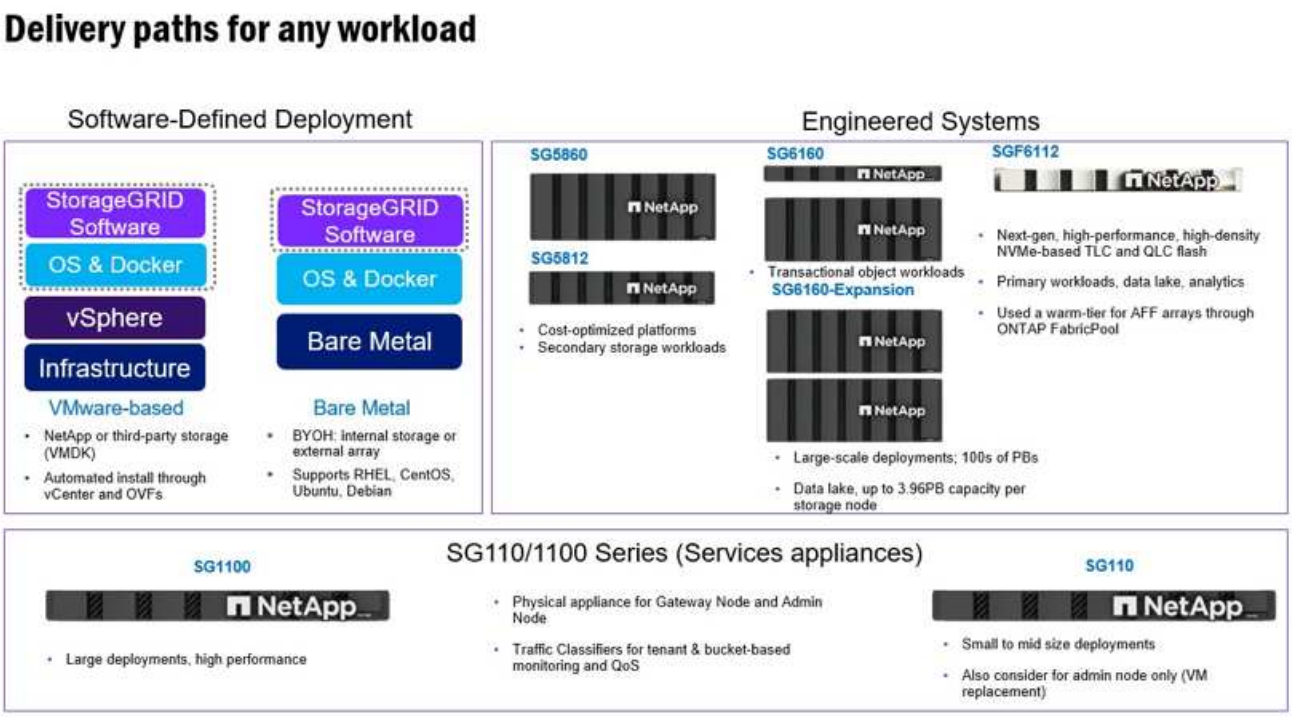
StorageGRID は、ソフトウェアのみ、VMware 仮想マシン アプライアンス、または専用アプライアンスとして導入できます。

ストレージ ノードは次のように展開できます。

- オブジェクト数を最大化するメタデータのみのノード

- オブジェクトスペースを最大化するオブジェクトストレージ専用ノード
- オブジェクト数とオブジェクトスペースの両方を追加するメタデータとオブジェクトストレージノードの組み合わせ

各ストレージ ノードは、オブジェクト ストレージ用に数ペタバイトの容量まで拡張でき、数百ペタバイトの単一の名前空間が可能になります。 StorageGRID は、ゲートウェイ ノードと呼ばれる S3 API 操作用の統合ロード バランサーも提供します。



StorageGRID は、サイト トポロジに配置されたノードのコレクションで構成されます。 StorageGRID内のサイトは、固有の物理的な場所に配置することも、論理構造としてグリッド内の他のサイトと同じ物理的な場所に配置することもできます。 StorageGRIDサイトは複数の物理的な場所にまたがってはなりません。サイトは、共有ローカル エリア ネットワーク (LAN) インフラストラクチャと障害ドメインを表します。

StorageGRIDおよび障害ドメイン

StorageGRIDには障害ドメインの複数のレイヤが含まれており、ソリューションの設計方法、データの格納方法、障害のリスクを軽減するためのデータの格納場所を決定する際に考慮する必要があります。

- グリッドレベル-複数のサイトで構成されるグリッドでは、サイト障害や分離が発生しても、アクセス可能なサイトはグリッドとして動作し続けることができます。
- サイトレベル-サイト内で障害が発生した場合、そのサイトの運用に影響する可能性がありますが、グリッドの残りの部分には影響しません。
- ノードレベル-ノード障害がサイトの運用に影響することはありません。
- ディスクレベル-ディスク障害はノードの動作に影響しません。

オブジェクトデータとメタデータ

オブジェクトストレージでは、ストレージの単位がファイルやブロックではなく、オブジェクトになります。ファイルシステムやブロックストレージのツリー階層とは異なり、オブジェクトストレージでは、フラットで非構造化されたレイアウトでデータが編成されます。オブジェクトストレージでは、データの物理的な場所と、データを格納および読み出す方法が切り離されています。

オブジェクトベースのストレージシステムの各オブジェクトには、オブジェクトデータとオブジェクトメタデータという 2 つの要素があります。

- オブジェクト データは、写真、動画、医療記録など、実際の基礎データを表します。
- オブジェクトメタデータは、オブジェクトについて記述された任意の情報です。

StorageGRID では、オブジェクトメタデータを使用してグリッド全体のすべてのオブジェクトの場所を追跡し、各オブジェクトのライフサイクルを継続的に管理します。

オブジェクトメタデータには、次のような情報が含まれます。

- システム メタデータには、各オブジェクトの一意の ID、オブジェクト名、S3 バケットの名前、テナントアカウント名または ID、オブジェクトの論理サイズ、オブジェクトが最初に作成された日時、オブジェクトが最後に変更された日時が含まれます。
- 各オブジェクトの複製コピーまたは消失訂正符号化フラグメントの現在の保存場所。
- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア
- セグメント化されたオブジェクトとマルチパート オブジェクトの場合、セグメント識別子とデータ サイズ。

オブジェクトメタデータはカスタマイズと拡張が可能なため、アプリケーションに合わせて柔軟に設定できます。StorageGRIDがオブジェクトメタデータを格納する方法と場所の詳細については、を参照してください "オブジェクトメタデータストレージを管理する"。

StorageGRIDの情報ライフサイクル管理（ILM）システムは、StorageGRIDシステム内のすべてのオブジェクトデータの配置、期間、取り込み動作のオーケストレーションに使用されます。ILMルールは、オブジェクトのレプリカを使用したり、ノードやサイト間でオブジェクトをイレイジャーコーディングしたりして、StorageGRIDが時間の経過に伴ってオブジェクトを格納する方法を決定します。このILMシステムは、グリッド内のオブジェクトデータの整合性を維持します。

イレイジャーコーディング

StorageGRID は、ノード レベルとドライブ レベルでデータを消去コード化する機能を提供します。StorageGRIDアプライアンスでは、ノード内のすべてのドライブにわたって各ノードに保存されているデータを消去コード化し、データの損失や中断を引き起こす複数のディスク障害に対するローカル保護を提供します。ドライブ障害からの再構築はノードに対してローカルであり、ネットワーク経由でデータを複製する必要はありません。

さらに、 StorageGRIDアプライアンスは、消失訂正符号スキームを使用して、サイト内のノード全体またはStorageGRIDシステム内の 3 つ以上のサイトに分散されたオブジェクト データを保存し、StorageGRID の ILM ルールによってノード障害から保護します。

イレージャー コーディングは、レプリケーションよりも低いオーバーヘッドで、ノードおよびサイトの障害に対して耐性のあるストレージ レイアウトを提供します。データ チャンクを保存するために必要な最小数の

ノードが満たされていれば、すべてのStorageGRID消去コーディング スキームを単一のサイトに展開できます。つまり、4+2 の EC スキームでは、データを受信するために少なくとも 6 つのノードが必要になります。

Erasure-coding scheme (*k+m*)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

メタデータの整合性

StorageGRIDでは、整合性と可用性を確保するために、メタデータは通常、サイトごとに3つのレプリカとともに格納されます。この冗長性により、障害が発生した場合でも、データの整合性とアクセス性が維持されます。

デフォルトの整合性は、グリッド全体のレベルで定義されます。整合性はバケットレベルでいつでも変更できます。

StorageGRIDで使用できるバケット整合性オプションは次のとおりです。

- **all**:最高レベルの一貫性を提供します。グリッド内のすべてのノードがすぐにデータを受信しないと、要求は失敗します。
- 強力なグローバル:
  - レガシー ストロング グローバル: すべてのサイトにわたるすべてのクライアント要求の書き込み後の読み取り一貫性を保証します。
    - これは、新しい Quorum Strong Global に手動で変更せずに 11.9 以前から 12.0 にアップグレードされたすべてのシステムのデフォルトの動作です。
  - **Quorum Strong-global**: すべてのサイトにわたるすべてのクライアント要求の書き込み後の読み取り一貫性を保証します。メタデータ レプリカ クォーラムが達成可能な場合は、複数のノードまたはサイト障害に対しても一貫性を提供します。
    - これは、12.0 以降で新しくインストールされたすべてのシステムのデフォルトの動作です。
    - QUORUM の一貫性は、ストレージ ノード メタデータ レプリカのクォーラムとして定義され、各

サイトには 3 つのメタデータ レプリカがあります。これは次のように計算できる: 1+((N*3)/2) ここでNはサイトの総数である

- たとえば、サイト内のレプリカが最大 3 つである 3 つのサイト グリッドからは、最小 5 つのレプリカを作成する必要があります。

- *strong-site *：サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されます。
- * Read-after-new-write *（デフォルト）：新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
- * available *：新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3 バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

オブジェクトデータの整合性

メタデータはサイト内およびサイト間で自動的にレプリケートされますが、オブジェクトデータのストレージ配置はユーザが決定します。オブジェクトデータは、サイト内およびサイト間のレプリカ、サイト内またはサイト間のイレイジャーコーディング、またはそれらの組み合わせまたはレプリカとイレイジャーコーディングされたストレージスキームに格納できます。ILMルールは、すべてのオブジェクトに適用することも、特定のオブジェクト、バケット、テナントにのみ適用するようにフィルタリングすることもできます。ILMルールは、オブジェクトの格納方法、レプリカやイレイジャーコーディング、それらの場所にオブジェクトを格納する期間、レプリカの数やイレイジャーコーディングスキームの変更、場所の変更などを定義します。

各ILMルールでは、オブジェクトを保護するための3つの取り込み動作（Dual commit、balanced、またはstrict）のいずれかを設定します。

デュアル コミット オプションは、グリッド内の任意の 2 つの異なるストレージ ノードに 2 つのコピーを直ちに作成し、要求が成功したことをクライアントに返します。ノードの選択はリクエストのサイト内で試行されますが、状況によっては別のサイトのノードが使用される場合があります。オブジェクトは ILM キューに追加され、ILM ルールに従って評価および配置されます。

バランス オプションは、オブジェクトを ILM ポリシーに対して直ちに評価し、要求が成功したことをクライアントに返す前にオブジェクトを同期的に配置します。停止または配置要件を満たすためのストレージ不足のために ILM ルールを直ちに満たすことができない場合、代わりにデュアル コミットが使用されます。問題が解決されると、ILM は定義されたルールに基づいてオブジェクトを自動的に配置します。

厳密なオプションは、オブジェクトを ILM ポリシーに対して直ちに評価し、要求が成功したことをクライアントに返す前にオブジェクトを同期的に配置します。停止または配置要件を満たすためのストレージ不足のために ILM ルールを直ちに満たすことができない場合、要求は失敗し、クライアントは再試行する必要があります。

ロードバランシング

StorageGRIDは、統合ゲートウェイノード、外部の3rdパーティロードバランサ、DNSラウンドロビンを介してクライアントアクセスを使用して導入することも、ストレージノードに直接導入することもできます。1つのサイトに複数のゲートウェイノードを導入し、ハイアベイラビリティグループに構成して、ゲートウェイノードに障害が発生した場合の自動フェイルオーバーとフェイルバックを実現できます。ソリューション内のロードバランシング方式を組み合わせて、ソリューション内のすべてのサイトに単一のアクセスポイントを提供できます。

ゲートウェイ ノードは、デフォルトでゲートウェイ ノードが存在するサイト内のストレージ ノード間で負荷

を分散します。StorageGRID は、ゲートウェイ ノードが複数のサイトのノードを使用して負荷を分散できるように構成できます。この構成により、クライアントの要求に対する応答の遅延に、これらのサイト間の遅延が追加されます。これは、合計遅延がクライアントにとって許容できる場合にのみ構成する必要があります。

ローカル負荷分散とグローバル負荷分散を組み合わせることで、RTO ゼロを実現できます。中断のないクライアント アクセスを確保するには、クライアント要求の負荷分散が必要です。StorageGRIDソリューションには、各サイトに多数のゲートウェイ ノードと高可用性グループを含めることができます。サイト障害が発生した場合でも、どのサイトのクライアントにも中断のないアクセスを提供するには、 StorageGRID Gateway ノードと組み合わせて外部の負荷分散ソリューションを構成する必要があります。各サイト内の負荷を管理するゲートウェイ ノードの高可用性グループを構成し、外部ロード バランサを使用して高可用性グループ間で負荷を分散します。リクエストが稼働中のサイトにのみ送信されるように、ヘルス チェックを実行するように外部ロード バランサを構成する必要があります。StorageGRIDによる負荷分散の詳細については、 "StorageGRIDロードバランサのテクニカルレポート"。

StorageGRIDによるゼロRPOの要件

オブジェクトストレージシステムで目標復旧時点（RPO）をゼロにするには、障害発生時に次のことを行うことが重要です。

- メタデータとオブジェクトコンテンツの両方が同期され、整合性があるとみなされる
- 障害が発生しても、オブジェクトコンテンツには引き続きアクセスできます。

マルチサイト展開の場合、Quorum Strong Global は、すべてのサイト間でメタデータが同期されることを保証するための推奨される一貫性モデルであり、ゼロ RPO 要件を満たすために不可欠です。

ストレージ システム内のオブジェクトは、ライフサイクル全体にわたってデータがどのようにどこに保存されるかを指示する情報ライフサイクル管理 (ILM) ルールに基づいて保存されます。同期レプリケーションの場合、厳密な実行とバランスの取れた実行のどちらかを検討できます。

- RPOをゼロにするには、これらのILMルールを厳密に実行する必要があります。これは、オブジェクトが定義された場所に配置される際に遅延やフォールバックが発生することなく、データの可用性と整合性が維持されるためです。
- StorageGRIDのILM Balanceの取り込み動作は、高可用性と耐障害性のバランスを実現し、サイト障害が発生した場合でもデータの取り込みを継続できるようにします。

複数サイト間での同期導入

マルチサイト ソリューション: StorageGRID を使用すると、グリッド内の複数のサイト間でオブジェクトを同期的に複製できます。バランスや厳密な動作を伴う情報ライフサイクル管理 (ILM) ルールを設定すると、オブジェクトは指定された場所にすぐに配置されます。バケットの一貫性レベルを Quorum Strong Global に構成すると、同期メタデータのレプリケーションも保証されます。 StorageGRID は単一のグローバル名前空間を使用し、オブジェクトの配置場所をメタデータとして保存するため、すべてのノードはすべてのコピーまたは消去コード化された部分がどこにあるかを認識します。要求が行われたサイトからオブジェクトを取得できない場合は、フェイルオーバー手順を必要とせずにリモート サイトから自動的に取得されます。

障害が解決されると、手動のフェイルバック作業は必要ありません。レプリケーションパフォーマンスは、ネットワークスループット、レイテンシ、パフォーマンスが最も低いサイトによって異なります。サイトのパフォーマンスは、ノード数、CPUコア数と速度、メモリ、ドライブ数、ドライブタイプに基づいて決まります。

マルチグリッドソリューション： StorageGRIDでは、クロスグリッドレプリケーション（CGR）を使用し

て、複数のStorageGRIDシステム間でテナント、ユーザ、バケットをレプリケートできます。CGRを使用すると、選択したデータを16以上のサイトに拡張し、オブジェクトストアの使用可能な容量を増やし、ディザスタリカバリを実現できます。CGRを使用したバケットのレプリケーションには、オブジェクト、オブジェクトバージョン、メタデータが含まれ、双方向でも一方向でもかまいません。Recovery Point Objective（RPO；目標復旧時点）は、各StorageGRIDシステムのパフォーマンスと、それらのシステム間のネットワーク接続によって異なります。

概要：

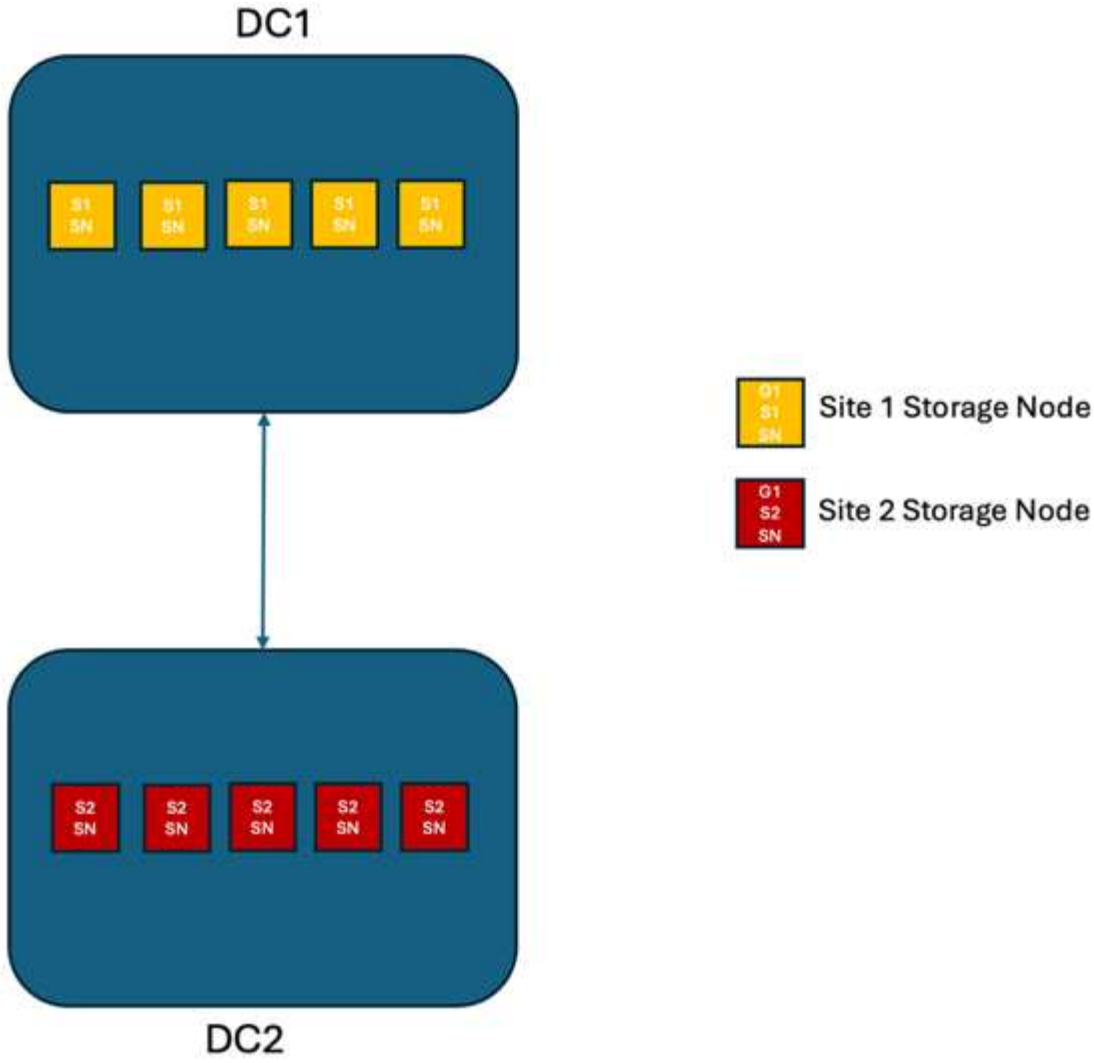
- グリッド内レプリケーションには同期レプリケーションと非同期レプリケーションの両方が含まれており、ILMの取り込み動作とメタデータの整合性制御を使用して設定できます。
- グリッド間レプリケーションは非同期のみです。

単一グリッドのマルチサイト環境

次のシナリオでは、 StorageGRIDソリューションは、統合ロード バランサーの高可用性グループへの要求を管理するオプションの外部ロード バランサーを使用して構成されています。これにより、RPO ゼロに加えて RTO ゼロも実現されます。ILM は、同期配置用のバランスの取れた取り込み保護を使用して構成されています。各バケットは、3 つ以上のサイトのグリッドの場合は強力なグローバル整合性モデルのクォーラム バージョンで構成され、2 つのサイトの場合は強力なグローバル整合性のレガシー バージョンで構成されます。

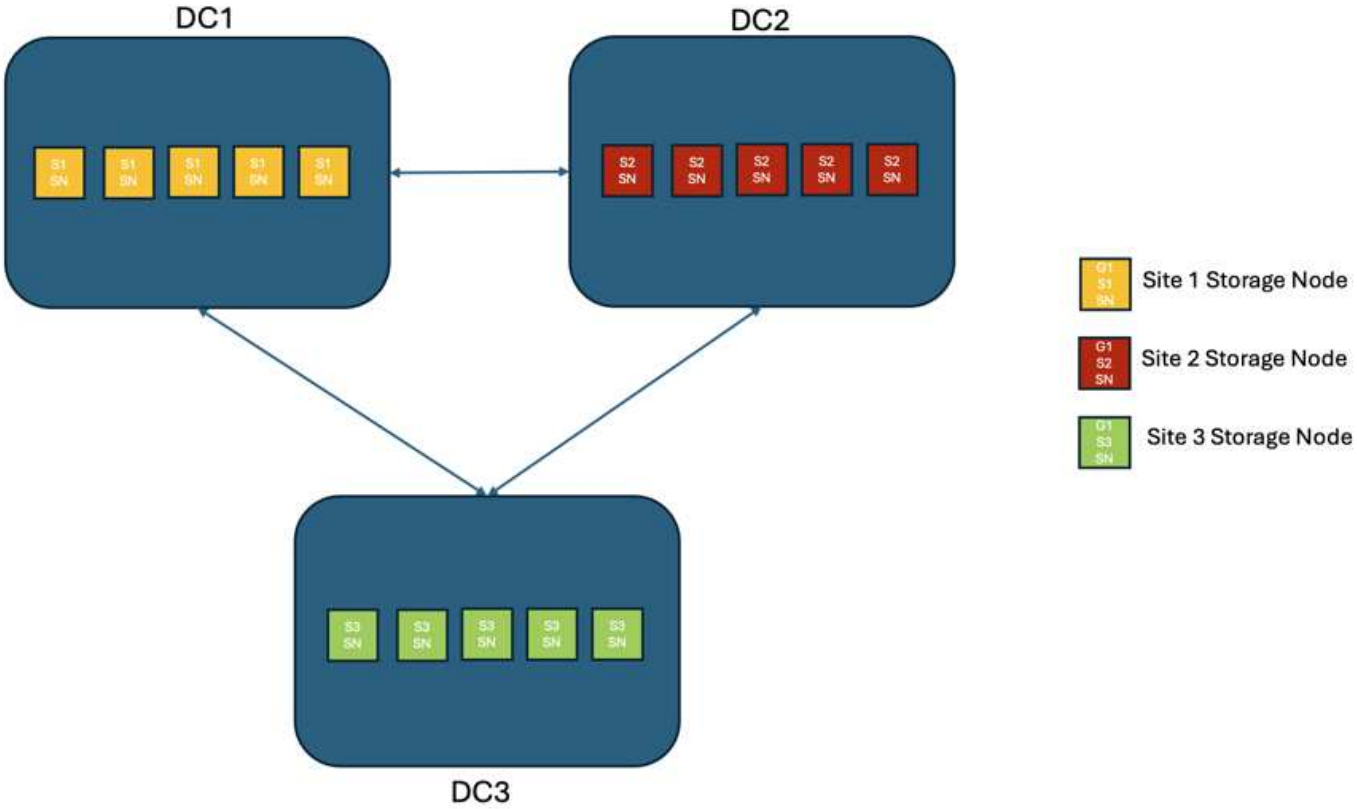
シナリオ**1:**

2 サイトのStorageGRIDソリューションでは、すべてのオブジェクトのレプリカが少なくとも 2 つあり、すべてのメタデータのレプリカが 6 つあります。障害回復時に、停止からの更新は回復されたサイト/ノードに自動的に同期されます。サイトが 2 つしかない場合、サイト全体の損失を超える障害シナリオでゼロ RPO を達成することはほとんど不可能です。



シナリオ**2:**

3 つ以上のサイトのStorageGRIDソリューションでは、すべてのオブジェクトのレプリカまたは EC チャンクが少なくとも 3 つあり、すべてのメタデータのレプリカが 9 つあります。障害回復時に、停止からの更新は回復されたサイト/ノードに自動的に同期されます。3 つ以上のサイトがあれば、RPO ゼロを実現できます。



複数サイトの障害のシナリオ

障害	**2**サイトの成果 **+** レガシーストロンググローバル	**3**つ以上のサイトの成果 **+ Quorum Strong Global**
単一ノードドライブ障害	各アプライアンスは複数のディスクグループを使用し、中断やデータ損失を発生させることなく、グループごとに少なくとも1本のドライブに障害が発生しても運用を継続できます。	各アプライアンスは複数のディスクグループを使用し、中断やデータ損失を発生させることなく、グループごとに少なくとも1本のドライブに障害が発生しても運用を継続できます。
1つのサイトでの単一ノード障害	運用の中断やデータ損失は発生しません。	運用の中断やデータ損失は発生しません。
1つのサイトでの複数ノードの障害	このサイトに転送されるクライアント処理が中断されますが、データ損失はありません。 もう一方のサイトに転送される処理は中断されず、データ損失も発生しません。	処理は他のすべてのサイトに転送され、中断されず、データ損失も発生しません。

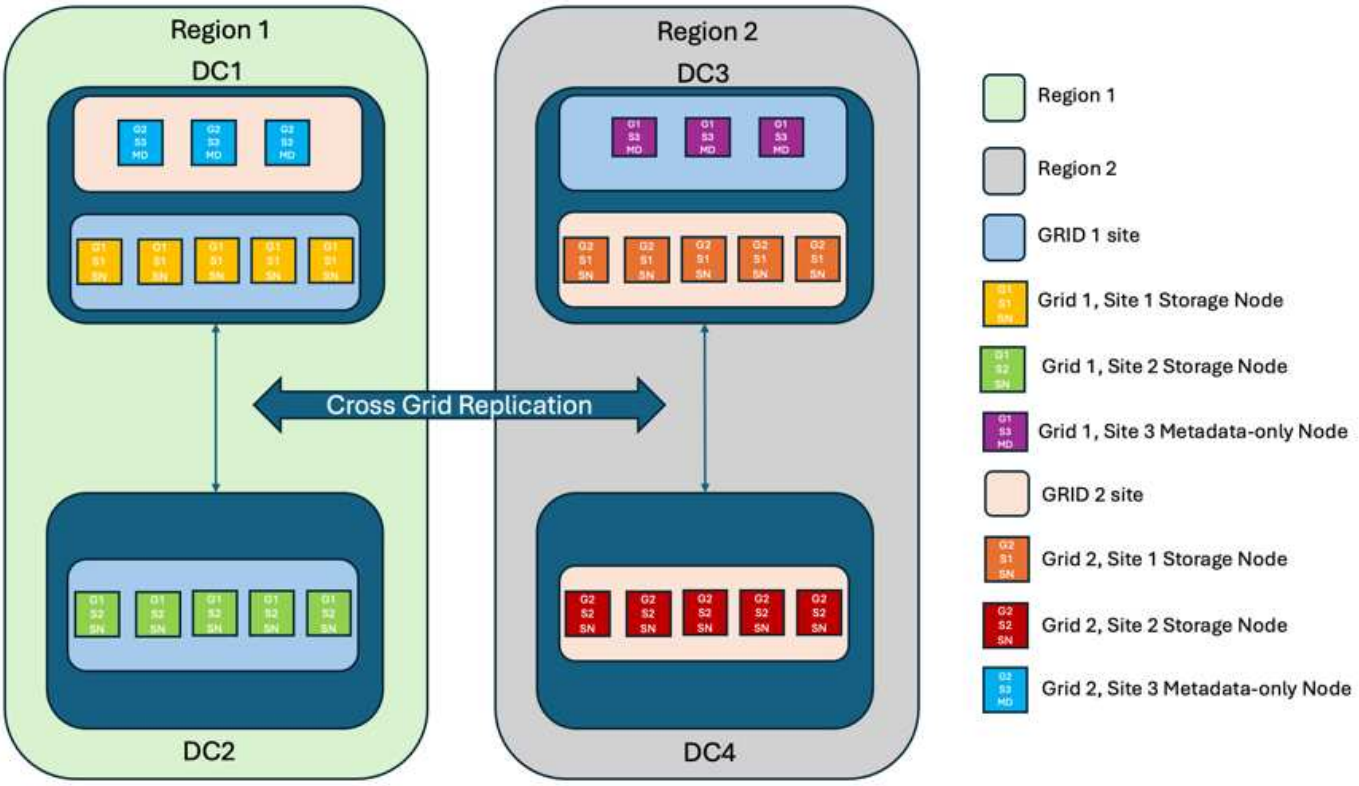
障害	**2**サイトの成果 **+** レガシーストロンググローバル	**3**つ以上のサイトの成果 **+ Quorum Strong Global**
複数サイトでの単一ノード障害	次の場合、システムの停止やデータ損失はゼロ • グリッド内に少なくとも 1 つの複製コピーが存在します • グリッドに十分な数のECチャンクが存在する 次の場合には、運用が停止し、データ損失のリスクが発生します。 • 複製コピーは存在しない • ECチャックが不十分	次の場合、システムの停止やデータ損失はゼロ • グリッド内に少なくとも 1 つの複製コピーが存在する • グリッドに十分な数のECチャンクが存在する 次の場合には、運用が停止し、データ損失のリスクが発生します。 • 複製コピーは存在しない • オブジェクトを読み出すための十分なECチャックが存在しません
単一サイト障害	障害が解決されるまで、一部のクライアント操作は中断されます。GET および HEAD 操作は中断されることなく続行されます。この障害状態でも操作を中断せずに継続するには、バケットの一貫性を新規書き込み後の読み取り以下に下げます。	運用の中断やデータ損失は発生しません。
単一サイトと単一ノードの障害	いずれかの障害が解決されるまで、一部のクライアント操作は中断されます。HEAD 操作は中断されることなく継続されます。複製コピーまたは十分な EC チャンクが存在する場合、GET 操作は中断されることなく続行されます。この障害状態でも操作を中断せずに継続するには、バケットの一貫性を新規書き込み後の読み取り以下に下げます。	業務の中断やデータの損失はありません。複製コピーの数に応じてデータが失われる可能性があります。ローカル消去コーディングにより、データの損失を防ぐことができます。
1つのサイトと残りの各サイトの1つのノード	存在するサイトは 2 つだけです。参照: 単一サイトと単一ノード。	メタデータ レプリカ クォーラムを満たすことができない場合、操作は中断されます。この障害状態でも操作を中断せずに継続するには、バケットの一貫性を新規書き込み後の読み取り以下に下げます。複製コピーの数によっては、永続的な障害によりデータが失われる可能性があります。ローカル消去コーディングにより、データの損失を防ぐことができます。

障害	**2**サイトの成果 **+** レガシーストロンググローバル	**3**つ以上のサイトの成果 **+ Quorum Strong Global**
複数サイト障害	稼働中のサイトは残っていません。少なくとも 1 つのサイトを完全に回復できない場合は、データが失われます。	メタデータ レプリカ クォーラムを満たすことができない場合、操作は中断されます。この障害状態でも操作を中断せずに継続するには、バケットの一貫性を新規書き込み後の読み取り以下に下げます。十分な消去コード化されたチャンクが残っていない場合、永続的な障害によりデータが失われる可能性があります。ローカル消去コーディングまたは複製コピーにより、データ損失を防ぐことができます。
サイトのネットワーク分離	いずれかの障害が解決されるまで、クライアント操作は中断されます。この障害状態でも操作を中断せずに継続するには、バケットの一貫性を新規書き込み後の読み取り以下に下げます。データ損失なし	分離されたサイトでは操作が中断されますが、データは失われません。この障害状態でも操作を中断せずに継続するには、バケットの一貫性を新規書き込み後の読み取り以下に下げます。残りのサイトでの業務は中断されず、データも失われません。

マルチサイトマルチグリッド環境

冗長性をさらに高めるために、このシナリオでは 2 つのStorageGRIDクラスターを採用し、クロスグリッド レプリケーションを使用してそれらの同期を維持します。このソリューションでは、各StorageGRIDクラスターに 3 つのサイトが含まれます。 2 つのサイトはオブジェクト ストレージとメタデータに使用され、3 番目のサイトはメタデータ専用に使用されます。両方のシステムは、バランスのとれた ILM ルールを使用して構成され、2 つのデータ サイトのそれぞれで消去コーディングを使用してオブジェクトを同期的に保存します。バケットは、Quorum Strong Global 整合性モデルを使用して構成されます。各グリッドは、すべてのバケットで双方向のクロスグリッド レプリケーションが構成されるように構成されます。これにより、リージョン間の非同期レプリケーションが実現します。オプションで、グローバル ロード バランサを実装して、両方のStorageGRIDシステムの統合ロード バランサ高可用性グループへの要求を管理し、RPO ゼロを実現できます。

このソリューションでは、2つのリージョンに均等に分割された4つのロケーションを使用します。リージョン1には、リージョンのプライマリグリッドであるグリッド1の2つのストレージサイトと、グリッド2のメタデータサイトが含まれます。リージョン2には、リージョンのプライマリグリッドであるグリッド2の2つのストレージサイトと、グリッド1のメタデータサイトが含まれます。各リージョンでは、同じ場所にそのリージョンのプライマリグリッドのストレージサイトと、他のリージョンのメタデータ専用サイトを格納できます。メタデータのみのノードを3番目のサイトとして使用すると、メタデータに必要な整合性が確保され、その場所にあるオブジェクトのストレージが複製されることはありません。



このソリューションには4つの場所があり、2つのStorageGRIDシステムの完全な冗長性が確保されます。RPOは0に維持され、マルチサイトの同期レプリケーションとマルチグリッドの非同期レプリケーションの両方が利用されます。いずれかのサイトで障害が発生しても、両方のStorageGRIDシステムでクライアント処理が中断されることはありません。

このソリューションでは、各オブジェクトのイレイジャーコーディングコピーが4つ、すべてのメタデータのレプリカが18個あります。これにより、クライアント処理に影響を与えることなく、複数の障害シナリオに対応できます。障害が発生すると、障害からのリカバリの更新が障害が発生したサイト/ノードに自動的に同期されます。

マルチサイト、マルチグリッドの障害シナリオ

障害	成果
単一ノードドライブ障害	各アプライアンスは複数のディスクグループを使用し、中断やデータ損失を発生させることなく、グループごとに少なくとも1本のドライブに障害が発生しても運用を継続できます。
グリッド内の一方のサイトでの単一ノード障害	運用の中断やデータ損失は発生しません。
各グリッドの1つのサイトでの単一ノード障害	運用の中断やデータ損失は発生しません。
グリッド内の1つのサイトでの複数ノードの障害	運用の中断やデータ損失は発生しません。
各グリッドの1つのサイトでの複数ノードの障害	運用の中断やデータ損失は発生しません。
グリッド内の複数のサイトにおける単一ノード障害	運用の中断やデータ損失は発生しません。
各グリッドの複数サイトでの単一ノード障害	運用の中断やデータ損失は発生しません。
グリッド内の単一サイト障害	運用の中断やデータ損失は発生しません。

障害	成果
各グリッドにおける単一サイト障害	運用の中断やデータ損失は発生しません。
グリッド内の単一サイトと単一ノードの障害	運用の中断やデータ損失は発生しません。
単一のグリッド内の単一のサイトと各サイトのノード	運用の中断やデータ損失は発生しません。
単一ロケーション障害	運用の中断やデータ損失は発生しません。
各グリッドDC1およびDC3での単一ロケーション障害	障害が解決されるかバケットの整合性が低下するまで処理が中断され、各グリッドで2つのサイトが失われる すべてのデータが2箇所に存在
各グリッドDC1およびDC4またはDC2およびDC3での単一ロケーション障害	運用の中断やデータ損失は発生しません。
各グリッドDC2およびDC4での単一ロケーション障害	運用の中断やデータ損失は発生しません。
サイトのネットワーク分離	分離されたサイトの処理は中断されるが、データは失われない 残りのサイトの処理が中断されたり、データが失われたりすることはありません。

まとめ

StorageGRIDでゼロ目標復旧時点（RPO）を達成することは、サイト障害が発生した場合にデータの保持と可用性を確保するための重要な目標です。マルチサイト同期レプリケーションやマルチグリッド非同期レプリケーションなど、StorageGRIDの堅牢なレプリケーション戦略を活用することで、中断のないクライアント処理を維持し、複数の場所でデータの整合性を確保できます。情報ライフサイクル管理（ILM）ポリシーの実装とメタデータのみのノードの使用により、システムの耐障害性とパフォーマンスがさらに強化されます。StorageGRIDを使用すると、複雑な障害シナリオが発生した場合でも、データへのアクセス性と一貫性を維持しながら、企業は自信を持ってデータを管理できます。データ管理とレプリケーションに対するこの包括的なアプローチは、RPOゼロを達成し、貴重な情報を保護するための綿密な計画と実行の重要性を強調しています。

AWSまたはGoogle Cloud用のクラウドストレージプールを作成します

StorageGRID オブジェクトを外部のS3バケットに移動する場合は、クラウドストレージプールを使用できます。外部バケットはAmazon S3（AWS）またはGoogle Cloudに属することができます。

必要なもの

- StorageGRID 11.6が設定されました。
- AWSまたはGoogle Cloudで外部のS3バケットをすでにセットアップしておきます。

手順

1. Grid Managerで、* ILM *>*ストレージプール*に移動します。
2. ページのクラウドストレージプールセクションで、 * 作成 * を選択します。

   クラウドストレージプールの作成ポップアップが表示されます。

3. 表示名を入力します。
4. [Provider Type]ドロップダウンリストから[**Amazon S3**]を選択します。

   このプロバイダタイプはAWS S3またはGoogle Cloudに対応しています。

5. クラウドストレージプールに使用するS3バケットのURIを入力します。

   次の2つの形式を使用できます。

   https://host:port`

   http://host:port`

6. S3バケット名を入力します。

   指定する名前はS3バケットの名前と完全に一致する必要があります。一致していないと、クラウドストレージプールの作成が失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。

7. 必要に応じて、アクセスキーIDとシークレットアクセスキーを入力します。
8. ドロップダウンから[* Do not verify Certificate*（証明書を検証しない*）]を選択します。
9. [保存（ Save ）] をクリックします。

想定される結果です

Amazon S3またはGoogle Cloud用のクラウドストレージプールが作成されていることを確認します。

ジョナサン・ウォン著

Azure Blob Storage用のクラウドストレージプールを作成します

StorageGRID オブジェクトを外部のAzureコンテナに移動する場合は、クラウドストレージプールを使用できます。

必要なもの

- StorageGRID 11.6が設定されました。
- 外部のAzureコンテナはすでにセットアップされています。

手順

1. Grid Managerで、* ILM *>*ストレージプール*に移動します。
2. ページのクラウドストレージプールセクションで、 * 作成 * を選択します。

クラウドストレージプールの作成ポップアップが表示されます。

3. 表示名を入力します。
4. プロバイダタイプドロップダウンリストから「* Azure Blob Storage *」を選択します。
5. クラウドストレージプールに使用するS3バケットのURIを入力します。

   次の2つの形式を使用できます。

   https://host:port`

   http://host:port`

6. Azureコンテナ名を入力します。

   指定する名前はAzureコンテナ名と完全に一致する必要があります。一致していないと、クラウドストレージプールの作成は失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。

7. 必要に応じて、Azureコンテナに関連付けられたアカウント名と認証用のアカウントキーを入力します。
8. ドロップダウンから[* Do not verify Certificate*（証明書を検証しない*）]を選択します。
9. [保存（ Save ）] をクリックします。

想定される結果です

Azure Blob Storage用のクラウドストレージプールが作成されていることを確認します。

ジョナサン・ウォン著

クラウドストレージプールをバックアップに使用する

バックアップ用にクラウドストレージプールにオブジェクトを移動するILMルールを作成できます。

必要なもの

- StorageGRID 11.6が設定されました。
- 外部のAzureコンテナはすでにセットアップされています。

手順

1. Grid Managerで、* ILM > Rules > Create *の順に移動します。
2. 概要 を入力します。
3. ルールをトリガーする基準を入力します。
4. 「 * 次へ * 」をクリックします。
5. オブジェクトをストレージノードにレプリケートします。
6. 配置ルールを追加します。
7. オブジェクトをクラウドストレージプールにレプリケートします

8. 「 * 次へ * 」をクリックします。
9. [保存（ Save ）] をクリックします。

想定される結果です

保持図に、バックアップ用にStorageGRID とクラウドストレージプールにローカルに格納されているオブジェクトが示されていることを確認します。

ILMルールがトリガーされたときにクラウドストレージプールにコピーが存在し、オブジェクトのリストアを実行せずにローカルでオブジェクトを読み出すことができることを確認します。

ジョナサン・ウォン著

StorageGRID 検索統合サービスを設定する

このガイドでは、Amazon OpenSearchサービスまたはオンプレミスの Elasticsearch とNetApp StorageGRID検索統合サービスを設定するための詳細な手順について説明します。

はじめに

StorageGRID は、3種類のプラットフォームサービスをサポートしています。

- * StorageGRID CloudMirrorレプリケーション*。StorageGRID バケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングします。
- 通知。バケット単位のイベント通知：オブジェクトに対して実行された特定の処理に関する通知を、指定された外部のAmazon Simple Notification Service（Amazon SNS）に送信します。
- 検索統合サービス。外部サービスを使用してメタデータを検索または分析できるように、指定されたElasticsearchインデックスにSimple Storage Service（S3）オブジェクトメタデータを送信します。

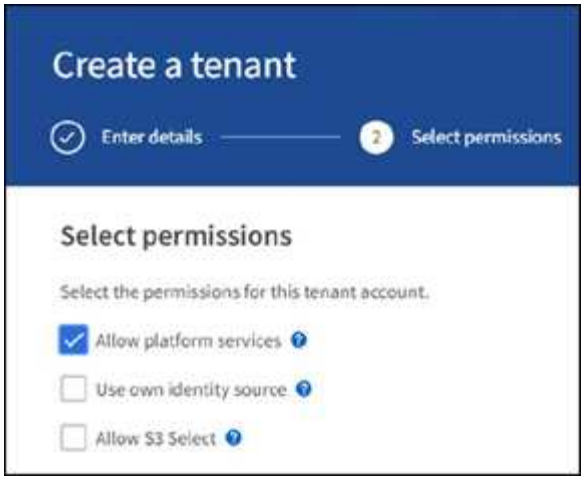
プラットフォームサービスは、テナントマネージャのUIを使用してS3テナントによって設定されます。詳細については、を参照してください "プラットフォームサービスの使用に関する考慮事項"。

このドキュメントは、の補足資料として機能します "StorageGRID 11.6テナントガイド" およびに、検索統合サービス用のエンドポイントとバケットの設定手順と例を示します。ここで紹介するAmazon Web Services（AWS）またはオンプレミスのElasticsearchセットアップの手順は、基本的なテストやデモ目的にのみ使用します。

対象読者は、Grid Manager、テナントマネージャに精通している必要があり、S3ブラウザにアクセスして、StorageGRID 検索統合テストの基本的なアップロード（PUT）処理とダウンロード（GET）処理を実行できます。

テナントを作成し、プラットフォームサービスを有効にします

1. Grid Managerを使用してS3テナントを作成し、表示名を入力してS3プロトコルを選択する。
2. [アクセス許可]ページで、[プラットフォームサービスを許可する]オプションを選択します。必要に応じて、他の権限を選択します。



3. テナントのrootユーザの初期パスワードを設定するか、グリッドでフェデレーションが有効になっている場合は、テナントアカウントを設定するためのrootアクセス権限を持つフェデレーテッドグループを選択します。
4. [ルートとしてサインイン]をクリックし、[バケット：バケットの作成と管理]を選択します。

   Tenant Managerのページが表示されます。

5. Tenant Managerで、My Access Keysを選択してS3アクセスキーを作成およびダウンロードし、あとでテストを実施します。

Amazon OpenSearchとの検索統合サービス

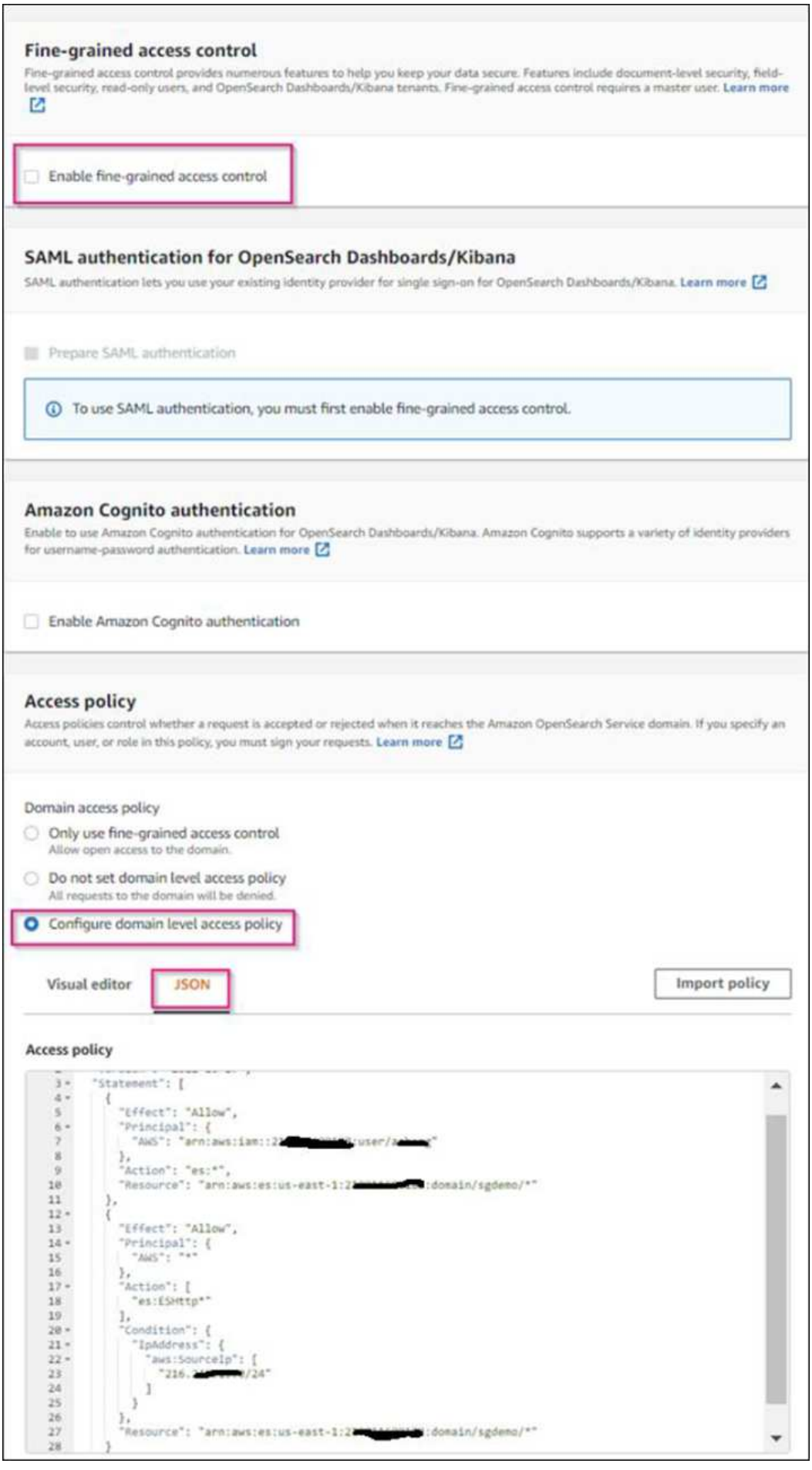
Amazon OpenSearch（旧Elasticsearch）サービスのセットアップ

この手順 は、テスト/デモ目的でのみOpenSearchサービスをすばやく簡単にセットアップするために使用します。検索統合サービスにオンプレミスのElasticsearchを使用している場合は、を参照してください 検索統合サービスをオンプレミスのElasticsearchと利用できます。

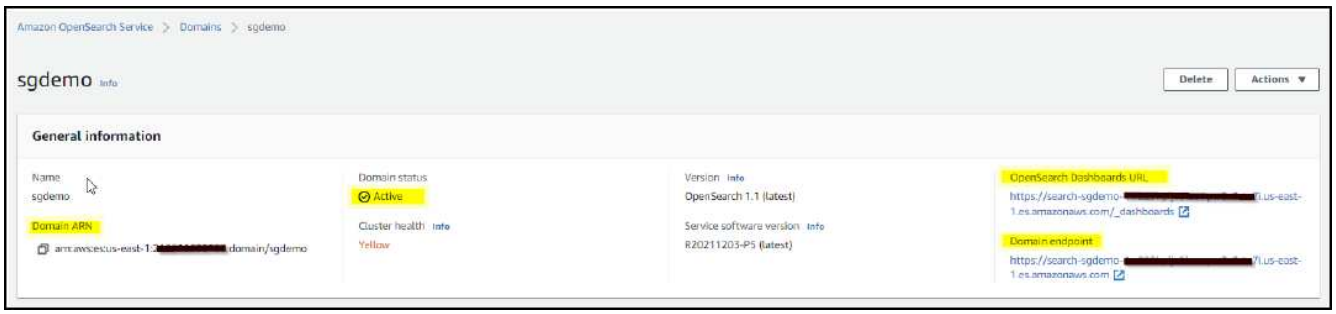
OpenSearchサービスに登録するには、有効なAWSコンソールログイン、アクセスキー、シークレットアクセスキー、および権限が必要です。

1. の手順に従って、新しいドメインを作成します "AWS OpenSearchサービス開始前の準備"次の場合を除きます。
   - 手順 4ドメイン名：sgdemo
   - 手順10：きめ細かなアクセスコントロール：「きめ細かなアクセスコントロールを有効にする」オプションの選択を解除します。
   - 手順12.アクセスポリシー：Configure Level Access Policyを選択し、JSONタブを選択して次の例を使用してアクセスポリシーを変更します。
     - 強調表示されたテキストを、AWS Identity and Access Management（IAM）IDとユーザ名に置き換えます。
     - 強調表示されているテキスト（IPアドレス）を、AWSコンソールへのアクセスに使用したローカルコンピュータのパブリックIPアドレスに置き換えます。
     - ブラウザタブを開き、に移動します "https://checkip.amazonaws.com" をクリックして、パブリックIPを検索してください。

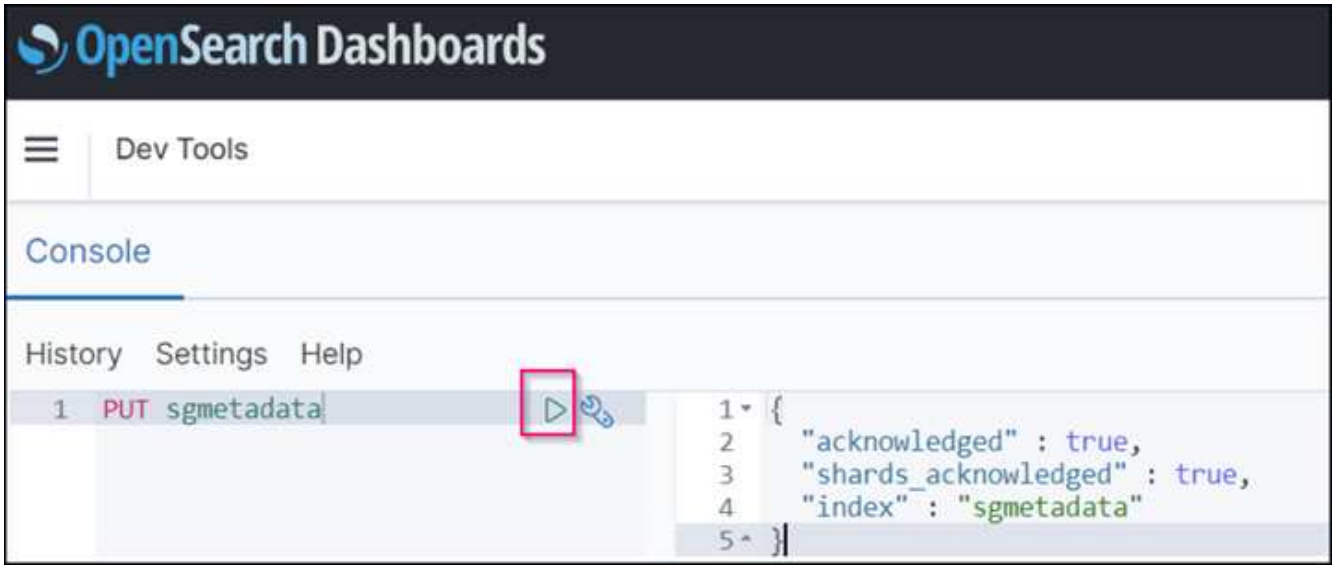
```
{

    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal":
        {"AWS": "arn:aws:iam:: nnnnnn:user/xyzabc"},
        "Action": "es:*",
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        },
        {
        "Effect": "Allow",
        "Principal": {"AWS": "*"},
        "Action": [
        "es:ESHttp*"
                ],
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": [ "nnn.nnn.nn.n/nn"
                    ]
                }
        },
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        }
    ]
}
```


Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
Enable fine-grained access control
SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more
Prepare SAML authentication
To use SAML authentication, you must first enable fine-grained access control.
Amazon Cognito authentication
Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more
Enable Amazon Cognito authentication
Access policy
Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more
Domain access policy
Only use fine-grained access control
Allow open access to the domain.
Do not set domain level access policy
All requests to the domain will be denied.
Configure domain level access policy
Visual editor
JSON
Import policy
Access policy
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::2[redacted]:user/A[redacted]"
},
"Action": "es:*",
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": [
"es:ESHttp*"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": [
"216.[redacted]/24"
]
}
},
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
}

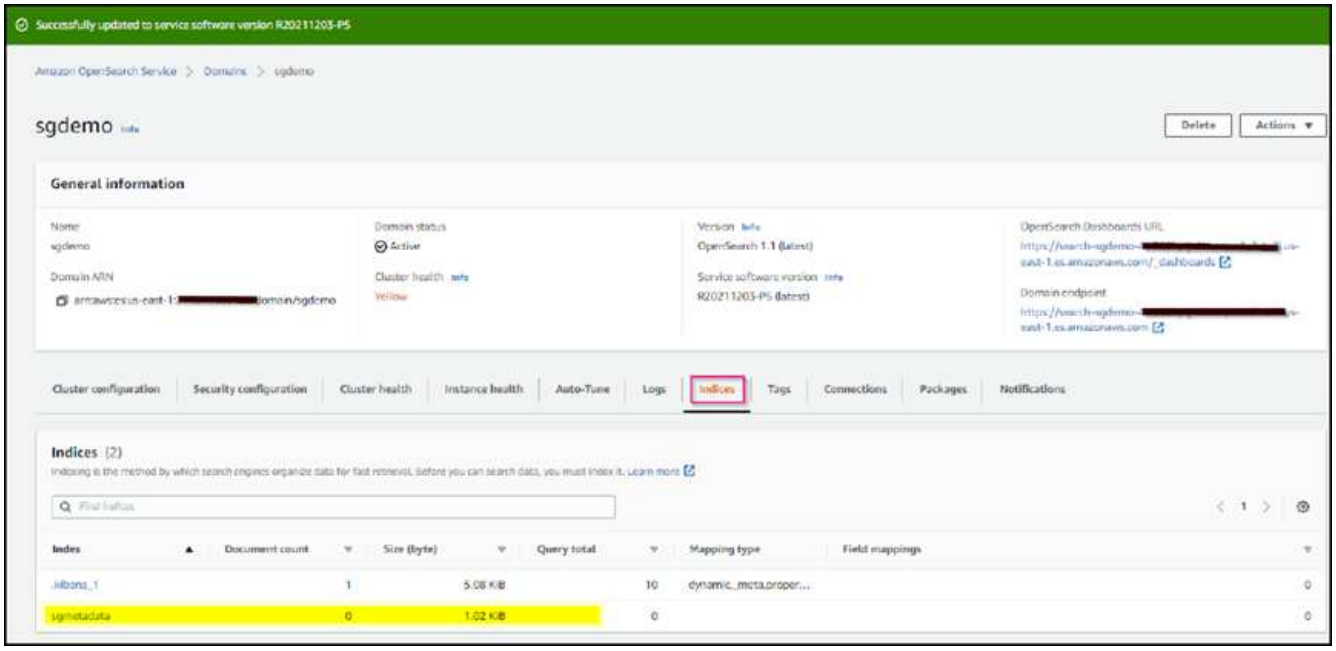
2. ドメインがアクティブになるまで15～20分待ちます。



3. OpenSearch Dashboards URLをクリックして、新しいタブでドメインを開き、ダッシュボードにアクセスします。access deniedエラーが表示された場合は、アクセスポリシーのソースIPアドレスがコンピュータのパブリックIPに正しく設定されていて、ドメインダッシュボードへのアクセスが許可されていることを確認します。
4. ダッシュボードの開始ページで、自分で探索（Explore on your own）を選択します。メニューから、[管理]→[開発ツール]を選択します
5. Dev Tools → Consoleで、StorageGRID オブジェクトメタデータの保存にインデックスを使用する「Put <index>」と入力します。次の例では、インデックス名「メタデータ」を使用します。小さい三角形の記号をクリックして、PUTコマンドを実行します。次のスクリーンショットの例に示すように、正しい結果が右側のパネルに表示されます。



6. インデックスがAmazon OpenSearch UIのsgdomain > Indicesの下に表示されていることを確認します。

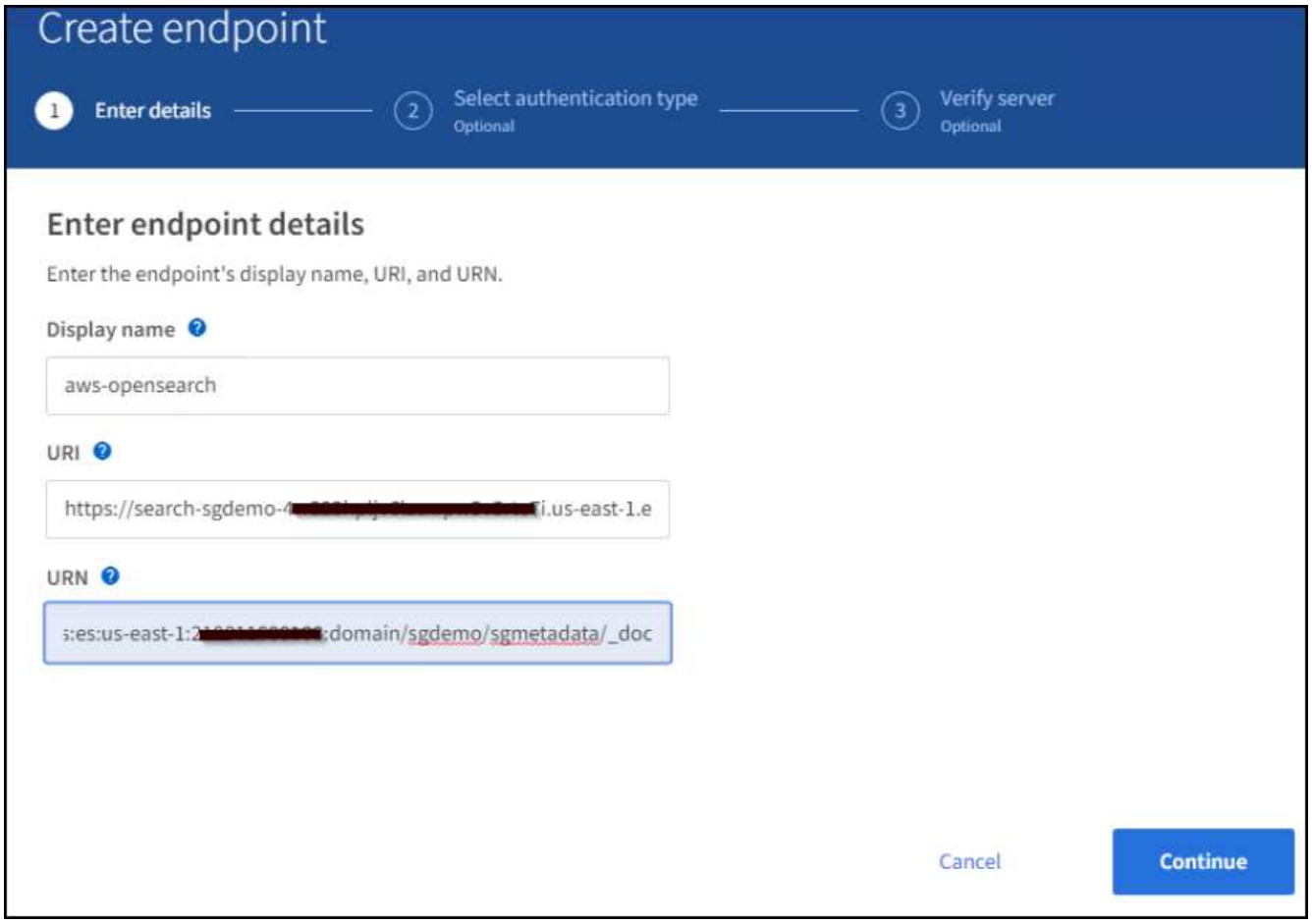


プラットフォームサービスエンドポイントの設定

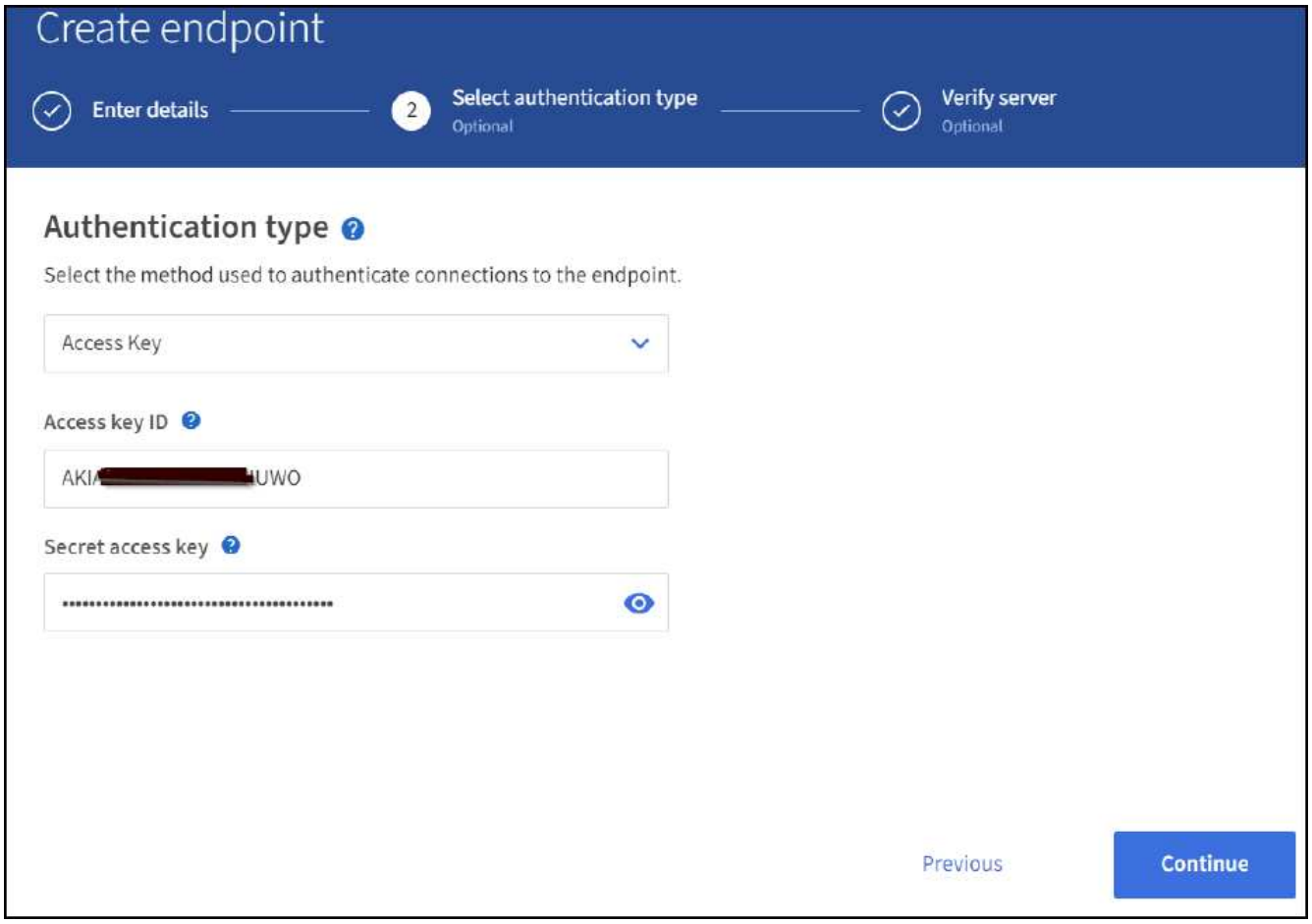
プラットフォームサービスエンドポイントを設定するには、次の手順を実行します。

1. Tenant Managerで、ストレージ（S3）>プラットフォームサービスのエンドポイントに移動します。
2. [エンドポイントの作成]をクリックし、次のように入力して、[続行]をクリックします。
   - 表示名の例は「AWS- OpenSearch」です
   - 手順 フィールドの前の「URI」の手順2の下のスクリーンショットのドメインエンドポイント。
   - URNフィールドで前の手順 の手順2で使用したドメインARNの末尾に'/<index>/_docを追加します

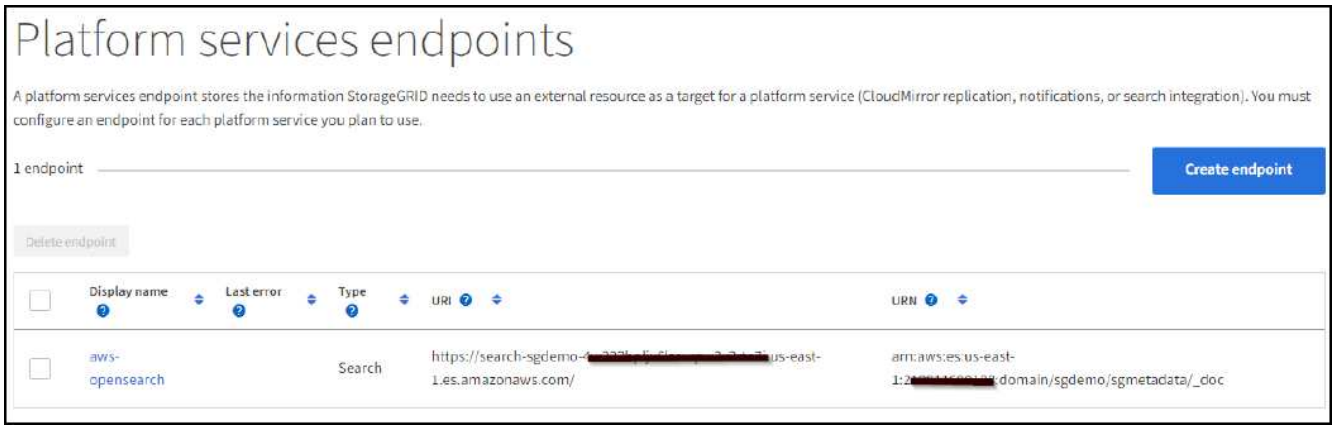
     この例では、URNはarn：aws：es：us-east -1：211234567890：domain/sgdemo/sgmedata/_docになります。



3. Amazon OpenSearchのsgdomainにアクセスするには、認証タイプとしてAccess Keyを選択し、Amazon S3のアクセスキーとシークレットキーを入力します。次のページに移動するには、[続行]をクリックします。



4. エンドポイントを確認するには、Use Operating System CA Certificate and Test and Create Endpointを選択します。検証に成功すると、次の図のようなエンドポイント画面が表示されます。検証に失敗した場合は、URNのパスの末尾に「/<index>/_doc」が含まれていて、AWSアクセスキーとシークレットキーが正しいことを確認してください。



検索統合サービスをオンプレミスの**Elasticsearch**と利用できます

オンプレミスの**Elasticsearch**セットアップ

この手順 は、テスト目的でのみDockerを使用するElasticsearchとKibanaオンプレミスを迅速にセットアップするためのものです。ElasticsearchサーバとKibanaサーバがすでに存在する場合は、ステップ5に進みます。

1. これを実行します "Dockerインストール手順 の略" Dockerをインストールするため。を使用します "CentOS Dockerは手順 をインストールする" このセットアップでは、

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

   - リブート後にDockerを起動するには、次のように入力します。

```
sudo systemctl enable docker
```

   - 「vm.max_map_count」値を262144に設定します。

```
sysctl -w vm.max_map_count=262144
```

   - リブート後も設定を維持するには、次のように入力します。

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. に従ってください "Elasticsearchクイックスタートガイド" ElasticsearchとKibana Dockerを自己管理のためのセクションでインストールして実行できます。この例では、バージョン8.1をインストールしました。

Elasticsearchが作成したユーザ名/パスワードとトークンをメモしておきます。これらのトークンは、Kibana UIおよびStorageGRID プラットフォームエンドポイント認証を開始するために必要です。

Elasticsearch Service | Self-managed

Install and run Elasticsearch

1. Install and start Docker Desktop.
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- Certificates and keys are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.

NOTE You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.

NOTE If you need to reset the password for the `elastic` user or other built-in users, run the `elasticsearch-reset-password` tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the `elasticsearch-create-enrollment-token` tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

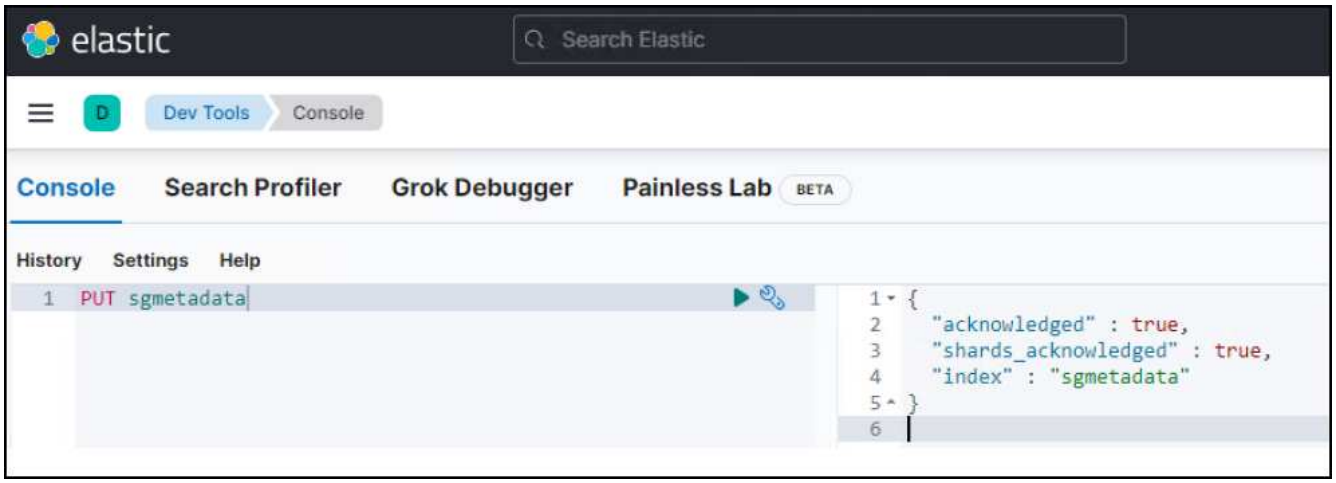
1. In a new terminal session, run:

```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/ki
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.
   a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
   b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

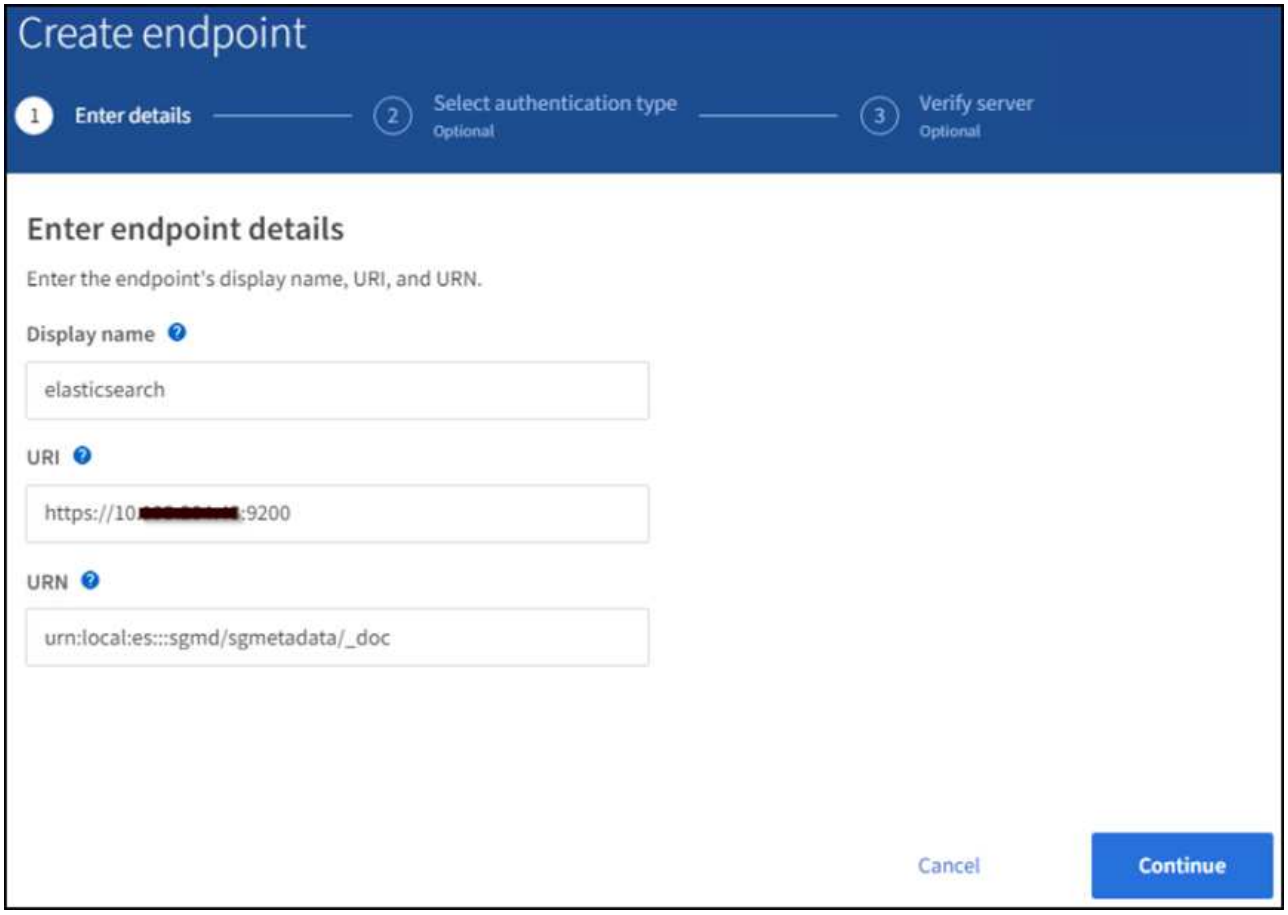
3. Kibana Dockerコンテナが起動すると、コンソールにURLリンク「\ https://0.0.0.0:5601`」が表示されます。0.0.0.0を、URL内のサーバIPアドレスと置き換えます。
4. ユーザ名「elastic」と、前述の手順でElasticによって生成されたパスワードを使用して、Kibana UIにログインします。
5. 初めてログインする場合は、ダッシュボードのようこそページで、自分でエクスプローラ（Explore on your own）を選択します。メニューから、Management > Dev Toolsを選択します。
6. Dev Tools Console画面で、StorageGRID オブジェクトメタデータの保存にこのインデックスを使用する「Put <index>」と入力します。この例では'インデックス名sgmetadataを使用します小さい三角形の記号をクリックして、PUTコマンドを実行します。次のスクリーンショットの例に示すように、正しい結果が右側のパネルに表示されます。



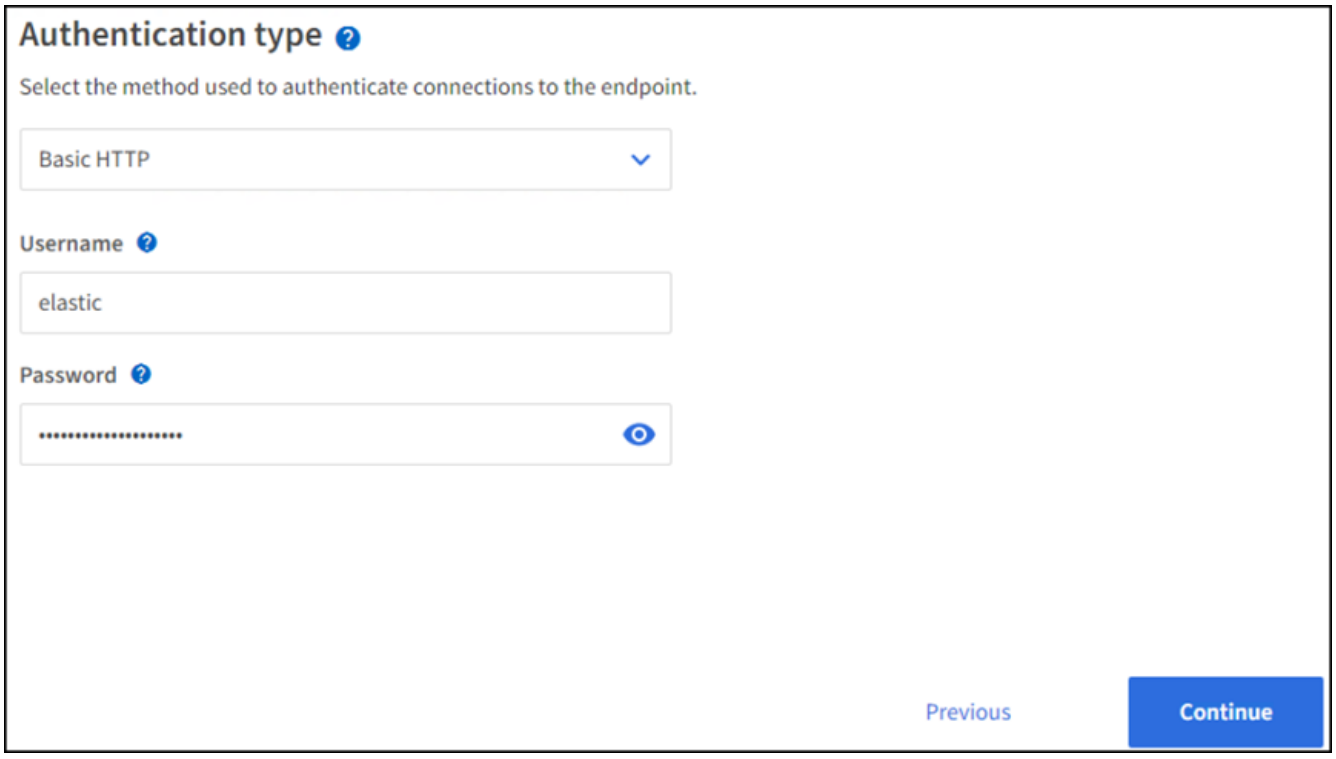
プラットフォームサービスエンドポイントの設定

プラットフォームサービスのエンドポイントを設定するには、次の手順を実行します。

1. Tenant Managerで、ストレージ（S3）>プラットフォームサービスのエンドポイントに移動します
2. [エンドポイントの作成]をクリックし、次のように入力して、[続行]をクリックします。
   - 表示名の例: elastic`
   - URI:`\https://<elasticsearch-server-ipまたはhostname>:9200`
   - urn:`urn:<何か>:es:::<se-unique text>/<index-name>/_doc`ここで、index-nameはKibanaコンソールで使用した名前です。例:`urn:local:es::sgmd/sgmetadata/_doc`

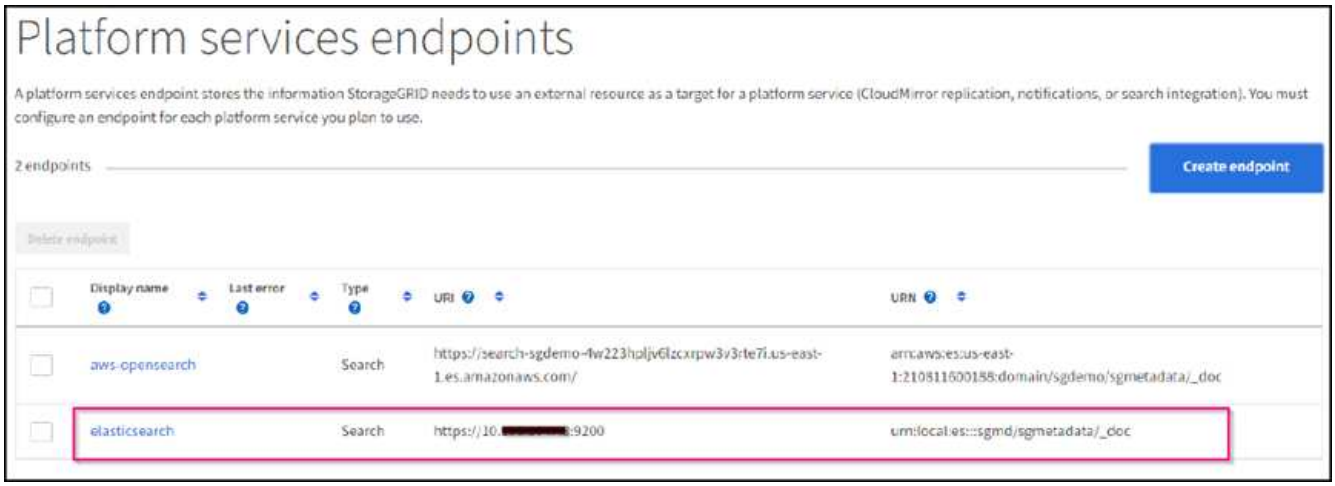


3. 認証タイプとしてBasic HTTPを選択し、Elasticsearchのインストールプロセスによって生成されたユーザ名「elastic」とパスワードを入力します。次のページに移動するには、[続行]をクリックします。



4. エンドポイントを確認するには、Do not verify Certificate and Test and Create Endpointを選択します。検

証に成功すると、次のスクリーンショットと同様のエンドポイント画面が表示されます。検証が失敗した場合は、URN、URI、およびユーザ名とパスワードのエントリが正しいことを確認してください。



バケット検索統合サービスの設定

プラットフォームサービスエンドポイントの作成後、次の手順では、オブジェクトの作成、削除、またはそのメタデータ/タグの更新が行われるたびに定義済みのエンドポイントにオブジェクトメタデータを送信するように、このサービスをバケットレベルで設定します。

Tenant Managerを使用して検索統合を設定し、カスタムのStorageGRID 設定XMLをバケットに次のように適用できます。

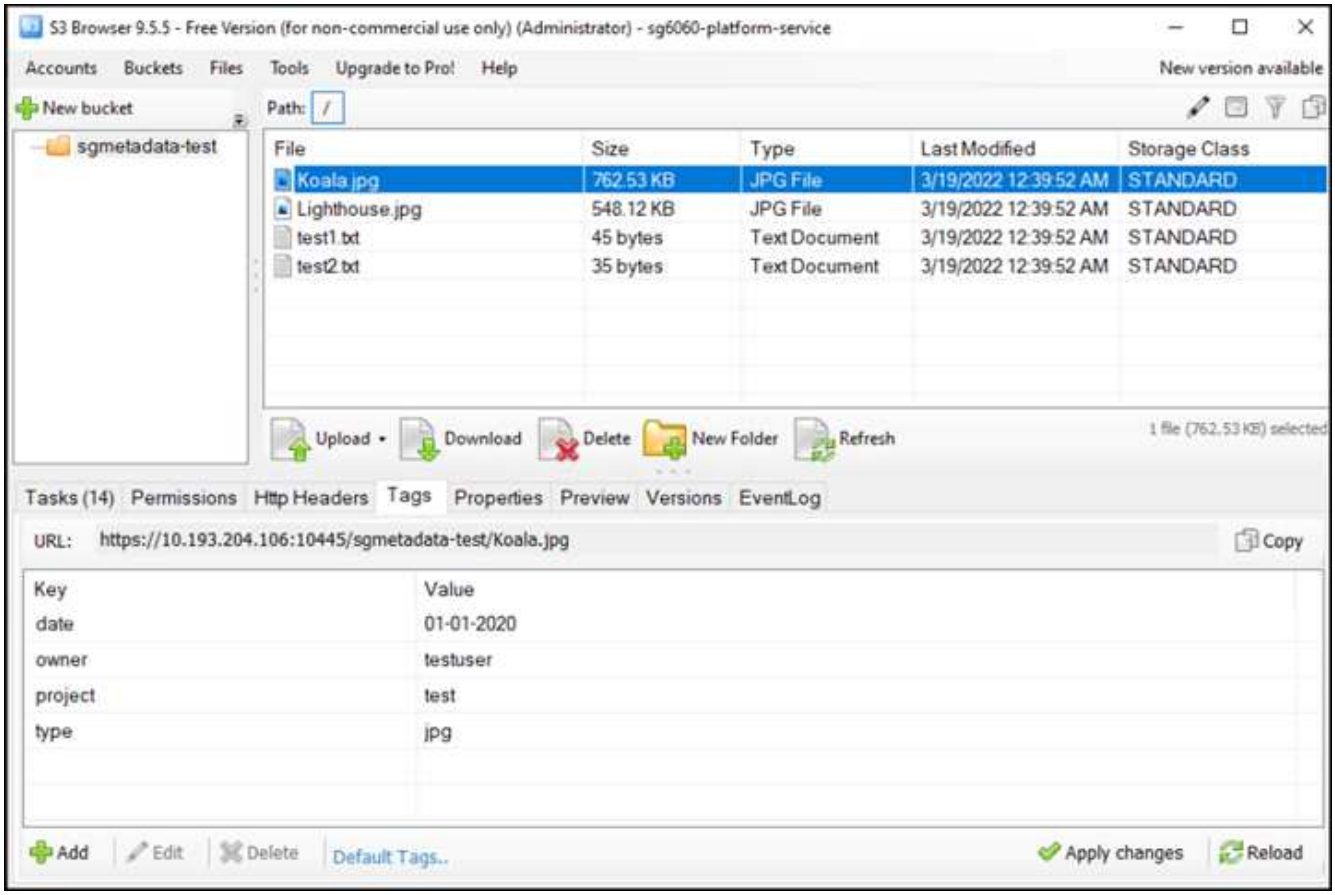
1. Tenant Managerで、Storage（S3）> Bucketsに移動します
2. Create Bucket（バケットの作成）をクリックし、バケット名（例：sgmetadatatest'）を入力して、デフォルトのus-east-1リージョンを受け入れます。
3. [Continue]>[Create Bucket]をクリックします。
4. バケットの概要ページを表示するには、バケット名をクリックし、プラットフォームサービスを選択します。
5. [検索統合を有効にする]ダイアログボックスを選択します。表示されたXMLボックスに、この構文を使用して設定XMLを入力します。

   強調表示されたURNは、定義したプラットフォームサービスエンドポイントと一致する必要があります。別のブラウザタブを開いてTenant Managerにアクセスし、定義済みのプラットフォームサービスエンドポイントからURNをコピーできます。

   この例ではプレフィックスを使用していません。つまり、このバケット内のすべてのオブジェクトのメタデータが、前に定義したElasticsearchエンドポイントに送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

6. S3 Browserを使用して、テナントアクセス/シークレットキーを使用してStorageGRID に接続し、テストオブジェクトを「sgmetadata-test」バケットにアップロードし、タグまたはカスタムメタデータをオブジェクトに追加します。



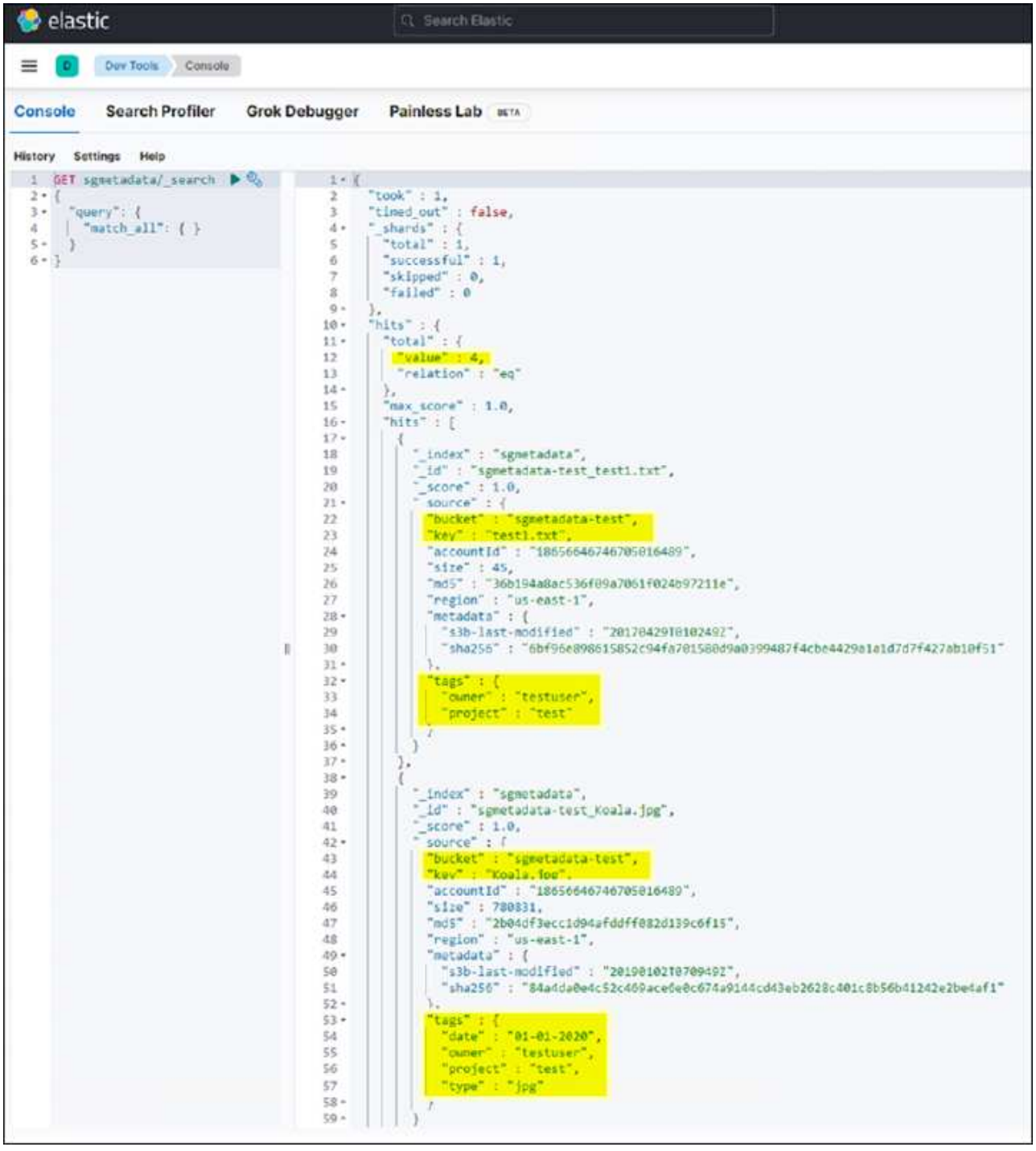
7. Kibana UIを使用して、オブジェクトメタデータがsgmetadataのインデックスにロードされたことを確認します。

   a. メニューから、Management > Dev Toolsを選択します。

   b. 左側のコンソールパネルにサンプルクエリを貼り付け、三角形の記号をクリックして実行します。

      次の例のスクリーンショットでは、クエリ1のサンプル結果に4つのレコードが表示されています。これはバケット内のオブジェクトの数に一致します。

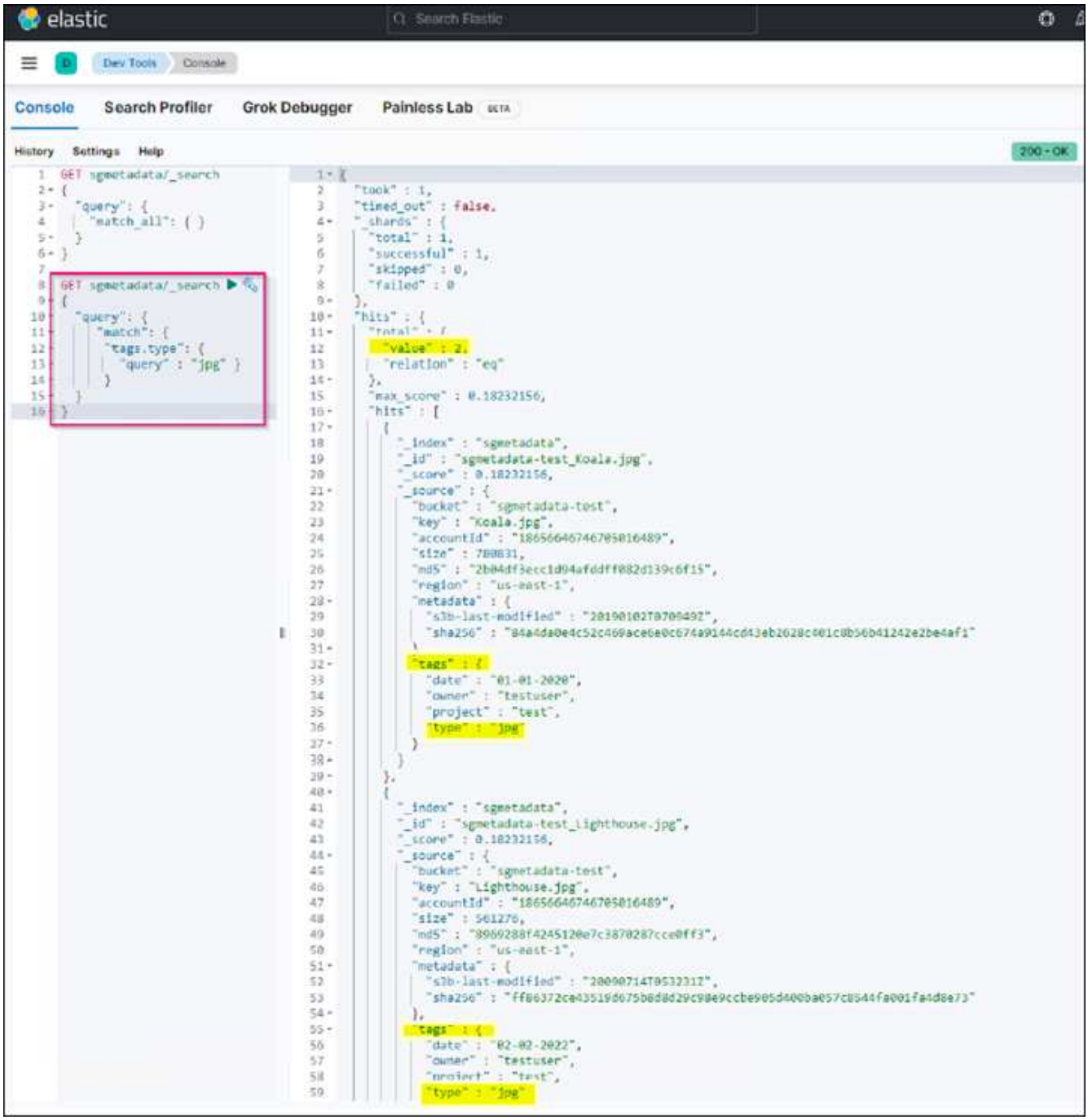
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



次のスクリーンショットのクエリ2のサンプル結果は、タグタイプがjpgの2つのレコードを示しています。

```
GET sgmetadata/_search
{
    "query": {
        "match": {
            "tags.type": {
                "query" : "jpg" }
                }
            }
}
```

+



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。

- "プラットフォームサービスとは"
- "StorageGRID 11.6 ドキュメント"

Angela Cheng著_

ノードクローン

ノードクローンに関する考慮事項とパフォーマンス

ノードクローンに関する考慮事項

ノードクローンを使用すると、機器更改（Tech Refresh）の際に既存のアプライアンスノードをすばやく交換したり、容量を増やしたり、StorageGRID システムのパフォーマンスを向上させたりできます。ノードクローンは、KMSを使用したノード暗号化への変換や、ストレージノードをDDP8からDDP16に変更する場合にも役立ちます。

- ソースノードの使用済み容量は、クローンプロセスの完了に必要な時間とは関係ありません。ノードクローンは、ノードの空きスペースを含むノードのフルコピーです。
- ソースアプライアンスとデスティネーションアプライアンスのPGEバージョンが同じである必要があります
- デスティネーションノードの容量は常にソースノードよりも大きくする必要があります
  - 新しいデスティネーションアプライアンスのドライブサイズがソースよりも大きいことを確認します
  - デスティネーションアプライアンスのドライブサイズが同じで、DDP8用に設定されている場合は、DDP16用にデスティネーションを設定できます。ソースがすでにDDP16用に設定されている場合、ノードのクローニングは実行できません。
  - SG5660またはSG5760アプライアンスからSG6060アプライアンスに移行する場合、SG5x60には容量ドライブが60本搭載されていますが、SG6060には58本しか搭載されていません。
- ノードのクローニングプロセスでは、クローニングプロセスの実行中はソースノードがグリッドに対してオフラインになっている必要があります。この間に追加のノードがオフラインになると、クライアントサービスに影響する可能性があります。
- 11.8以降：ストレージノードをオフラインにできるのは15日間です。クローニングプロセスの推定日数が15日に近い場合、または15日を超える場合は、拡張と運用停止の手順を使用します。
  - 11.9：15日間の制限が削除されました。
- 拡張シェルフを使用するSG6060またはSG6160では、正しいシェルフドライブサイズの時間をベースアプライアンスの時間に追加して、フルクローン期間を取得する必要があります。
- ターゲットストレージアプライアンスのボリューム数は、ソースノードのボリューム数以上である必要があります。16個のオブジェクトストアボリューム（rangedb）を含むソースノードを、12個のオブジェクトストアボリュームを含むターゲットストレージアプライアンスにクローニングすることはできません。これは、ターゲットアプライアンスの容量がソースノードよりも大きい場合でも同様です。ほとんどのストレージアプライアンスにはオブジェクトストアボリュームが16個ありますが、オブジェクトストアボリュームが12個しかないSGF6112ストレージアプライアンスは除きます。たとえば、SG5760からSGF6112

にクローニングすることはできません。

ノードクローンのパフォーマンスを見積もります

次の表に、ノードクローンの所要時間の推定値を示します。条件は状況によって異なるため、*太字*で示されたエントリは、ノードが停止した場合に15日を超えるリスクがあります。

DDP8

SG5612 / SG5712 / SG5812 →任意

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	1 日	2日	2.5日	3日	4日	4.5日	5.5日
25GB	1 日	2日	2.5日	3日	4日	4.5日	5.5日

SG5660 → SG5760 / SG5860

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	3.5日	7 日	8.5日	10.5日	• 13.5日*	• 15.5日*	• 18.5日*
25GB	3.5日	7 日	8.5日	10.5日	• 13.5日*	• 15.5日*	• 18.5日*

SG5660 → SG6060 / SG6160

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	2.5日	4.5日	5.5日	6.5日	9日	10日間	• 12日*
25GB	2日間	4日	5日	6日	8日間	9日	10日間

SG5760 / SG5860 → SG5760 / SG5860

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	3.5日	7 日	8.5日	10.5日	• 13.5日*	• 15.5日*	• 18.5日*

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
25GB	3.5日	7 日	8.5日	10.5日	• 13.5日*	• 15.5日*	• 18.5日*

SG5760 / SG5860 → SG6060 / SG6160

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	2.5日	4.5日	5.5日	6.5日	9日	10日間	• 12日*
25GB	2日間	3.5日	4.5日	5.5日	7 日	8日間	9.5日

SG6060 / SG6160 → SG6060 / SG6160

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	2.5日	4.5日	5.5日	6.5日	8.5日	9.5日	11.5日
25GB	2日間	3日	4日	4.5日	6日	7 日	8.5日

DDP16

SG5760 / SG5860 → SG5760 / SG5860

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	3.5日	6.5日	8日間	9.5日	• 12.5日*	• 14日*	• 17日*
25GB	3.5日	6.5日	8日間	9.5日	• 12.5日*	• 14日*	• 17日*

SG5760 / SG5860 → SG6060 / SG6160

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	2.5日	5日	6日	7.5日	10日間	11日だ	• 13日*

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
25GB	2日間	3.5日	4日	5日	6.5日	7 日	8.5日

SG6060 / SG6160 → SG6060 / SG6160

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	3日間	5日	6日	7 日	9.5日	10.5日	• 13日*
25GB	2日間	3.5日	4.5日	5日	7 日	7.5日	9日

拡張シェルフ（ソースアプライアンスのシェルフごとに上記の**SG6060 / SG6160**に追加）

ネットワークインターフェイスの速度	**4TB**ドライブサイズ	**8TB**ドライブサイズ	**10TB**ドライブサイズ	**12TB**ドライブサイズ	**16TB**ドライブサイズ	**18TB**のドライブサイズ	**22TB**のドライブサイズ
10Gb	3.5日	5日	6日	7 日	9.5日	10.5日	• 12日*
25GB	2日間	3日	4日	4.5日	6日	7 日	8.5日

アロンクライン著

グリッドサイトの再配置とサイト全体のネットワーク変更手順

このガイドでは、マルチサイトグリッドでのStorageGRIDサイトの再配置の準備と手順について説明します。この手順を完全に理解し、スムーズなプロセスを実現し、クライアントの中断を最小限に抑えるために事前に計画しておく必要があります。

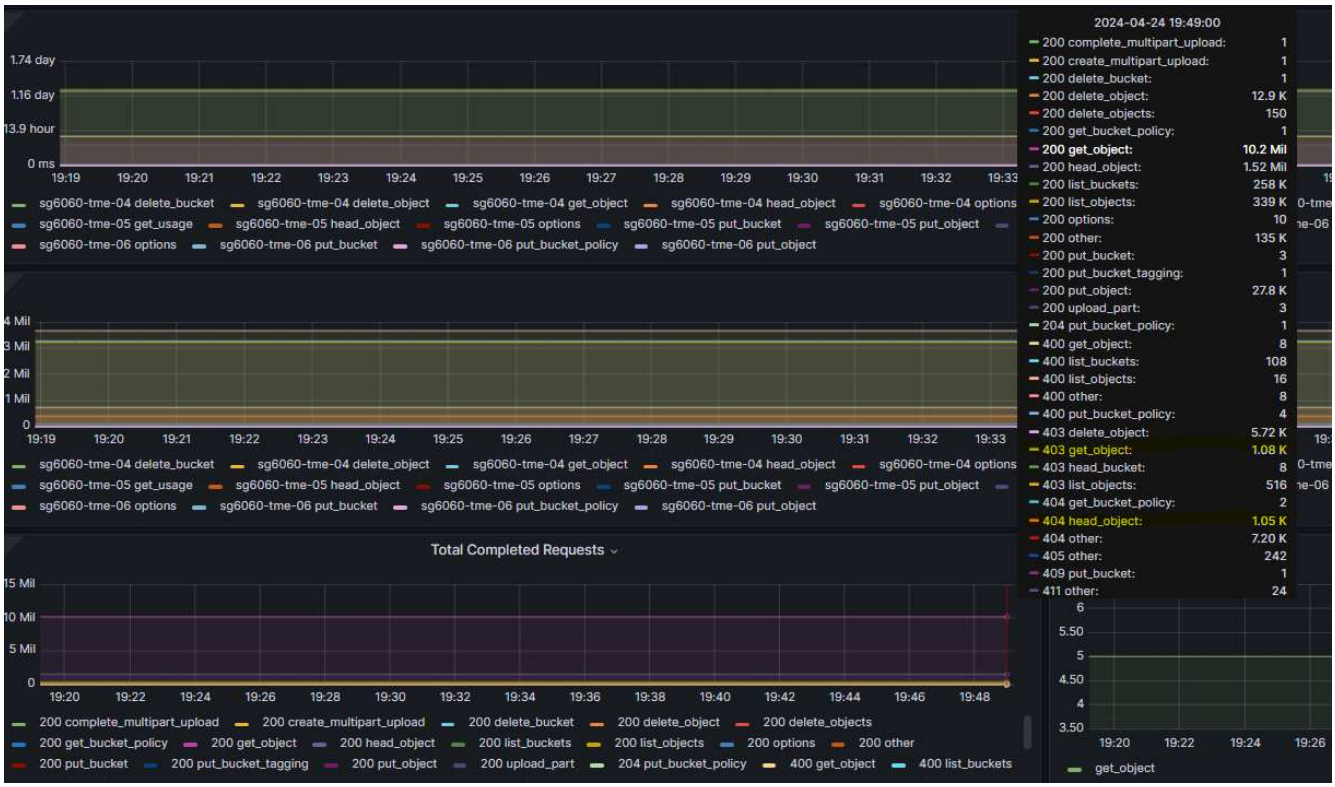
グリッド全体のグリッドネットワークを変更する必要がある場合は、を参照してください。
"グリッド内のすべてのノードの IP アドレスを変更します"。

サイトの再配置前の考慮事項

- Cassandraデータベースの再構築を回避するには、サイトの移動を完了し、すべてのノードを15日以内にオンラインにします。
  "ストレージノードを 15 日以上停止した状態にリカバリします"
- アクティブポリシー内のいずれかのILMルールで厳密な取り込み動作が使用されている場合は、サイトの再配置中にオブジェクトを引き続きグリッドに配置する必要がある場合は、負荷分散またはデュアルコミットに変更することを検討してください。
- ストレージアプライアンスに60本以上のドライブが搭載されている場合は、ディスクドライブが取り付けられているシェルフを移動しないでください。 パック/移動の前に、各ディスクドライブにラベルを付

け、ストレージエンクロージャから取り外します。

- StorageGRIDアプライアンスの変更グリッドネットワークVLANは、管理ネットワークまたはクライアントネットワーク経由でリモートで実行できます。 または、勤務地変更の前後にオンサイトで変更を実施する予定です。
- PUTの前に、お客様のアプリケーションがHEADを使用しているか、存在しないオブジェクトを取得しているかを確認「はい」の場合は、HTTP 500エラーを回避するためにバケットの整合性をstrong-siteに変更します。 不明な場合は、S3の概要Grafanaグラフ*[Grid manager]>[Support]>[Metrics]*を確認し、[Total Completed Request]グラフにカーソルを合わせます。 404 GET Objectまたは404 HEADオブジェクトの数が非常に多い場合は、1つ以上のアプリケーションがHEADまたはGET Non-existenceオブジェクトを使用している可能性があります。カウントは累積値です。異なるタイムライン上にマウスを移動すると、その差が表示されます。



サイトの再配置前に手順で**Grid IP**アドレスを変更

手順

1. 新しいグリッドネットワークサブネットが新しい場所で使用される場合は、"グリッドネットワークサブネットリストにサブネットを追加します。"
2. プライマリ管理ノードにログインし、change-ipを使用してグリッドIPを変更します。再配置用にノードをシャットダウンする前に、変更をステージングする必要があります*。
   a. [Grid IP]で[2]、[1]を選択します。

```
Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP/mask [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP/mask [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP/mask [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP/mask [     10.45.74.18/26 ]: 10.45.74.28/26
================================================================================
LONDON-ADM1 Grid    Gateway [         10.45.74.1 ]:
LONDON-S1   Grid    Gateway [         10.45.74.1 ]:
LONDON-S2   Grid    Gateway [         10.45.74.1 ]:
LONDON-S3   Grid    Gateway [         10.45.74.1 ]:
================================================================================
================================================================================
Site: OXFORD
================================================================================
OXFORD-ADM1 Grid    IP/mask [     10.45.75.14/26 ]:
OXFORD-S1   Grid    IP/mask [     10.45.75.16/26 ]:
OXFORD-S2   Grid    IP/mask [     10.45.75.17/26 ]:
OXFORD-S3   Grid    IP/mask [     10.45.75.18/26 ]:
================================================================================
OXFORD-ADM1 Grid    Gateway [         10.45.75.1 ]:
OXFORD-S1   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S2   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S3   Grid    Gateway [         10.45.75.1 ]:
================================================================================
Finished editing. Press Enter to return to menu.
```

b. 5を選択して変更を表示

```
================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP      [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP      [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP      [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP      [     10.45.74.18/26 ]: 10.45.74.28/26
Press Enter to continue
```

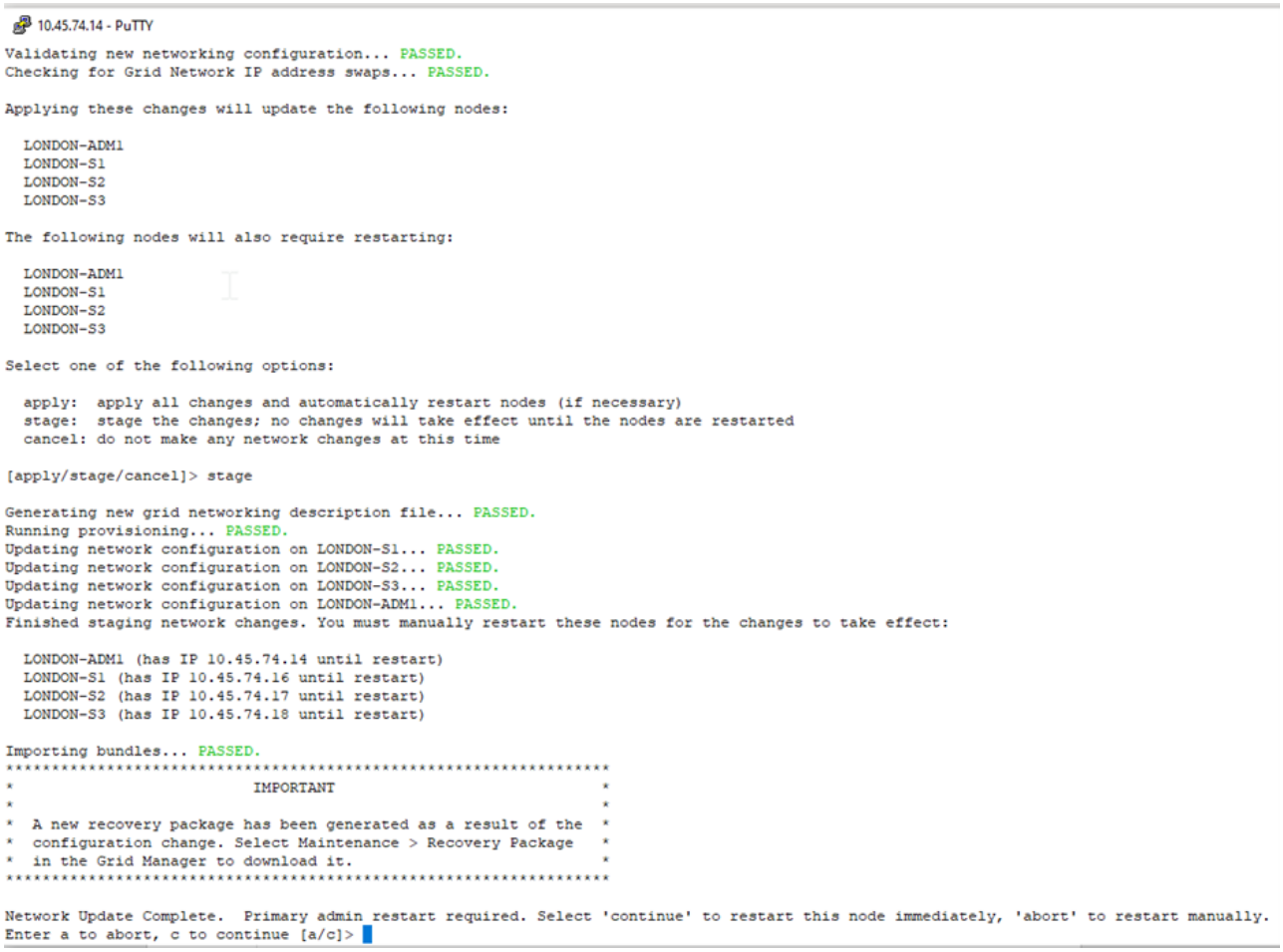
c. [10]を選択して確定し、変更を適用します。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection: 10
```

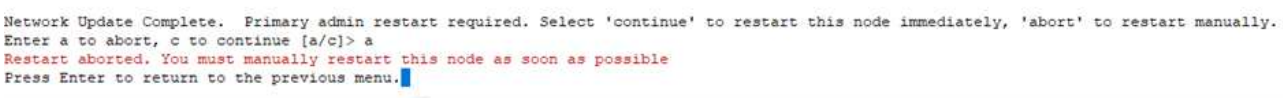
d. このステップで* stage *を選択する必要があります。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

The following nodes will also require restarting:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

Select one of the following options:

  apply:  apply all changes and automatically restart nodes (if necessary)
  stage:  stage the changes; no changes will take effect until the nodes are restarted
  cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. 上記の変更にプライマリ管理ノードが含まれている場合は、「**a**」と入力して手動でプライマリ管理ノードを再起動します



f. Enterキーを押して前のメニューに戻り、IPインターフェイスの変更を終了します。



3. Grid Managerから、新しいリカバリパッケージをダウンロードします。* Grid Manager **>***メンテナンス>* リカバリパッケージ*
4. StorageGRIDアプライアンスでVLANの変更が必要な場合は、を参照してください。 アプライアンスVLANの変更。
5. サイトのすべてのノードおよびアプライアンスをシャットダウンし、必要に応じてディスクドライブにラベルを付けて取り外し、ラックを開梱して梱包して移動します。
6. 管理ネットワークのIP、クライアントのVLAN、IPアドレスを変更する場合は、再配置後に変更を実行できます。

アプライアンス**VLAN**の変更

以下の手順は、リモートから変更を実行するために、StorageGRIDアプライアンスの管理ネットワークまたはクライアントネットワークにリモートアクセスできることを前提としています。

手順

1. アプライアンスをシャットダウンする前に、"アプライアンスをメンテナンスモードにします"。

2. ブラウザを使用したStorageGRIDアプライアンスインストーラGUIへのアクセス https://<admin-or-client-network-ip>:8443。 アプライアンスをメンテナンスモードでブートすると、すでに使用されている新しいグリッドIPとしてグリッドIPを使用することはできません。
3. グリッドネットワークのVLANを変更します。 クライアント・ネットワーク経由でアプライアンスにアクセスする場合、現時点ではクライアントVLANは変更できません。移動後に変更できます。
4. アプライアンスにSSH接続し、「shutdown -h now」を使用してノードをシャットダウン
5. 新しいサイトでアプライアンスの準備が完了したら、を使用してStorageGRIDアプライアンスインストーラのGUIにアクセスします。 https://<grid-network-ip>:8443。 GUIでping / nmapツールを使用して、ストレージが最適な状態であり、他のグリッドノードへのネットワーク接続が確立されていることを確認します。
6. クライアントネットワークIPの変更を計画している場合は、この段階でクライアントVLANを変更できます。 クライアントネットワークは、このあとの手順でIP変更ツールを使用してクライアントネットワークIPを更新するまで準備ができていません。
7. メンテナンスモードを終了します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。
8. すべてのノードが稼働し、[Grid]に接続問題が表示されなくなったら、必要に応じてchange-IPを使用してアプライアンスの管理ネットワークとクライアントネットワークを更新します。

ONTAP S3からStorageGRIDへのオブジェクトベースストレージの移行

オブジェクトベースストレージを**ONTAP S3**から**StorageGRID**にシームレスに移行し、エンタープライズクラスの**S3**を実現

オブジェクトベースストレージをONTAP S3からStorageGRIDにシームレスに移行し、エンタープライズクラスのS3を実現

移行のデモ

このデモでは、ユーザとバケットをONTAP S3からStorageGRIDに移行する方法について説明します。

オブジェクトベースストレージを**ONTAP S3**から**StorageGRID**にシームレスに移行し、エンタープライズクラスの**S3**を実現

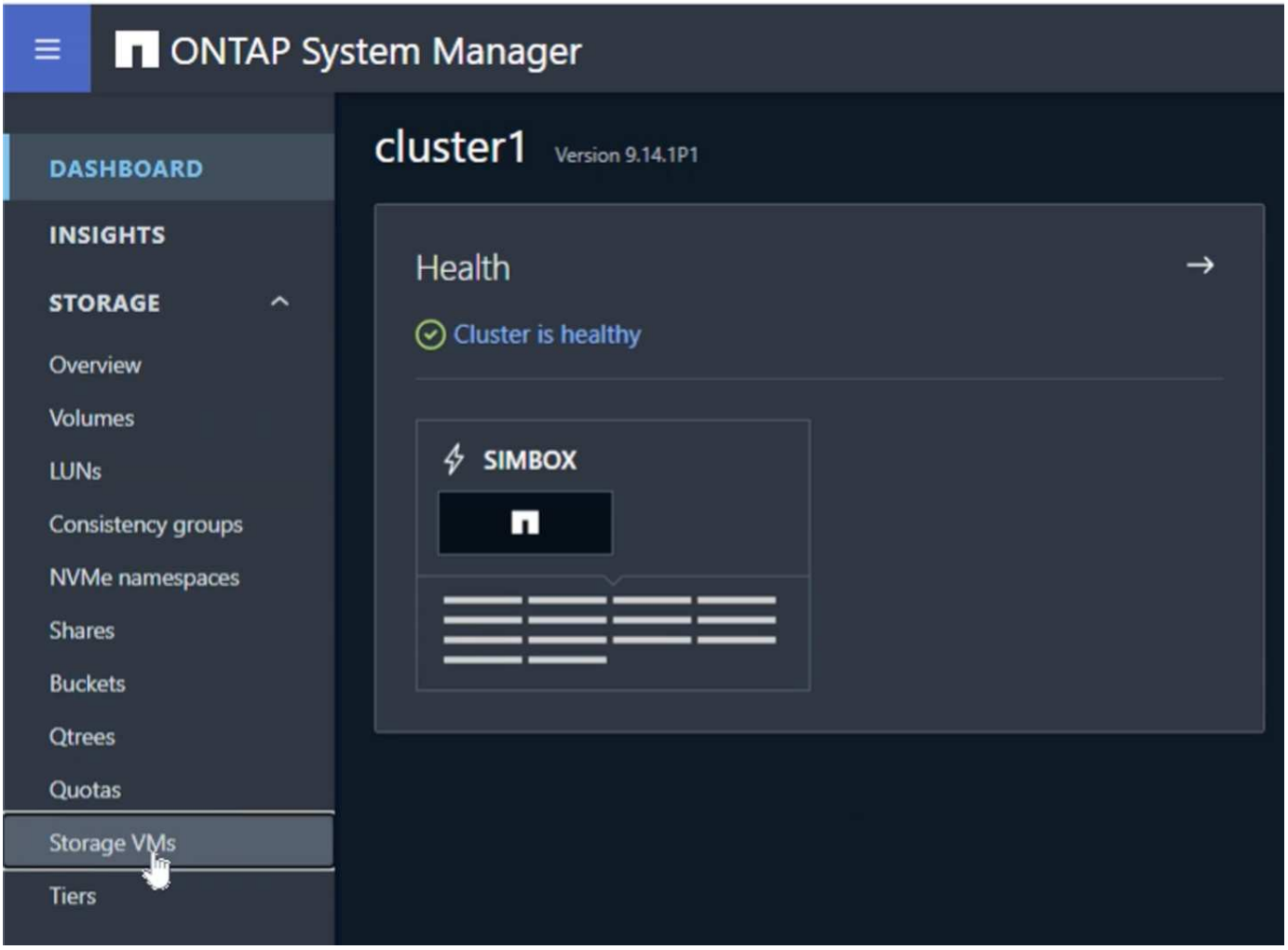
オブジェクトベースストレージをONTAP S3からStorageGRIDにシームレスに移行し、エンタープライズクラスのS3を実現

ONTAPの準備

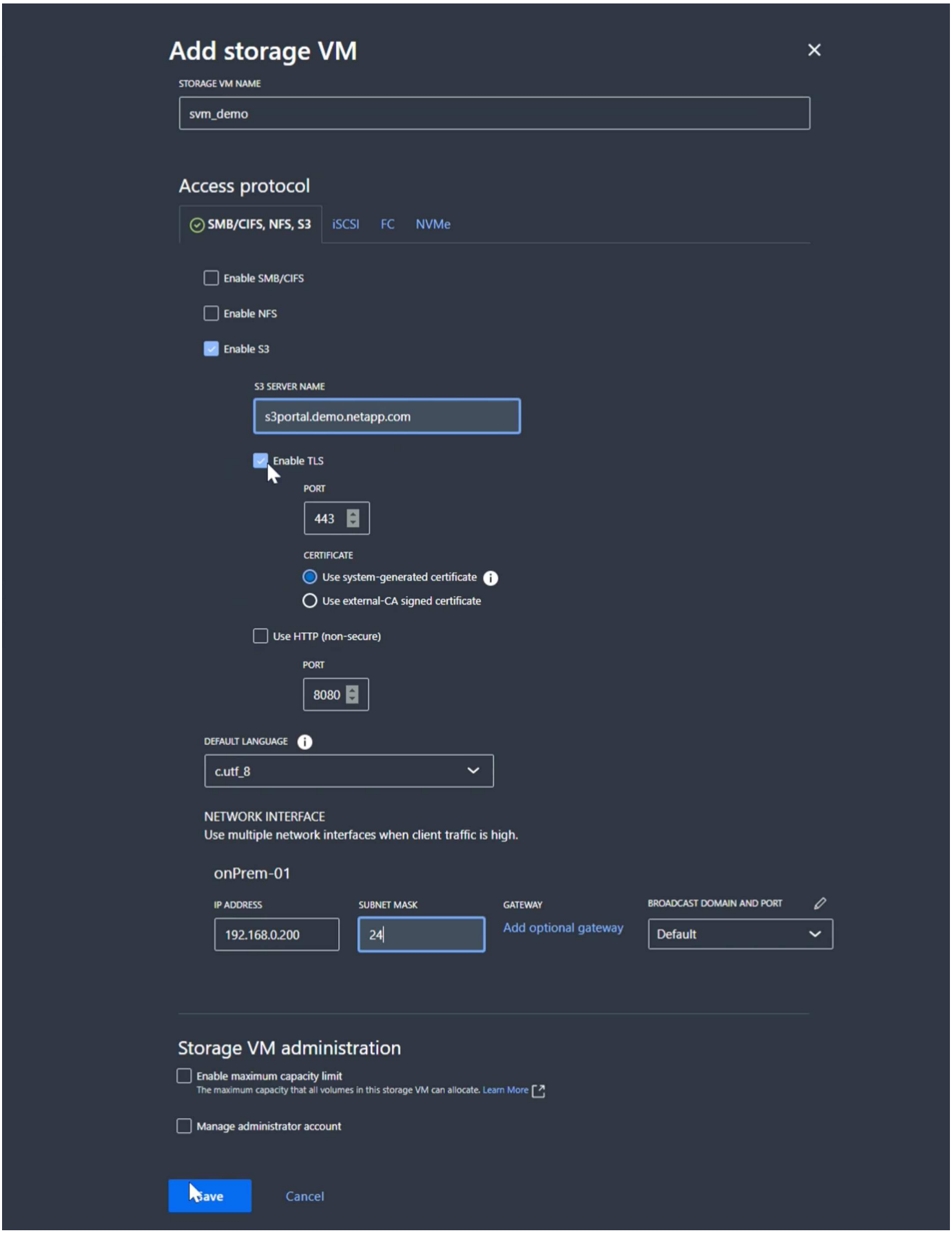
デモ用に、SVMオブジェクトストアサーバ、ユーザ、グループ、グループポリシー、およびバケットを作成します。

Storage Virtual Machineの作成

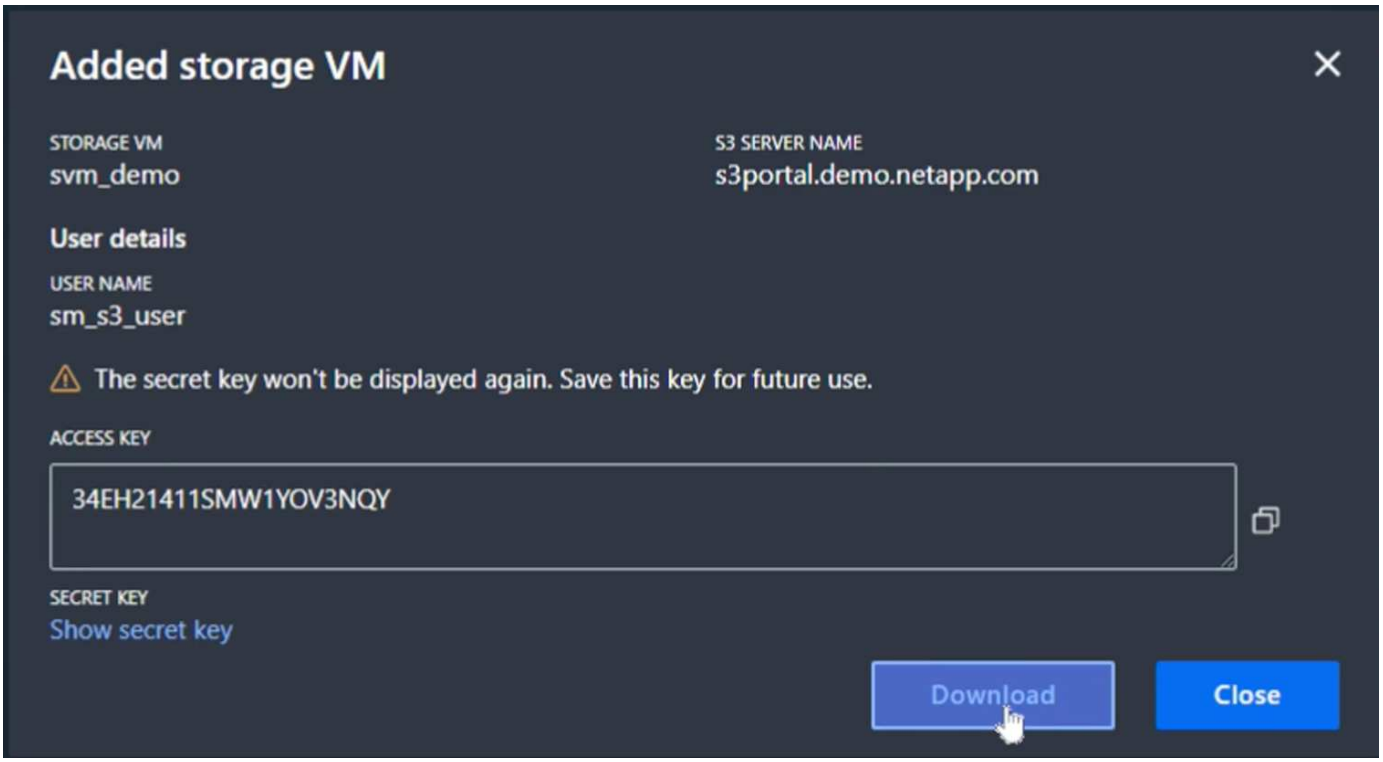
ONTAPシステムマネージャで、[Storage VM]に移動して新しいStorage VMを追加します。



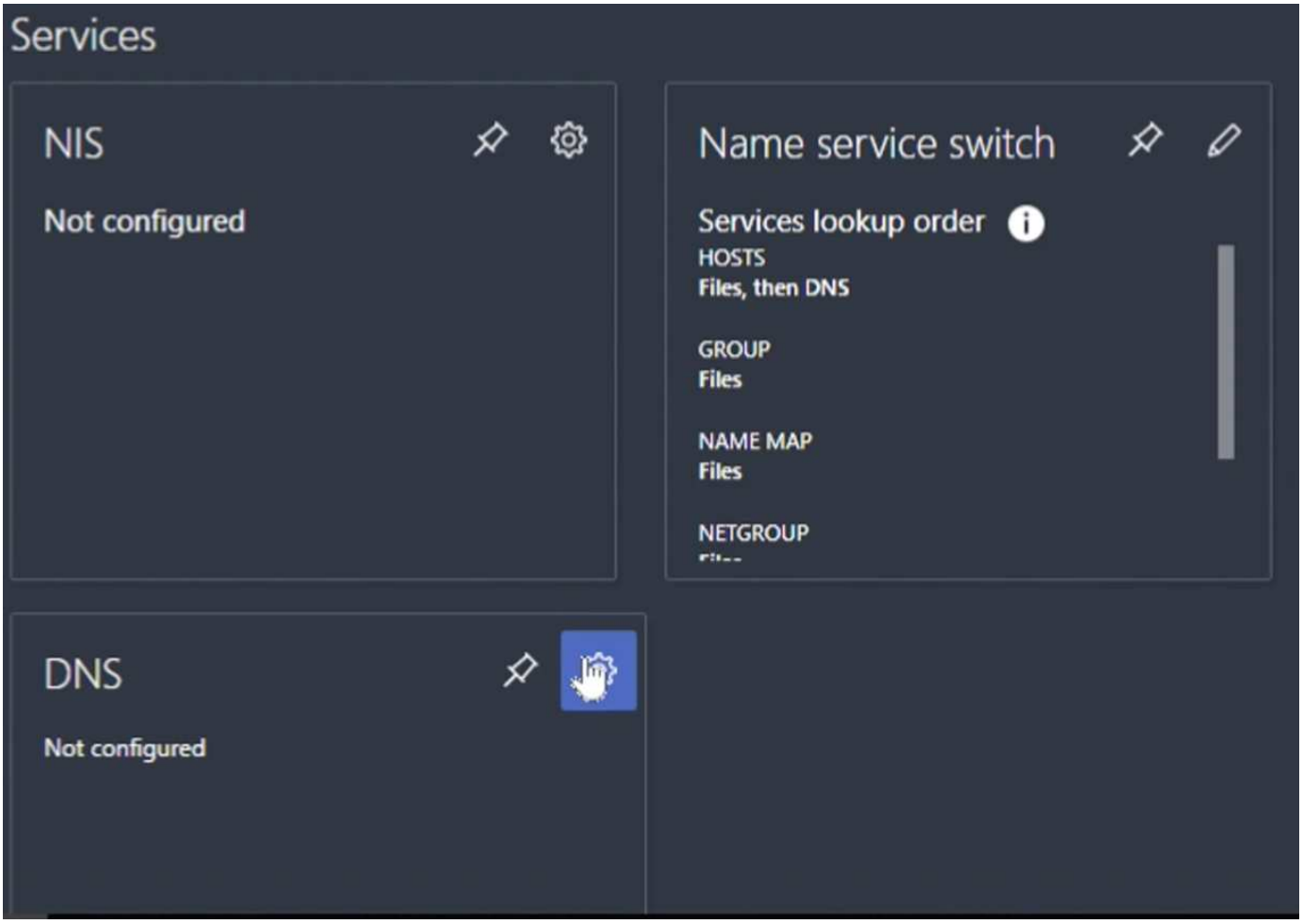
[Enable S3]と[Enable TLS]のチェックボックスを選択し、HTTP（S）ポートを設定します。デフォルトのまたは必須の環境を使用していない場合は、IP、サブネットマスク、およびゲートウェイとブロードキャストドメインを定義します。



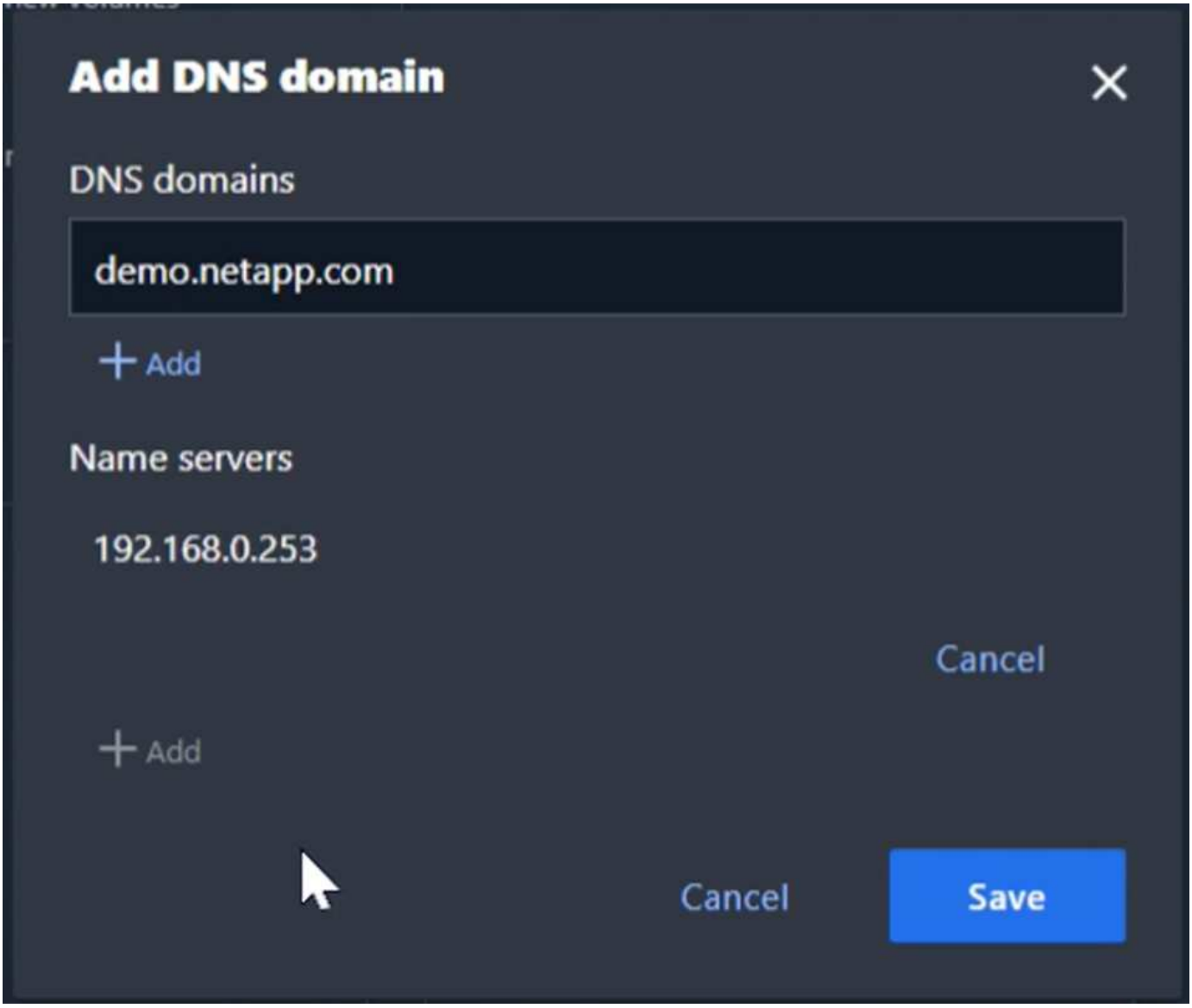
SVMの作成時にユーザが作成されます。このユーザのS3キーをダウンロードしてウィンドウを閉じます。



SVMが作成されたら、SVMを編集してDNS設定を追加します。

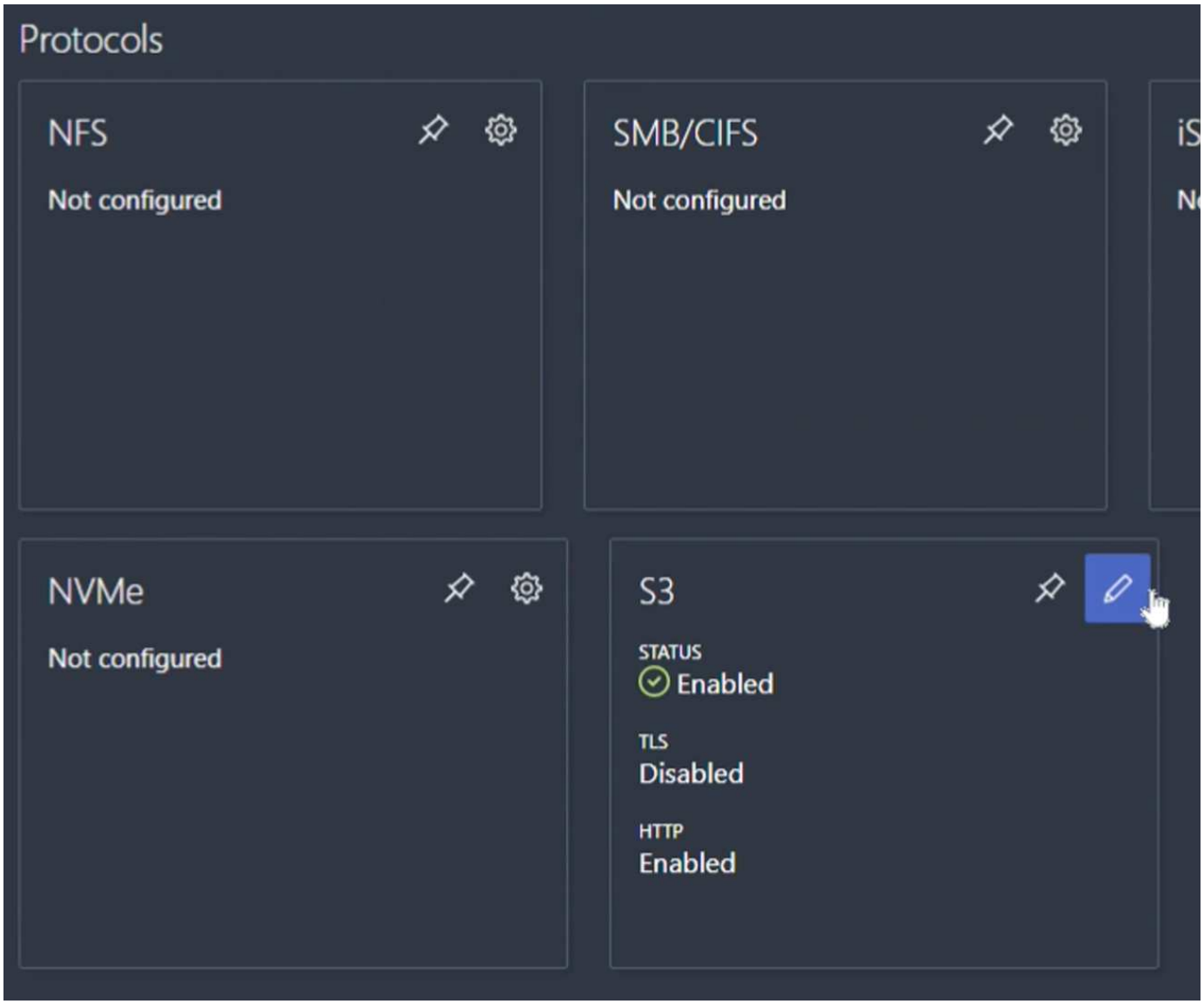


DNS名とIPを定義します。

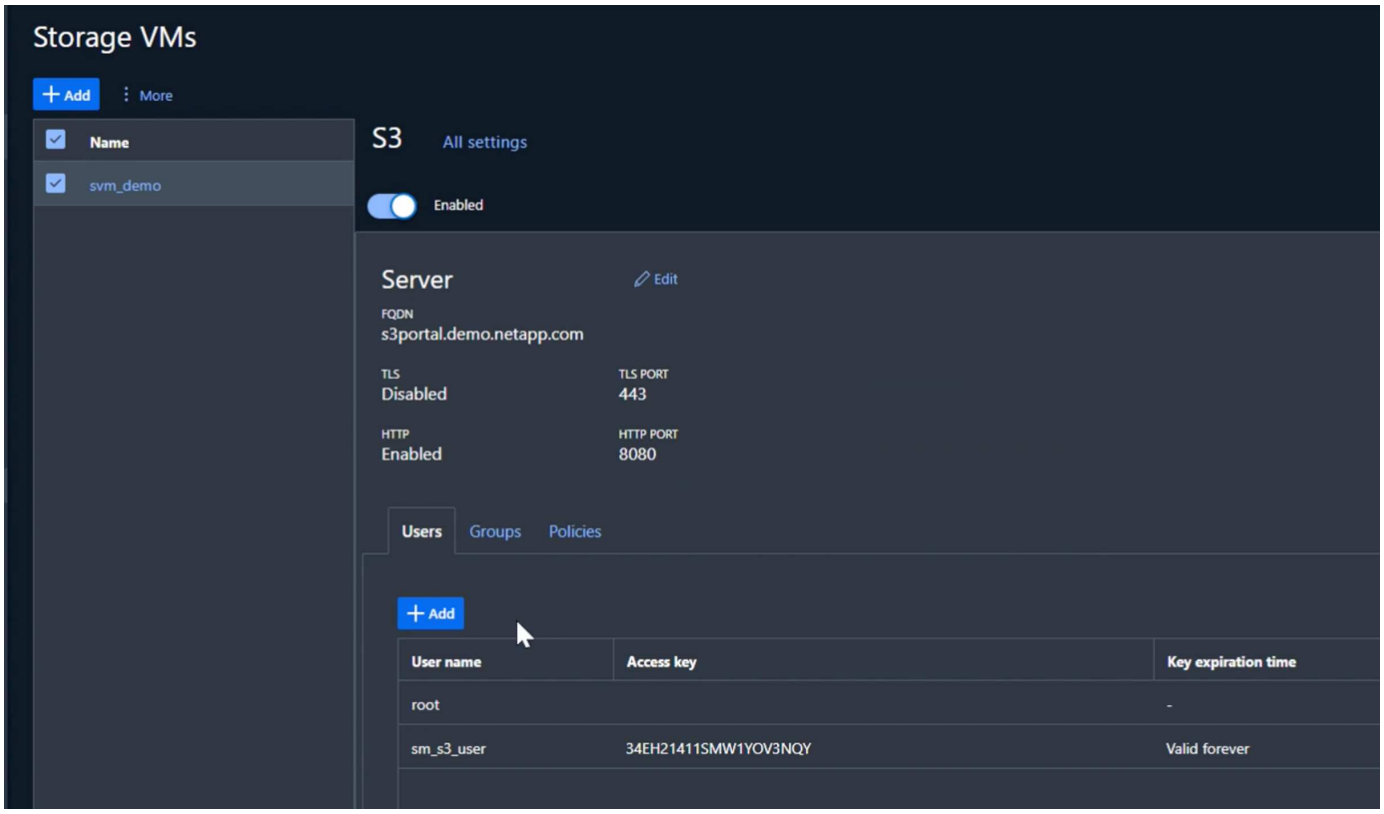


SVM S3ユーザの作成

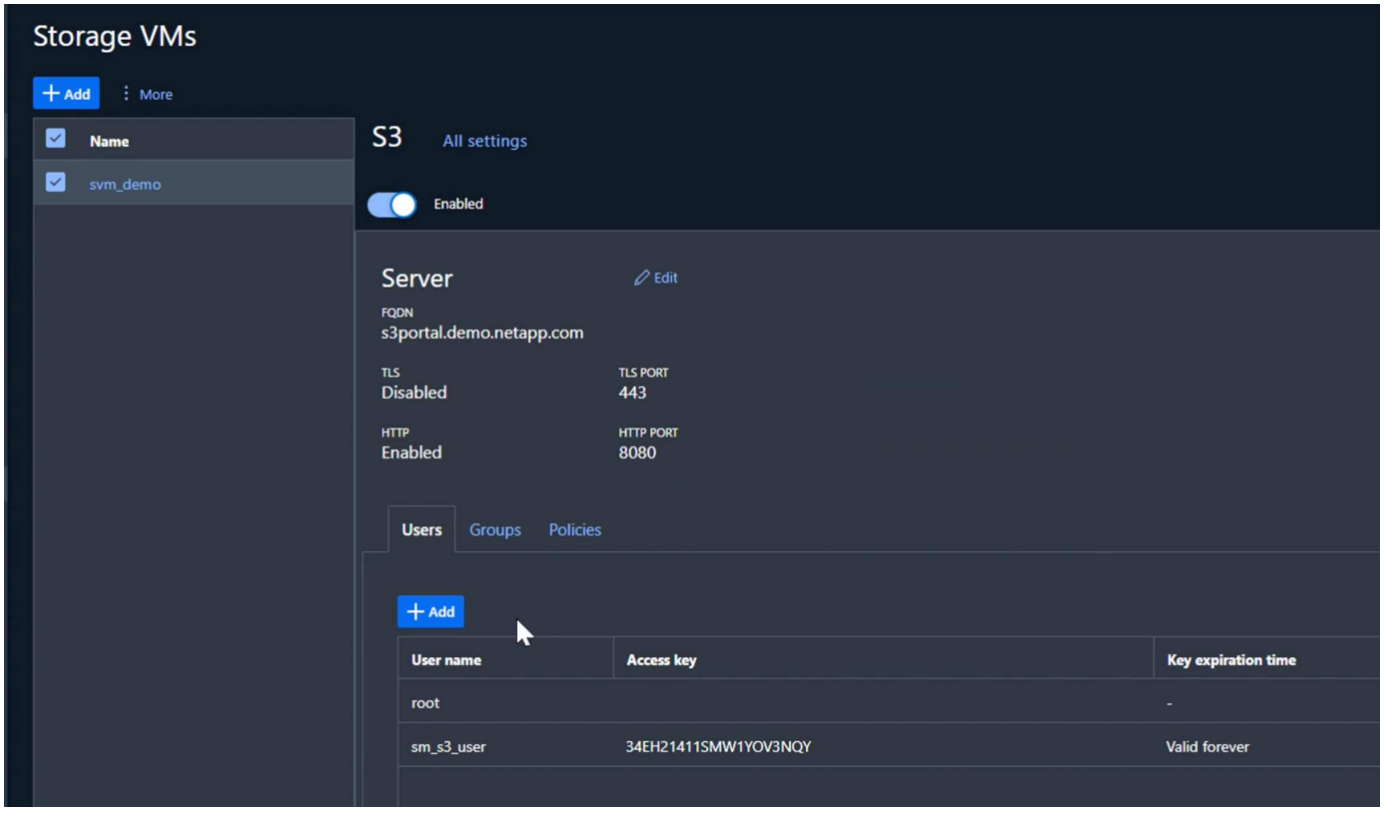
次に、S3ユーザとグループを設定します。S3設定を編集します。



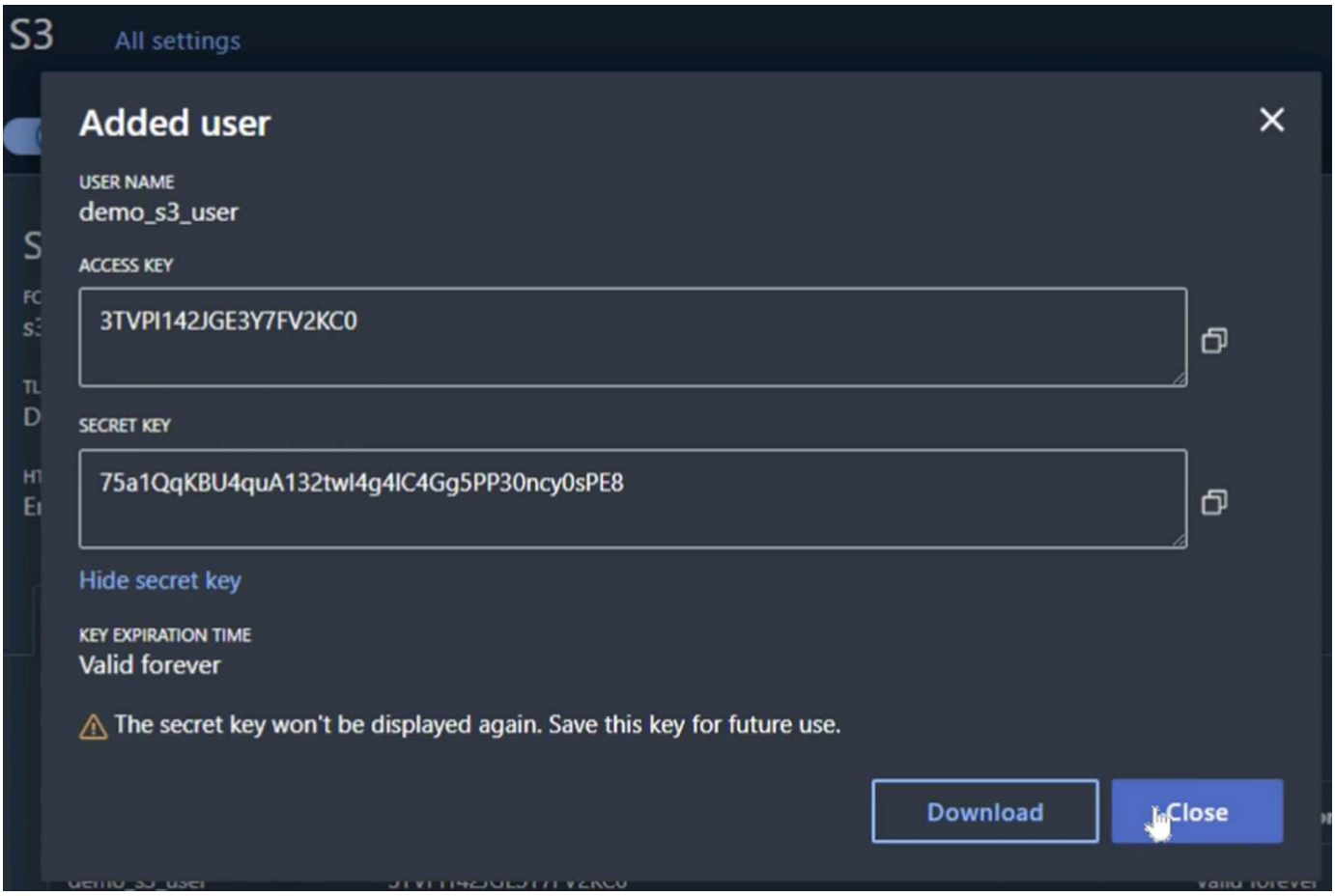
新しいユーザを追加します。



ユーザ名とキーの有効期限を入力します。

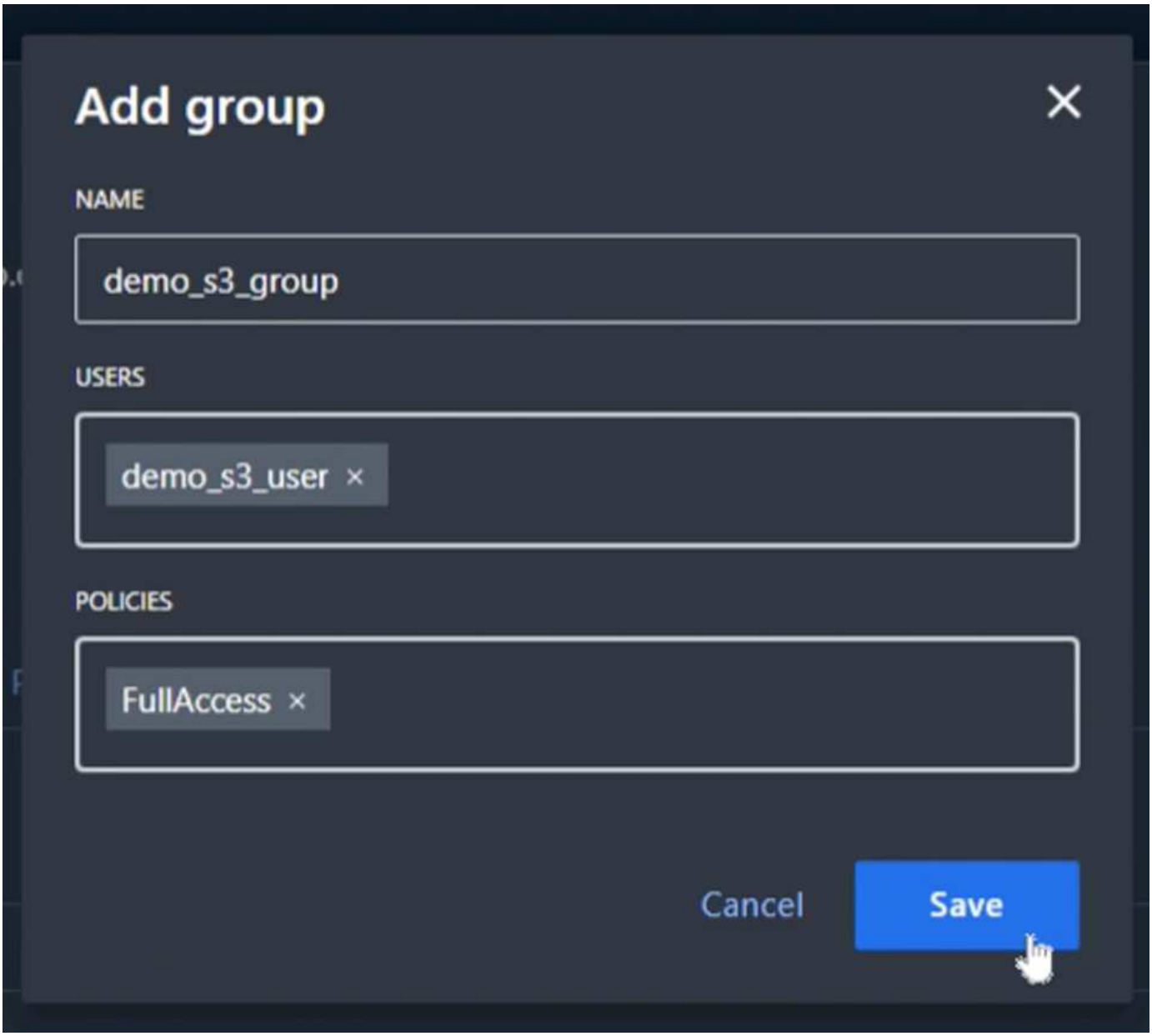


新しいユーザのS3キーをダウンロードします。



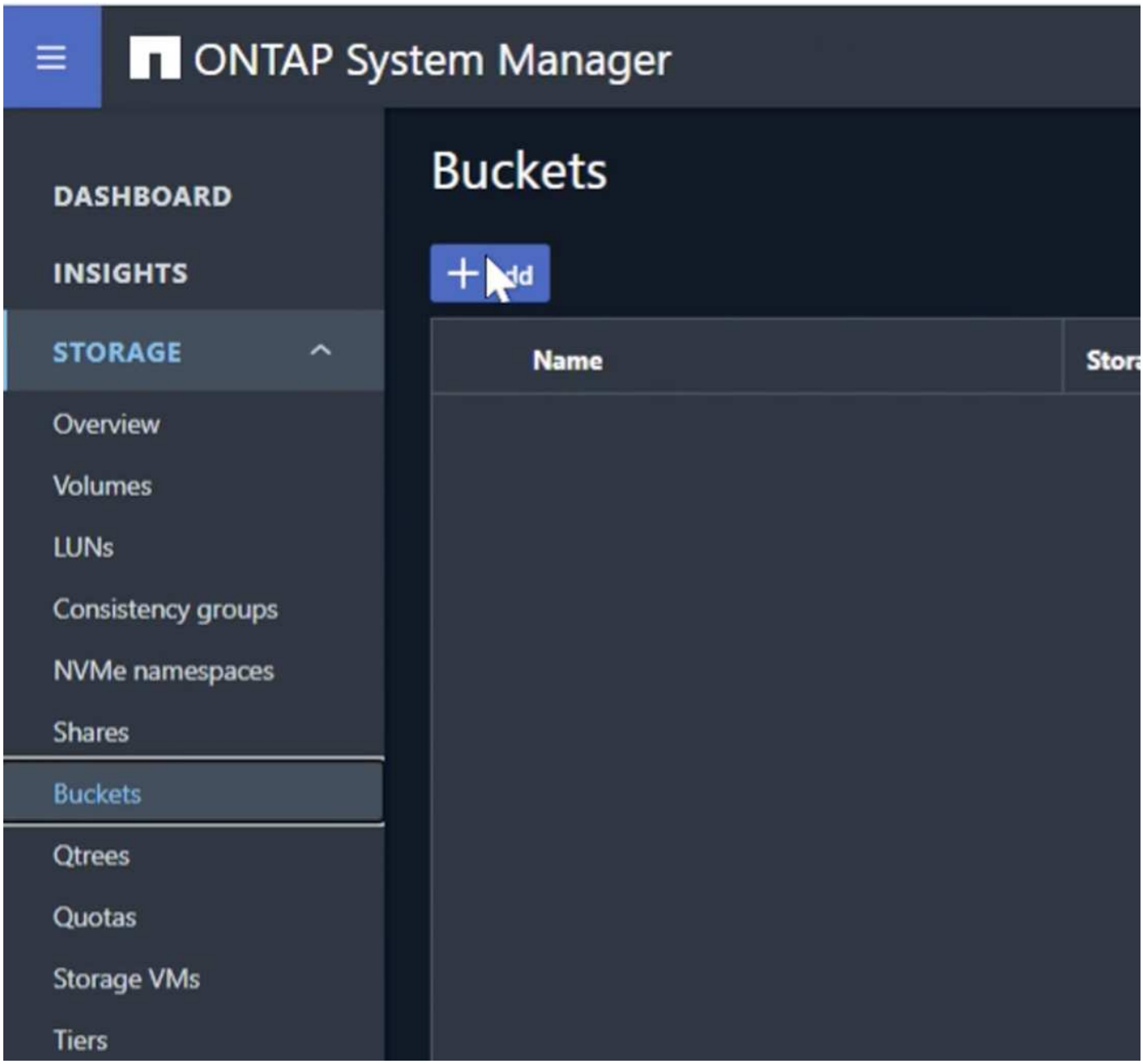
SVM S3グループの作成

SVM S3設定の[Groups]タブで、上記で作成したユーザとFullAccess権限を持つ新しいグループを追加します。

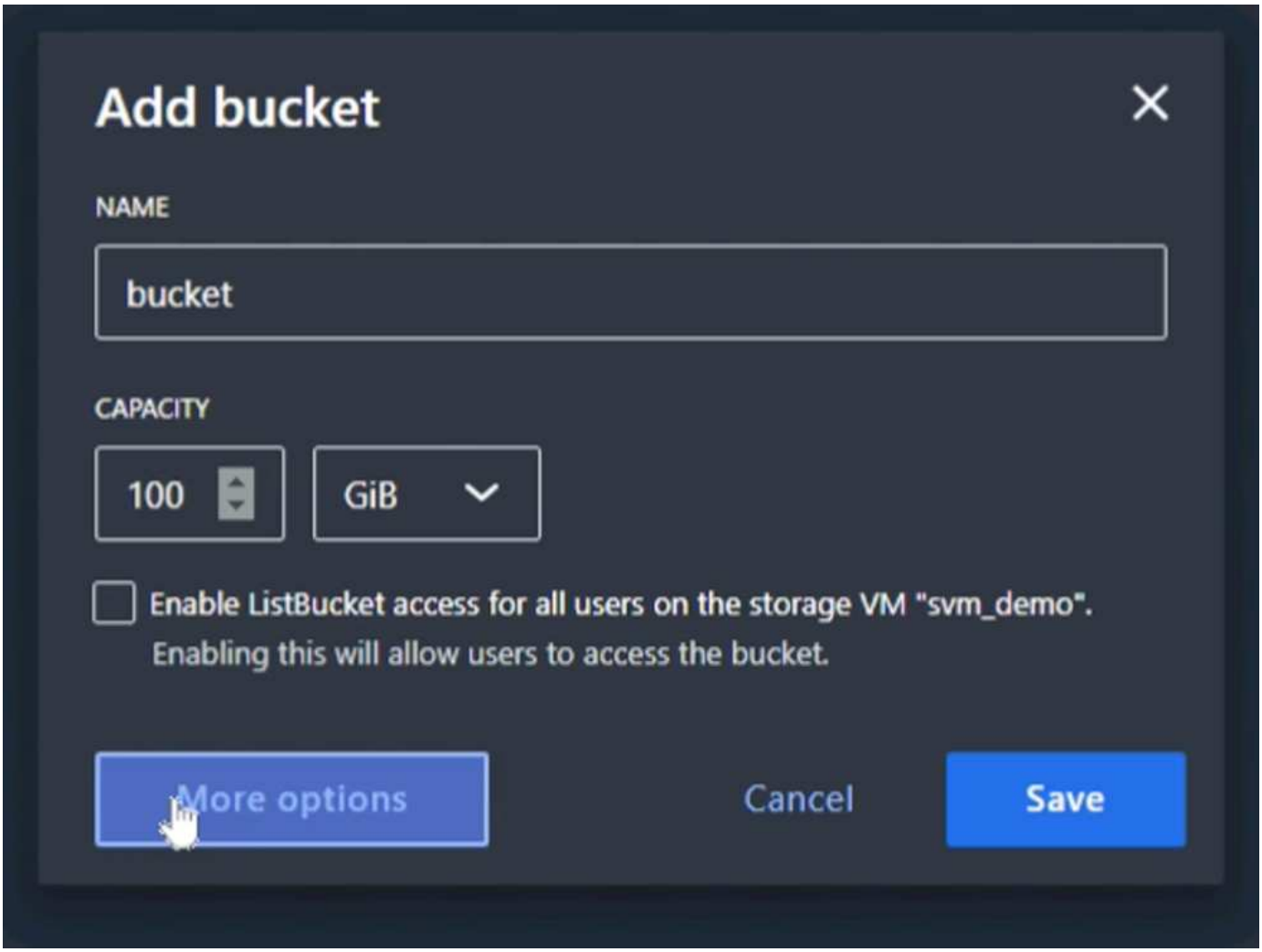


SVM S3バケットの作成

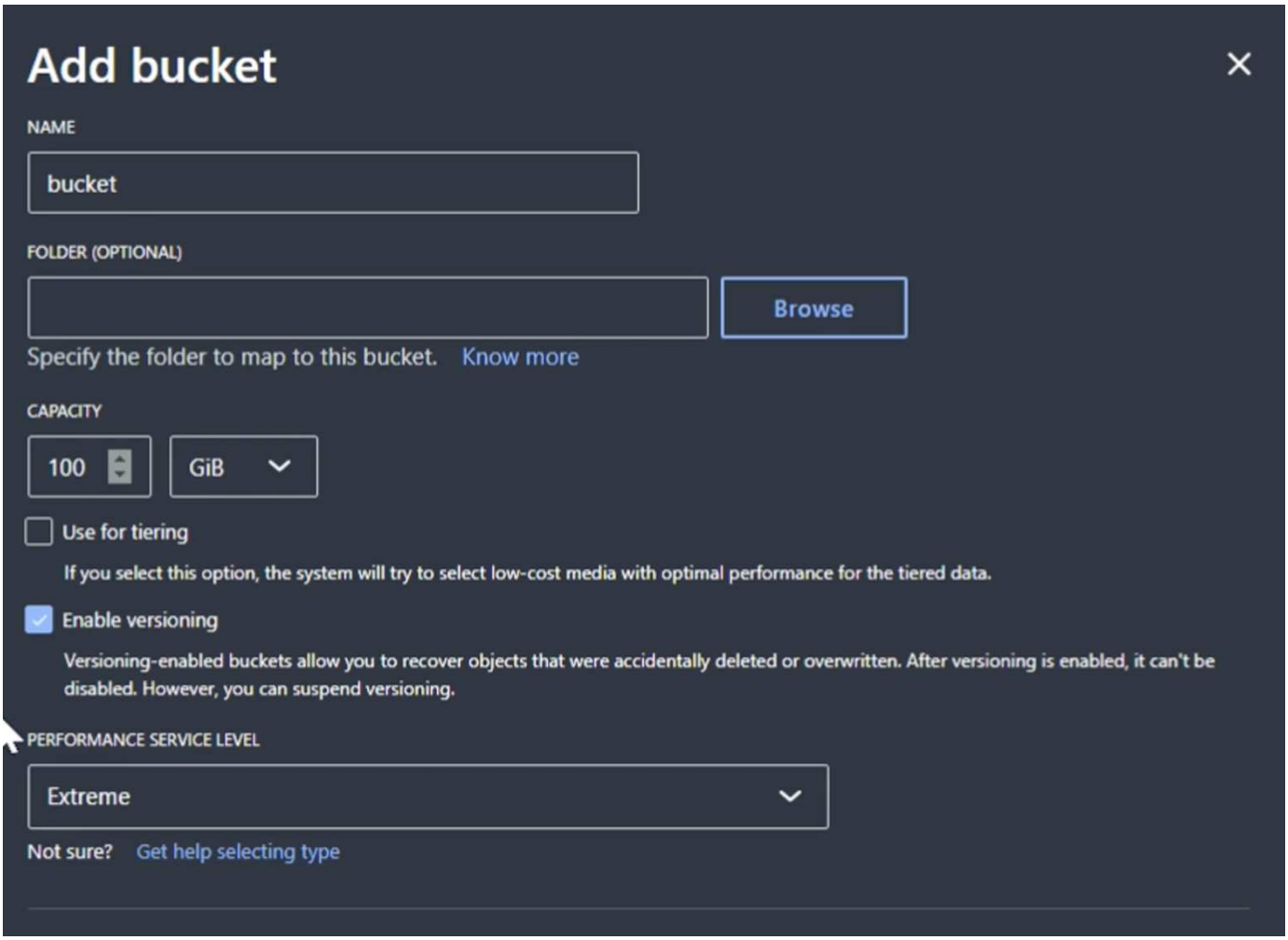
[Buckets]セクションに移動し、[+ Add]ボタンをクリックします。



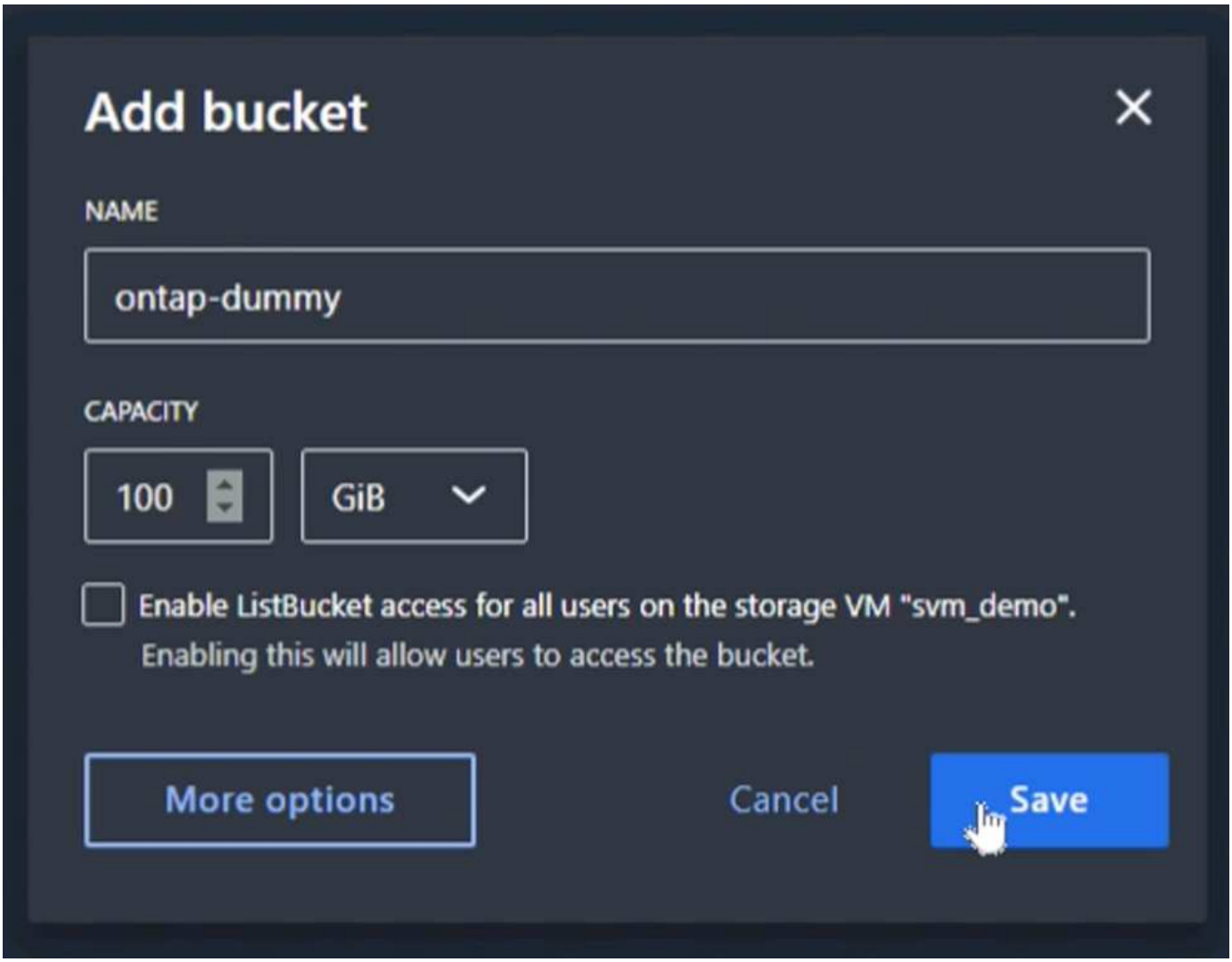
名前と容量を入力し、[Enable ListBucket access…]チェックボックスをオフにして、[More options]ボタンをクリックします。



[その他のオプション]セクションで、バージョン管理を有効にするチェックボックスを選択して[保存]ボタンをクリックします。



同じ手順を繰り返し、バージョン管理を有効にせずに2つ目のバケットを作成します。バケット名と同じ容量を入力し、[Enable ListBucket access…]チェックボックスの選択を解除して、[Save]ボタンをクリックします。



Rafael Guedes、Aron Klein著_

オブジェクトベースストレージを**ONTAP S3**から**StorageGRID**にシームレスに移行し、エンタープライズクラスの**S3**を実現

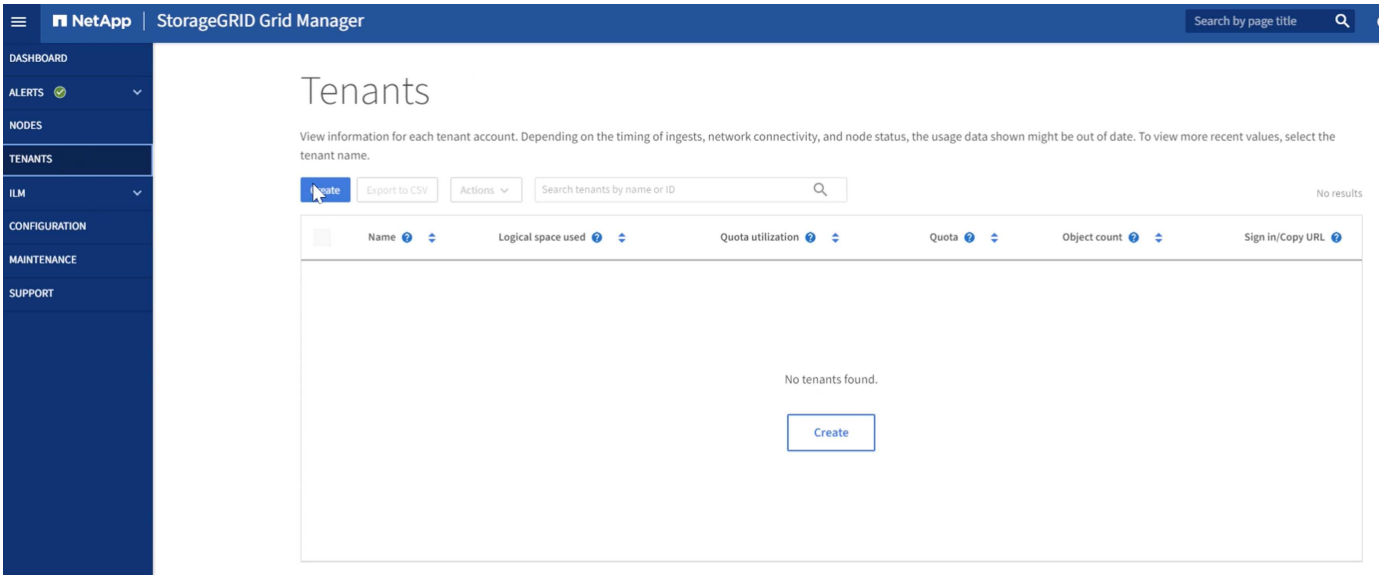
オブジェクトベースストレージをONTAP S3からStorageGRIDにシームレスに移行し、エンタープライズクラスのS3を実現

StorageGRID を準備しています

このデモの設定では、引き続きテナント、ユーザ、セキュリティグループ、グループポリシー、バケットを作成します。

テナントを作成

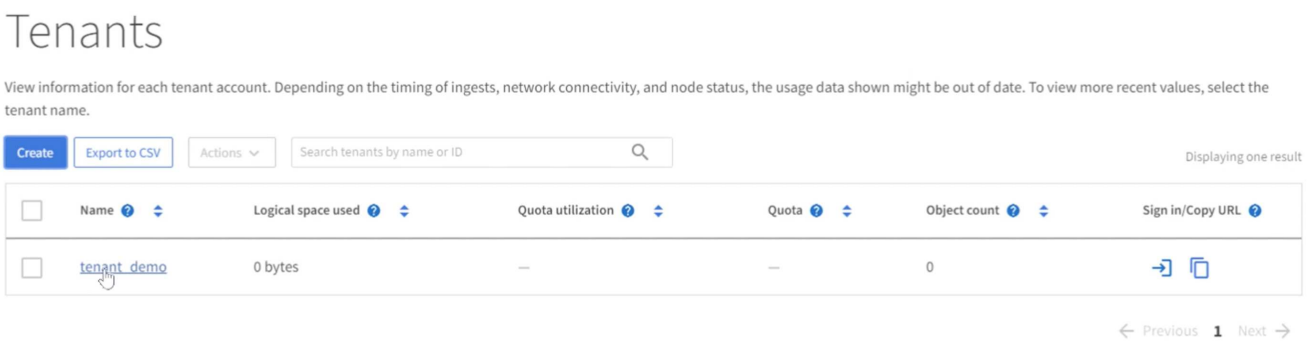
[Tenants]タブに移動し、[Create]ボタンをクリックします。



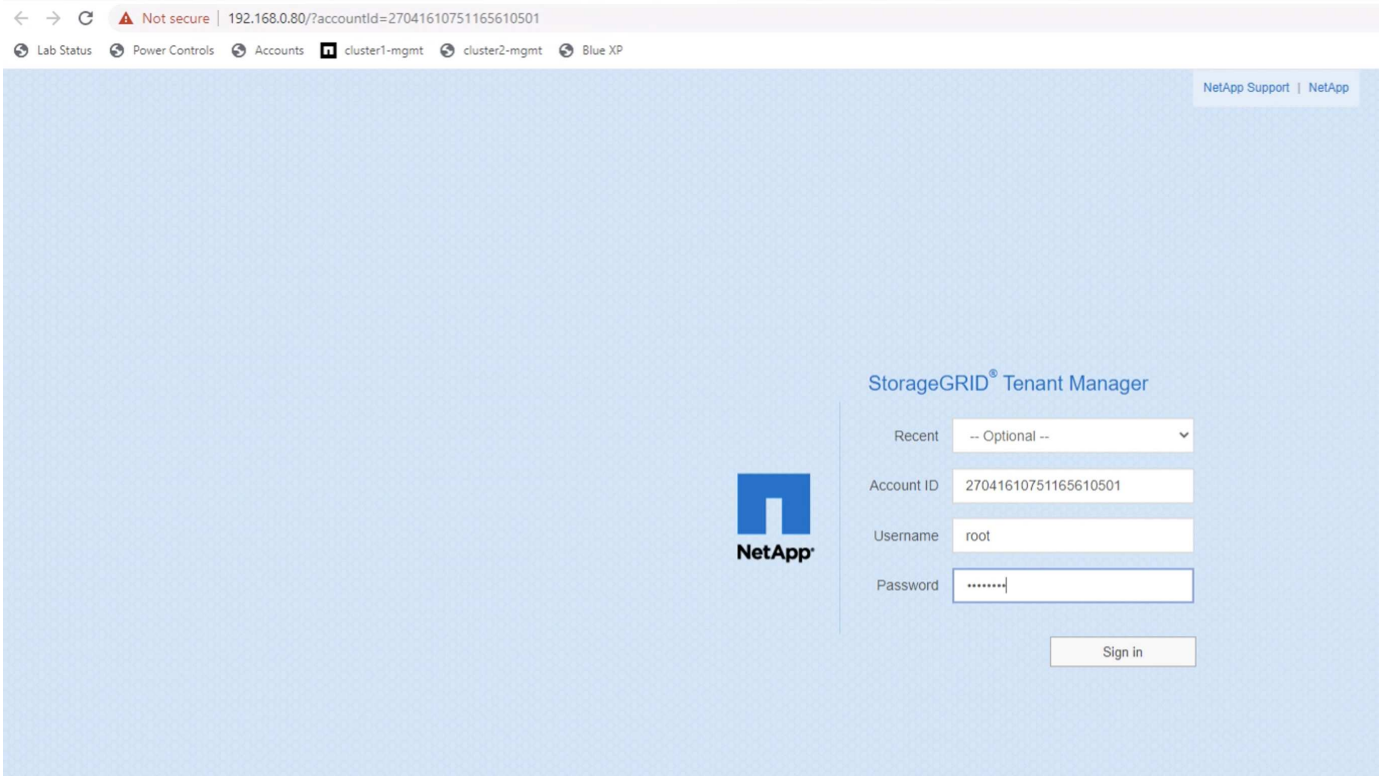
ボタン"]

テナント名を指定してテナントの詳細を入力し、クライアントタイプとして[S3]を選択します。クォータは必要ありません。プラットフォームサービスを選択する必要も、S3の選択を許可する必要もありません。必要に応じて、独自のアイデンティティソースを使用することもできます。rootパスワードを設定して[完了]ボタンをクリックします。

テナント名をクリックすると、テナントの詳細が表示されます。テナント**ID**は後で必要になりますので、コピーしてください。[サインイン]ボタンをクリックします。テナントポータルログインが表示されます。あとで使用するためにURLを保存しておきます。

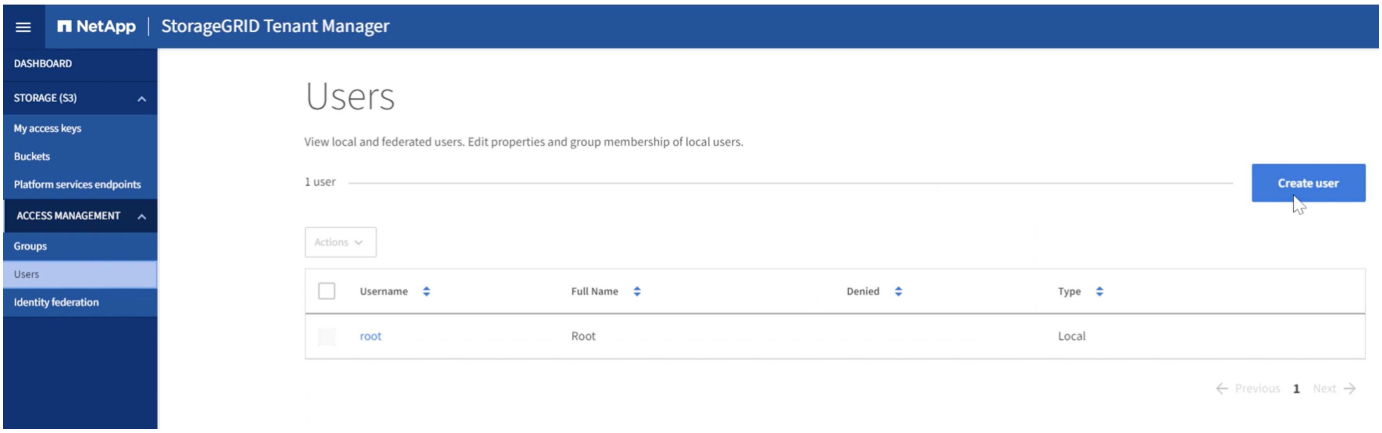


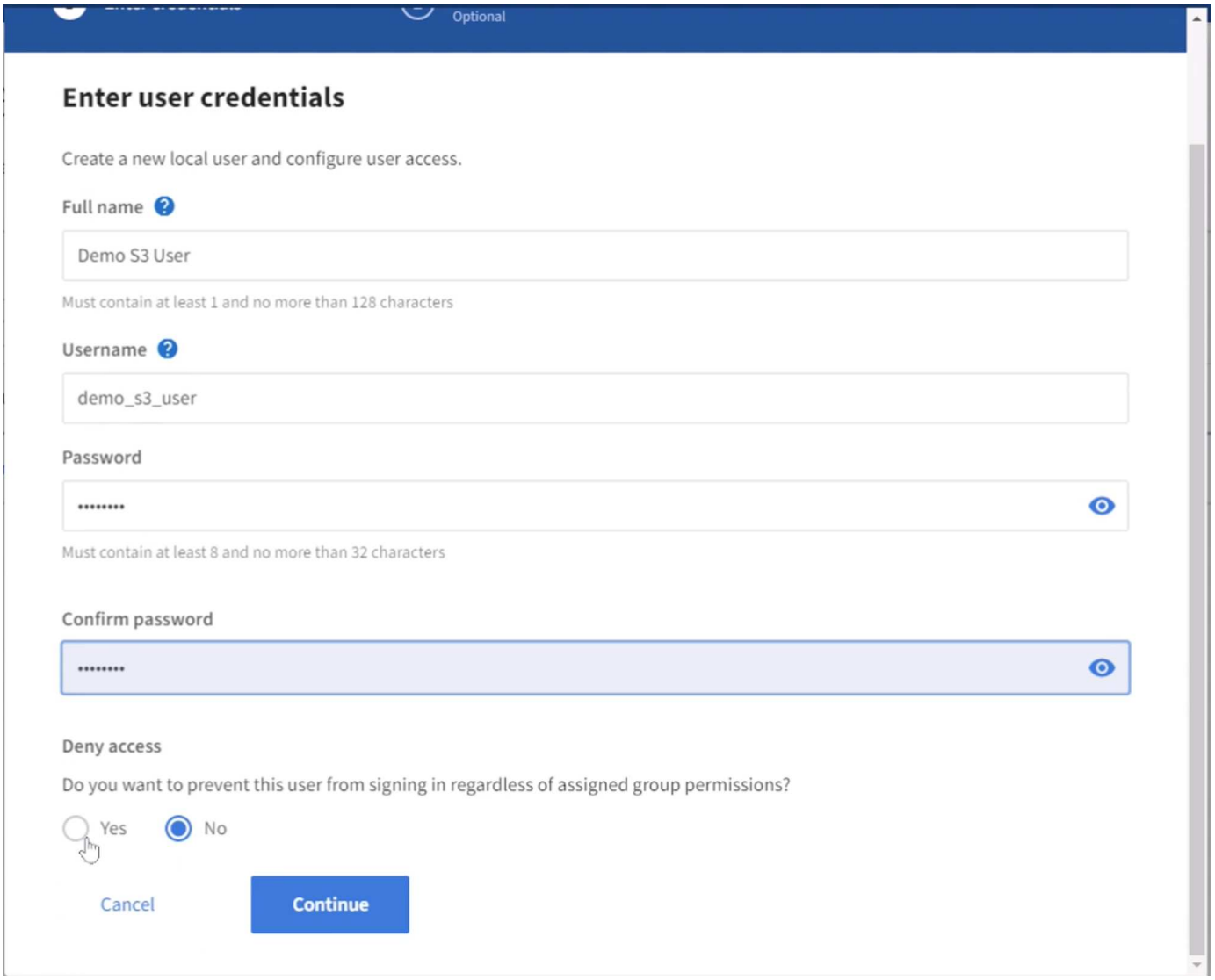
テナントポータルログインが表示されます。あとで使用できるようにURLを保存し、rootユーザクレデンシャルを入力します。



ユーザの作成

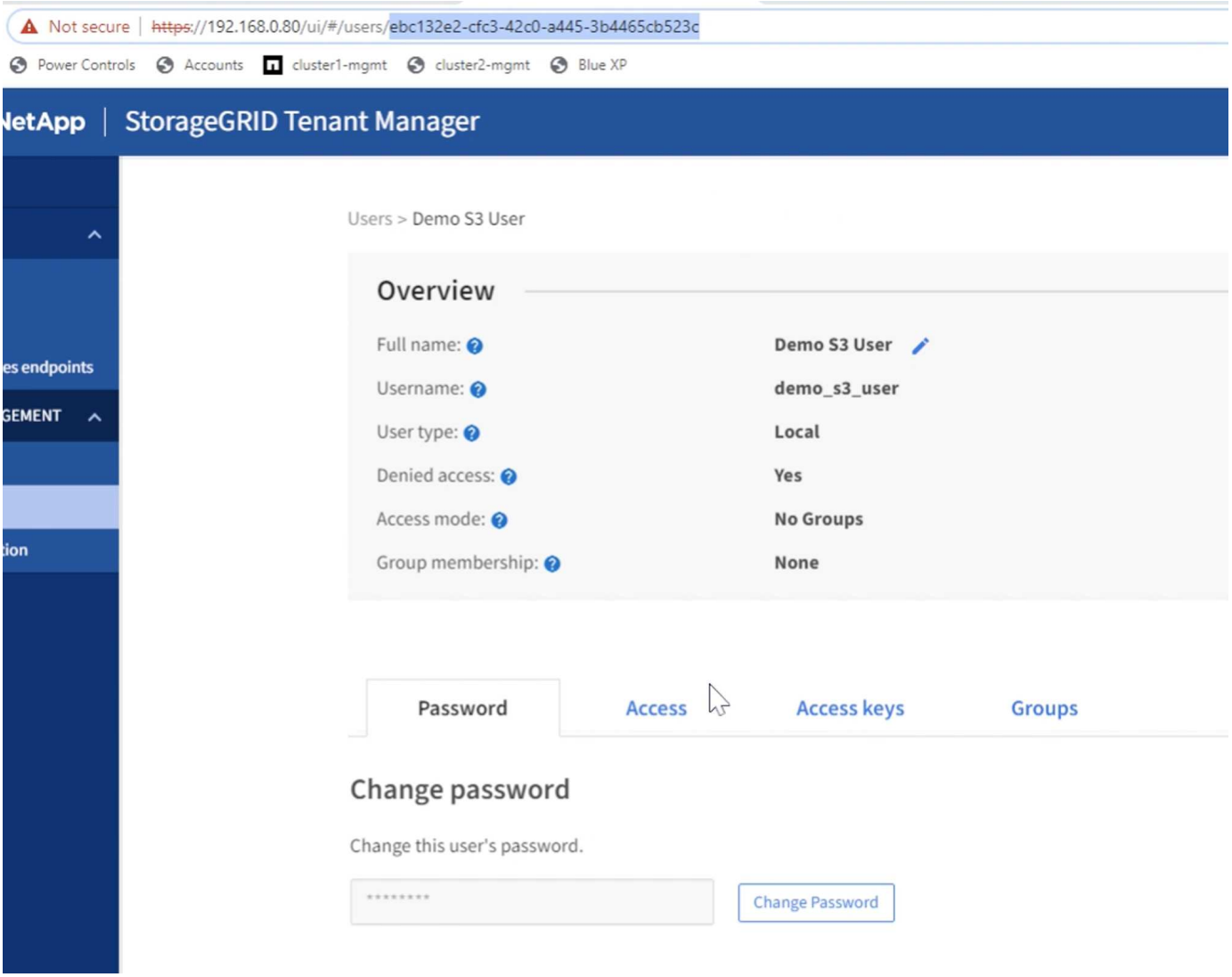
[Users]タブに移動し、新しいユーザを作成します。



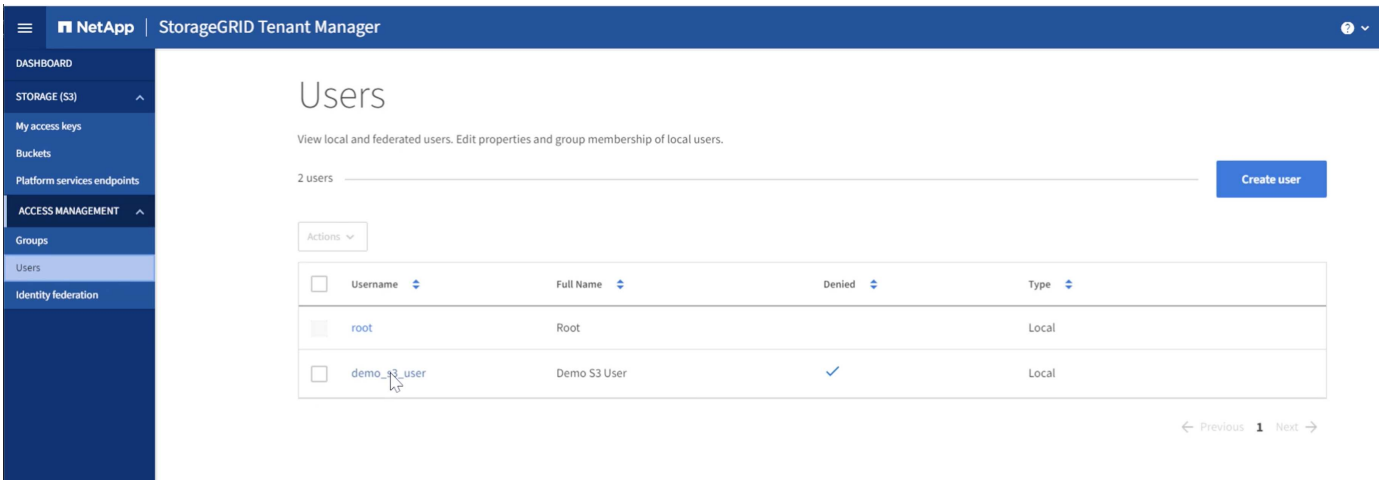


新しいユーザが作成されたら、ユーザ名をクリックしてユーザの詳細を開きます。

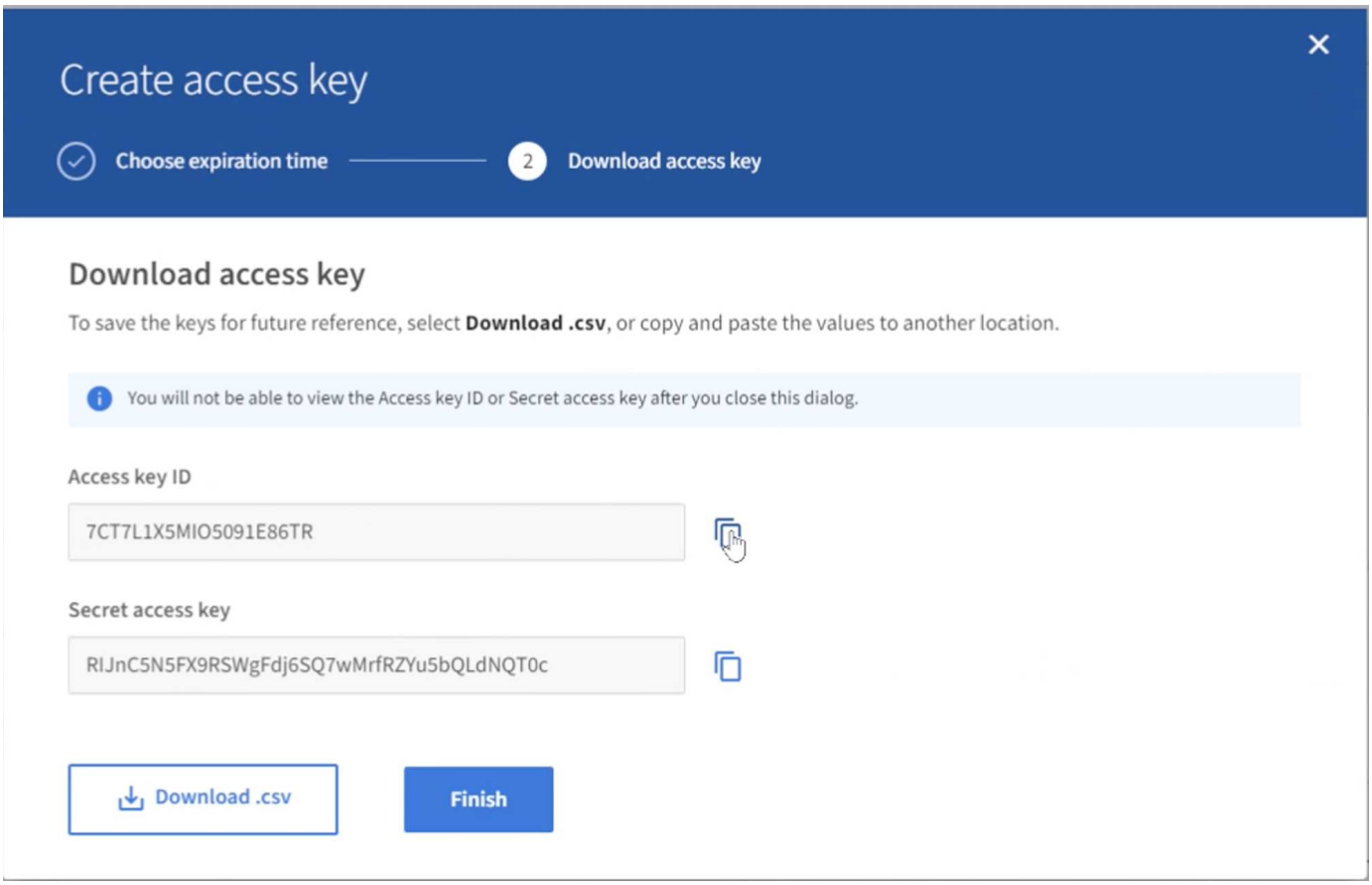
後で使用するURLからユーザIDをコピーします。



S3キーを作成するには、ユーザ名をクリックします。

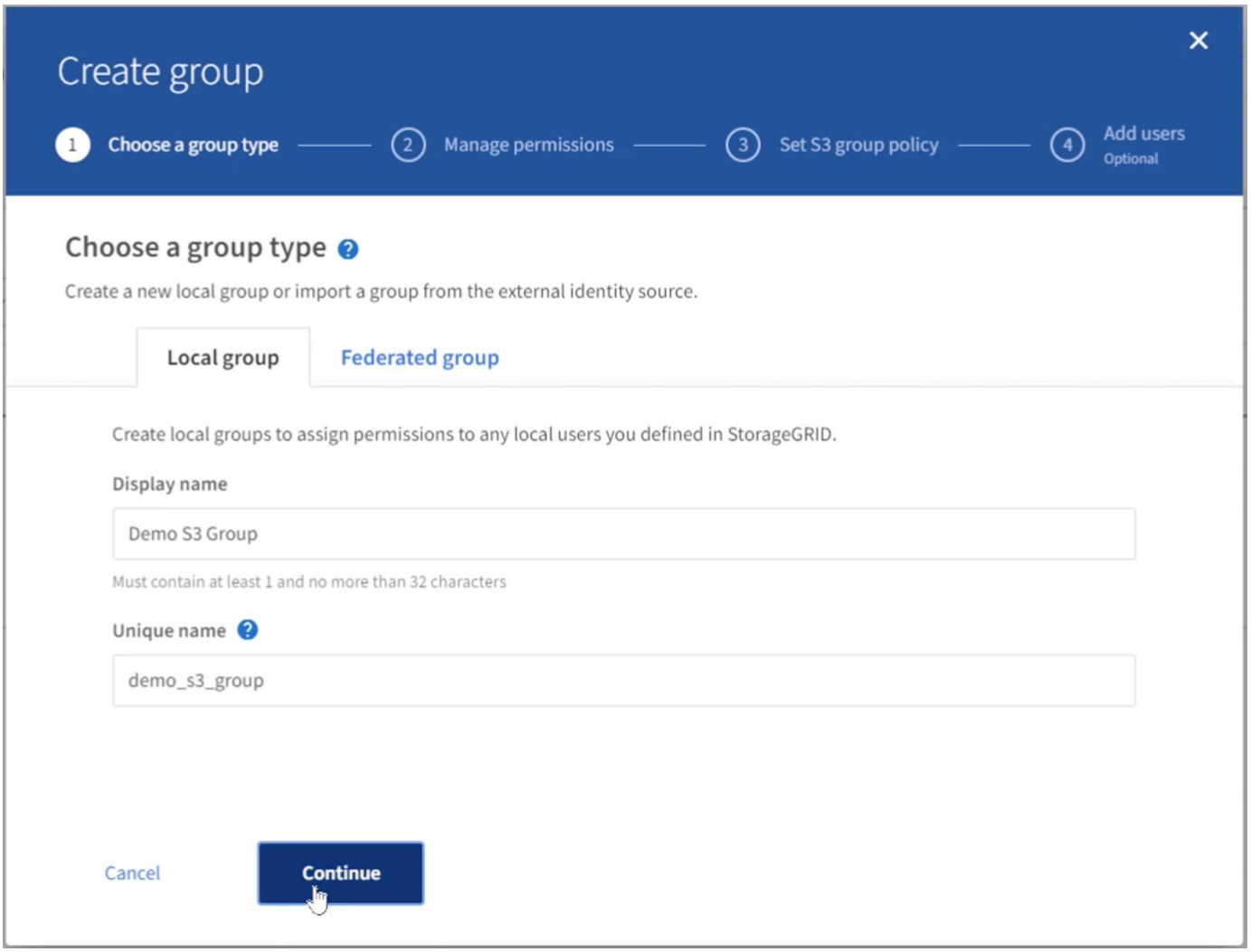


[アクセスキー]タブを選択し、[キーの作成]ボタンをクリックします。有効期限を設定する必要はありません。ウィンドウを閉じると再度取得できないため、S3キーをダウンロードしてください。

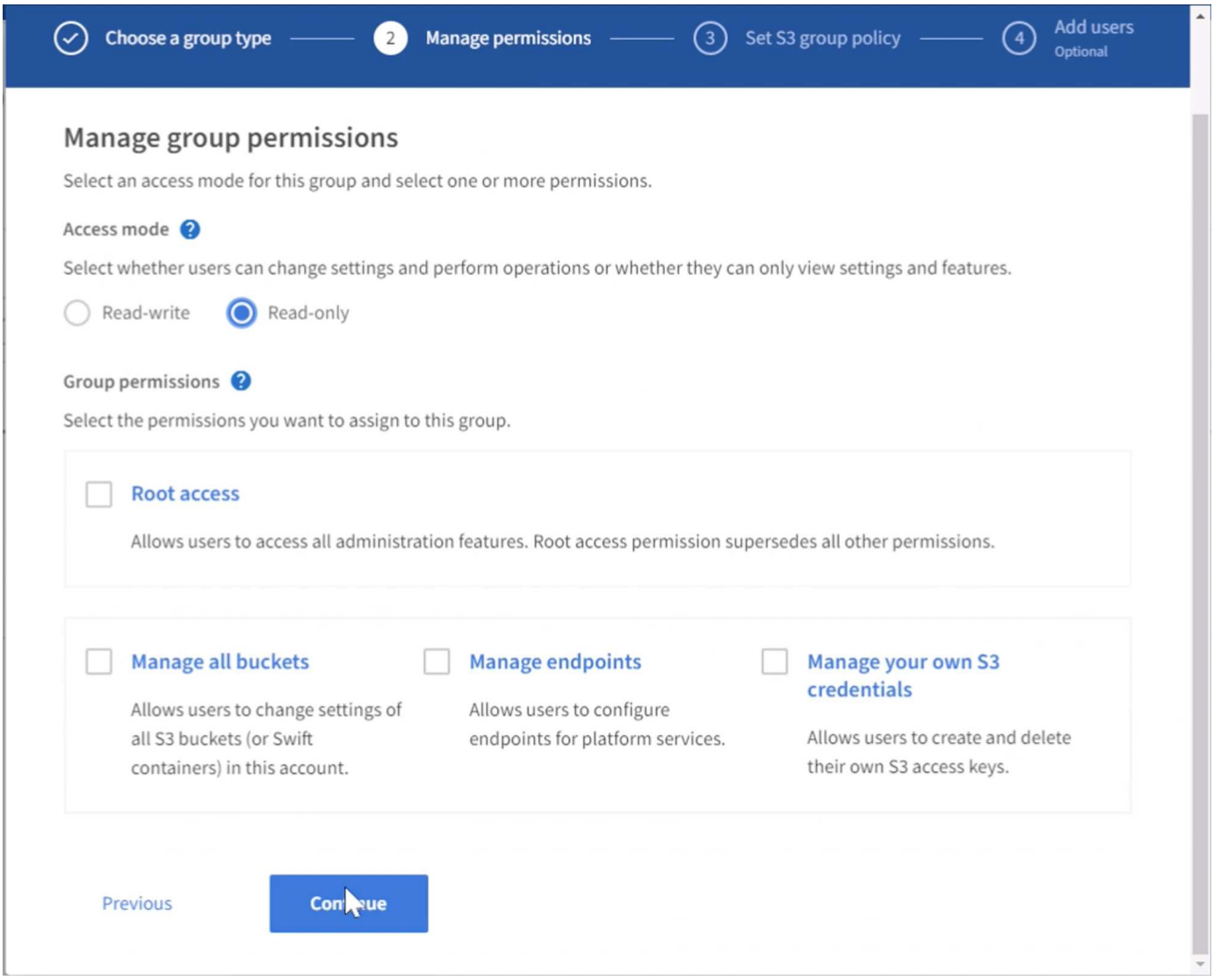


セキュリティグループを作成する

[グループ]ページに移動し、新しいグループを作成します。

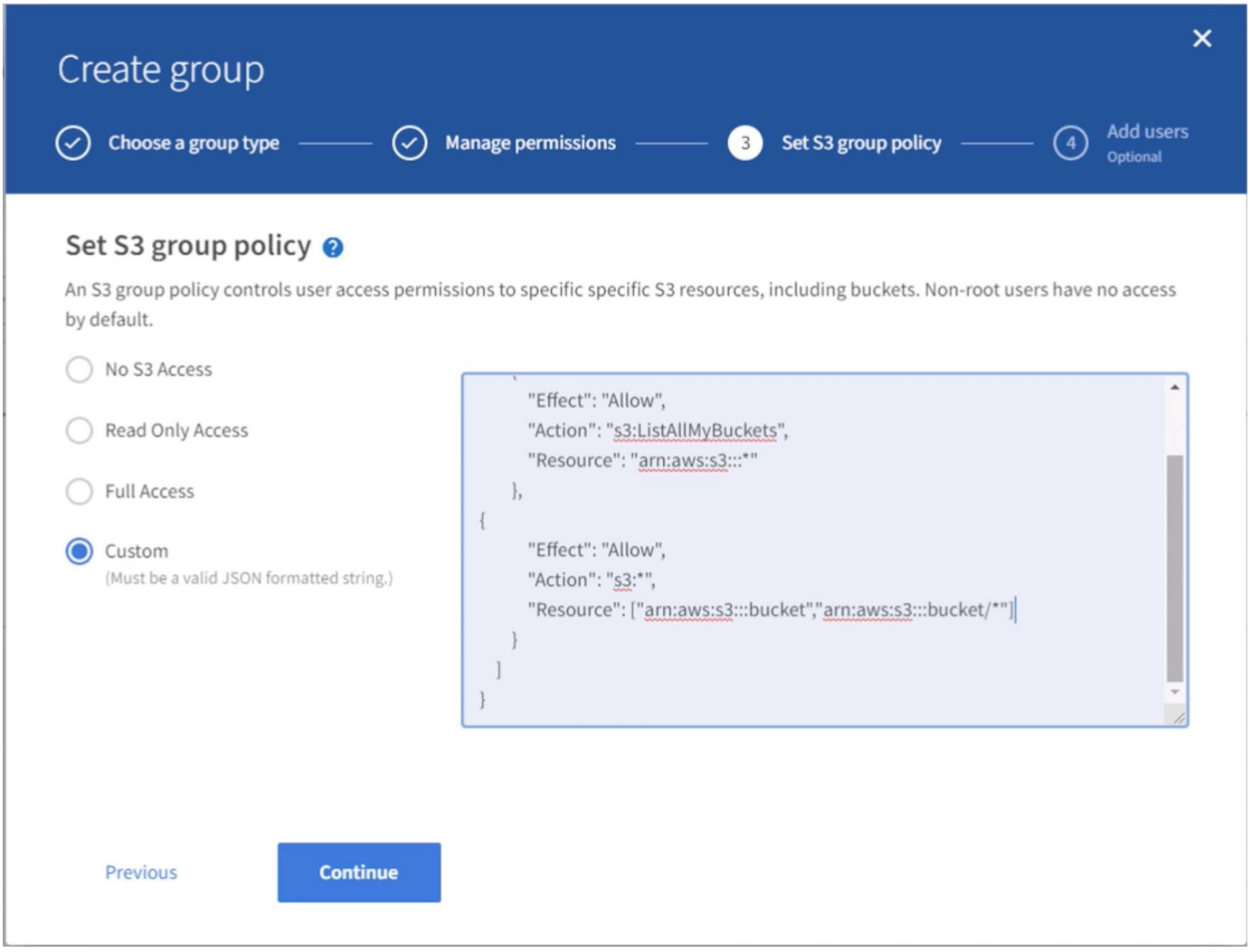


グループ権限を読み取り専用に設定します。これはテナントUIの権限であり、S3の権限ではありません。

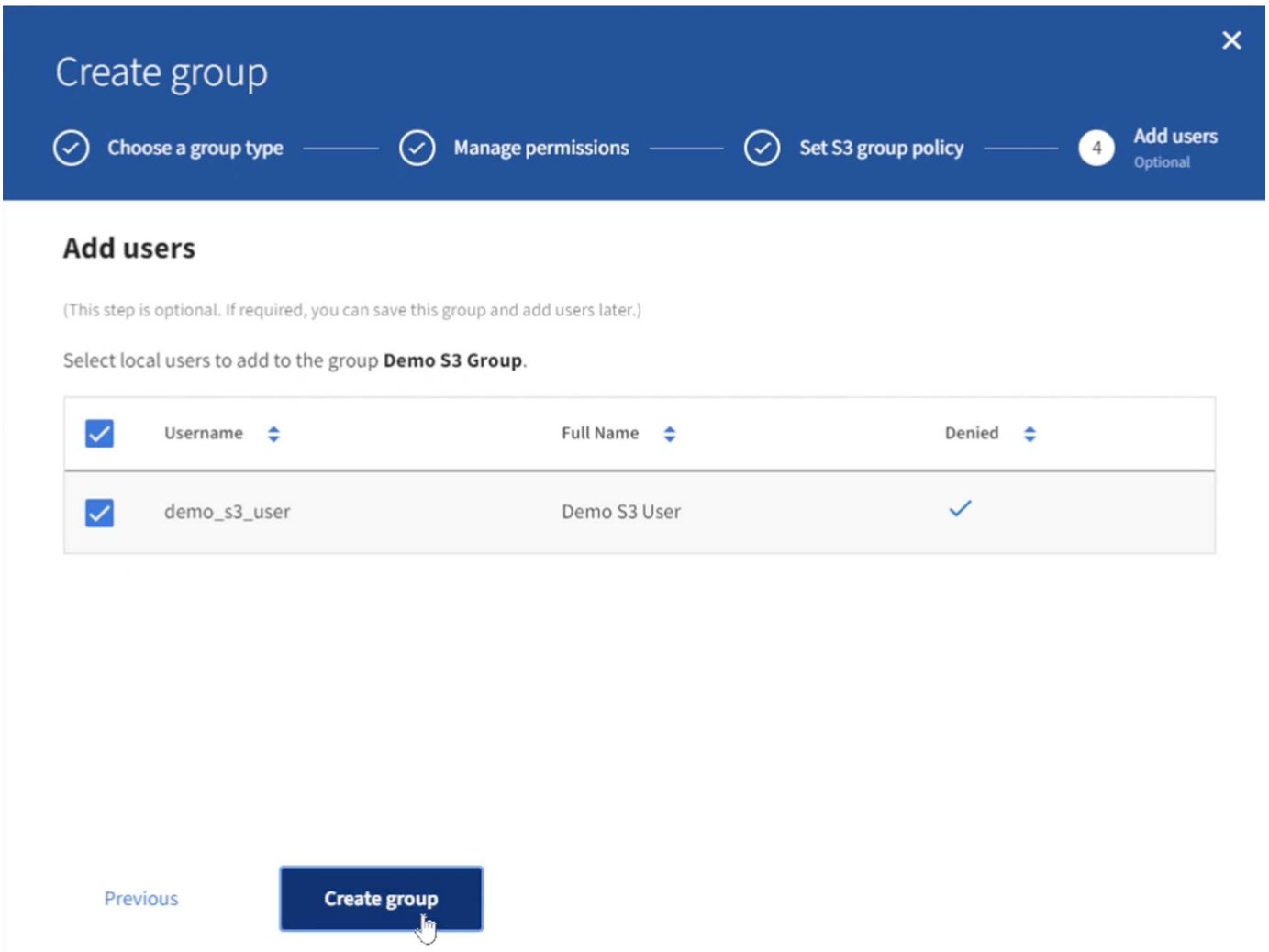


S3権限はグループポリシー（IAMポリシー）で制御されます。グループポリシーをcustomに設定し、JSONポリシーをボックスに貼り付けます。このポリシーを使用すると、このグループのユーザはテナントのバケットを一覧表示し、「bucket」という名前のバケットまたは「bucket」という名前のバケットのサブフォルダ内のS3処理を実行できます。

```
{
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
        "Action": "s3:*",
        "Resource": ["arn:aws:s3:::bucket","arn:aws:s3:::bucket/*"]
      }
    ]
}
```

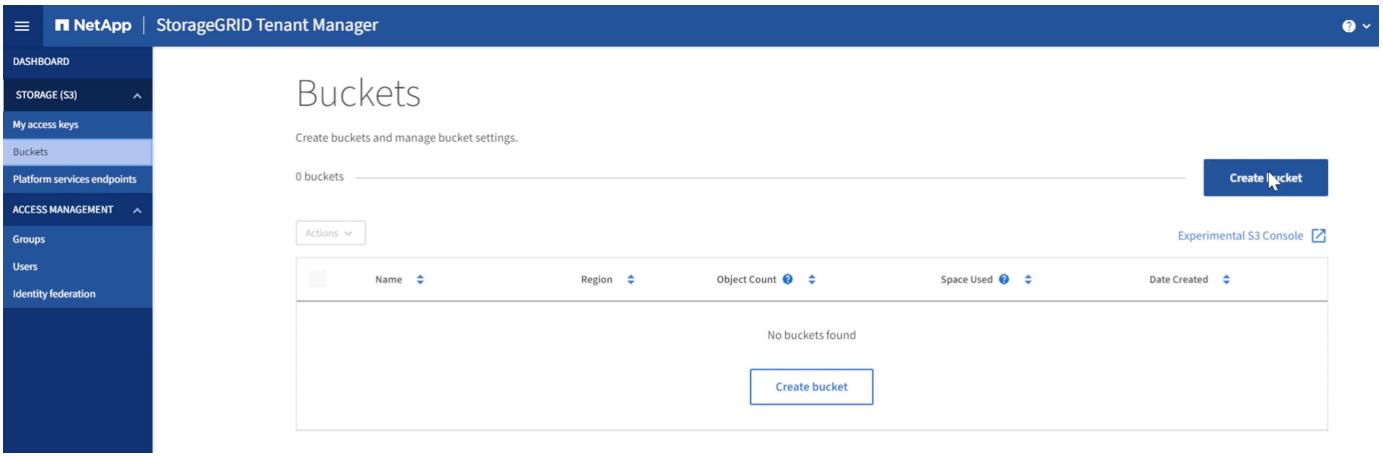


最後に、ユーザをグループに追加して終了します。



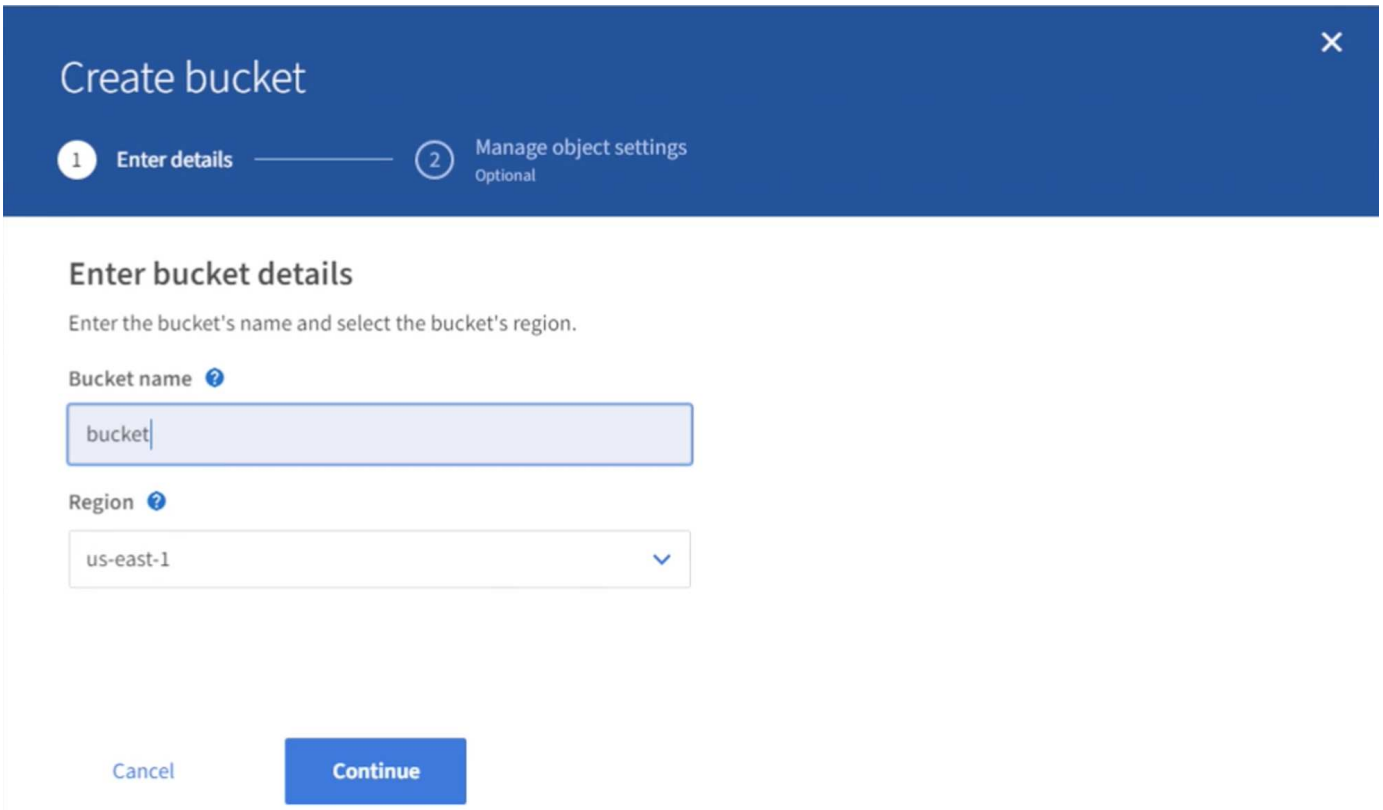
2つのバケットの作成

[Buckets]タブに移動し、[Create bucket]ボタンをクリックします。



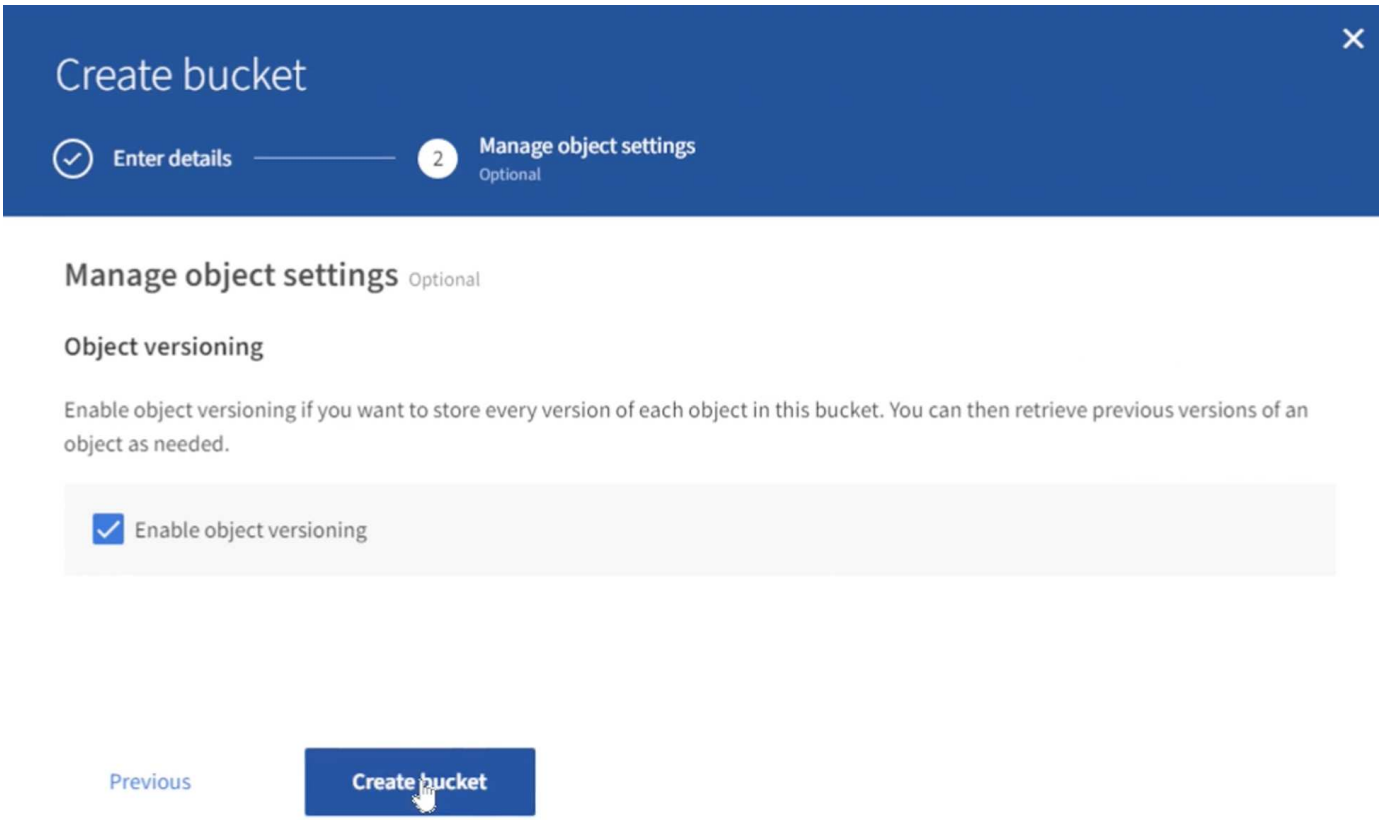
ページ"]

バケット名とリージョンを定義します。

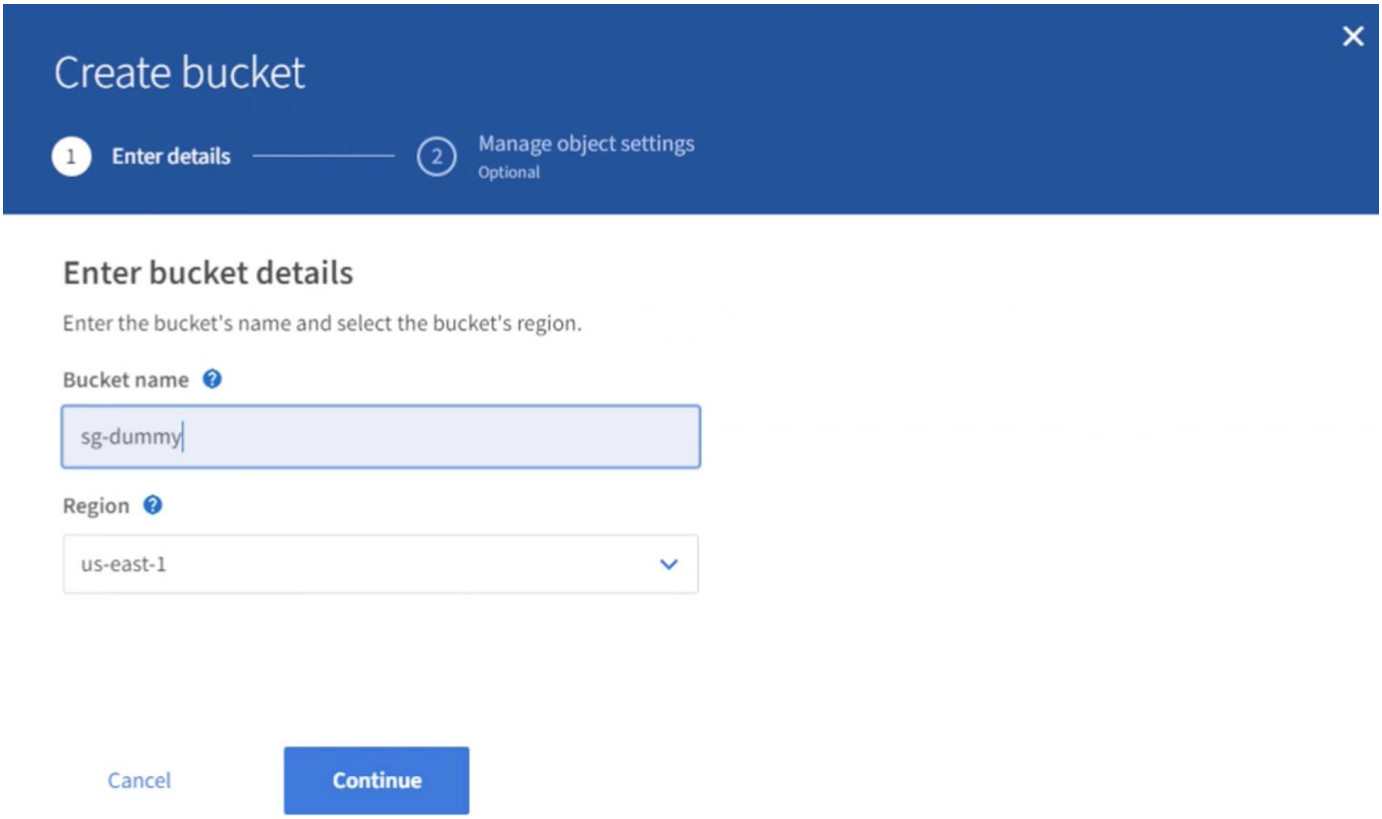


ページ"]

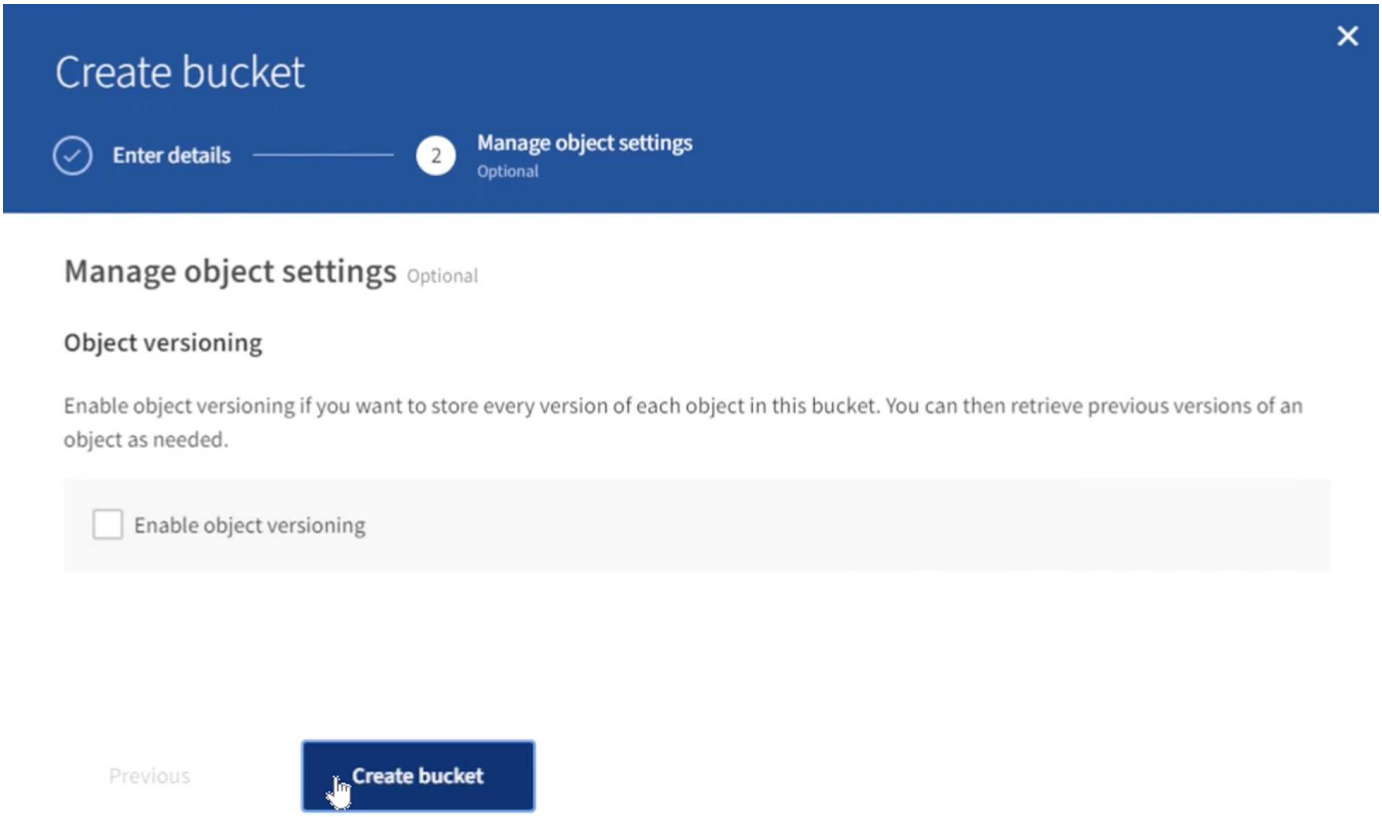
最初のバケットでバージョン管理を有効にします。



次に、バージョン管理を有効にせずに2つ目のバケットを作成します。



この2つ目のバケットではバージョン管理を有効にしないでください。



Rafael Guedes、Aron Klein著_

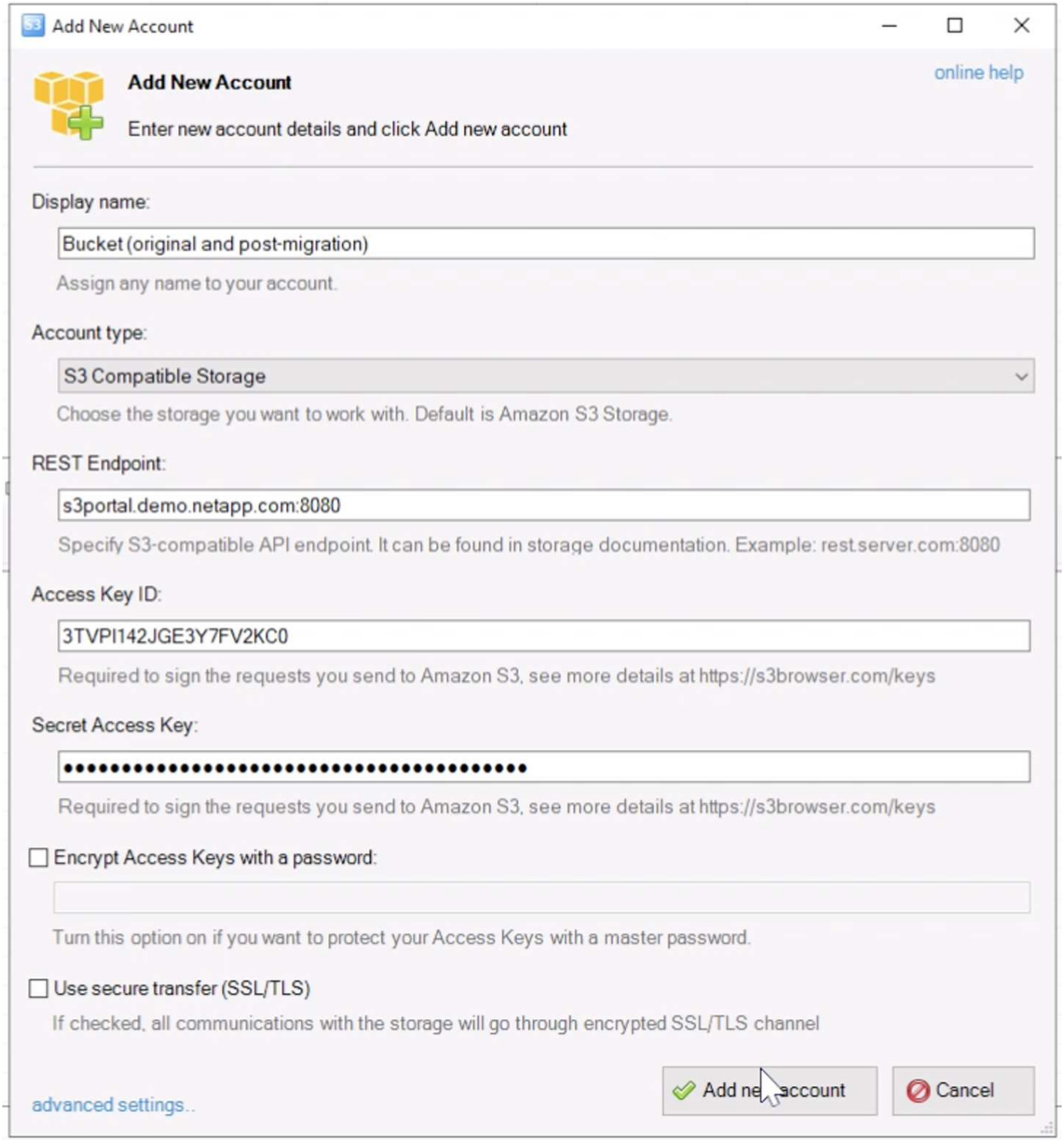
オブジェクトベースストレージを**ONTAP S3**から**StorageGRID**にシームレスに移行し、エンタープライズクラスの**S3**を実現

オブジェクトベースストレージをONTAP S3からStorageGRIDにシームレスに移行し、エンタープライズクラスのS3を実現

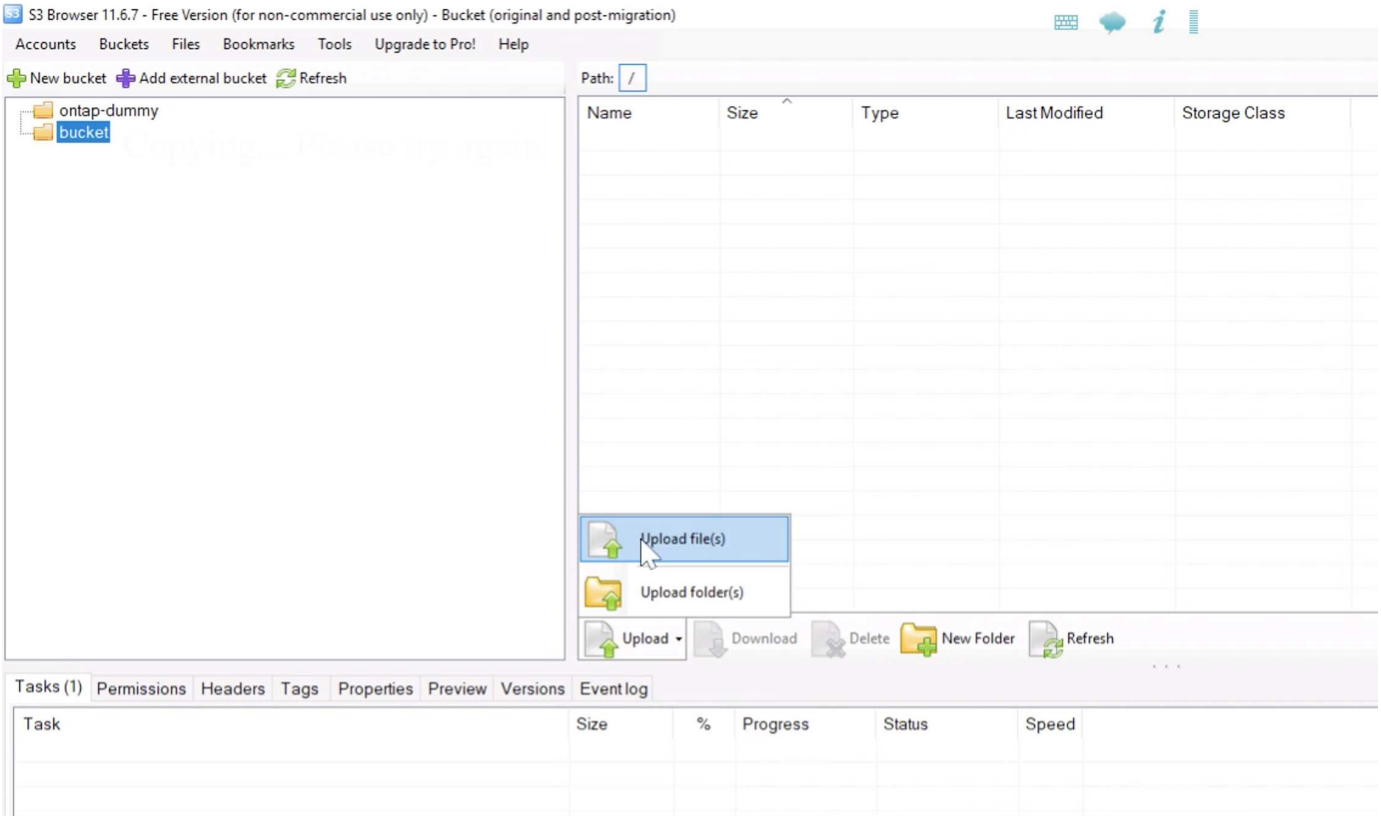
ソースバケットへの入力

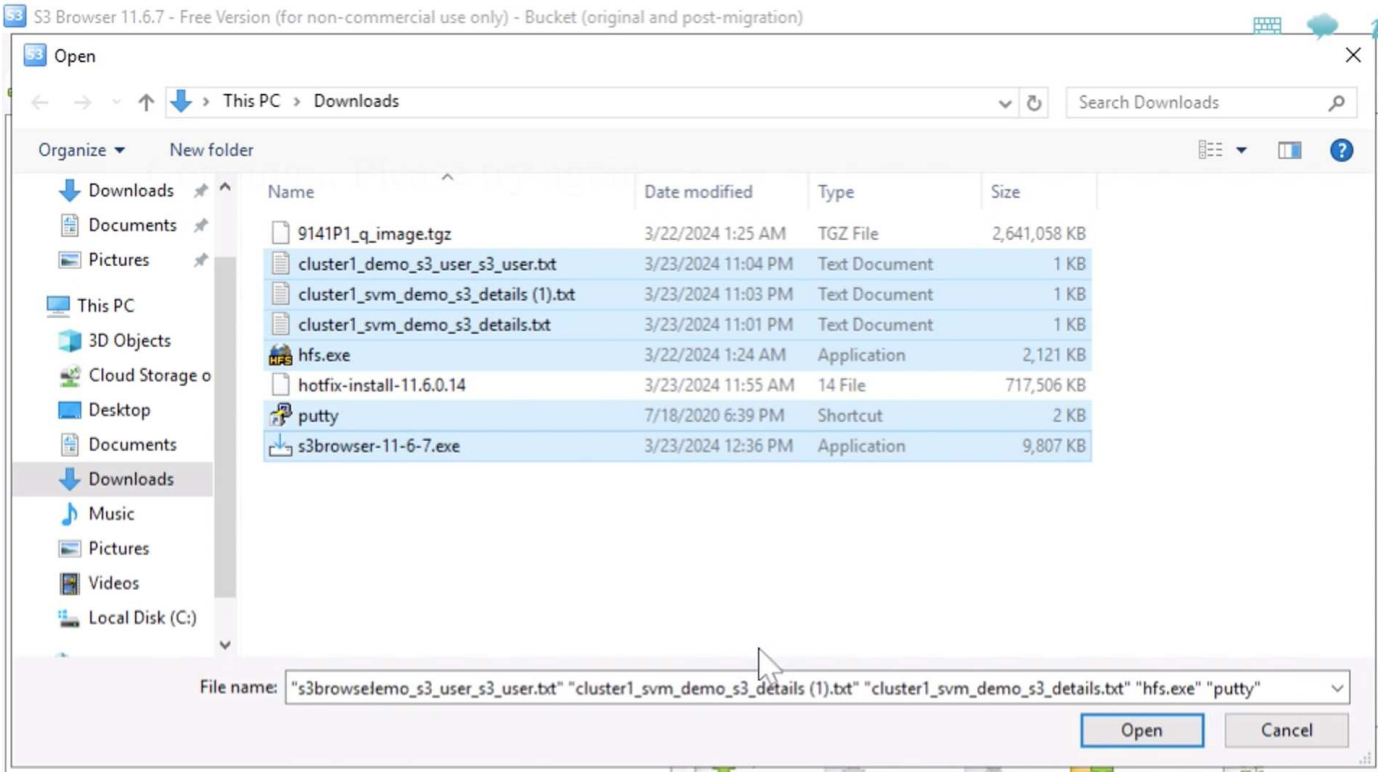
ソースONTAPバケットにオブジェクトを追加しましょう。このデモではS3Browserを使用しますが、使い慣れた任意のツールを使用できます。

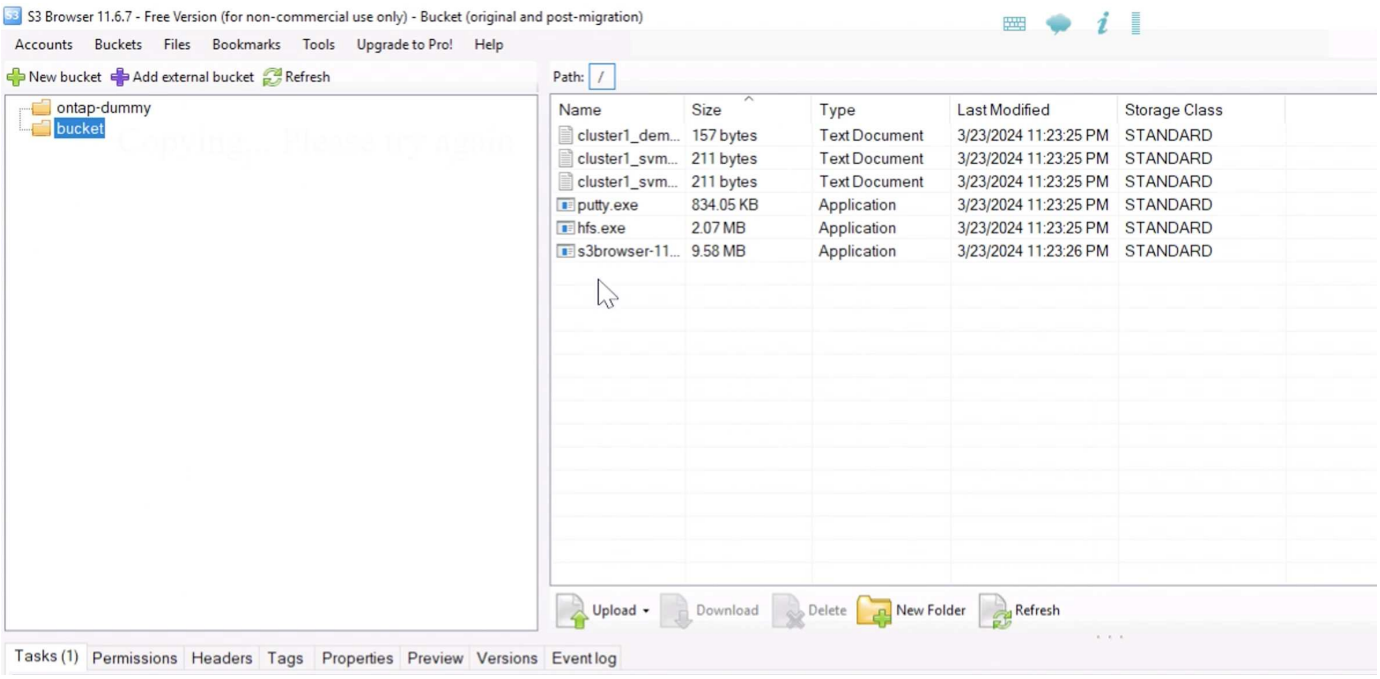
上記で作成したONTAPユーザーs3キーを使用して、ONTAPシステムに接続するようにS3Browserを設定します。



次に、いくつかのファイルをバージョン管理が有効なバケットにアップロードします。

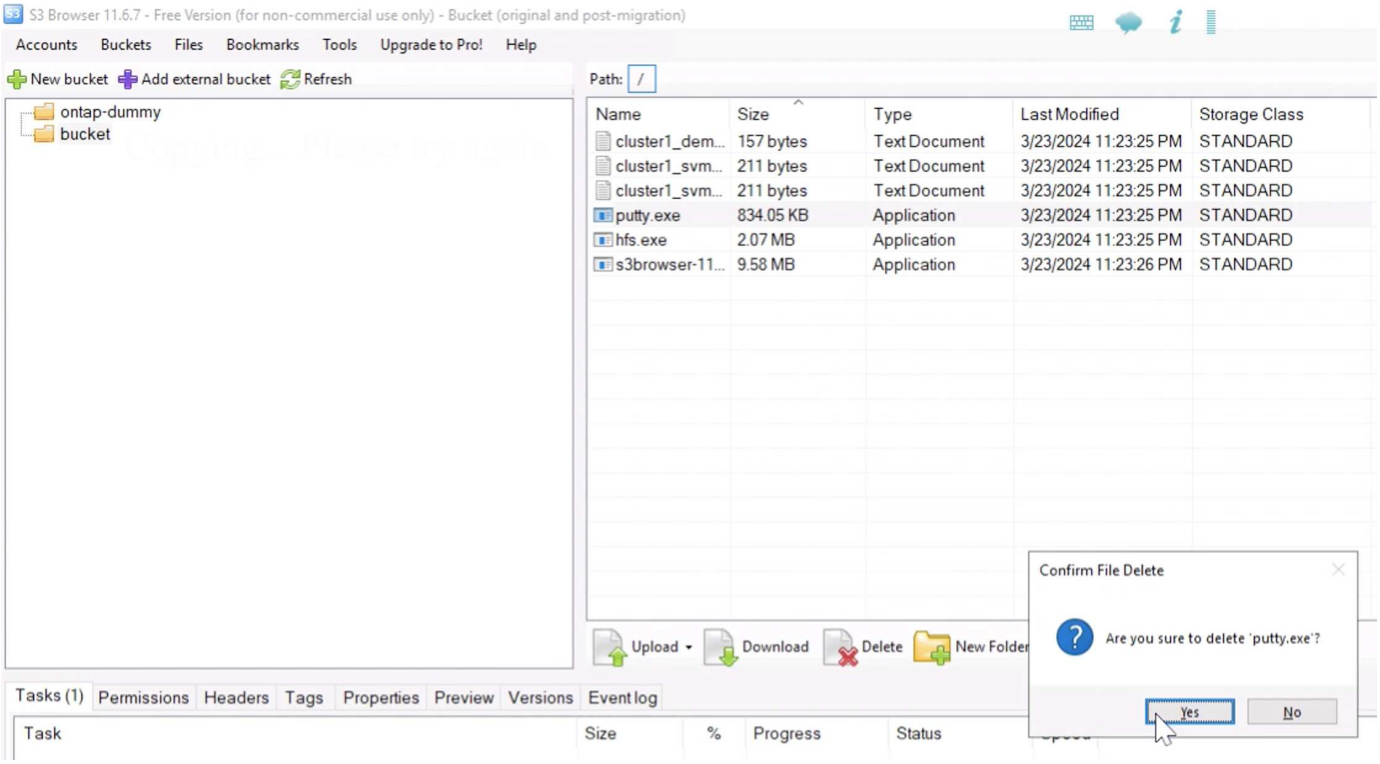

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
Upload
Download
Delete
New Folder
Refresh
Tasks (1)
Permissions
Headers
Tags
Properties
Preview
Versions
Event log
Task
Size
%
Progress
Status
Speed


S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Open
This PC
Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
This PC
3D Objects
Cloud Storage o
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
9141P1_q_image.tgz
3/22/2024 1:25 AM
TGZ File
2,641,058 KB
cluster1_demo_s3_user_s3_user.txt
3/23/2024 11:04 PM
Text Document
1 KB
cluster1_svm_demo_s3_details (1).txt
3/23/2024 11:03 PM
Text Document
1 KB
cluster1_svm_demo_s3_details.txt
3/23/2024 11:01 PM
Text Document
1 KB
hfs.exe
3/22/2024 1:24 AM
Application
2,121 KB
hotfix-install-11.6.0.14
3/23/2024 11:55 AM
14 File
717,506 KB
putty
7/18/2020 6:39 PM
Shortcut
2 KB
s3browser-11-6-7.exe
3/23/2024 12:36 PM
Application
9,807 KB
File name:
"s3browselemo_s3_user_s3_user.txt" "cluster1_svm_demo_s3_details (1).txt" "cluster1_svm_demo_s3_details.txt" "hfs.exe" "putty"
Open
Cancel

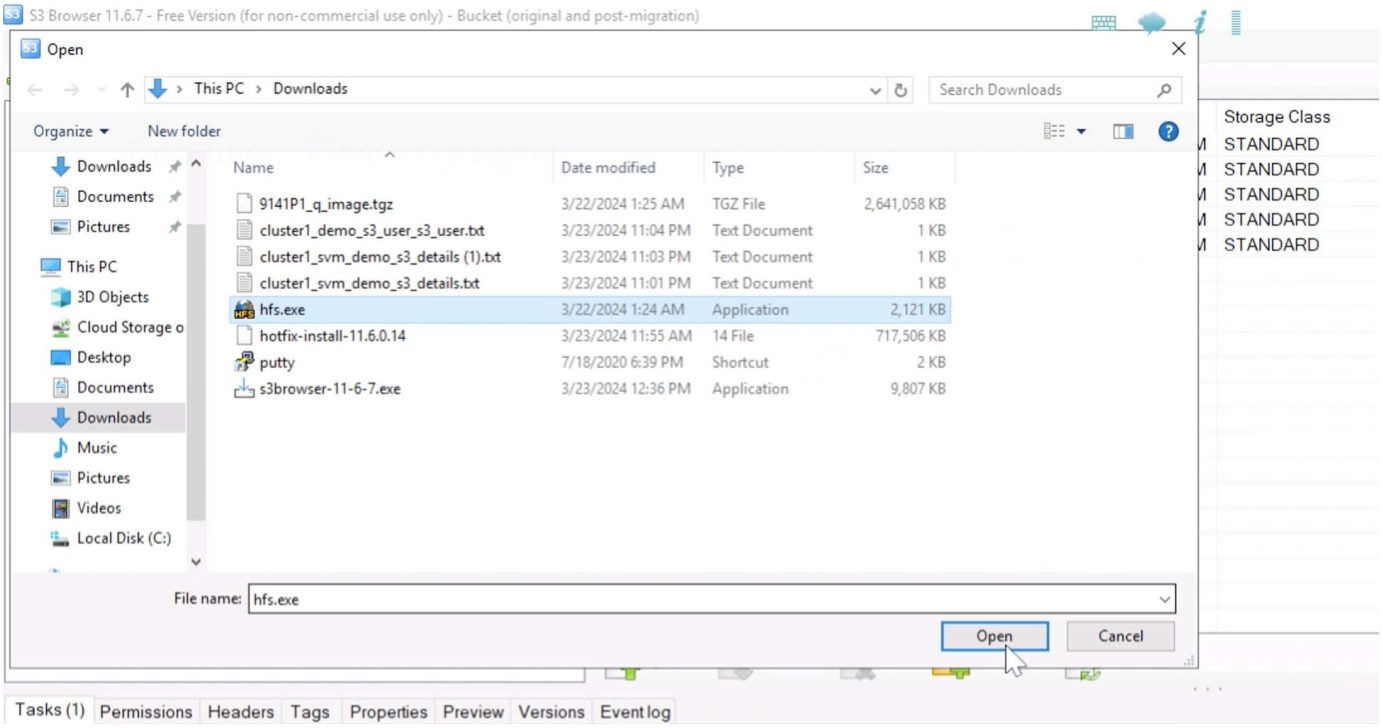


次に、バケットにいくつかのオブジェクトバージョンを作成します。

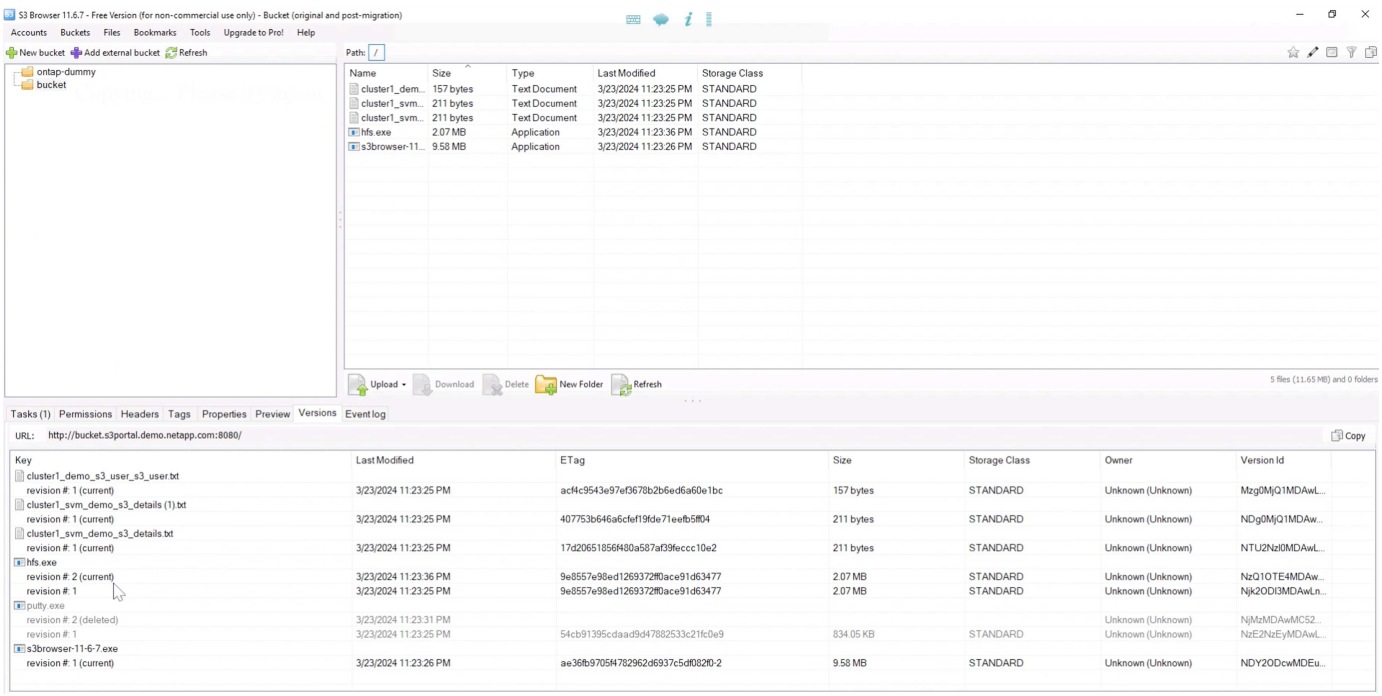
ファイルを削除します。



バケットにすでに存在するファイルをアップロードしてファイルをコピーし、新しいバージョンを作成します。



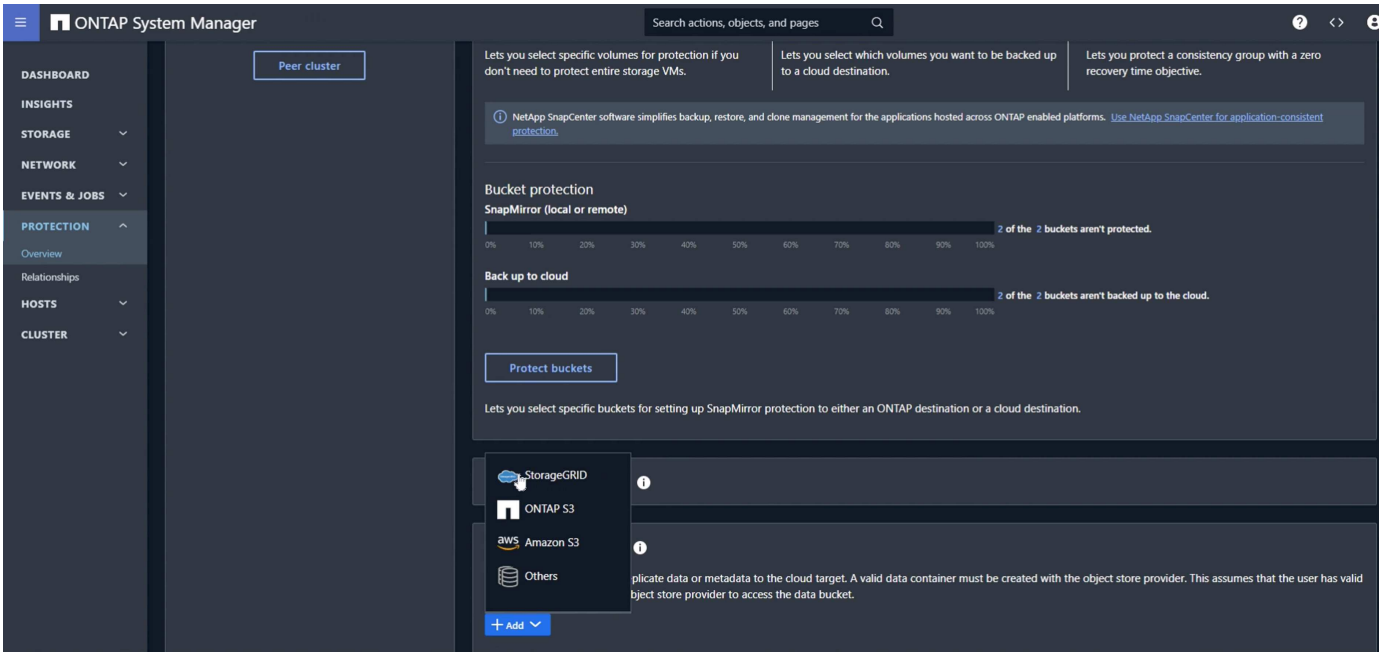
S3Browserでは、作成したオブジェクトのバージョンを表示できます。



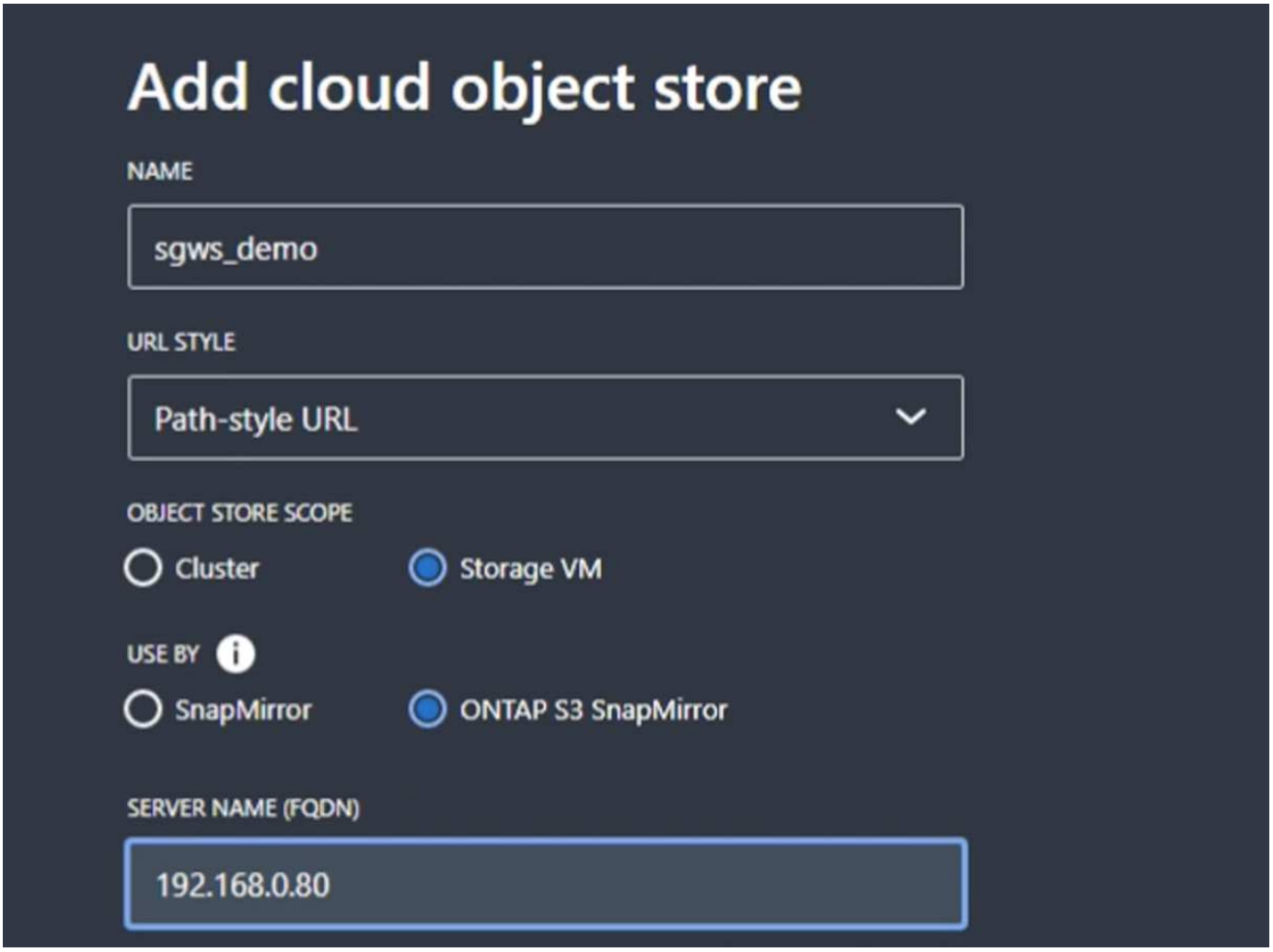
レプリケーション関係を確立

ONTAPからStorageGRIDへのデータ送信を開始します。

ONTAPシステムマネージャで[Protection/Overview]に移動します。[クラウドオブジェクトストア]まで下にスクロールし、[追加]ボタンをクリックして[StorageGRID]を選択します。



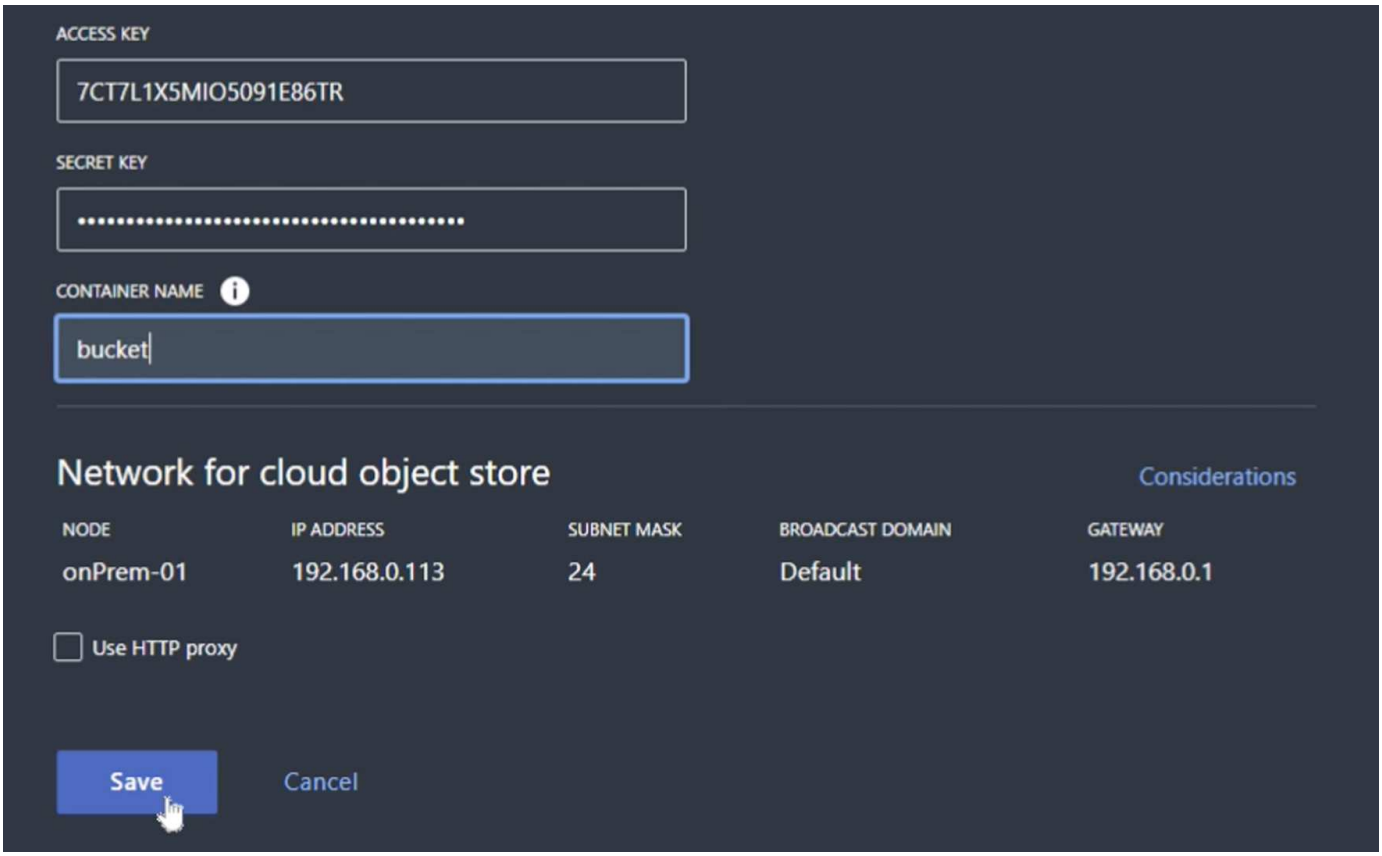
名前とURLスタイルを入力して、StorageGRID情報を入力します(このデモでは、Path-styl URLを使用します)。オブジェクトストアのスコープを「Storage VM」に設定します。



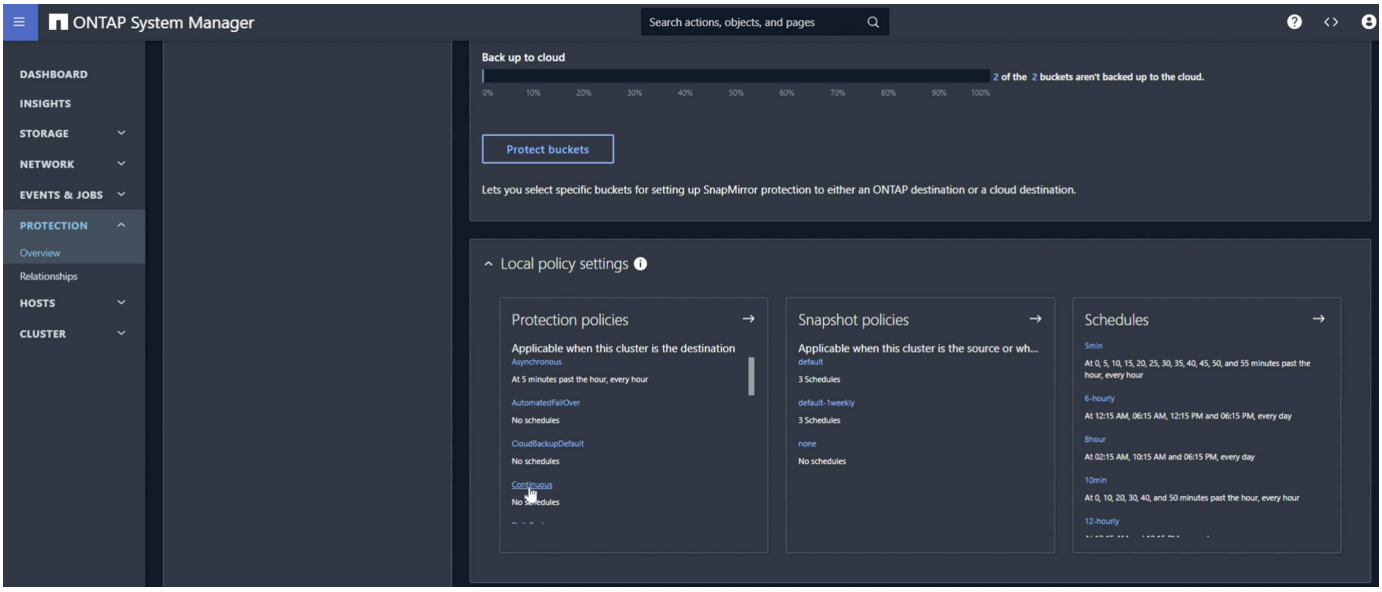
SSLを使用している場合は、ロードバランサエンドポイントのポートを設定し、StorageGRIDエンドポイント

の証明書をここでコピーします。SSLを使用している場合は、[SSL]ボックスをオフにして、HTTPエンドポイントのポートをここに入力します。

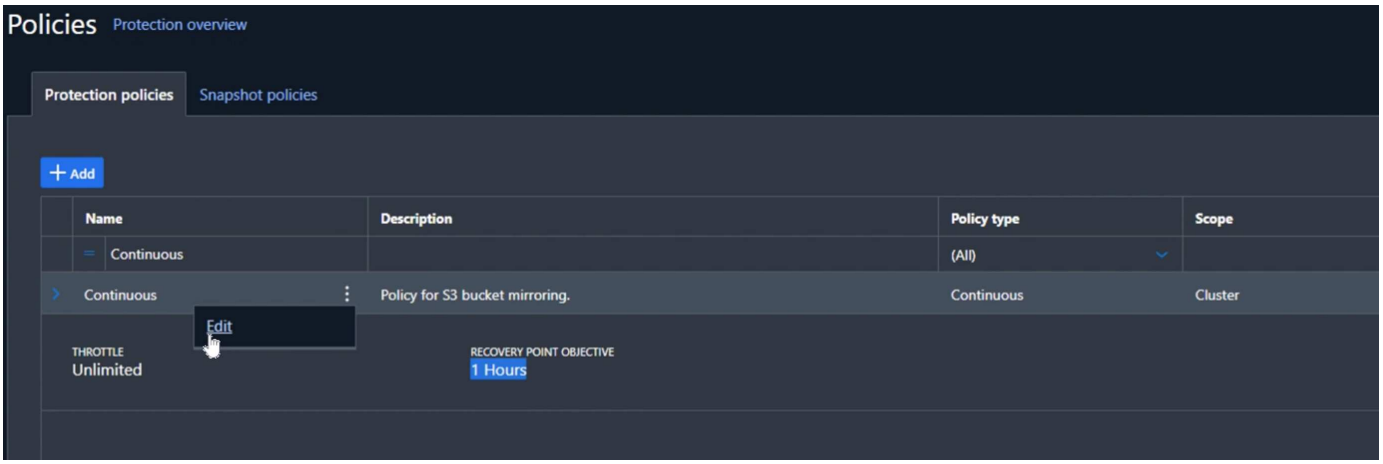
デスティネーションの上記のStorageGRID設定のStorageGRIDユーザのS3キーとバケット名を入力します。



宛先ターゲットが構成されたので、ターゲットのポリシー設定を構成できます。[Local policy settings]を展開し、[continuous]を選択します。

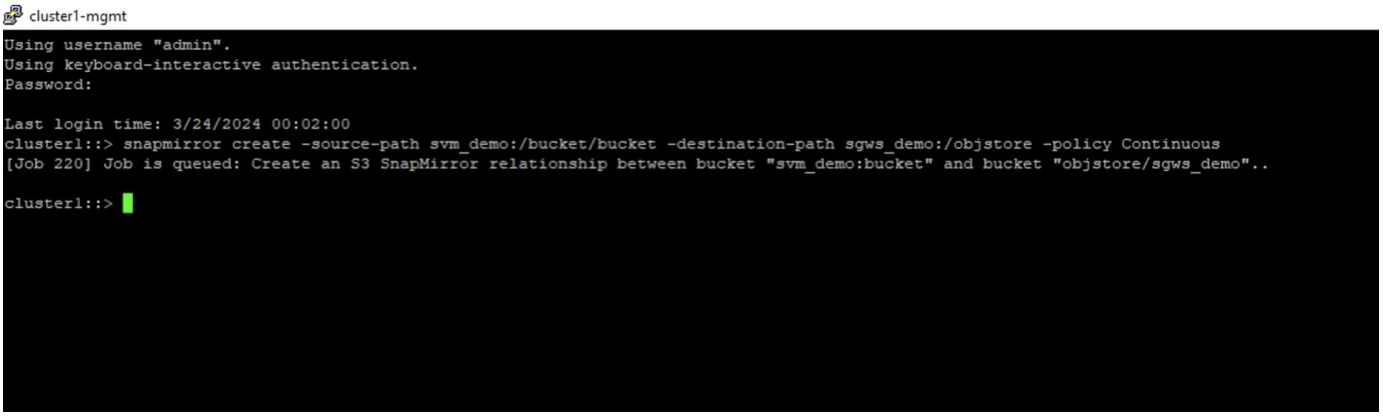


継続的なポリシーを編集し、「目標復旧時点」を「1時間」から「3秒」に変更します。



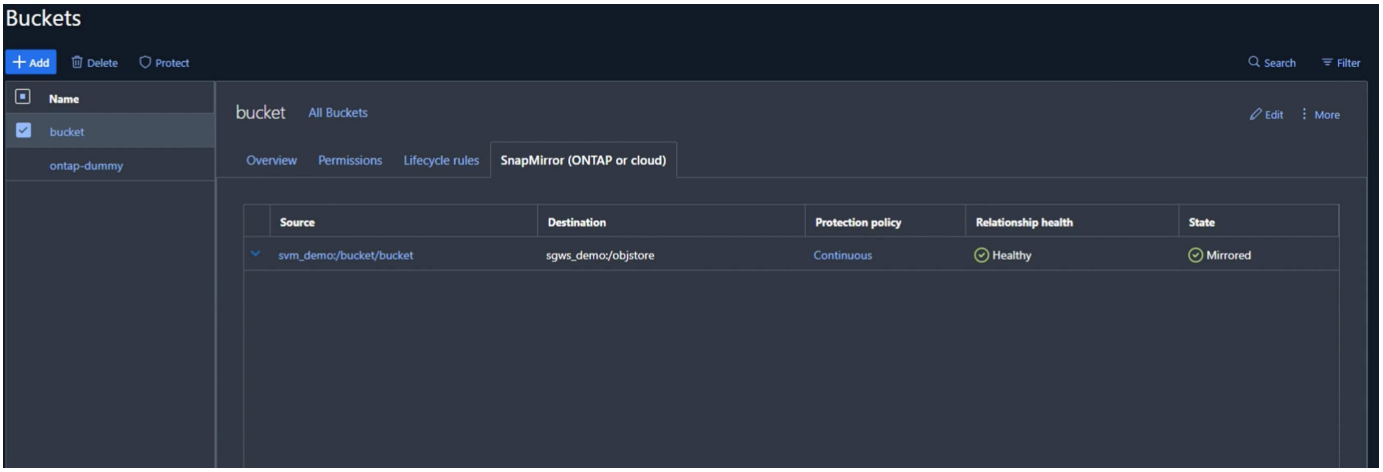
これで、バケットをレプリケートするようにSnapMirrorを設定できます。

```
SnapMirror create -source-path sv_demo：/bucket/bucket-destination-path sgws_demo：/objstore-policy Continuous
```



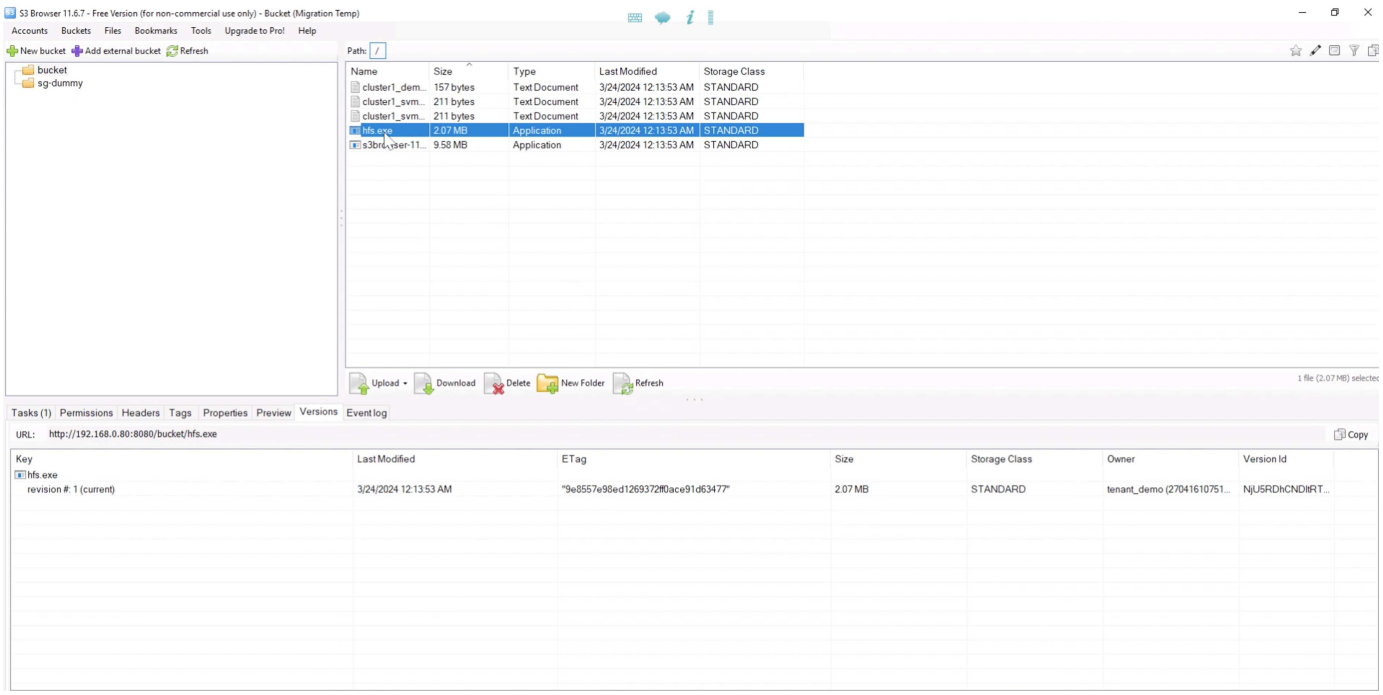
これで、保護対象のバケットリストにクラウドのアイコンが表示されます。

バケットを選択して「SnapMirror（ONTAPまたはCloud）」タブに移動すると、SnapMirrorの返品ステータスが表示されます。

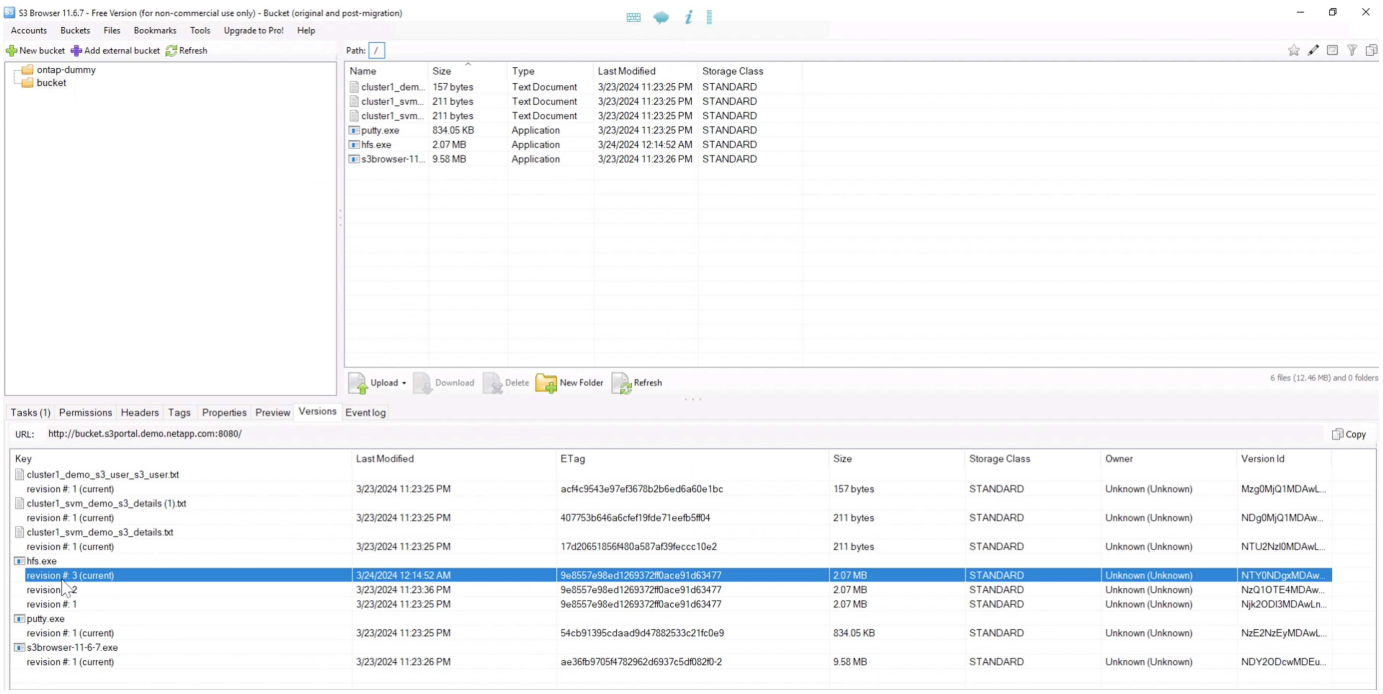


レプリケーションの詳細

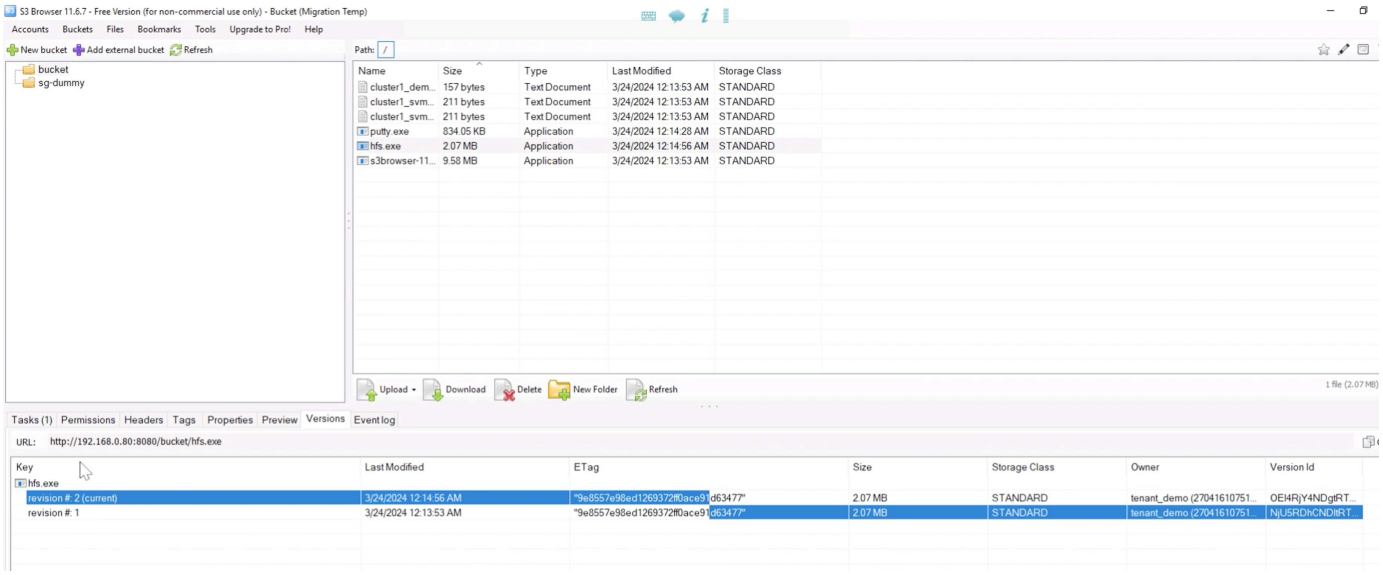
これで、バケットをONTAPからStorageGRIDに正常にレプリケートできるようになりました。では実際に何を複製しているのでしょうか？ソースとデスティネーションはどちらもバージョン管理されたバケットです。以前のバージョンもデスティネーションにレプリケートされますか。S3Browserを使用してStorageGRIDバケットを確認すると、既存のバージョンがレプリケートされず、削除されたオブジェクトも存在せず、そのオブジェクトの削除マーカーもありません。複製されたオブジェクトのStorageGRIDバケットにはバージョンが1つしかありません。



ONTAPバケットで、以前使用したのと同じオブジェクトに新しいバージョンを追加し、それがどのようにレプリケートされるかを確認します。



StorageGRID側を見ると、このバケットにも新しいバージョンが作成されていますが、SnapMirror関係以前の初期バージョンが欠落しています。



これは、ONTAP SnapMirror S3プロセスがオブジェクトの現在のバージョンのみをレプリケートするためです。そのため、デスティネーションとしてStorageGRID側にバージョン管理されたバケットを作成しました。これにより、StorageGRIDはオブジェクトのバージョン履歴を保持できます。

Rafael Guedes、Aron Klein著_

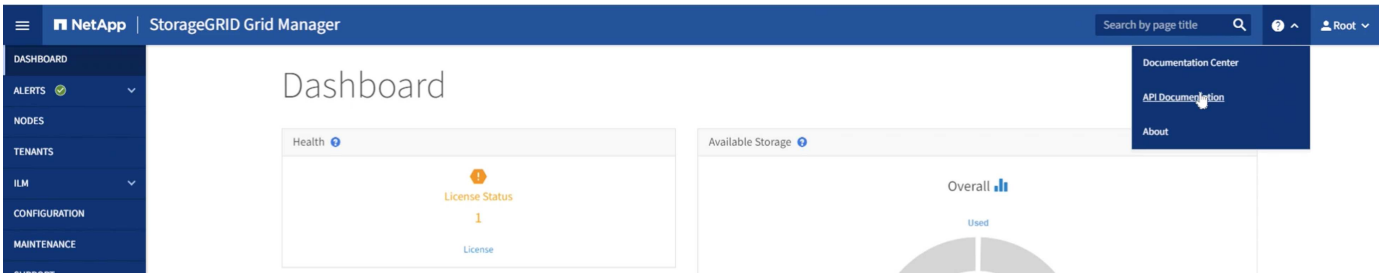
オブジェクトベースストレージを**ONTAP S3**から**StorageGRID**にシームレスに移行し、エンタープライズクラスの**S3**を実現

オブジェクトベースストレージをONTAP S3からStorageGRIDにシームレスに移行し、エンタープライズクラスのS3を実現

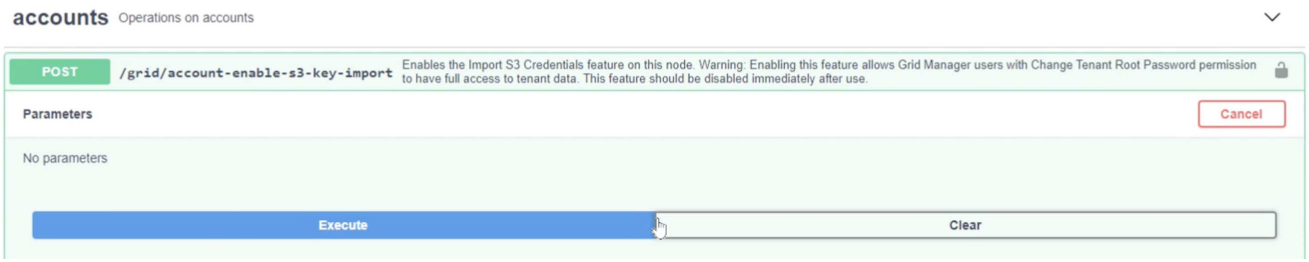
S3キーの移行

移行の場合、ほとんどの場合、移行先で新しいクレデンシャルを生成するのではなく、ユーザのクレデンシャルを移行する必要があります。StorageGRIDには、s3キーをユーザーにインポートできるAPIが用意されています。

（テナントマネージャUIではなく）StorageGRID管理UIにログインすると、[API Documentation] swaggerページが開きます。

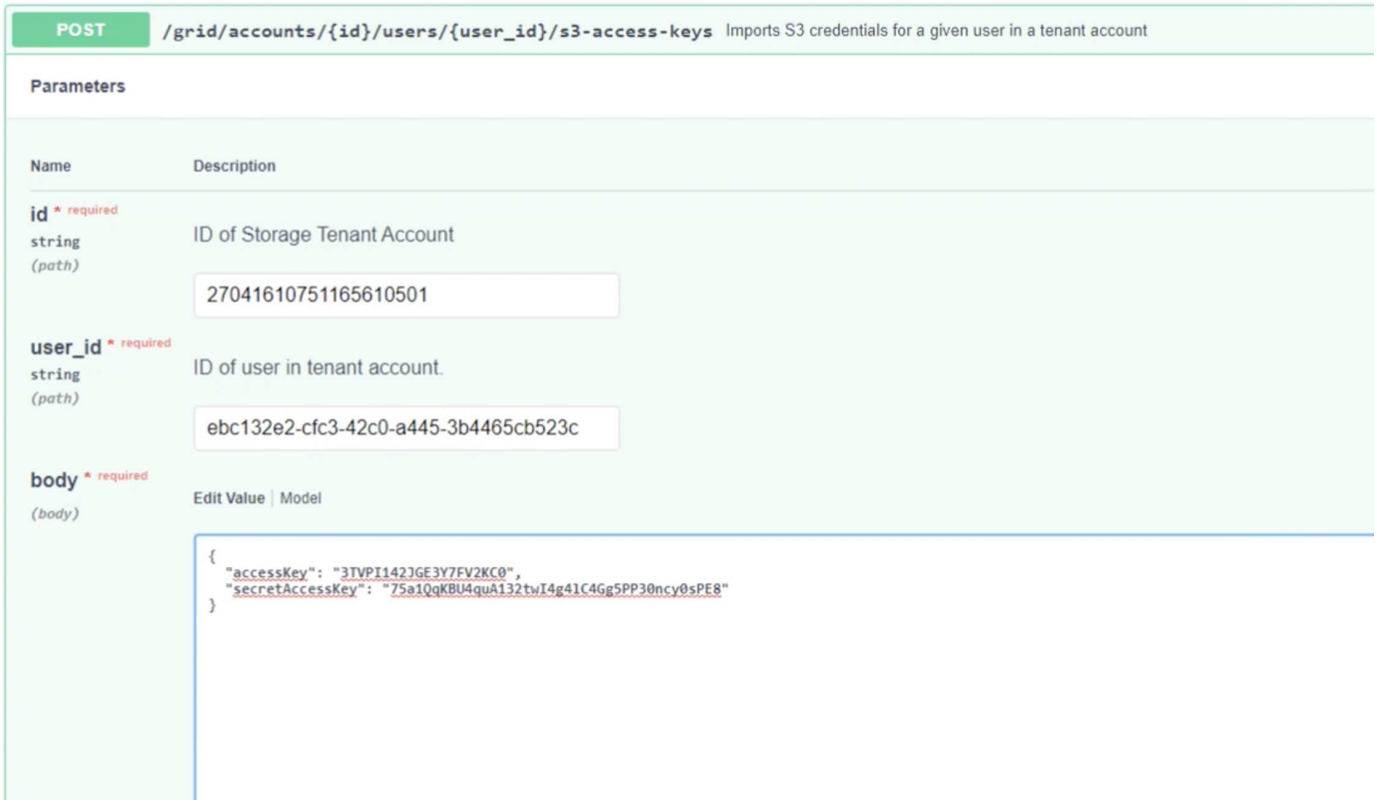


「accounts」セクションを展開し、「POST /grid/account-enable-s3-key-import」を選択し、「Try it out」ボタンをクリックしてから、実行ボタンをクリックします。

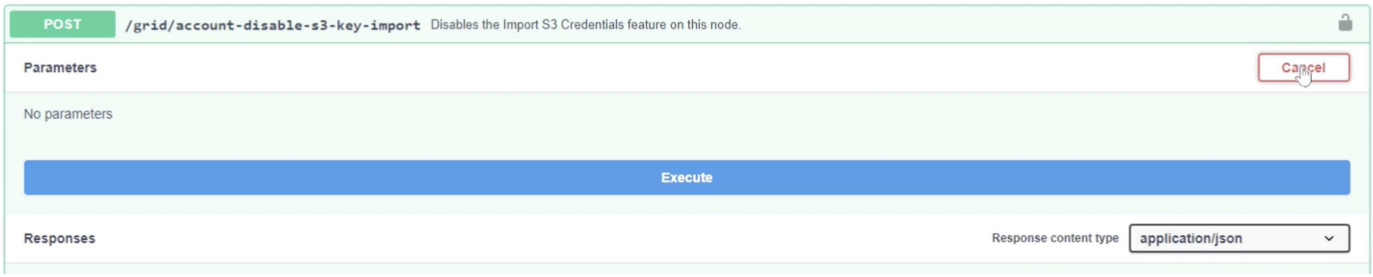


[accounts]の下にスクロールして[POST /grid/accounts/｛id｝/users/｛user_id｝/s3-access-keys]に移動します。

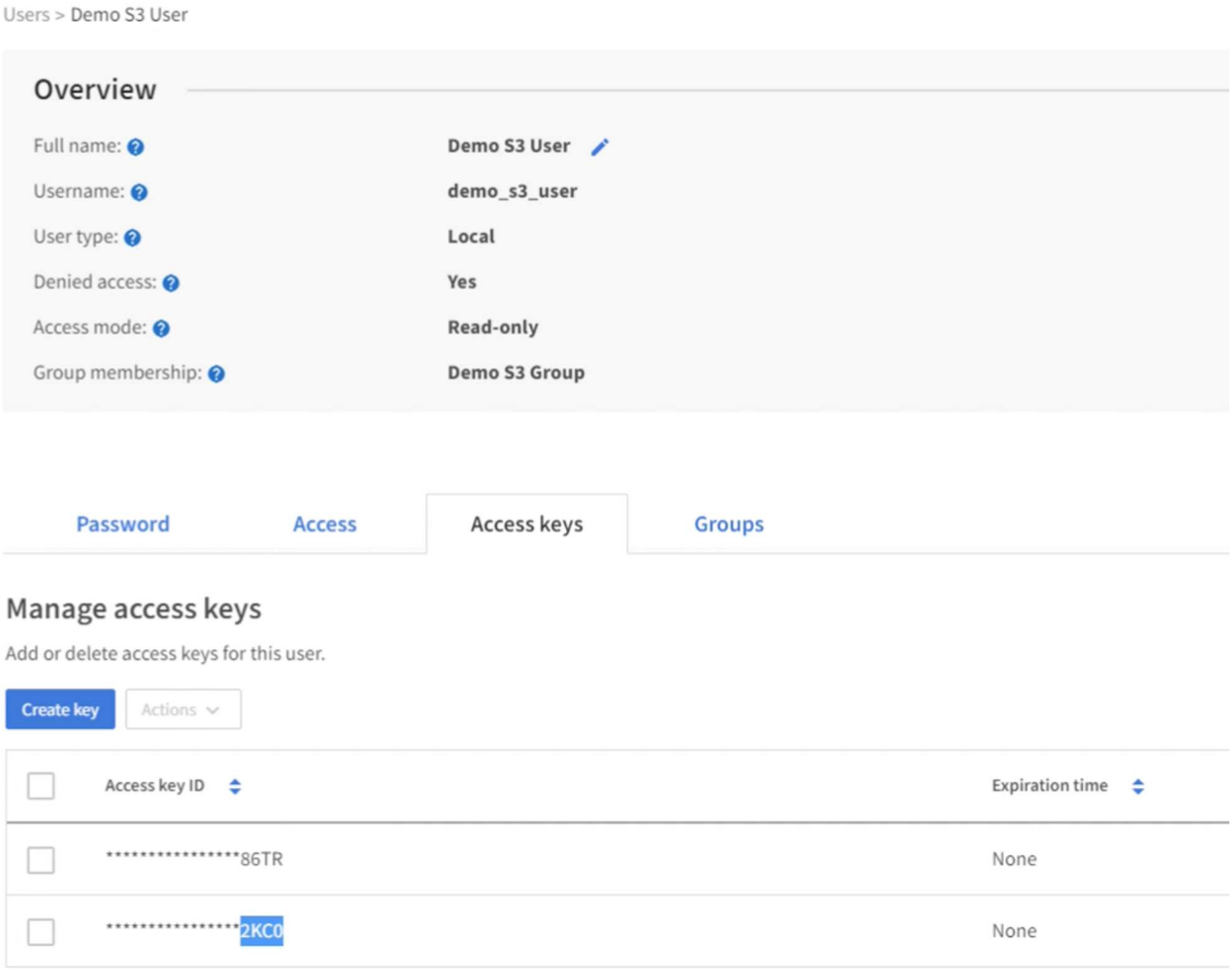
ここでは、先ほど収集したテナントIDとユーザアカウントIDを入力します。JSONボックスにONTAPユーザのフィールドとキーを入力します。キーの有効期限を設定するか、「,"Expires":123456789」を削除して[実行]をクリックします。



すべてのユーザキーのインポートが完了したら、「accounts」POST /grid/account-disable-s3-key-importのキーインポート機能を無効にする必要があります。



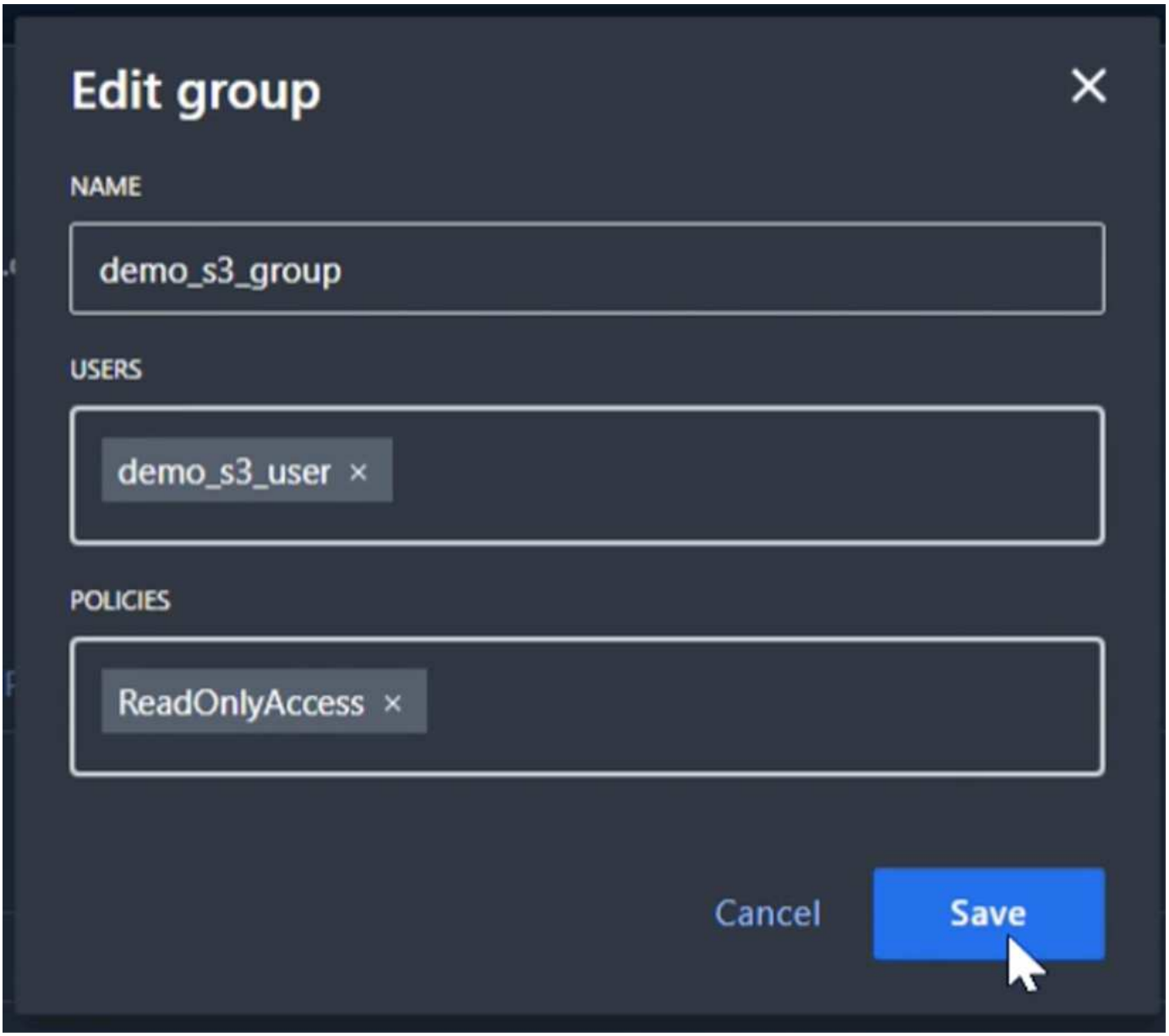
テナントマネージャのUIでユーザアカウントを確認すると、新しいキーが追加されていることがわかります。



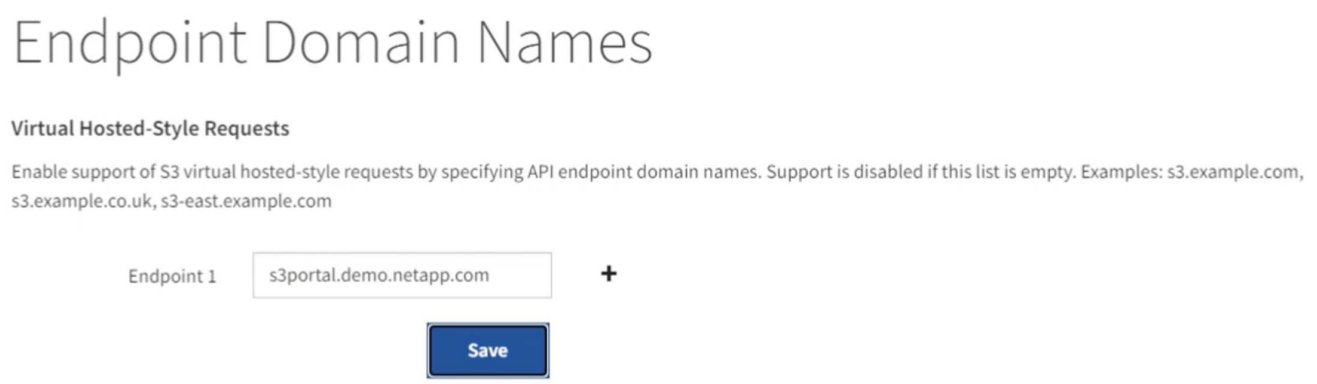
最終的なカットオーバー

バケットをONTAPからStorageGRIDに永続的にレプリケートする場合は、ここで終了できます。ONTAP S3からStorageGRIDへの移行の場合は、移行を終了してカットオーバーします。

ONTAPシステムマネージャでS3グループを編集し、「ReadOnlyAccess」に設定します。これにより、ユーザがONTAP S3バケットに書き込むことができなくなります。



あとは、ONTAPクラスタからStorageGRIDエンドポイントを指すようにDNSを設定するだけです。エンドポイント証明書が正しいことを確認し、仮想ホスト形式の要求が必要な場合は、StorageGRIDでエンドポイントのドメイン名を追加します。



クライアントはTTLが期限切れになるのを待つか、DNSをフラッシュして新しいシステムに解決し、すべてが機能していることをテストする必要があります。あとは、（インポートされたキーではなく）StorageGRIDデータアクセスのテストに使用した最初の一時的なS3キーをクリーンアップし、SnapMirror関係を削除し、ONTAPデータを削除するだけです。

Rafael Guedes、Aron Klein著_

ツールおよびアプリケーションガイド

StorageGRID でCloudera Hadoop S3Aコネクタを使用します

Angela Cheng著_

Hadoopは、しばらくの間データサイエンティストのお気に入りでした。Hadoopでは、シンプルなプログラミングフレームワークを使用して、複数のコンピュータクラスタにまたがる大規模なデータセットを分散処理できます。Hadoopは、ローカルのコンピューティングとストレージを所有するマシンごとに、単一のサーバから数千のマシンにスケールアップするように設計されています。

S3AをHadoopワークフローに使用する理由

データ量の増加に伴い、新しいマシンにコンピューティングとストレージを個別に追加するアプローチは非効率的になっています。リニアに拡張すると、リソースの効率的な使用やインフラの管理が難しくなります。

このような課題に対処するために、Hadoop S3AクライアントはS3オブジェクトストレージに対する高性能なI/Oを提供します。S3Aを使用してHadoopワークフローを実装することで、オブジェクトストレージをデータリポジトリとして活用でき、コンピューティングとストレージを分離することができます。これにより、コンピューティングとストレージを別々に拡張できます。コンピューティングリソースとストレージを分離することで、コンピューティングジョブに適切な量のリソースを割り当て、データセットのサイズに基づいて容量を提供することもできます。そのため、Hadoopワークフローの総所有コストを削減することができます。

StorageGRID を使用するようにS3Aコネクタを構成します

前提条件

- StorageGRID S3エンドポイントのURL、テナントS3アクセスキー、およびHadoop S3A接続テスト用のシークレットキー。
- クラスタ内の各ホストに対するClouderaクラスタとrootまたはsudo権限を付与して、Javaパッケージをインストールします。

2022年4月時点で、StorageGRID 11.0.14とCloudera 7.1.7のJava 11.0.14が、11.5および11.6に対してテストされました。ただし、Javaのバージョン番号は新規インストール時と異なる場合があります。

Javaパッケージをインストールします

1. を確認します "Clouderaサポートマトリックス" を参照してください。
2. をダウンロードします "Java 11.xパッケージ" Clouderaクラスタオペレーティングシステムと同じです。このパッケージをクラスタ内の各ホストにコピーします。この例では、CentOSにrpmパッケージを使用しています。
3. 各ホストにrootとしてログインするか、sudo権限を持つアカウントを使ってログインします。各ホストで次の手順を実行します。
   a. パッケージをインストールします。

```
$ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
```

b. Javaがインストールされている場所を確認します。複数のバージョンがインストールされている場合は、新しくインストールしたバージョンをデフォルトに設定します。

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. この行を/etc/profile'の末尾に追加しますパスは、上記の選択のパスと一致する必要があります。

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. 次のコマンドを実行して、プロファイルを有効にします。

```
source /etc/profile
```

Cloudera HDFS S3A構成

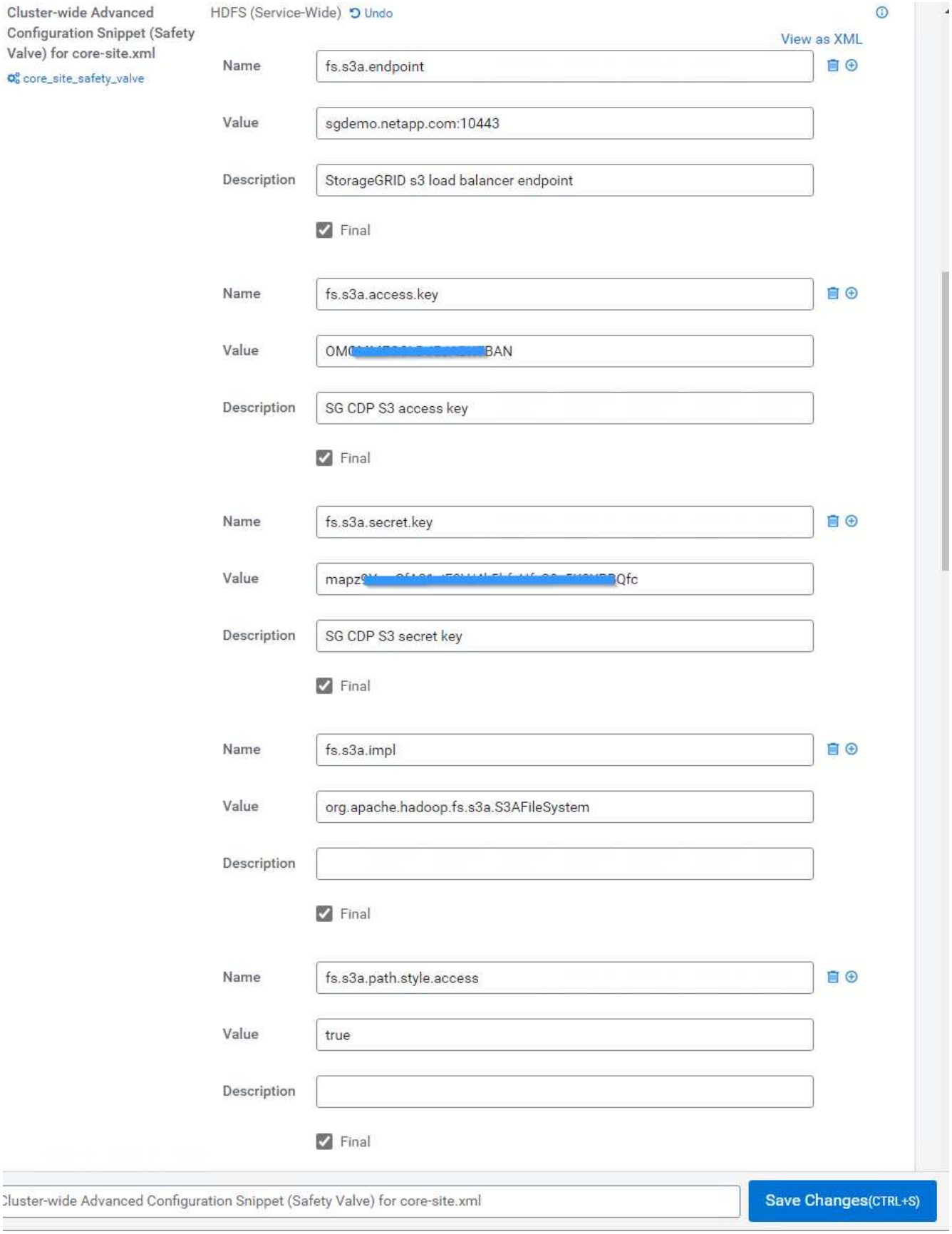
- 手順 *

1. Cloudera Manager GUIで、クラスタ（Clusters）> HDFSを選択し、構成（Configuration）を選択します。
2. カテゴリでAdvancedを選択し、下にスクロールして「core-site .xml」用のクラスタ全体のAdvanced Configuration Snippet（Safety Valve）を探します。
3. （+）記号をクリックし、次の値ペアを追加します。

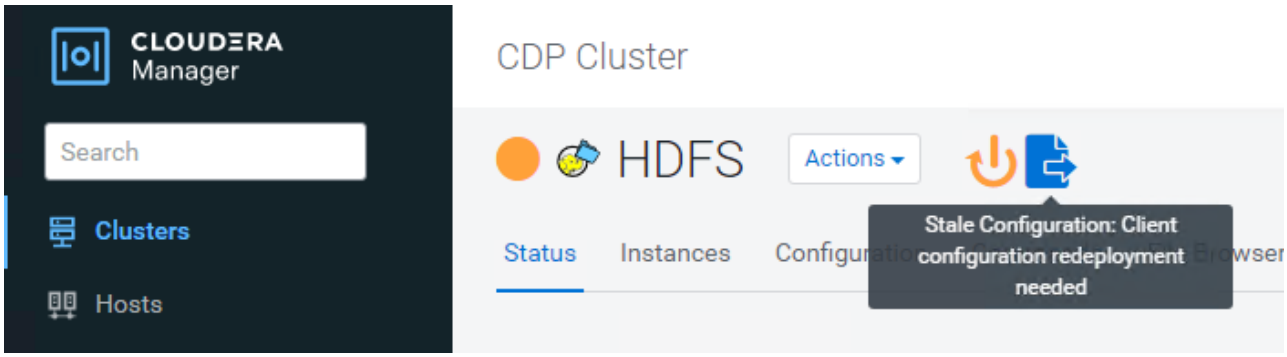
名前	価値
fs.s3a.access.key	*<tenant StorageGRID のs3アクセスキー_*
fs.s3a.secret.key	*<tenant s3 secret key from StorageGRID >*
FS.s3a.connection.ssl.enabled	[true or false]（このエントリがない場合のデフォルトはhttps）
FS.s3a.endpoint	_ StorageGRID S3エンドポイント：port>_

名前	価値
FS.s3a.impl	org.apache.hadoop .fs.s3a.S3AFileSystem
FS.s3a.path.style.access	[true or false]（このエントリがない場合のデフォルトの仮想ホスト形式）

サンプルスクリーンショット



1. [Save Changes]ボタンをクリックします。HDFSメニューバーからStale Configurationアイコンを選択し、次のページでRestart Stale Servicesを選択して、Restart Nowを選択します。



StorageGRID へのS3A接続をテストします

基本的な接続テストを実行します

Clouderaクラスタのいずれかのホストにログインし、「hadoop fs s-ls s3a：//<*bucket-name*>/`」と入力します。

次の例では、パスsyleと既存のHDFSテストバケットおよびテストオブジェクトを使用します。

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

トラブルシューティング

シナリオ **1**

StorageGRID へのHTTPS接続を使用し、15分後に「handshake_failure」エラーを取得します。

*理由：StorageGRID への接続に古いTLS暗号スイートまたはサポートされていないTLS暗号スイートを使用しているJRE／JDKの旧バージョン。

エラーメッセージの例

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

*解決策: JDK 11.x以降がインストールされていることを確認し'デフォルトのJavaライブラリに設定しますを参照してください Javaパッケージをインストールします 詳細については、を参照してください。

シナリオ**2**：

StorageGRID に接続できませんでした。エラーメッセージ「要求されたターゲットへの有効な証明書パスが見つかりませんでした」が表示されます。

理由： StorageGRID S3エンドポイントサーバ証明書がJavaプログラムで信頼されていません。

エラーメッセージの例：

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

*解決策：ネットアップは、既知のパブリック証明書署名機関が発行するサーバ証明書を使用して、認証がセキュアであることを確認することを推奨しています。または、Javaの信頼ストアにカスタムのCA証明書またはサーバ証明書を追加します。

StorageGRID カスタムCA証明書またはサーバ証明書をJava信頼ストアに追加するには、次の手順を実行します。

1. 既存のデフォルトのJava cacertsファイルをバックアップします。

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. StorageGRID S3エンドポイント証明書をJava信頼ストアにインポートします。

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

1. Hadoopログレベルを引き上げてデバッグします。

   'export hadoop root_logger = hadoop .root.logger = debug、console'

2. コマンドを実行し、ログメッセージをerror.logに送信します。

   「hadoop fs s-ls s3a：//<*bucket-name*>_ error.log

Angela Cheng著_

S3cmdを使用して、StorageGRID でS3アクセスをテストおよび実証します

アロンクライン著

S3cmdは、S3処理用の無償のコマンドラインツールおよびクライアントです。s3cmdを使用して、StorageGRID でのS3アクセスをテストして実証できます。

S3cmdをインストールして構成します

ワークステーションまたはサーバにS3cmdをインストールするには、からダウンロードします "コマンドラインS3クライアント"。s3cmdは、トラブルシューティング用のツールとして、各StorageGRID ノードにあらかじめインストールされています。

初期設定手順

1. s3cmd --設定
2. 残りのキーには、access-keyとsecret_keyだけを指定してデフォルトのままにします。
3. 指定したクレデンシャルでアクセスをテストします[Y/n]：n（失敗するため、テストをバイパスする）
4. 設定を保存しますか？[y/N] y
   a. 設定を「/root/.s3cfg」に保存しました。
5. s3cfgで、「=」記号のあとにhost_baseフィールドとhost_bucketフィールドを空にします。
   a. host_base=
   b. host_bucket=

手順4でhost_baseとhost_bucketを指定した場合は、CLIで—hostのエンドポイントを指定する必要はありません。例

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

基本的なコマンドの例

- バケットを作成：

  s3cmd mb s3：//s3cmdbucket --host=<endpoint>：<port>--no-check-certificate-`

- すべてのバケットを表示：

  s3cmd ls --host=<endpoint>：<port>--no-check-certificate'

- すべてのバケットとその内容を表示：

  s3cmd la --host=<endpoint>：<port>-- no-check-certificate'

- 特定のバケット内のオブジェクトをリストします。

  s3cmd ls s3：//<bucket>--host=<endpoint>：<port>--no-check-certificate-`

- バケットを削除：

  s3cmd rb s3：//s3cmdbucket --host=<endpoint>：<port>--no-check-certificate'

- オブジェクトを置きなさい:

  s3cmd put <file>s3://<bucket>--host=<endpoint>:<port>--no-check-certificate`

- オブジェクトを取得：

  s3cmd get s3：//<バケット>/<オブジェクト><ファイル>--host=<endpoint>：<port>--no-check-certificate'

- オブジェクトを削除：

  s3cmd del s3：//<bucket>/<object>--host=<endpoint>：<port>：-no-check-certificate-`

NetApp StorageGRID を共有ストレージとして使用したVertica Eonモードのデータベース

Angela Cheng著_

このガイドでは、NetApp StorageGRID のパブリックストレージを使用してVertica Eon Modeデータベースを作成する手順 について説明します。

はじめに

Verticaは分析データベース管理ソフトウェアです。大量のデータを処理するように設計されたカラム型ストレージ・プラットフォームであり'従来の負荷の高いシナリオでは非常に高速なクエリー・パフォーマンスを実現しますVerticaデータベースは、EonまたはEnterpriseのいずれかのモードで動作します。両方のモードをオンプレミスまたはクラウドに導入できます。

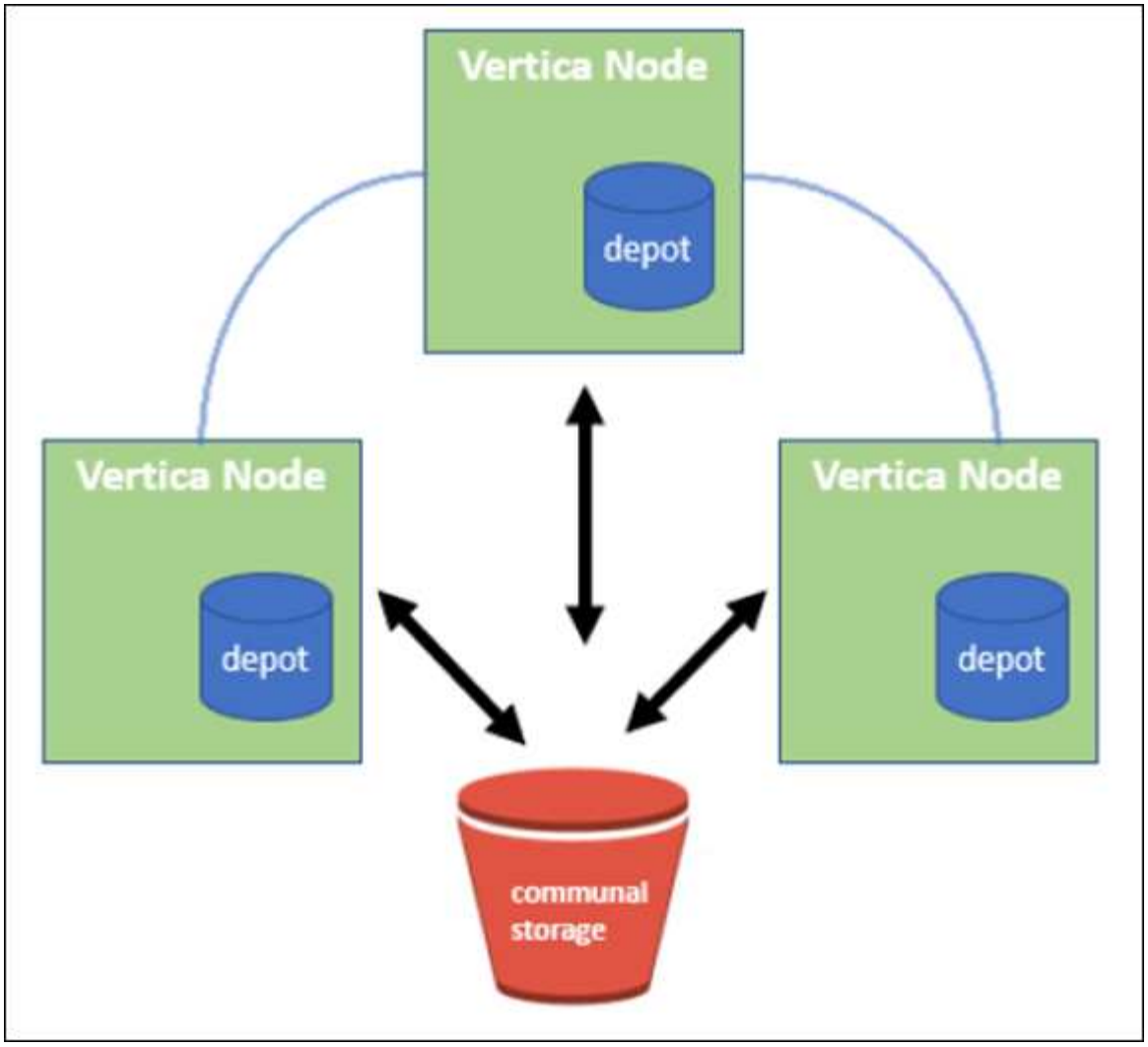
EonモードとEnterpriseモードは、主にデータの保存場所によって異なります。

- Eonモードのデータベースは、データ用に共有ストレージを使用します。これはVerticaがお勧めします。
- Enterprise Modeデータベースでは、データベースを構成するノードのファイルシステムにデータがローカルに格納されます。

Eon Modeアーキテクチャ

Eonモードでは、計算リソースがデータベースの共有ストレージレイヤから分離され、コンピューティングとストレージを別々に拡張できます。EonモードのVerticaは、さまざまなワークロードに対応し、コンピューティングリソースとストレージリソースを別々に使用してワークロードを分離するように最適化されています。

Eon Modeは、パブリックストレージと呼ばれる共有オブジェクトストアにデータを格納します。パブリックストレージとは、オンプレミスまたはAmazon S3上にホストされるS3バケットです。



共有ストレージ

Eonモードでは、データをローカルに格納する代わりに、すべてのデータとカタログ（メタデータ）に単一の共有ストレージロケーションを使用します。共有ストレージとは、データベースの一元管理されたストレージの場所で、データベースノード間で共有されるものです。

共有ストレージには次のプロパティがあります。

- クラウドまたはオンプレミスのオブジェクトストレージ内の共有ストレージは、個々のマシンのディスク上のストレージよりも耐障害性が高く、ストレージ障害によるデータ損失の影響を受けにくくなっています。
- すべてのデータは、同じパスを使用して任意のノードで読み取ることができます。
- ノードのディスクスペースによる容量制限はありません。
- データは通信環境に保管されるため、変化するニーズに合わせてクラスタを柔軟に拡張できます。データがノードにローカルに格納されていた場合は、ノードを追加または削除するときに、ノード間で移動するデータが大量に必要になります。これを行うには、削除対象のノードから移動するか、新しく作成したノードに移動する必要があります。

デポ

共有ストレージの欠点の1つは速度です。共有クラウド上の場所からデータにアクセスする場合、ローカルディスクからデータを読み取る場合よりも時間がかかります。また、多数のノードが一度にデータを読み取っている場合、共有ストレージへの接続がボトルネックになる可能性があります。データアクセス速度を向上させるために、Eon Modeデータベース内のノードは、デポと呼ばれるデータのローカルディスクキャッシュを保持します。クエリを実行するとき、ノードはまず、必要なデータがデポにあるかどうかをチェックします。存在する場合は、データのローカルコピーを使用してクエリが完了します。データがデポにない場合、ノードは共有ストレージからデータを取得し、デポにコピーを保存します。

NetApp StorageGRID の推奨事項

Verticaは、データベースのデータをオブジェクトストレージに何千（数百万）もの圧縮オブジェクトとして格納します（1オブジェクトあたり200～500MB）。ユーザーがデータベースクエリを実行すると、Verticaはバイト範囲GET呼び出しを使用して、圧縮されたオブジェクトから選択したデータ範囲を並列に取得します。バイト範囲GETはそれぞれ約8KBです。

10TBのデータベースデポのユーザクエリテストでは、1秒あたり4、000~ 10、000個のGET（バイト範囲GET）要求がグリッドに送信されました。SG6060アプライアンスを使用してこのテストを実行した場合、アプライアンスノードあたりのCPU利用率は（20$_{30\%程度}$）が低いため、CPU時間の2/3でI/Oを待機していますSGF6024では、I/O待機時間のごく一部（0% 0.5%）が確認されます。

IOPSは小さいが高いことから、レイテンシの要件は非常に低い（平均値は0.01秒未満）ため、オブジェクトストレージサービスにはSFG6024を使用することを推奨します。非常に大きなデータベースサイズにSG6060が必要な場合は、お客様はデポサイジングのVerticaアカウントチームと協力して、照会中のデータセットをサポートする必要があります。

管理ノードとAPIゲートウェイノードの場合は、お客様がSG100またはSG1000を使用できます。選択する内容は、ユーザのクエリ要求の並列サイズとデータベースサイズによって異なります。他社製ロードバランサを使用する場合は、ハイパフォーマンスが要求されるワークロードに専用のロードバランサを使用することを推奨します。StorageGRID のサイジングについては、ネットアップアカウントチームにお問い合わせください。

StorageGRID 構成に関するその他の推奨事項は次のとおりです。

- グリッドトポロジ。同じグリッドサイトにある他のストレージアプライアンスモデルとSGF6024を混在させないでください。長期アーカイブ保護にSG6060を使用する場合は、アクティブデータベース用に専用のグリッドロードバランサを使用してSGF6024の負荷を専用のグリッドサイト（物理サイトまたは論理サイト）に配置し、パフォーマンスを向上させます。同じサイトに異なるモデルのアプライアンスを混在させると、サイト全体のパフォーマンスが低下します。
- データ保護。レプリケートコピーを使用して保護します。アクティブデータベースにはイレイジャーコーディングを使用しないでください。イレイジャーコーディングを使用することで、アクセス頻度の低いデータベースを長期にわたって保護できます。
- グリッド圧縮を有効にしないでください。Verticaは、オブジェクトを圧縮してからオブジェクトストレージに格納します。グリッド圧縮を有効にしてもストレージ使用量はこれ以上削減されず、バイト範囲のGETパフォーマンスが大幅に低下します。
- * HTTPとHTTPS S3エンドポイント接続*。ベンチマークテストでは、VerticaクラスタからStorageGRIDロードバランサエンドポイントへのHTTP S3接続を使用した場合、パフォーマンスが約5%向上しました。この選択は、顧客のセキュリティ要件に基づいて行う必要があります。

Vertica構成に関する推奨事項は次のとおりです。

- * Verticaデータベースのデフォルトデポ設定は、読み取りおよび書き込み操作で有効(値=1)になっています。*パフォーマンスを向上させるために、これらのデポ設定を有効にしておくことを強く推奨します。
- *ストリーミング制限を無効にします。*設定の詳細については、を参照してください ストリーミング制限を無効にしています。

StorageGRID 上の共有ストレージを使用してオンプレミスモードをインストールする

以下のセクションでは、StorageGRID 上に共同ストレージを使用してオンプレミスにEonモードをインストールするための手順 について説明します。オンプレミスのSimple Storage Service（S3）互換オブジェクトストレージを設定する手順 は、Vertica guideの手順 に似ています。 "オンプレミスにEonモードデータベースをインストールします"。

機能テストには次のセットアップを使用しました。

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Verticaノードをクラスタに構成するために、CentOS 7.x OSを搭載した3台の仮想マシン（VM）。このセットアップは、Verticaプロダクションデータベースクラスタではなく、機能テストのみを対象としています。

これらの3つのノードにはSecure Shell（SSH）キーが設定されており、クラスタ内のノード間でパスワードを設定することなくSSHを使用できます。

NetApp StorageGRID で必要な情報

StorageGRID 上で共有ストレージを使用してオンプレミスにEonモードをインストールするには、次の前提条件情報が必要です。

- StorageGRID S3エンドポイントのIPアドレスまたは完全修飾ドメイン名（FQDN）とポート番号。HTTPSを使用する場合は、StorageGRID S3エンドポイントに実装されているカスタムの認証局（CA）または自己署名SSL証明書を使用します。
- バケット名。このパラメータは、あらかじめ存在し、空である必要があります。
- バケットへの読み取り/書き込みアクセスが可能なアクセスキーIDとシークレットアクセスキー。

S3エンドポイントにアクセスするための認証ファイルを作成します

S3エンドポイントにアクセスする許可ファイルを作成する際には、次の前提条件が適用されます。

- Verticaがインストールされている。
- クラスタをセットアップして設定し、データベースを作成できる状態にします。

S3エンドポイントにアクセスするための認証ファイルを作成するには、次の手順を実行します。

1. 「admintools」を実行してEon Modeデータベースを作成するVerticaノードにログインします。

   デフォルトのユーザーは'dbadmin'で'Verticaクラスタのインストール時に作成されます

2. テキスト・エディタを使用して'/HOME/dbadminディレクトリの下にファイルを作成しますファイル名には'たとえばsg_auth.confなど'任意の名前を指定できます

3. S3エンドポイントが標準のHTTPポート80またはHTTPSポート443を使用している場合は、ポート番号を省略します。HTTPSを使用するには、次の値を設定します。

   ◦ `awsenablehttps=1’それ以外の場合は'0`に値を設定します

   ◦ `awsauth=<s3 access key ID>：<secret access key>`

   ◦ `awsendpoint=< StorageGRID s3 endpoint>:<port>`

   StorageGRID S3エンドポイントのHTTPS接続にカスタムCA証明書または自己署名SSL証明書を使用するには、証明書の完全なファイルパスとファイル名を指定します。このファイルは、各Verticaノード上の同じ場所にあり、すべてのユーザーに読み取り権限が与えられている必要があります。StorageGRID S3エンドポイントのSSL証明書が一般に知られているCAによって署名されている場合は、この手順を省略します。

   -awscafile=<filepath/filename>`

   たとえば、次のサンプルファイルを参照してください。

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

> 本番環境では、一般に知られているCAによって署名されたサーバ証明書をStorageGRID S3ロードバランサエンドポイントに実装する必要があります。

すべての**Vertica**ノードのデポパスを選択します

デポストレージパスの各ノードにディレクトリを選択または作成します。デポストレージパスパラメータに指定するディレクトリには、次のものが必要です。

- クラスタ内のすべてのノードで同じパス（例：/home/dbadmin/depot）
- dbadminユーザによる読み書きが可能になります
- 十分なストレージ

  デフォルトでは、Verticaはデポ保存用のディレクトリを含むファイルシステム領域の60%を使用します。'create-db’コマンドの—depot-size’引数を使用すると、デポのサイズを制限できます。を参照してください "EonモードデータベースのVertica Clusterのサイジング" Verticaの一般的なサイジングガイドラインについては、こちらをご覧ください。Vertica Account Managerにお問い合わせください。

  'admintools create-db’ツールは’存在しない場合に備えて’デポパスを作成しようとします

オンプレミスデータベースの作成

オンプレミスデータベースを作成するには、次の手順を実行します。

1. データベースを作成するには'admintools create-db'ツールを使用します

   この例で使用されている引数の簡単な説明を次に示します。すべての必須引数とオプション引数の詳細については、Verticaのドキュメントを参照してください。

   - -x <で作成された認証ファイルのパス/ファイル名 「S3エンドポイントにアクセスするための認証ファイルの作成」 >。

     認証の詳細は、正常に作成された後、データベース内に保存されます。S3シークレットキーの公開を回避するために、このファイルを削除できます。

   - --son/storagegrid-sstorage -location <s3：//storagegrid bucketname>
   - -s <このデータベースに使用するVerticaノードのカンマ区切りリスト>
   - -d <作成するデータベースの名前>
   - -p <この新しいデータベースに設定するパスワード>。たとえば、次のコマンド例を参照してください。

     ```
     admintools -t create_db -x sg_auth.conf --communal-storage
     -location=s3://vertica --depot-path=/home/dbadmin/depot --shard
     -count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
     '<password>'
     ```

     データベースのノード数によっては、新しいデータベースの作成に数分かかることがあります。データベースを初めて作成するときに、ライセンス契約に同意するように求められます。

たとえば'次のサンプル認証ファイルと'create db'コマンドを参照してください

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1

[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
```

```
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
    Success: package AWS installed
Installing ComplexTypes package
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
    Success: package VFunctions installed
Installing approximate package
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
```

```
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

オブジェクトのサイズ（バイト）	バケット/オブジェクトキーの完全パス
61`	s3://Vertica/051/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a07/026d63ae9d4a33237bf0e2cf2a794a00a0000000000000021a07_00.dfd
145`	s3://Vertica/2c4/026d63ae9d4a33237bf0e2cf2a794a794a794a00000000000000021a3d/026d63ae9d4a33237bf0e2cf2a794a794a00a000000000000021a3_0.dfd
146 `	s3://Vertica/33C/026d63ae9d4a33237bf0e2cf2a794a0000000021a1d/026d63ae9d4a33237bf0e2cf2a794a0000000000021a1d_0.dfd
「40」	s3://Vertica/382/026d63ae9d4a33237bf0e2cf2a794a794a0000000021a31/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a31_0.dfs
145`	s3://Vertica/42f/026d63ae9d4a33237bf0e2cf2a794a794a00000000211/026d63ae9d4a33237bf0e2cf2a794a0000000000000021a_0.dfd
34`	s3://Vertica/472/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a25/026d63ae9d4a33237bf0e2cf2a794a00000000000000021a25_0.df

オブジェクトのサイズ（バイト）	バケット/オブジェクトキーの完全パス
41.	s3://Vertica/476/026d63ae9d4a33237bf0e2cf2a794a794a00000000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000000021a2_0.dfd
61`	s3://Vertica/52A/026d63ae9d4a33237bf0e2cf2a794a794a0000000021a5d/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a5d_0.df
「131」	s3://Vertica/5d2/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a19/026d63ae9d4a33237bf0e2cf2a794a00a0000000000000021a19_0.df
「91」	s3://Vertica/5f7/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a11/026d63ae9d4a33237bf0e2cf2a794a00a00000000000021a11_0.df
「118」	s3://Vertica/82D/026d63ae9d4a33237bf0e2cf2a794a794a0000000021a15/026d63ae9d4a33237bf0e2cf2a794a0000000000000021a15_0.df
「115」	s3://Vertica/922/026d63ae9d4a33237bf0e2cf2a794a794a0000000021a61/026d63ae9d4a33237bf0e2cf2a794a0000000000000021a61_0.df
「33」	s3://Vertica/ACD/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a29/026d63ae9d4a33237bf0e2cf2a794a794a00000000000021a29_0.dfs
「133」	s3://Vertica/b98/026d63ae9d4a33237bf0e2cf2a794a794a00a00000000000021a4d/026d63ae9d4a33237bf0e2cf2a794a794a00a000000000021a4d_0.df
「38」	s3://Vertica/db3/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a49/026d63ae9d4a33237bf0e2cf2a794a00a0000000000000021a49_0.df

オブジェクトのサイズ（バイト）	バケット/オブジェクトキーの完全パス
「38」	`s3://Vertica/eba/026d63ae9d4a33237bf0e2cf2a794a794a000000000021a59/026d63ae9d4a33237bf0e2cf2a794a794a0000000021a59_0.dfdfs.dfs
21521920`	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a0000000000000215e2/026d63ae9d4a33237bf0e2c2cf2a794a000000215e2.tar
6865408`	s3://vertica/metodat/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a0000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00000000000000021602.tar
「204217344」	s3://vertica/metodata/mart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a0000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000000000021610.tar
16109056`	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a0000000000217e0.tar
12853248`	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000000000000000218.tar
「8937984」と入力します	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a00002187a.tar
「56260`606060860」	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a0000000000218b2.tar
「53947904」	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a0000000000219ba.tar

オブジェクトのサイズ（バイト）	バケット/オブジェクトキーの完全パス
44932`608	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a000000000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00000000000000219de.tar
「256306688」	s3://vertica/metadata/VMart/Librarys/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00000000000000021a6e.tar
「8062464`」	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000021e34/026d63ae9d4a33237bf0e2c2cf2a794a00000000000000021e34.tar
「20024832」	s3://vertica/metadata/VMart/Library/Libraryd63ae9d4a33237bf0e2c2cf2a794a00a00000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00000000000000021e70.tar
「10444」	`s3://vertica/metadata/VMart/cluster _config.json
「823266」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checks/C13_13/chkpt_1.cat.gz
「254」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checks/C13_13/Completed
「2958」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C2_2/chkpt_1.cat.gz
231`	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checks/C2_2/Completed
「822521」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checks/C4_4/chkpt_1.cat.gz

オブジェクトのサイズ（バイト）	バケット/オブジェクトキーの完全パス
231`	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checks/C4_4/Completed
746513`	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat
「2596」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz
821065`	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz
6440`	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat
「8518」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat
「 0 」	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922`	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints /Checkpoints /C14-7/chkpt_1.cat.gz
「232」	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints /Checkpoints /C14-7/Completed
822930`	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz

オブジェクトのサイズ（バイト）	バケット/オブジェクトキーの完全パス
755033`	`s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat`
「 0 」	`s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`
822922`	`s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/Checkpoints /C14-7/chkpt_1.cat.gz`
「232」	`s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/Checkpoints /C14-7/Completed`
822930`	`s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz`
755033`	`s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat`
「 0 」	`s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`

ストリーミング制限を無効にしています

この手順 は、他のオンプレミスオブジェクトストレージのVertica guideに基づいており、StorageGRID に適用する必要があります。

1. データベースを作成したら’AWSStreamingConnectionPercentage’設定パラメータを0に設定して無効にしますこの設定は、共同ストレージを使用したオンプレミス環境でのEonモードのインストールには不要です。この設定パラメータは、Verticaがストリーミング読み取りに使用するオブジェクトストアへの接続数を制御します。クラウド環境では、この設定が有効な場合、オブジェクトストアからのストリーミングデータが使用可能なすべてのファイルハンドルを使い使わないようにすることができます。他のオブジェクトストア処理に使用できるファイルハンドルが残っています。オンプレミスのオブジェクトストアのレイテンシが低いため、このオプションは不要です。
2. パラメータ値を更新するには’vsql’文を使用しますパスワードは、「オンプレミスデータベースの作成」で設定したデータベースパスワードです。たとえば、次の出力例を参照してください。

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

デポの設定を確認してい

Verticaデータベースのデフォルトデポ設定は、読み取りおよび書き込み操作に対して有効(値=1)です。パフォーマンスを向上させるために、これらのデポ設定を有効にしておくことを強く推奨します。

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

サンプルデータのロード（オプション）

このデータベースをテスト用に使用し、削除する場合は、サンプルデータをテスト用にこのデータベースにロードできます。Verticaには、各Verticaノードの「/opt/vertica/examples/VMart _Schema/」にあるサンプルデータセットVMartが付属しています。このサンプルデータセットの詳細については、を参照してください "こちらをご覧ください"。

サンプルデータをロードするには、次の手順を実行します。

1. いずれかのVerticaノードにdbadminとしてログインします。cd /opt/vertica/examples/VMart _Schema/
2. サンプルデータをデータベースにロードし、手順cとdでプロンプトが表示されたらデータベースのパスワードを入力します。
   a. 「cd /opt/vertica/examples/VMart _Schema'」と入力します
   b. 「./vmart_gen」
   c. vsql <vmart_define_schema.sql
   d. 「vsql <vmart_load_data.sql」
3. 事前定義された複数のSQLクエリがあります。そのうちの一部を実行して、テストデータがデータベースに正常にロードされたことを確認できます。たとえば、「vsql <vmart_queries1.sql」のようになります

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 11.7製品ドキュメント"

- "StorageGRID データシート"
- "Vertica 10.1製品マニュアル"

バージョン履歴

バージョン	日付	ドキュメントのバージョン履歴
バージョン 1.0 以降	2021年9月	初版リリース

Angela Cheng著_

エルクスタックを使用したStorageGRID ログ分析

Angela Cheng著_

StorageGRID syslog転送機能を使用すると、StorageGRIDログメッセージを収集および分析するように外部syslogサーバを設定できます。エルク（Elasticsearch、Logstash、Kibana）は、最も人気のあるログ分析ソリューションの1つになっています。ELK設定の例と、失敗したS3要求の特定とトラブルシューティングにELKを使用する方法については、を参照して "エルク・ビデオを使用したStorageGRID ログ解析" ください。StorageGRID 11.9では、ロードバランサエンドポイントのアクセスログの外部syslogサーバへのエクスポートがサポートされています。この新機能の詳細については、こちらをご覧 "YouTubeビデオ"ください。この記事では、StorageGRID ログの管理と分析をすばやく開始できるように、Logstashの設定、Kibanaのクエリ、グラフ、およびダッシュボードのサンプルファイルを紹介します。

要件

- StorageGRID 11.6.0.2以降
- Elk（Elasticsearch、Logstash、Kibana）7.1x以降がインストールされており、動作中です

サンプルファイル

- "Logstash 7.xサンプルファイルパッケージをダウンロードします" +*MD5チェックサム*148c23d0021d9a4bb4a6c0287464deab +*SHA256チェックサム*f51ec9e2e3f842d5a7861566b167a561beb4373038b4e7bb3c8be3d522adf2d6
- "Logstash 8.xサンプルファイルパッケージをダウンロードします" *MD5チェックサム*e11bae3a662f87c310ef363d0fe06835* SHA256チェックサム*5c670755742cfdfd5aa723a596ba087e0153a65bcaef3934afdb682f61cd278d
- "StorageGRID 11.9用のLogstash 8.xサンプルファイルパッケージのダウンロード"+* MD5チェックサム* 41272857c4a54600f95995f6ed74800d +* SHA256チェックサム* 67048ee8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

前提条件

読者はStorageGRID およびElkの用語および操作に精通しています。

指示

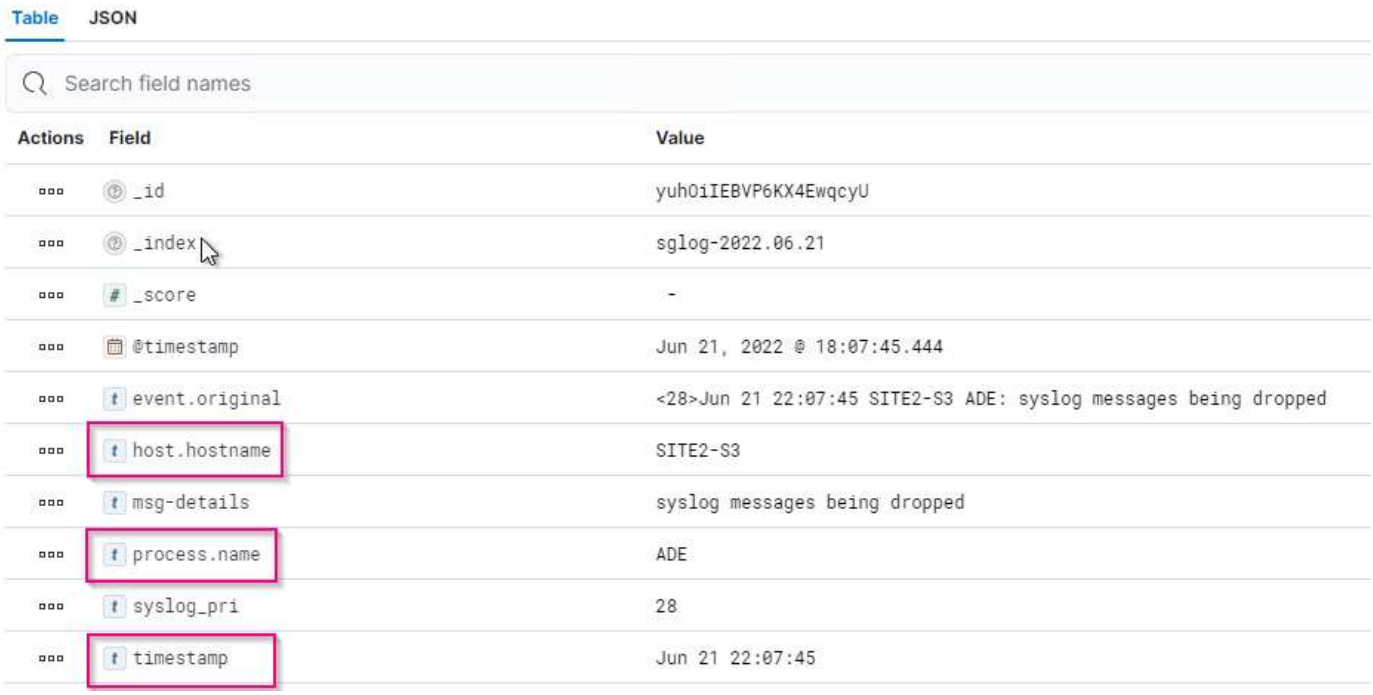
grokパターンで定義される名前の違いにより、2つのサンプルバージョンが提供されます。+たとえば、Logstash設定ファイルのSYSLOGBASE grokパターンでは、インストールされているLogstashのバージョンによってフィールド名が異なります。

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

- Logstash 7.17サンプル*

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

ログスタシュ**8.23**サンプル



- 手順 *

1. インストールされているエルクバージョンに基づいて、提供されたサンプルを解凍します。サンプル・フォルダには'Logstash configサンプルが2つ含まれています**sglog-2-file.conf :**この構成ファイルは'データ変換を行わずに**Logstash**上のファイルに**StorageGRID** ログ・メッセージを出力しますこの機能を使用すると、**Logstash**が**StorageGRID** メッセージを受信していることを確認したり、**StorageGRID** ログパターンを理解したりできます。**+** sglog-2-es.conf：*この構成ファイルは、さまざまなパターンやフィルタを使用してStorageGRID ログメッセージを変換します。この例には、パターンまたはフィルタに基づいてメッセージをドロップするDROPステートメントが含まれています。インデックスを作成するために出力がElasticsearchに送信されます。+ファイル内の指示に従って、選択した構成ファイルをカスタマイズします。
2. カスタマイズした構成ファイルをテストします。

```
/usr/share/logstash/bin/logstash --config.test_and_exit -f <config-file-path/file>
```

返される最後の行が次の行に似ている場合、構成ファイルに構文エラーはありません。

```
[LogStash::Runner] runner - Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
```

3. カスタマイズされたconfファイルをLogstashサーバのconfig:/etc/logstash/conf.d+にコピーします/etc/logstash/logstash.ymlでconfig.reload.automaticを有効にしていない場合は'Logstashサービスを再起動しますそれ以外の場合は、設定のリロード間隔が経過するのを待ちます。

```
 grep reload /etc/logstash/logstash.yml
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

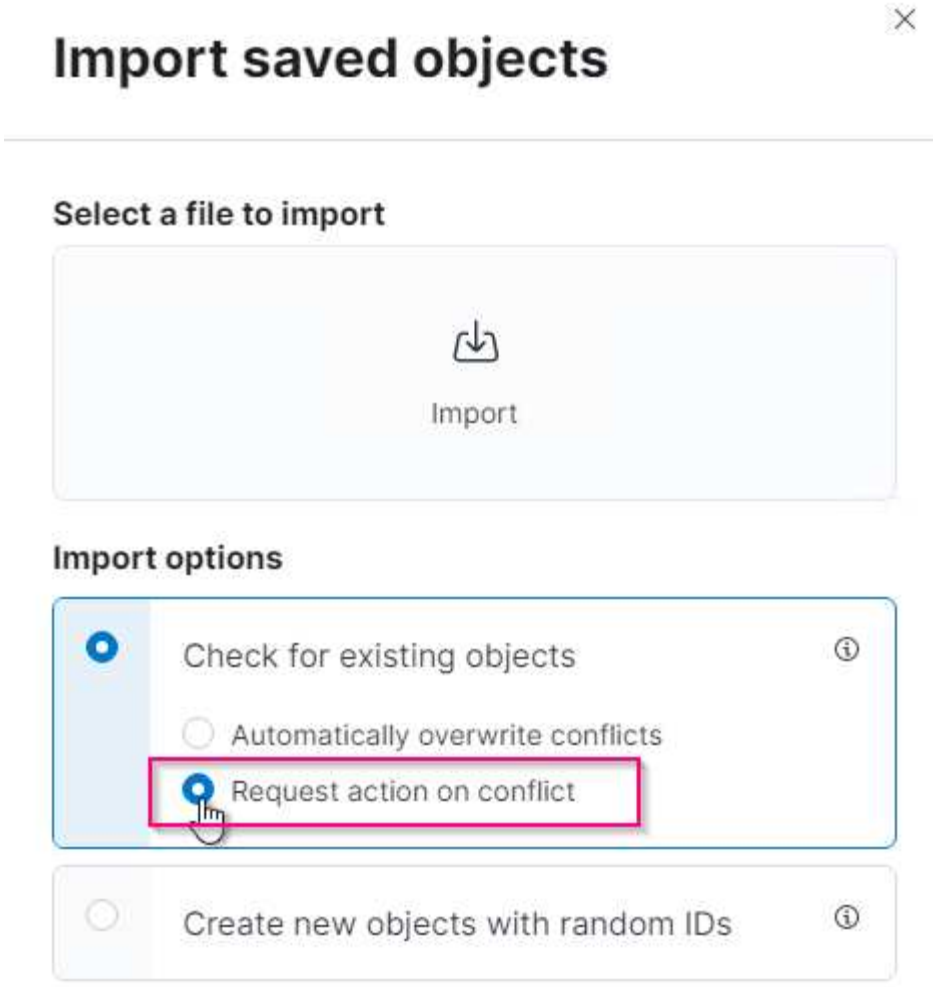
4. /var/log/logstash/logstash-plain.logを確認し、Logstashを新しい設定ファイルで起動する際にエラーがないことを確認します。
5. TCPポートが開始され、リスンしていることを確認する。+この例では、TCPポート5000が使用されています。

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

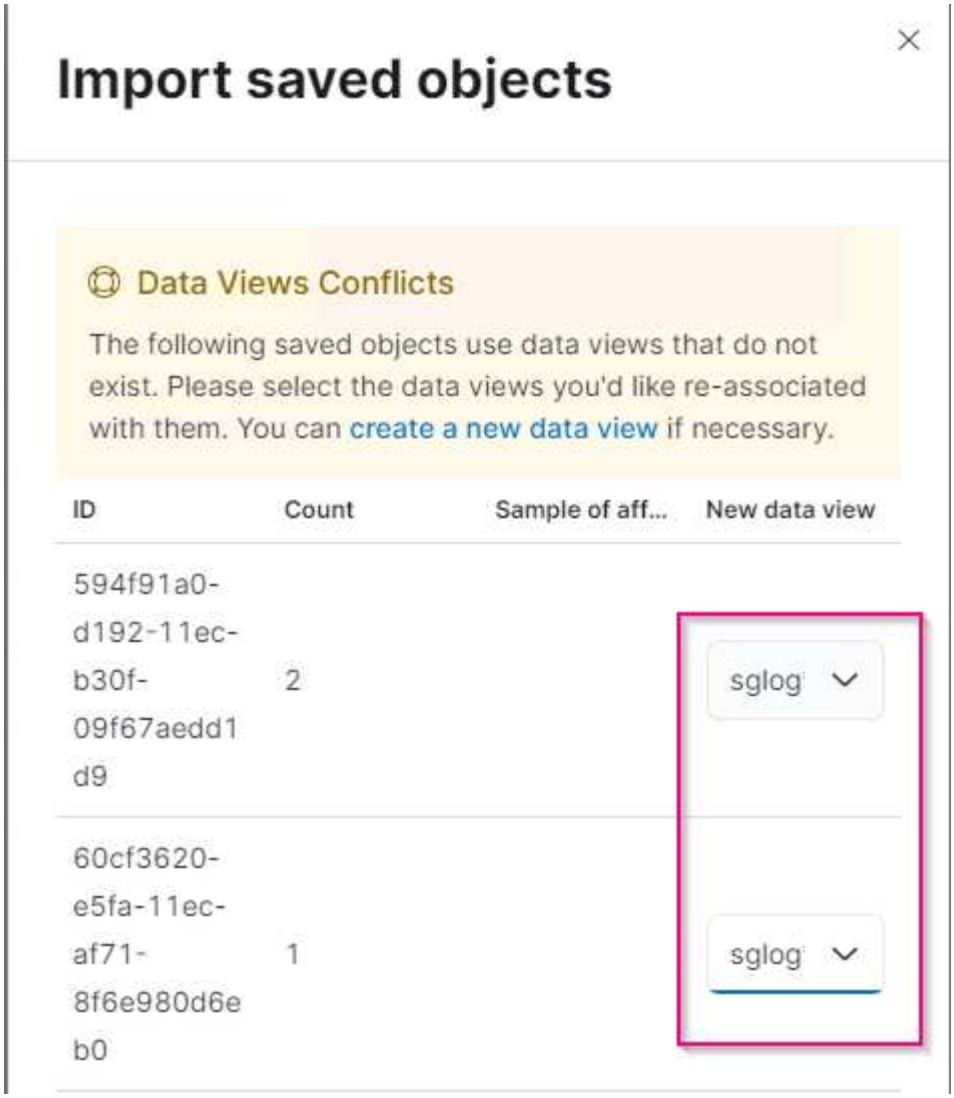
6. StorageGRID マネージャGUIから、ログメッセージをLogstashに送信するように外部syslogサーバを設定します。詳細については、を参照して "デモビデオ" ください。
7. 定義されたTCPポートへのStorageGRID ノード接続を許可するには、Logstashサーバ上でファイアウォールを設定または無効にする必要があります。
8. Kibana GUIから、[Management]→[Dev Tools]を選択します。Consoleページで、次のgetコマンドを実行して、Elasticsearch上に新しいインデックスが作成されていることを確認します。

```
GET /_cat/indices/*?v=true&s=index
```

9. Kibana GUIから、索引パターン（Elk 7.x）またはデータビュー（Elk 8.x）を作成します。
10. Kibana GUIから、上部中央にある検索ボックスに「saved objects」と入力します。+[保存済みオブジェクト]ページで、[インポート]を選択します。[インポートオプション]で、[競合時にアクションを要求]を選択します。



elk <version>-query-chart-sample.ndjsonをインポートします。+競合を解決するよう求められたら、手順8で作成したインデックスパターンまたはデータビューを選択します。



次のKibanaオブジェクトがインポートされます。* Query ** audit-msg-s3rq-orlm * bycastログs3関連メッセージ* loglevel warning以上+* failed security event * nginx-gwエンドポイントアクセスログ（elk8-sample-for-sg119.zipでのみbycast.log使用可能）* Chart **リクエストタイプ別***+*ダッシュボードリクエストの平均応答時間

これで、Kibanaを使用してStorageGRID ログ分析を実行する準備ができました。

その他のリソース

- "syslog101"
- "エルクスタックとは何ですか"
- "grokパターンリスト"
- "初心者向けのLogstashガイド: Grok"
- "ログスタシュの実践的なガイド：syslogの詳細"
- "Kibanaガイド–ドキュメントを参照してください"
- "StorageGRID 監査ログメッセージリファレンスです"

PrometheusとGrafanaを使用して指標の保持を拡張します

アロンクライン著

この技術レポートでは、外部の Prometheus および Grafana サービスを使用してNetApp StorageGRID を構成するための詳細な手順を説明します。

はじめに

StorageGRID は、Prometheusを使用して指標を保存し、組み込みのGrafanaダッシュボードでこれらの指標を視覚化します。Prometheus指標には、クライアントアクセス証明書を設定し、指定されたクライアントのPrometheusアクセスを有効にすることで、StorageGRID から安全にアクセスできます。現在、この指標データの保持期間は管理ノードのストレージ容量によって制限されています。これらの指標のカスタマイズされた可視化を実現するために、新しいPrometheusサーバとGrafanaサーバを導入し、新しいサーバでStorageGRIDWebscaleインスタンスから指標をスクラビングするように設定し、重要な指標を使用したダッシュボードを構築します。で収集されたPrometheus指標の詳細を確認できます "StorageGRID のドキュメント"。

Prometheusをフェデレーションする

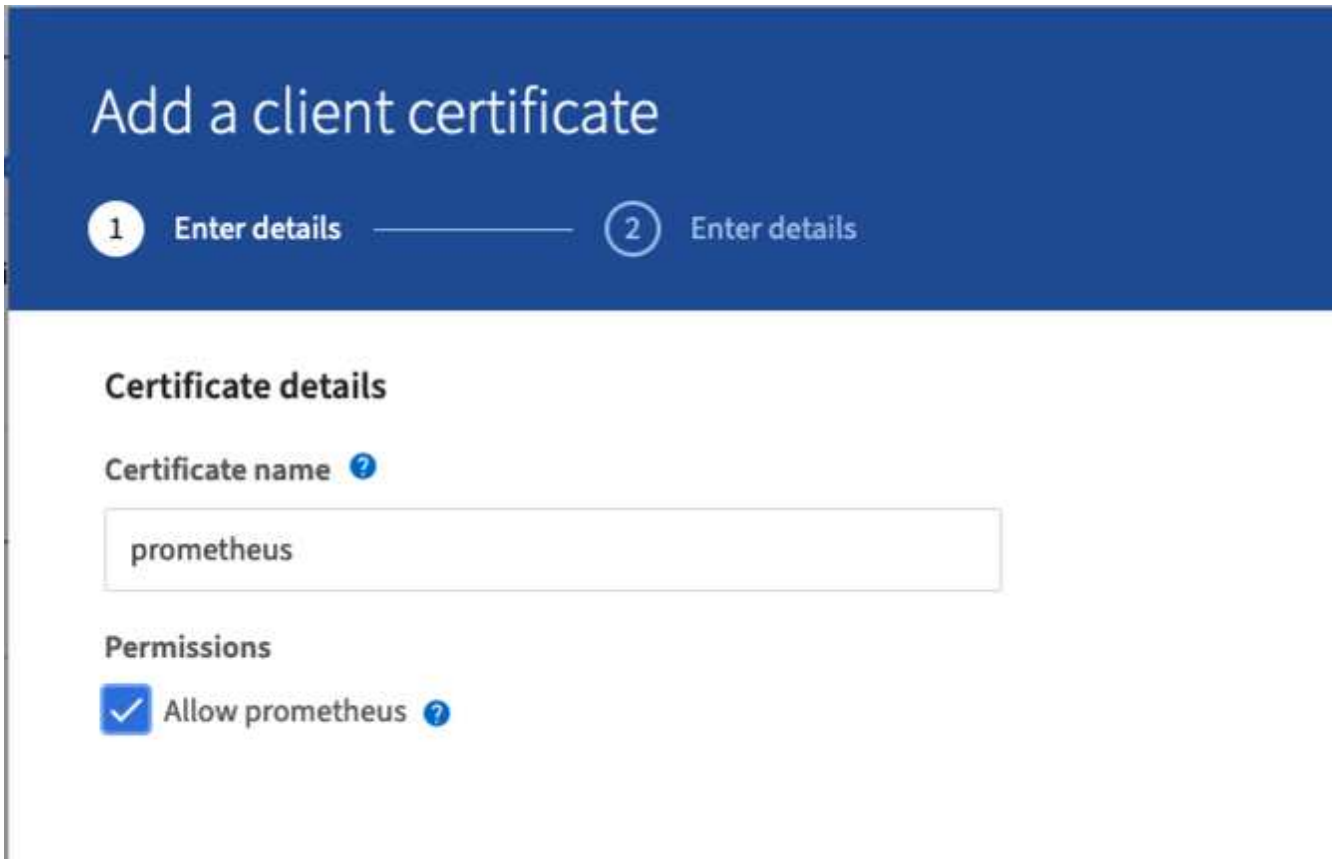
ラボの詳細

この例では、StorageGRID 11.6ノードとDebian 11サーバのすべての仮想マシンを使用します。StorageGRID管理インターフェイスには、公開されている信頼されたCA証明書が設定されています。この例では、StorageGRID システムやDebian Linuxのインストールと設定は行われません。PrometheusとGrafanaでサポートされている、任意のLinuxフレーバーを使用できます。PrometheusとGrafanaはどちらも、Dockerコンテナ、ソースからビルド、またはコンパイル済みのバイナリとしてインストールできます。この例では、PrometheusバイナリとGrafanaバイナリの両方を同じDebianサーバに直接インストールします。から基本的なインストール手順をダウンロードして実行します https://prometheus.io および https://grafana.com/grafana/ それぞれ。

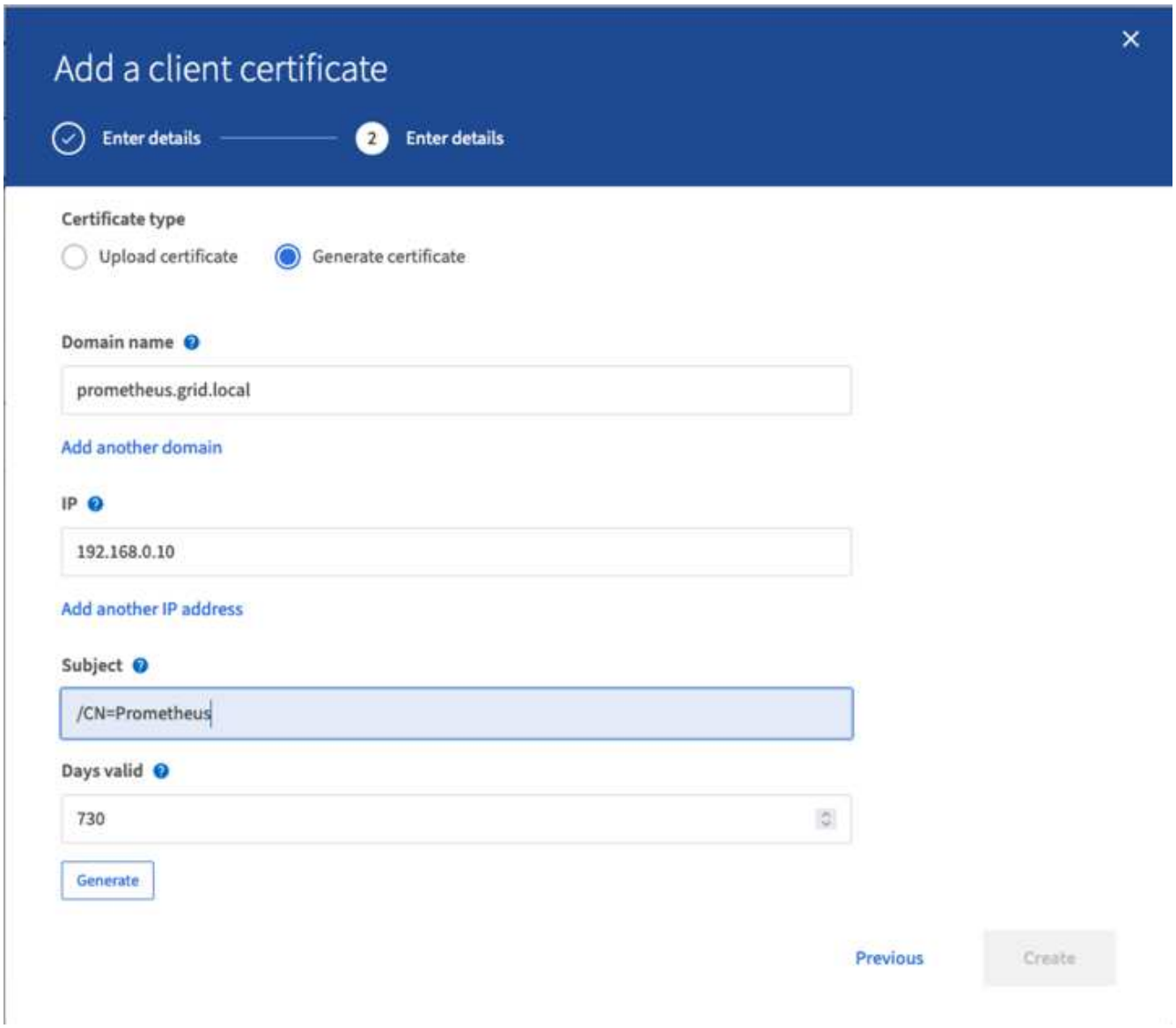
Prometheusクライアントアクセス用にStorageGRID を設定する

StorageGRID IDに格納されているPrometheus指標にアクセスするには、秘密鍵を使用してクライアント証明書を生成またはアップロードし、クライアントの権限を有効にする必要があります。StorageGRID 管理インターフェイスにはSSL証明書が必要です。この証明書は、信頼されたCAによってPrometheusサーバによって信頼されているか、自己署名されている場合は手動で信頼されている必要があります。詳細については、を参照してください "StorageGRID のドキュメント"。

1. StorageGRID 管理インターフェイスの左下にある「configuration」を選択し、2番目の列にある「Security」で「Certificates」をクリックします。
2. [証明書]ページで[クライアント]タブを選択し、[追加]ボタンをクリックします。
3. アクセスを許可するクライアントの名前を指定し、この証明書を使用します。「Allow Prometheus」の前の「Permissions」のボックスをクリックし、「Continue」ボタンをクリックします。

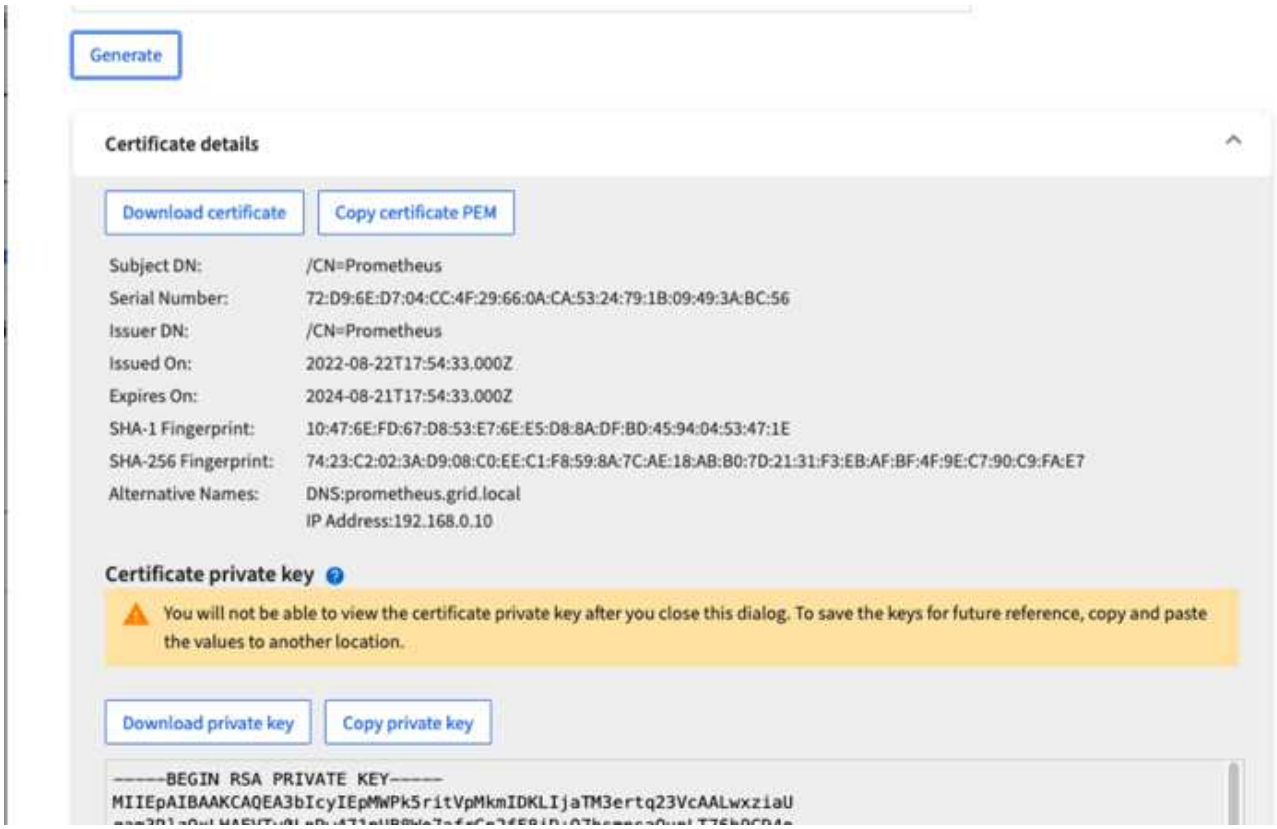


4. CA署名証明書がある場合は、[証明書のアップロード]のラジオボタンを選択できますが、この場合は、[証明書の生成]のラジオボタンを選択して、StorageGRID がクライアント証明書を生成できるようにします。入力する必須フィールドが表示されます。クライアントサーバのFQDN、サーバのIP、件名、有効日数を入力します。「生成」ボタンをクリックします。



> Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. 証明書のPEMファイルと秘密鍵のPEMファイルをダウンロードします。



> This is the only time you can download the private key, so make sure you do not skip this step.

Linuxサーバで**Prometheus**インストールを準備

Prometheusをインストールする前に、Prometheusユーザとディレクトリ構造を使用して環境を準備し、指標の格納場所の容量を設定します。

1. Prometheusユーザを作成します。

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. Prometheus、クライアント証明書、指標データのディレクトリを作成します。

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. 私はext4ファイルシステムでのメトリック保持のために使用するディスクをフォーマットしました。

```
mkfs -t ext4 /dev/sdb
```

4. そのあと、Prometheusのmetricsディレクトリにファイルシステムをマウントしました。

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. 指標データに使用するディスクのUUIDを取得します。

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. /etc/fstabにエントリを追加してマウントをリブート後も/dev/sdbのUUIDを使用して維持するようにします。

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

Prometheusをインストールして設定する

これでサーバの準備ができました。Prometheusのインストールを開始して、サービスを設定できます。

1. Prometheusインストールパッケージを展開します

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. バイナリを/usr/local/binにコピーし、前の手順で作成したPrometheusユーザに所有権を変更します

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. コンソールとライブラリを/etc/Prometheusにコピーします

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. 以前にStorageGRID からダウンロードしたクライアント証明書と秘密鍵のPEMファイルを/etc/prometheus/certsにコピーします
5. Prometheus設定YAMLファイルを作成します

```
sudo nano /etc/prometheus/prometheus.yml
```

6. 次の構成を挿入します。ジョブ名には、任意の名前を指定できます。「-targets：[']]」を管理ノードのFQDNに変更し、証明書と秘密鍵のファイル名を変更した場合は、tls_configセクションを更新して一致させてください。次に、ファイルを保存します。グリッド管理インターフェイスで自己署名証明書を使用している場合は、証明書をダウンロードして一意の名前のクライアント証明書に格納し、tls_configセクションadd ca_file：/etc/prometheus/cert/UIcert.pemに格納します

   a. この例では、alertmanager、cassandra、node、およびStorageGRID で始まるすべての指標を収集しています。Prometheus指標の詳細については、を参照してください "StorageGRID のドキュメント"。

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

グリッド管理インターフェイスで自己署名証明書が使用されている場合は、証明書をダウンロードして一意の名前でクライアント証明書に格納します。tls_configセクションで、クライアント証明書と秘密鍵の行の上に証明書を追加します

```
        ca_file: /etc/prometheus/cert/UIcert.pem
```

1. Prometheus内のすべてのファイルとディレクトリの所有権と、/var/lib/prometPrometheusユーザへの所有権を変更する

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. /etc/systemd/systemにPrometheusサービスファイルを作成します

```
sudo nano /etc/systemd/system/prometheus.service
```

3. 次の行を挿入します。--storage.tsd.dretention.time=1y#というメトリックデータの保持期間を1年にします。また、ストレージの制限に基づいて保持期間を設定する場合も、--storage.tsdb.retentionsize=300GiB#を使用することもできます。指標の保持を設定できるのは、この場所だけです。

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. システムdサービスをリロードして新しいPrometheusサービスを登録します。その後、Prometheusサービスを開始して有効にします。

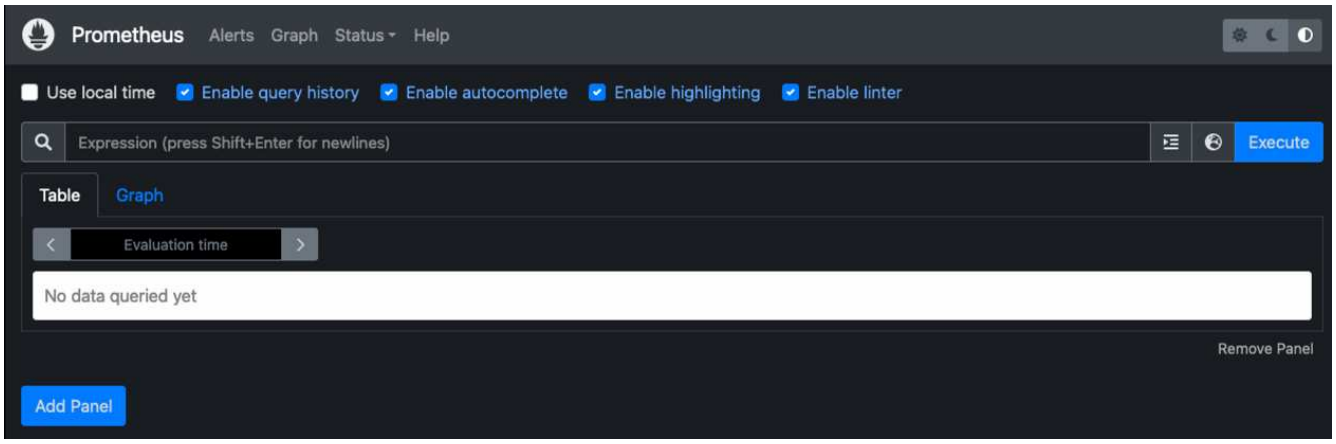
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. サービスが正常に実行されていることを確認します

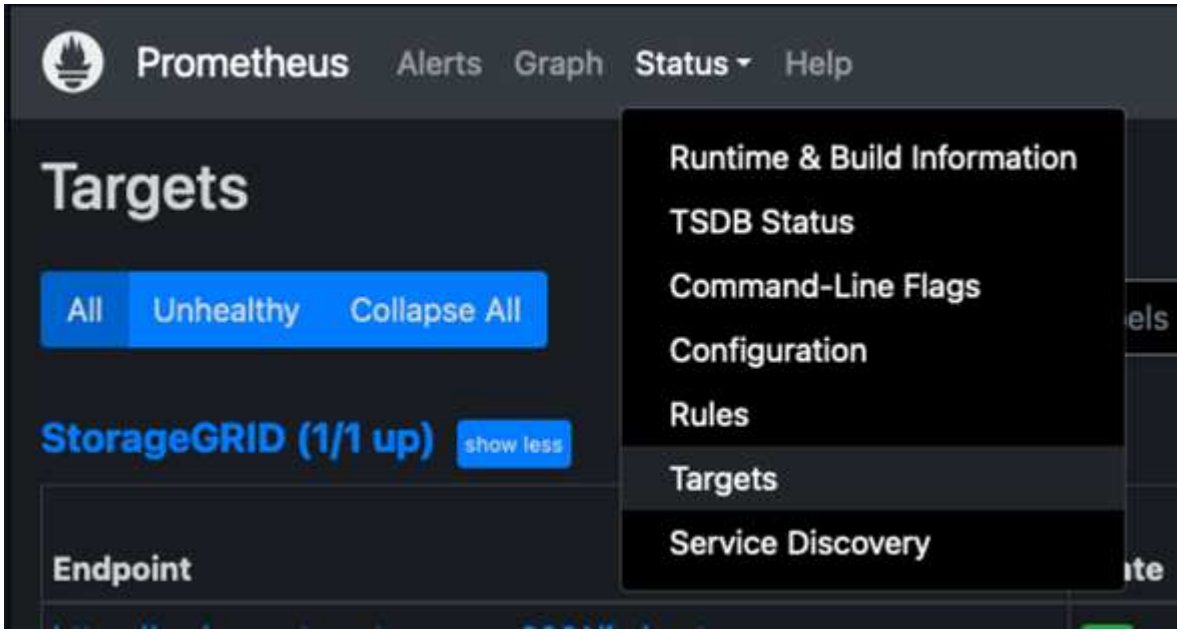
```
sudo systemctl status prometheus
```

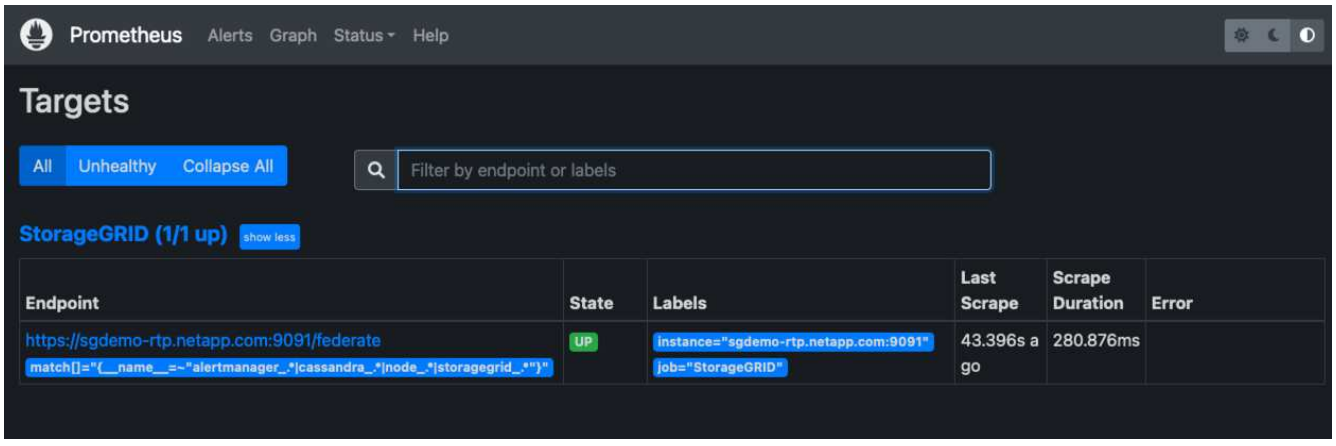
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. PrometheusサーバのUIにアクセスできるようになります http://Prometheus-server:9090 およびUIを参照してください

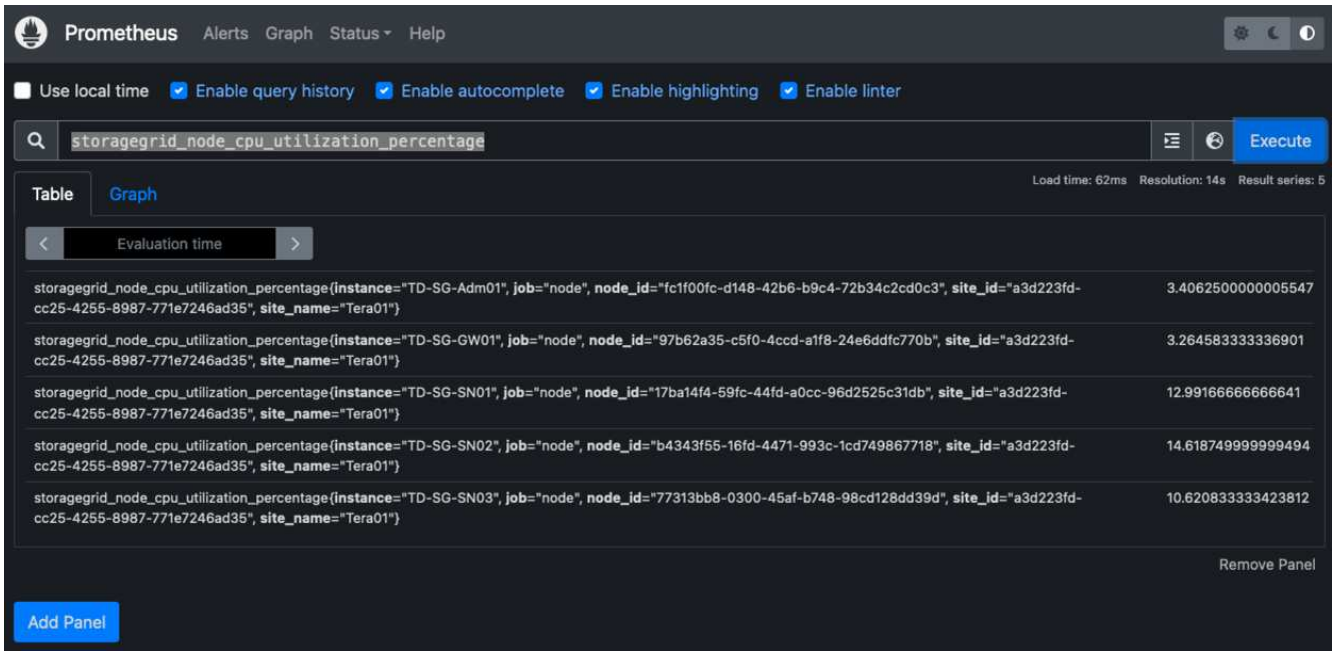


7. 「Status」ターゲットのPrometheusで設定したStorageGRID エンドポイントのステータスを確認できます





8. [グラフ]ページで、テストクエリを実行し、データが正常にスクレイピングされていることを確認できます。たとえば、クエリバーに「storagegrid_node_name utilization _percentage」と入力し、実行ボタンをクリックします。



Grafanaをインストールして設定します

Prometheusがインストールされて機能したので、Grafanaのインストールとダッシュボードの設定に進みます

Grafanaの分析

1. Grafanaの最新のエンタープライズエディションをインストールします

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. 安定版リリース用に次のリポジトリを追加します。

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. リポジトリを追加した後。

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. systemdサービスをリロードして新しいgrafanaサービスを登録します。次に、Grafanaサービスを開始して有効にします。

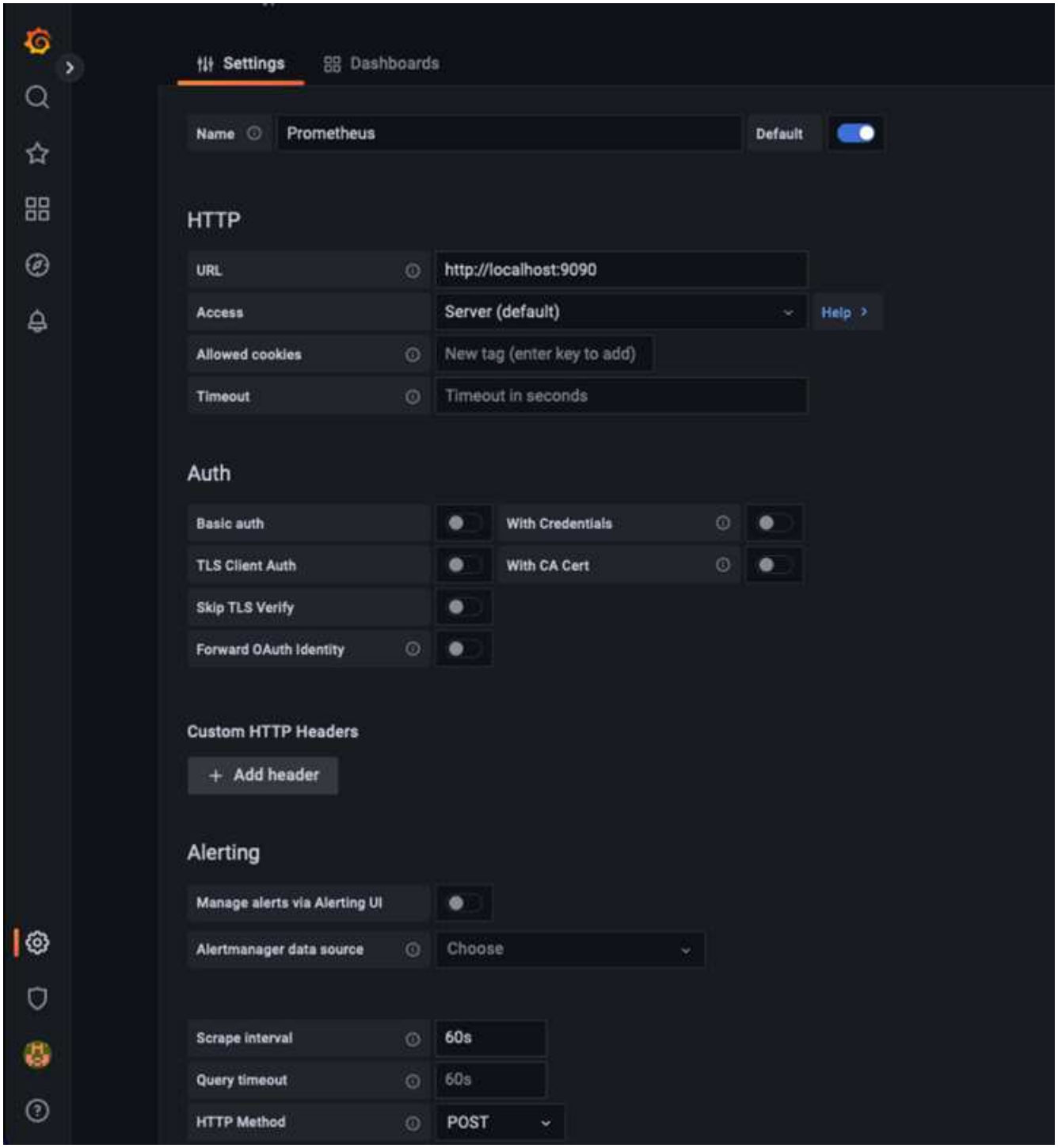
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafanaがインストールされて実行されるようになりました。ブラウザでHTTP：//prometheus-server：3000にアクセスすると、Grafanaのログインページが表示されます。
6. デフォルトのログインクレデンシャルはadmin / adminであり、新しいパスワードを要求されたときに設定する必要があります。

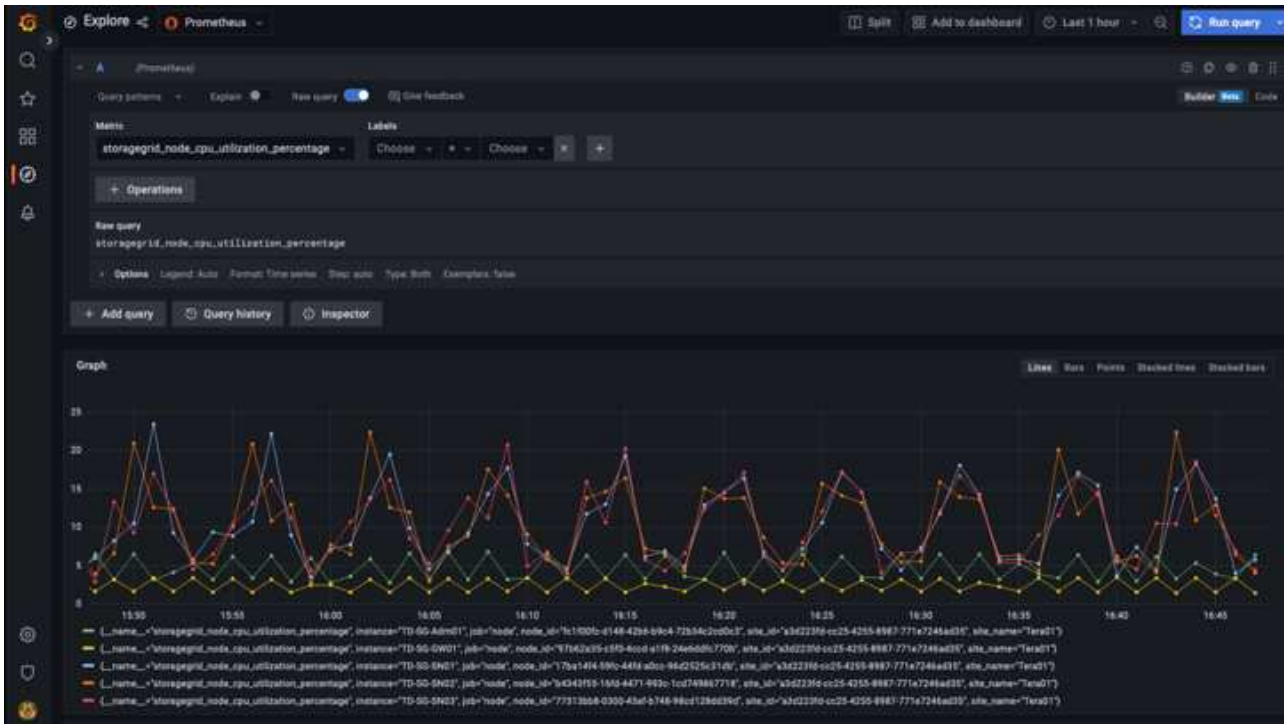
StorageGRID に対応した**Grafana**ダッシュボードを作成します

GrafanaとPrometheusがインストールされて実行されている状態で、データソースを作成してダッシュボードを構築することで、この2つを接続する時間が発生します

1. 左側のペインで[構成]を展開し、[データソース]を選択して、[データソースの追加]ボタンをクリックします
2. Prometheusは、最も人気のあるデータソースの1つです。検出されていない場合は、検索バーで「Prometheus」を特定します。
3. PrometheusインスタンスのURLとスクラビング間隔をPrometheusの間隔と一致するように入力して、Prometheusソースを設定します。Prometheusでアラートマネージャを設定しなかったため、アラートセクションも無効にしました。



4. 目的の設定を入力したら、下にスクロールして[保存してテスト]をクリックします。
5. 設定テストが正常に完了したら、[EXPLOR]ボタンをクリックします。
   a. 「調査」ウィンドウで、Prometheusで「storagegrid_node_name」に対してテストしたものと同じ指標を使用し、「Run query」ボタンをクリックします

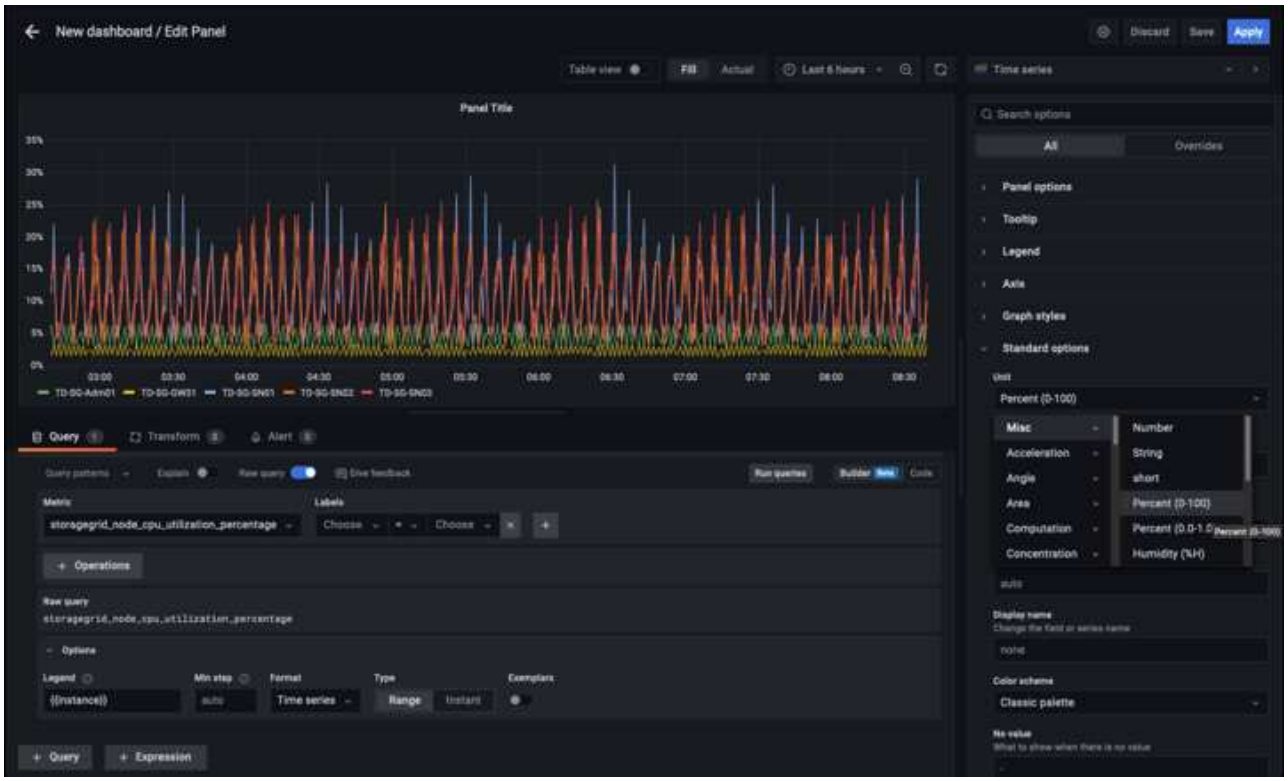


6. データソースを設定したら、ダッシュボードを作成します。

   a. 左側のペインで[ダッシュボード]を展開し、[+新しいダッシュボード]を選択します。

   b. 「新規パネルを追加」を選択します。

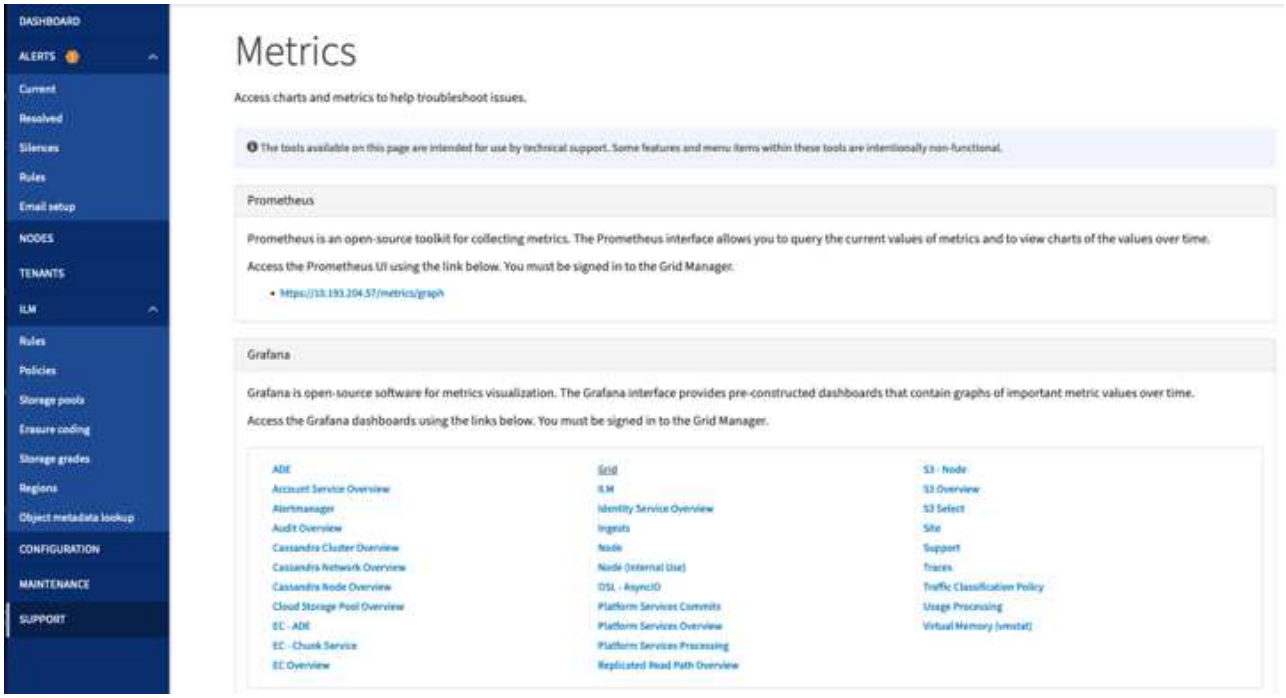
   c. メトリックを選択して新しいパネルを設定します。もう一度「storagegrid_node_name」を使用し、パネルのタイトルを入力し、下部に「Options」を展開して凡例をカスタムに変更し、「｛｛instance｝｝」と入力してノード名を定義します。右側のペインの「Standard options」set "Unit」を「Misc-100%」に設定します。[適用]をクリックして、パネルをダッシュボードに保存します。



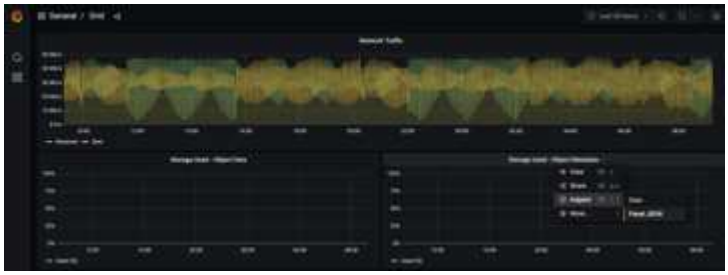
7. 必要な指標ごとにこのようなダッシュボードを構築し続けることもできますが、幸運にも、StorageGRIDにはダッシュボードがすでに用意されており、カスタムダッシュボードにコピーすることができます。

   a. StorageGRID 管理インターフェイスの左側のペインで、[サポート]を選択し、[ツール]列の下部にある[指標]をクリックします。

   b. 指標内で、中央の列の上部にある「グリッド」リンクを選択します。

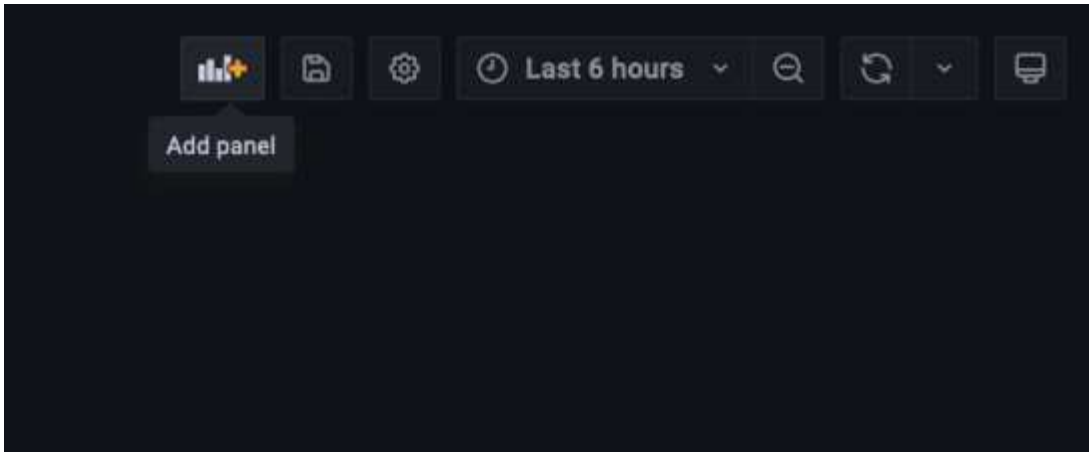


   c. グリッドダッシュボードで、「Storage Used - Object Metadata」パネルを選択します。メニューをドロップダウンするには、パネルタイトルの小さな下向き矢印と末尾をクリックします。このメニューから「Inspect」と「Panel JSON」を選択します。



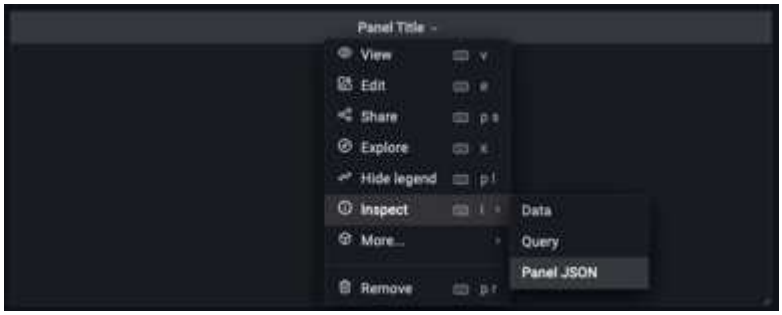
   d. JSONコードをコピーしてウィンドウを閉じます。

e. 新しいダッシュボードで、アイコンをクリックして新しいパネルを追加します。

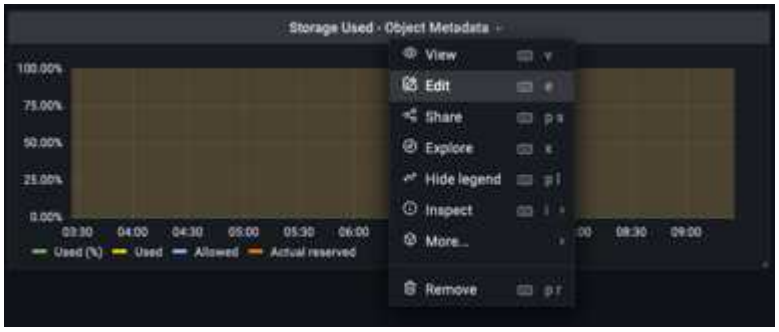


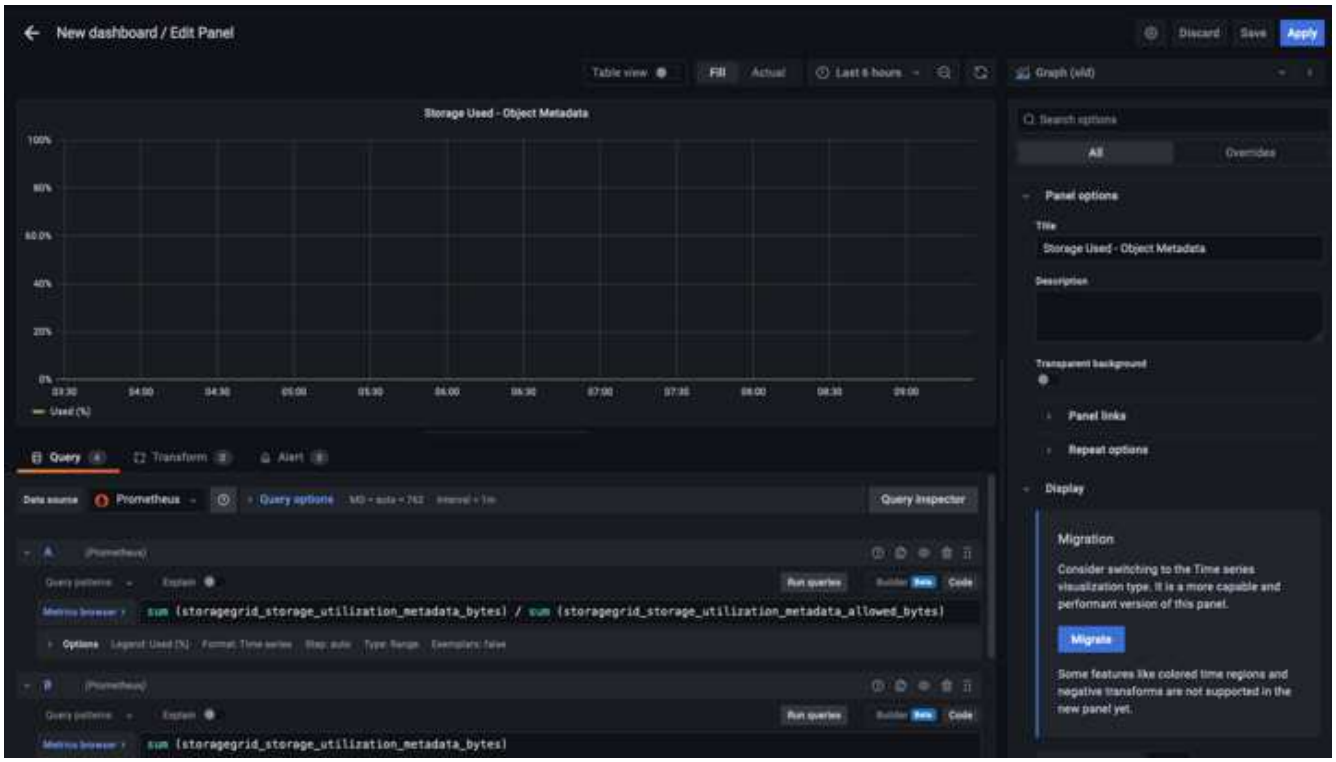
f. 変更を加えずに新しいパネルを適用します

g. StorageGRID パネルと同様に、JSONを確認します。JSONコードをすべて削除し、StorageGRID パネルからコピーしたコードに置き換えます。



h. 新しいパネルを編集すると、右側に「移行」ボタンを含む移行メッセージが表示されます。ボタンをクリックして、[適用]ボタンをクリックします。





8. すべてのパネルを所定の位置に配置し、必要に応じて構成したら、右上のディスクアイコンをクリックしてダッシュボードを保存し、名前を付けます。

まとめ

カスタマイズ可能なデータ保持機能とストレージ容量を備えたPrometheusサーバを導入しました。そのため、運用に最も関連性の高い指標を使用して独自のダッシュボードを構築し続けることができます。で収集されたPrometheus指標の詳細を確認できます "StorageGRID のドキュメント"。

F5 DNSを使用してStorageGRIDのグローバル負荷分散を行う

スティーブ・ゴーマン（*F5*）

この技術レポートでは、グリッドが複数のサイトや HA グループに分散されている場合に、グローバル ロード バランシング用の F5 DNS サービスを使用してNetApp StorageGRID を構成し、データの可用性と一貫性を高め、S3 トランザクション ルーティングを最適化するための詳細な手順を説明します。

はじめに

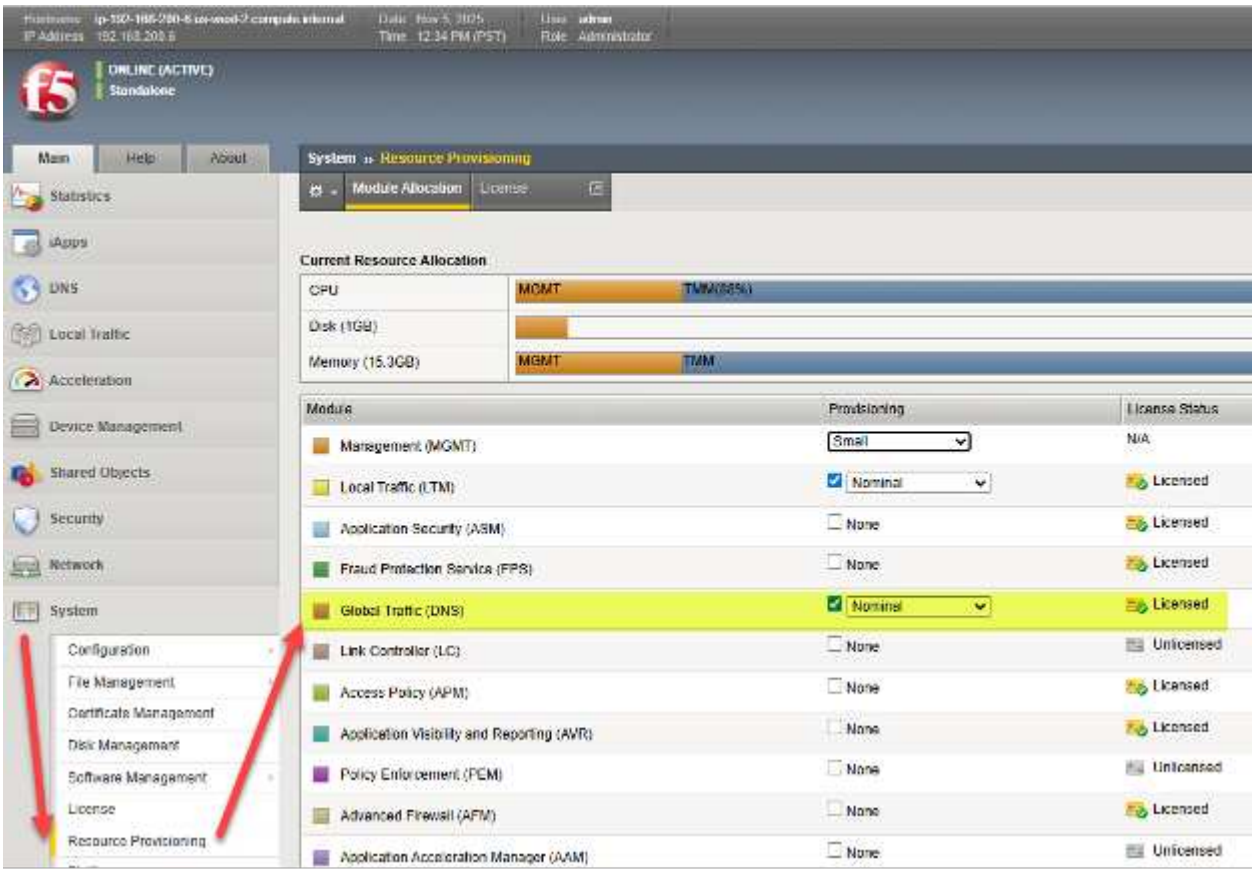
以前は BIG-IP GTM (Global Traffic Manager)、非公式には GSLB (Global Server Load Balancing) と呼ばれていた F5 BIG-IP DNS ソリューションは、複数のアクティブ/アクティブ HA グループおよびアクティブ/アクティブ マルチサイトStorageGRIDソリューション間でのシームレスなアクセスを効果的に実現します。

F5 BIG-IP マルチサイトStorageGRID構成

サポートされるStorageGRIDサイトの数に関係なく、少なくとも 2 台の BIG-IP アプライアンス (物理または仮想) で BIG-IP DNS モジュールが有効になっていて、設定されている必要があります。DNS アプライアンスの数が増えるほど、企業が享受できる冗長性の度合いが高まります。

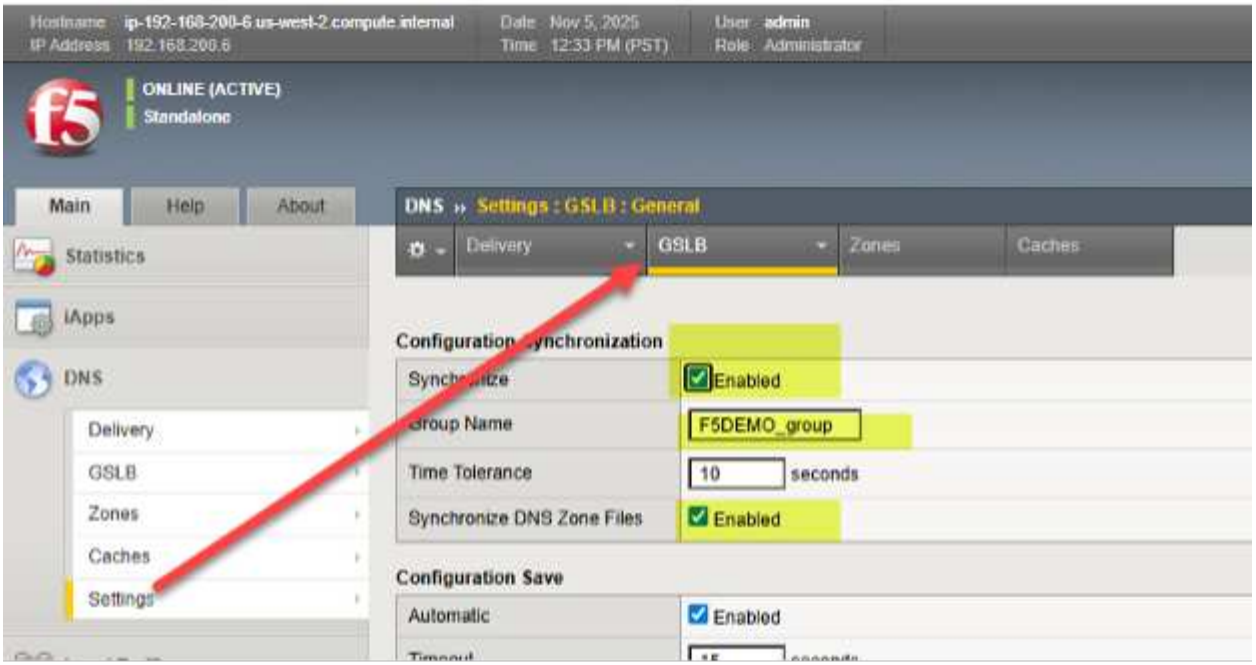
BIG-IP DNS - 初期設定の最初の手順

BIG-IP アプライアンスで少なくとも初期プロビジョニングが完了したら、Web ブラウザを使用して TMUI (BIG-IP GUI) インターフェイスにログインし、[システム] → [リソース プロビジョニング] を選択します。強調表示されているように、「グローバル トラフィック (DNS)」モジュールにチェック マークが付いており、ライセンスが付与されていることを確認します。なお、画像のように、「ローカル トラフィック (LTM)」を同じアプライアンスでプロビジョニングできるのが一般的です。

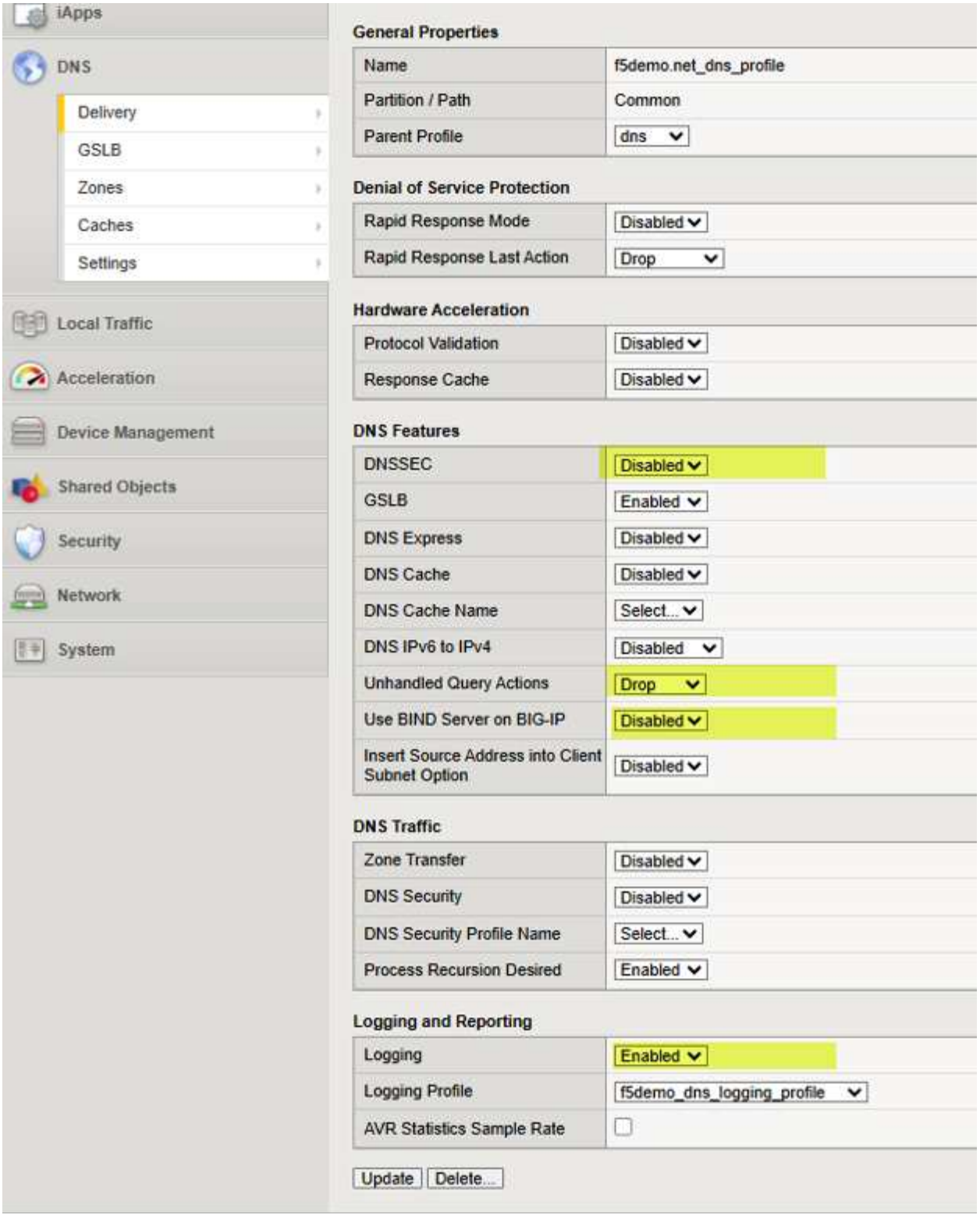


DNSプロトコルの基本要素を構成する

StorageGRIDサイトのグローバル トラフィック管理に向けた最初のステップは、ほぼすべてのグローバル トラフィック ステアリングが構成される DNS タブを選択し、[設定] → [GLSB] を選択することです。2 つの同期オプションを有効にし、参加している BIG-IP アプライアンス間で共有される DNS グループ名を選択します。



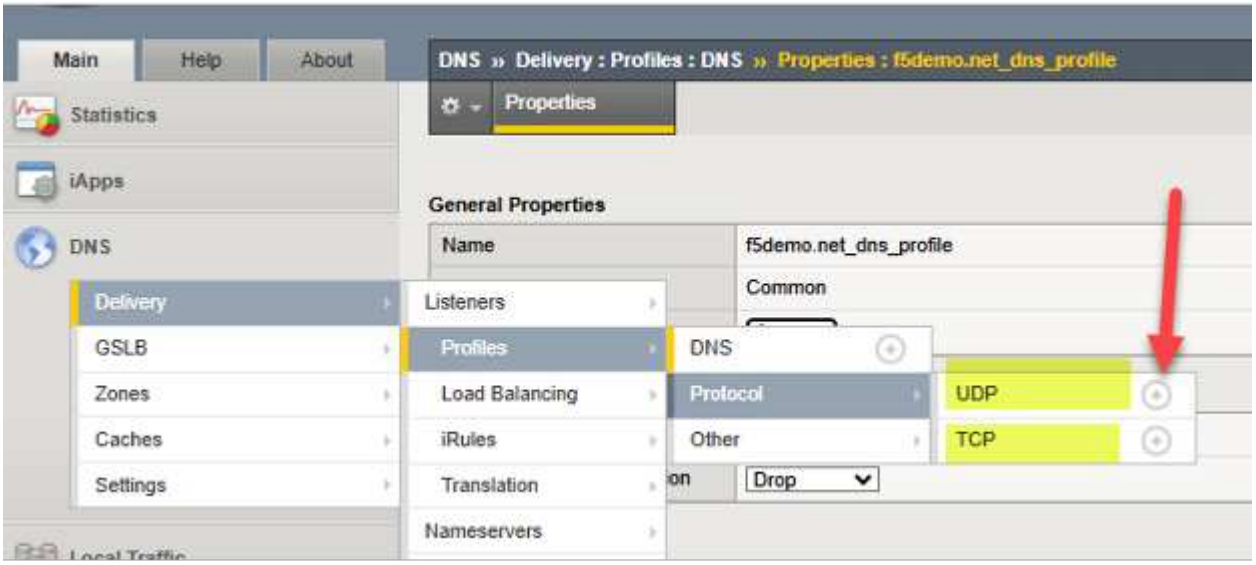
次に、「DNS」>「配信」>「プロファイル」>「DNS: 作成」に移動し、有効または無効にする DNS 機能を管理するプロファイルを作成します。特定の DNS ログの生成に興味がある場合は、前のリンクの DNS クラスルーム ガイドを参照してください。以下は動作中の DNS プロファイルの例です。重要な値の設定を表す 4 つのハイライト部分に注目してください。それぞれの設定については、以下のF5 KB（ナレッジベース）の記事で説明されています。 "こちらをご覧ください"。



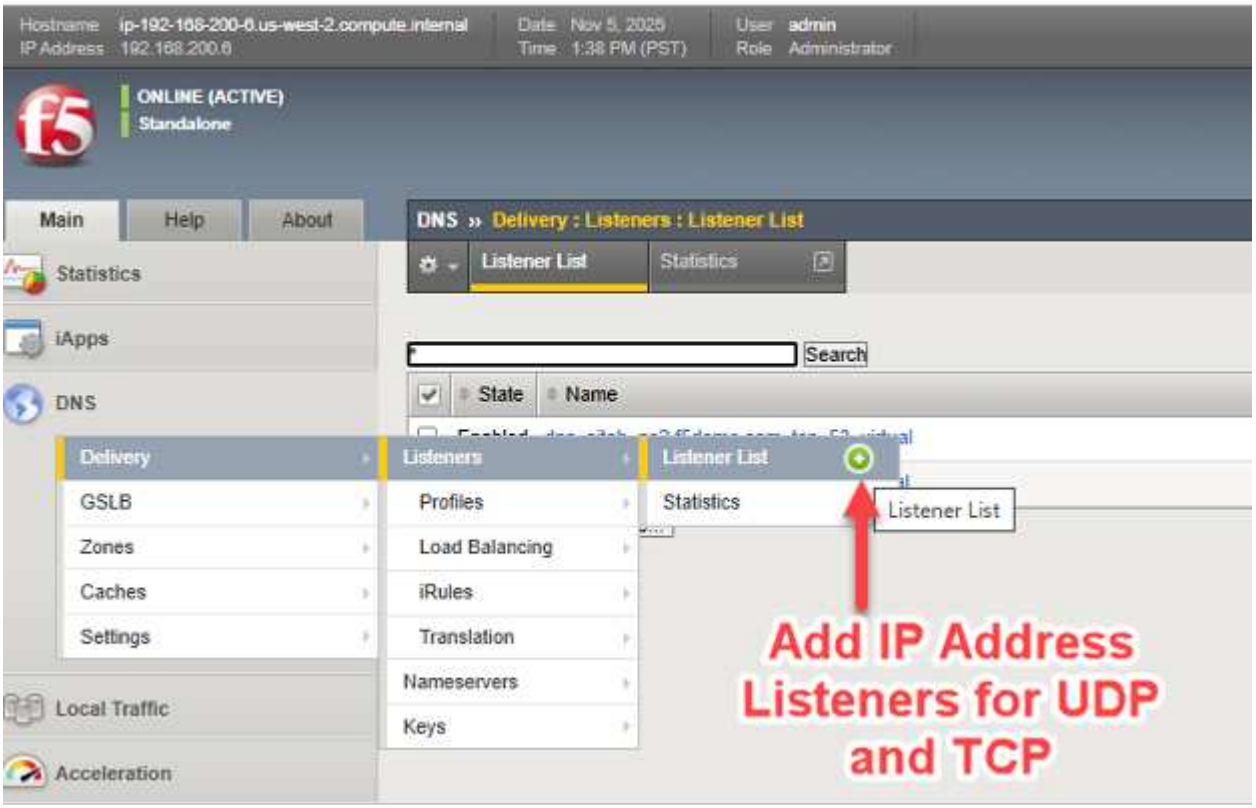
この時点で、作成された「プロファイル」を通じて UDP プロトコルと TCP プロトコルの特性を調整できます。これらのプロファイルはどちらも BIG-IP を含む DNS トラフィックを伝送できます。UDP と TCP 用の新しいプロファイルを 1 つ作成するだけです。DNS トラフィックが WAN リンクを通過すると仮定すると、WAN 環境で適切に動作することがわかっている UDP と TCP の特性を継承するのが良い方法です。それぞれを追加するには、各プロトコルの横にある「+」アイコンをクリックし、親プロファイルを次のように設定します。

UDP → 「親」プロファイル「udp_gtm_dns」を使用する

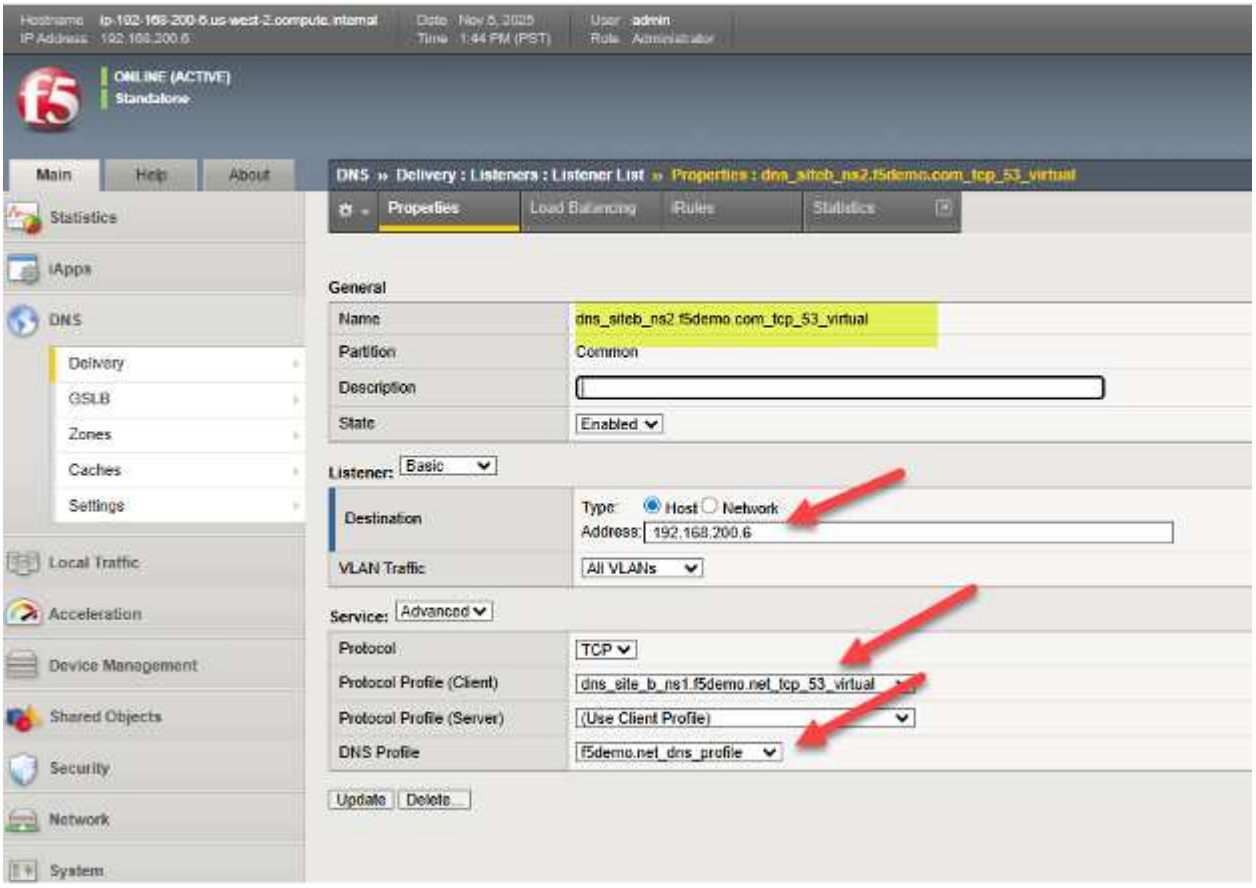
TCP → 「親」プロファイル「f5-tcp-wan」を使用する



ここで、BIG-IP DNS が関与する UDP トラフィックと TCP トラフィックの両方に IP アドレスを割り当てる必要があります。BIG-IP LTM に精通している方にとって、これは基本的に DNS 仮想サーバーの作成であり、仮想サーバーには「リスナー」 IP アドレスが必要です。スクリーンショットのように、矢印に従って DNS/UDP および DNS/TCP のリスナー/仮想サーバーを作成します。



以下はライブ BIG-IP DNS の 1 つの例です。この例では、TCP 仮想サーバー リスナーの設定が表示され、これまでの多くの手順がどのように結び付けられているかがわかります。これには、DNS プロファイルとプロトコル (TCP) プロファイルの参照、および DNS が使用する有効な IP アドレスの構成が含まれます。BIG-IP で作成するすべてのオブジェクトと同様に、割り当てられた名前の例では dns/siteb/TCP53 のように、オブジェクトが何であるかを自己識別するのに役立つ意味のある名前を使用すると便利です。



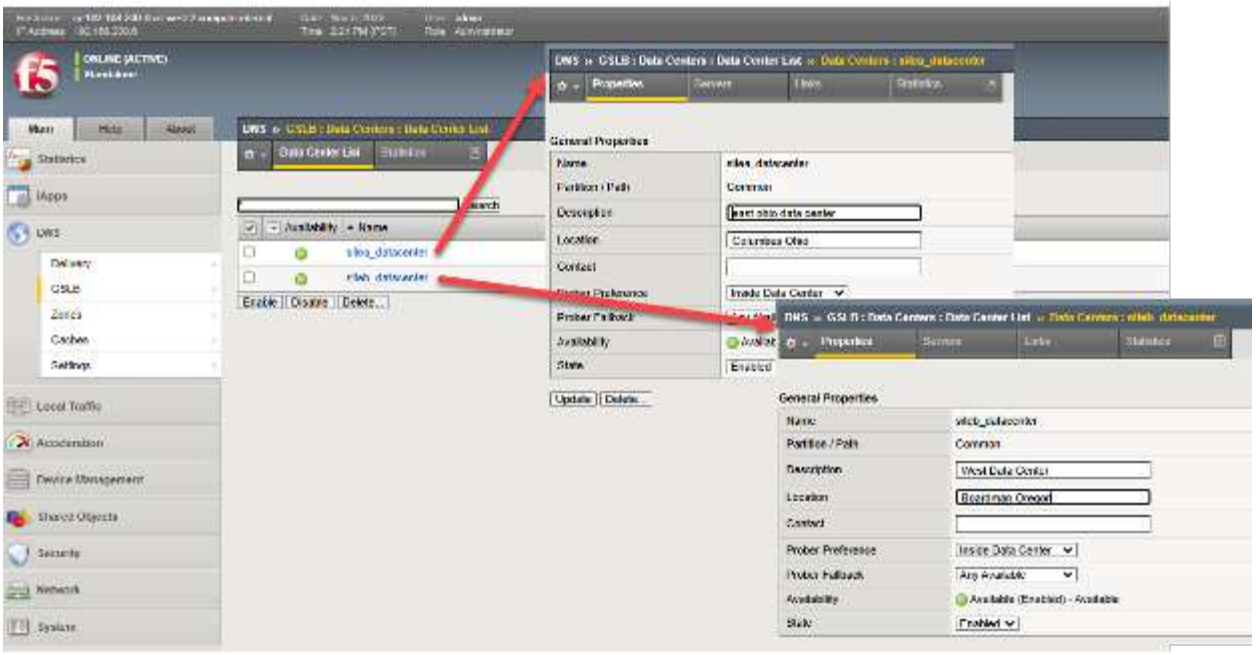
これで、DNS モジュールが有効になっている BIG-IP アプライアンスの、通常は「1 回限り」の予備セットアップ手順は完了です。この時点で、アプライアンスを使用したグローバル トラフィック管理ソリューションの設定の詳細に移る準備が整いました。これは当然、 StorageGRIDサイトの特性にリンクされます。

4つのステップでデータセンターサイトをセットアップし、BIG-IP間通信を確立する

ステップ1: データセンターを作成する

BIG-IP LTM によってローカルに負荷分散されるノードのクラスターを収容する各サイトは、BIG-IP DNS に入力する必要があります。トラフィック管理をサポートするために DNS 同期グループを作成しているため、この設定はグループの DNS メンバー間で共有されるため、この操作は 1 つの BIG-IP DNS でのみ実行する必要があります。

TMUI GUI から、[DNS] > [GSLB] > [データ センター] > [データ センター リスト] を選択し、 StorageGRIDサイトごとにエントリを作成します。図 1 に沿ったネットワーク設定を使用する場合、DNS アプライアンスがStorageGRID以外の他のサイトに配置されている場合は、ストレージ サイトに加えてこれらのサイトのデータ センターを追加します。この例では、サイト a と b がオハイオ州とオレゴン州に作成され、BIG-IP はデュアル DNS および LTM アプライアンスです。



ステップ **2:** サーバーの作成 **(**ソリューション内のすべての **BIG-IP** アプライアンスのリスト**)**

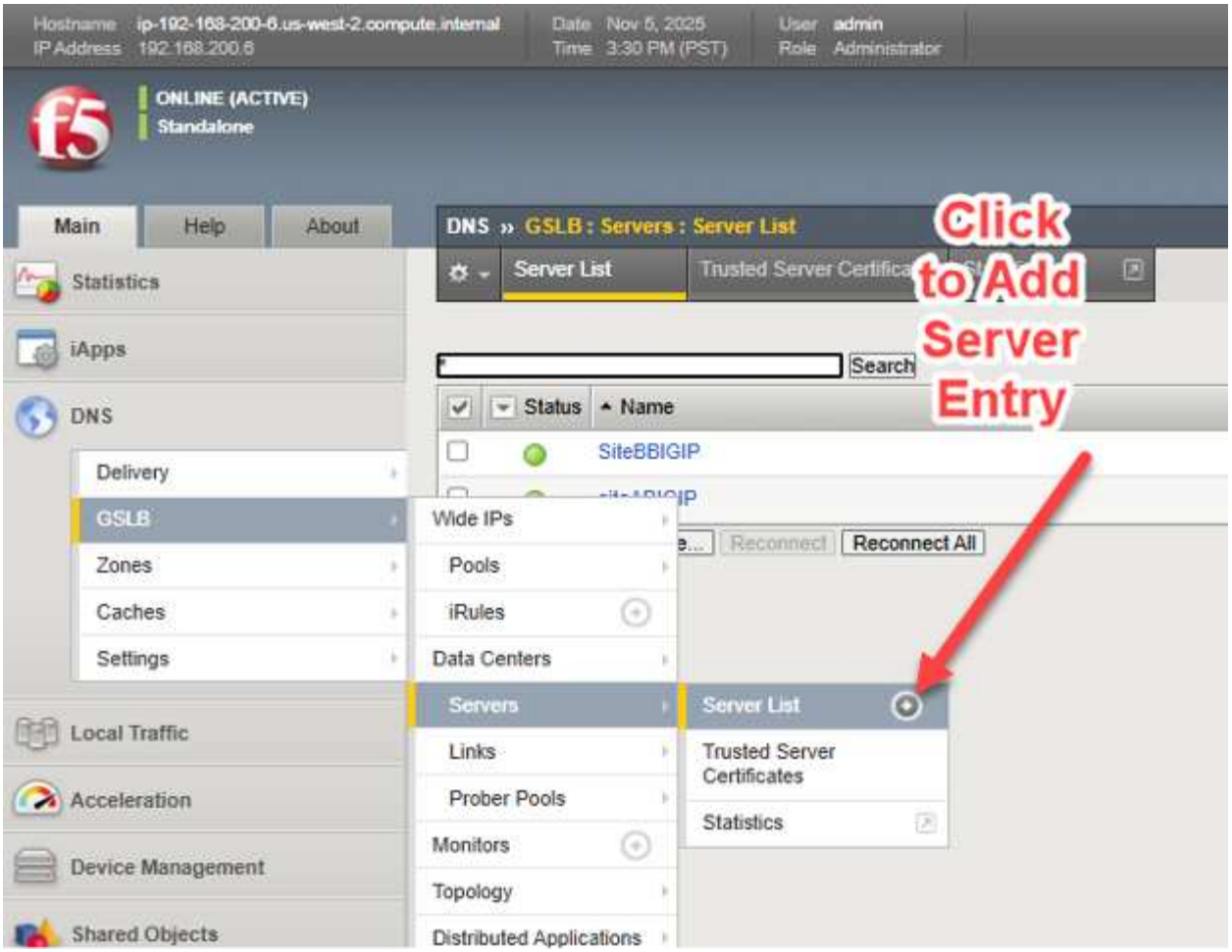
これで、個々のStorageGRIDサイト クラスターを BIG-IP DNS セットアップに接続する準備が整いました。各サイトの BIG-IP アプライアンスは、「バックエンド」 IP アドレス/ポートを使用して、「フロントエンド」の到達可能な IP アドレス/ポートをストレージノードアプライアンスのバックエンド「プール」のセットに結び付ける仮想サーバーの構成を通じて、S3 トラフィックの実際の負荷分散を実行します。

たとえば、サイトの廃止のため、またはリアルタイムのヘルス チェックの失敗によって予期せず、プール内のすべてのストレージ ノードが管理上オフラインになった場合、DNS クエリ応答が変更され、トラフィックは他のサイトに送信されます。

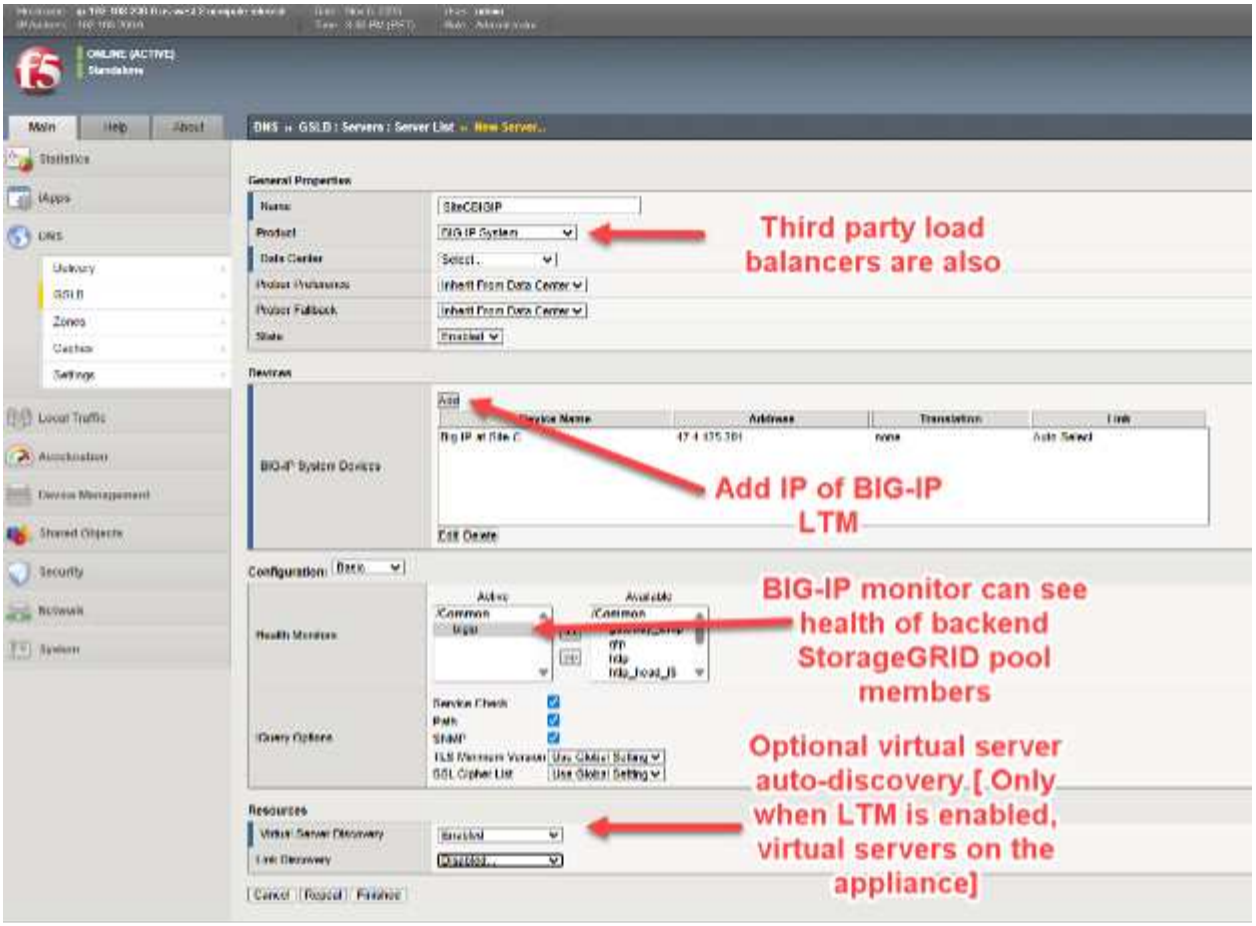
StorageGrid サイト、具体的にはローカル仮想サーバーを各アプライアンスの BIG-IP DNS 構成に結び付けるには、セットアップを 1 回だけ実行する必要があります。次のステップでは、BIG-IP DNS アプライアンスのグループ全体の設定が同期されます。

簡単に言うと、DNS、LTM、または DNS と LTM の両方のライセンスが付与されているすべての BIG-IP アプライアンスのリスト (サーバー リストと呼ばれる) を作成します。このマスター リストは、リストが完成するとすべての BIG-IP DNS アプライアンスと同期されます。

1 台の BIG-IP DNS ライセンス アプライアンスで、[DNS] > [GSLB] > [サーバー] > [サーバー リスト] を選択し、追加ボタン (+) を選択します。



各 BIG-IP を追加する際の 4 つの重要な要素は次のとおりです。 * 製品のプルダウンから BIG-IP を選択すると、他のロード バランサも選択できますが、通常、各サイトでバックエンド ノードの健全性が低下した場合のリアルタイムの可視性の応答性が欠如します。* BIG-IP DNS アプライアンスの IP アドレスを追加します。おそらく、BIG-IP DNS アプライアンスを初めて追加する場合、アドレスは現在の GUI アクセスされたアプライアンスになり、将来のアプライアンスはソリューション内の他のアプライアンスになります。* ヘルスモニターを選択し、追加するロードバランサーが BIG-IP アプライアンスである場合は、バックエンドのStorageGRIDノードのヘルスを考慮して、常に「BIG-IP」を使用します。* アプライアンスがデュアル DNS/LTM アプライアンスである場合は、オプションで仮想サーバーの自動検出を要求します。

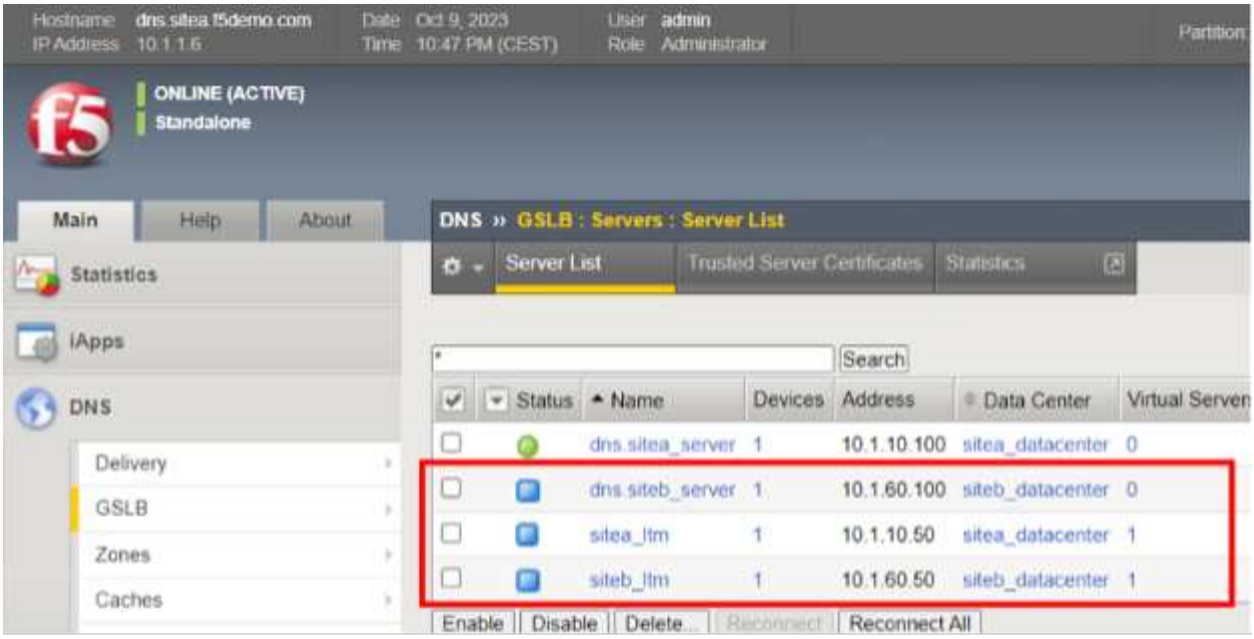


一時的なネットワークの問題やネットワークの場所間のファイアウォール ACL ルールなどの状況によっては、この段階でリモート アプライアンスを追加すると、仮想サーバーの検出で LTM が設定されたリモート アプライアンスのエントリが表示されないことがあります。このような場合、新しいアプライアンス (「サーバー」) を追加した後、以下に示すように仮想サーバーを手動で追加できます。BIG-IP DNS のみのアプライアンスを追加する場合、そのデバイスに検出または追加される仮想サーバーは存在しません。

すべてのサイトで、ソリューション内の各アプライアンス（BIG-IP DNS アプライアンス、BIG-IP LTM アプライアンス、DNS ユニットと LTM ユニットの両方の役割を果たすアプライアンスを含む）にこれらのサーバー エントリを追加する必要があります。

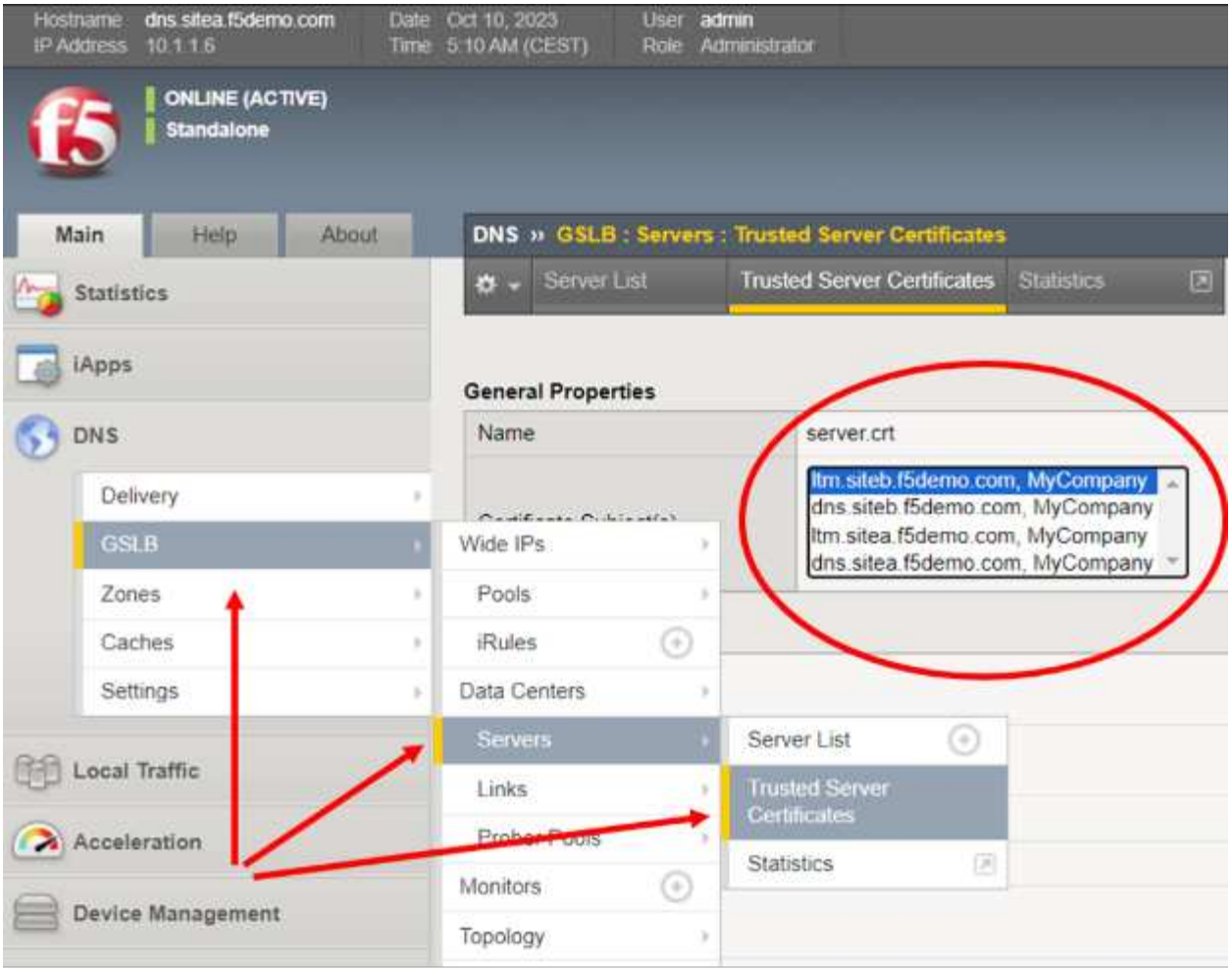
ステップ**3:** すべての**BIG-IP**アプライアンス間の信頼関係を確立する

次の例では、4 つのアプライアンスがサーバーとして追加され、2 つのサイトに分散されています。各サイトには専用の BIG-IP DNS と BIG-IP LTM があることに注意してください。ただし、現在ログインしているアプライアンス以外のすべてのアプライアンスの「ステータス」列には青いアイコンが表示されています。これは、他の BIG-IP アプライアンスとの信頼関係がまだ確立されていないことを意味します。



信頼を追加するには、GUI 経由で構成の詳細を入力した BIG-IP に SSH で接続し、「root」アカウントを使用して BIG-IP のコマンドライン インターフェイスにアクセスします。プロンプトで次の単一コマンドを発行します: *bigip_add*

「bigip_add」コマンドは、クラスタ内のGSLBサーバ間の暗号化された「iQuery」チャネルのセットアップ時に使用するために、宛先BIGIPデバイスから管理証明書を取得します。iQueryはデフォルトでTCPポート4353を使用して実行され、BOG-IP DNSメンバーが同期状態を維持できるようにするハートビートです。暗号化されたチャネルでは xml と gzip を使用します。オプションなしで「bigip_add」を実行すると、現在のユーザー名を使用してエンドポイントに接続し、GSLB サーバー リスト内のすべての BIGIP デバイスに対してコマンドが実行されます。成功を簡単に確認するには、BIG-IP GUI に戻り、表示されたプルダウン メニューにすべてのサーバーの証明書がリストされていることを確認します。



ステップ**4:** すべての**BIG-IP DNS**アプライアンスを**DNS**グループに同期する

最後のステップでは、1 つのユニットの TMUI GUI を使用するだけで、すべての BIG-IP DNS アプライアンスを完全に構成できるようになります。サンプルのケースでは、2 つのStorageGRIDサイトがあり、これは SSH を使用して 他の サイトの BIG-IP DNS のコマンド ラインにアクセスすることを意味します。ルートとして接続し、ファイアウォール ポリシー/ACL によって 2 つの BIG-IP DNS デバイスが TCP ポート 22 (SSH)、443 (HTTPS)、および 4354 (F5 iQuery プロトコル) で通信できることを確認した後、プロンプトで次のコマンドを実行します: *gtm_add* <すべての *GUI* 手順が以前に実行された最初のサイトの *BIG-IP DNS* の *IP* アドレス>

この時点で、グループに追加されたすべての BIG-IP DNS アプライアンスで、以降のすべての DNS 構成作業を実行できます。上記のコマンド gtm_add は、LTM のみであるアプライアンス メンバーに適用する必要はありません。DNS をサポートするアプライアンスのみ、同期された DNS グループの一部になるためにこのコマンドが必要です。

データセンターサイトのセットアップと**BIG-IP**間通信の確立

この時点で、基盤となる正常な BIG-IP DNS アプライアンス グループを作成するためのすべての手順が完了します。これで、各StorageGRIDデータセンターで公開されている分散 Web/S3 サービスを指す名前 (FQDN) の作成に進むことができます。

これらの名前は「ワイド IP」、または略して WIP と呼ばれ、DNS A リソース レコードを持つ通常の DNS FQDN です。ただし、従来の A リソース レコードのようにサーバーを指すのではなく、内部的には BIG-IP 仮想サーバーのプールを指します。各プールは、個別に、1 つ以上の仮想サーバーのセットで構成できます。

名前解決のために IP アドレスを要求する S3 クライアントは、ポリシーで選択された最適なStorageGRID サイトにある S3 仮想サーバーのアドレスを受け取ります。

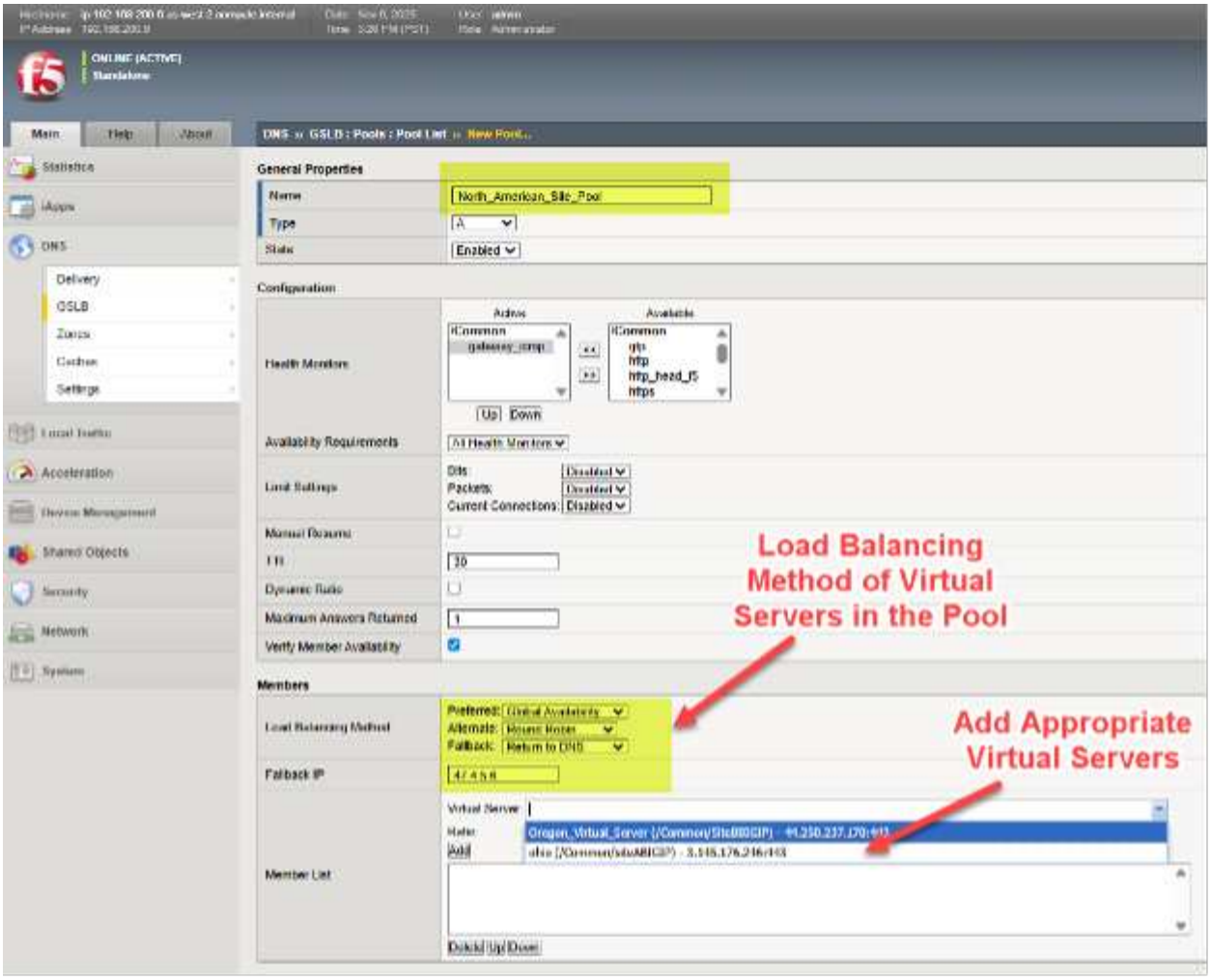
ワイド**IP**、プール、仮想サーバーの概要

簡単な架空の例として、**storage.quantumvault.com** という名前の WIP では、潜在的な仮想サーバーの 2 つのプールにリンクされた BIG-IP DNS ソリューションが表示される場合があります。最初のプールは北米の 4 つのサイトから構成され、2 番目のプールはヨーロッパの 3 つのサイトから構成される可能性があります。

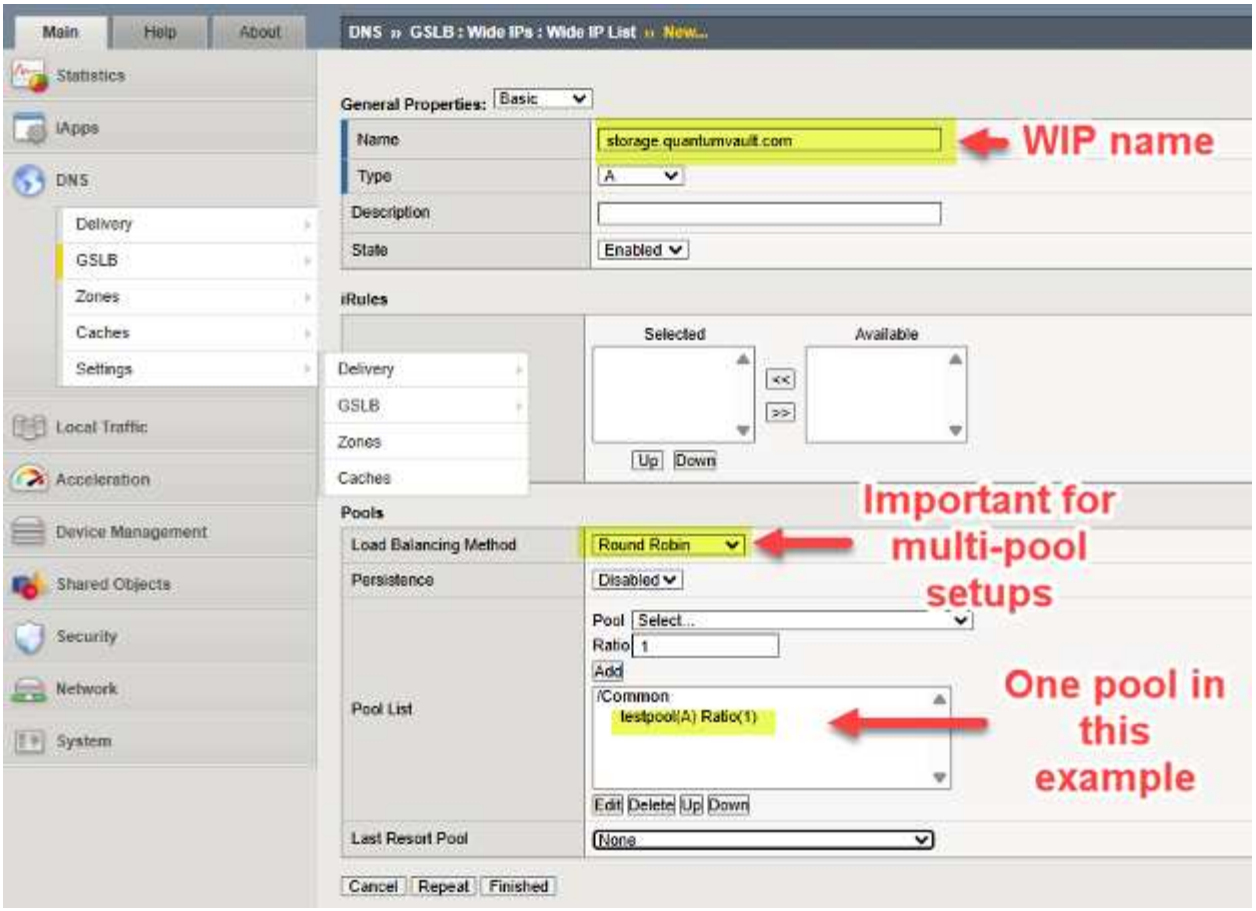
選択されたプールは、さまざまなポリシー決定から決定される可能性があります。たとえば、トラフィックの大部分を北米のStorageGRIDサイトに誘導するには、単純な 5:1 の比率を使用できます。おそらくもっと可能性が高いのは、トポロジ ベースの選択で、たとえば、ヨーロッパからのすべての S3 トラフィックがヨーロッパのサイトに送られ、世界の残りの S3 トラフィックが北米のデータ センターに送られるようなプールが選択されることです。

BIG-IP DNS によってプールに到達すると、北米のプールが選択されたと仮定すると、storage.quantumvault.com を解決するために返される実際の DNS A リソース レコードは、4 つの北米サイトのいずれかにある BIG-IP LTM によってサポートされている 4 つの仮想サーバーのいずれかになります。どちらが選択されるかについても、ポリシーに基づいており、ラウンドロビンなどの単純な「静的」アプローチが存在する一方で、ローカル DNS リゾルバーから各サイトの待ち時間を測定するパフォーマンス プローブなどのより高度な「動的」選択が維持され、サイト選択の基準として使用されます。

BIG-IP DNS 上に仮想サーバーのプールを設定するには、メニュー パス **DNS > GSLB >** プール **>** プール リスト **>** 追加 **(+)** に従います。この例では、さまざまな北米の仮想サーバーがプールに追加され、このプールが選択されたときに、負荷分散の優先アプローチが階層的に選択されていることがわかります。



DNS > GSLB > ワイド IP > ワイド IP リスト > 作成 (+) の順に選択して、DNS によって解決されるサービスの名前である WIP (ワイド IP) をデプロイメントに追加します。次の例では、S3 対応ストレージ サービスの WIP の例を示します。



グローバルトラフィック管理をサポートするために**DNS**を調整する

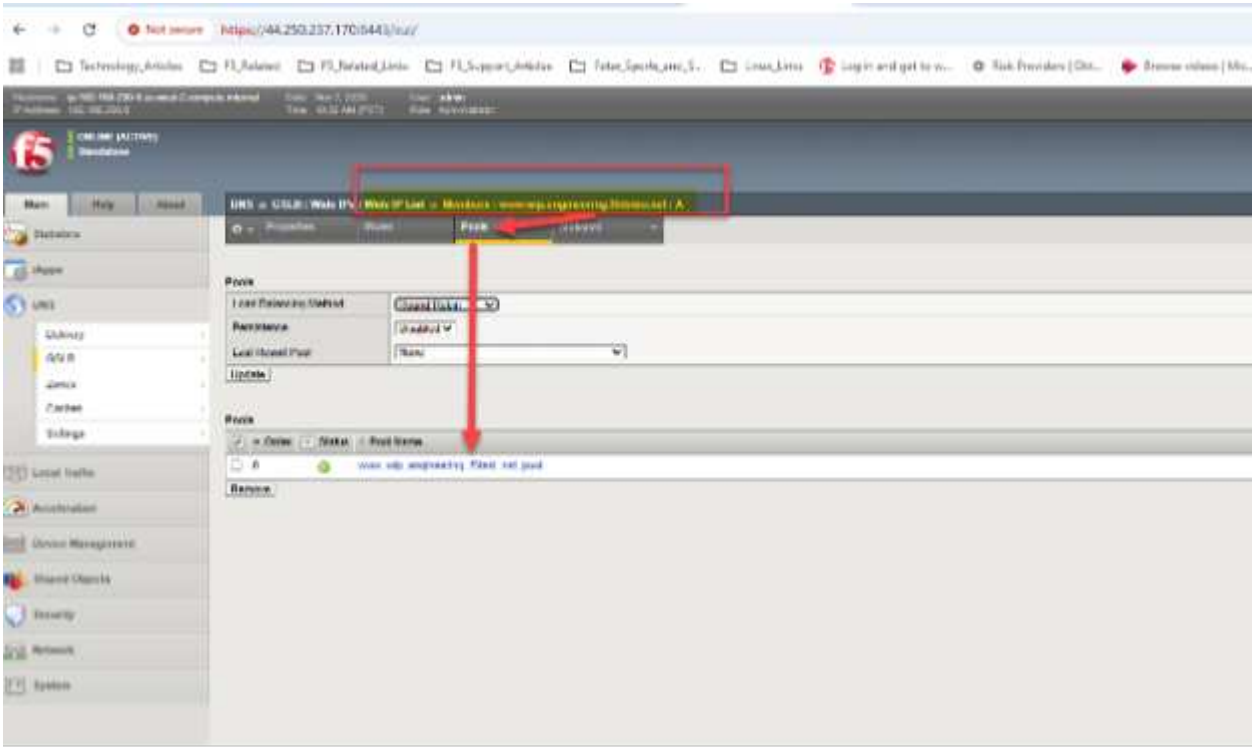
この時点で、基盤となるすべての BIG-IP アプライアンスは GSLB (グローバル サーバー ロード バランシング) を実行する準備が整います。ソリューションを活用するには、S3 トラフィック フローに使用される名前を調整して割り当てるだけです。一般的なアプローチは、企業の既存の DNS ドメインの一部を BIG-IP DNS の制御に委任することです。つまり、名前空間の一部であるサブドメインを「切り分け」、このサブドメインの制御を BIG-IP DNS アプライアンスに委任することになります。技術的には、これは、BIG-IP DNS アプライアンスがエンタープライズ DNS に DNS リソース レコード (RR) を持っていることを確認し、これらの名前/アドレスを委任されたドメインのネーム サーバー (NS) DNS リソース レコードにすることによって行われます。

現在、企業が DNS を維持する方法はさまざまですが、その 1 つの方法は完全にホストされたソリューションです。一例としては、Windows Server 2025 を介した DNS の運用と管理が挙げられます。企業が AWS Route53 や Squarespace などのクラウド DNS プロバイダーを活用するという別のアプローチもあります。

説明のために架空の例を示します。当社では、AWS Route53 によって管理される既存のドメインを使用して、S3 プロトコル経由でオブジェクトの読み取りと書き込みをサポートするStorageGRID を導入しています。既存のサンプル ドメインは f5demo.net です。

グローバル トラフィック管理のために、サブドメイン engineering.f5demo.net を BIG-IP DNS アプライアンスに割り当てます。これを行うには、engineering.f5demo.net の新しい NS (ネーム サーバー) リソース レコードを作成し、それを BIG-IP DNS アプライアンス名のリストにポイントします。この例では、2 つの BIG-IP DNS アプライアンスがあり、それらに対して 2 つの A リソース レコードを作成します。

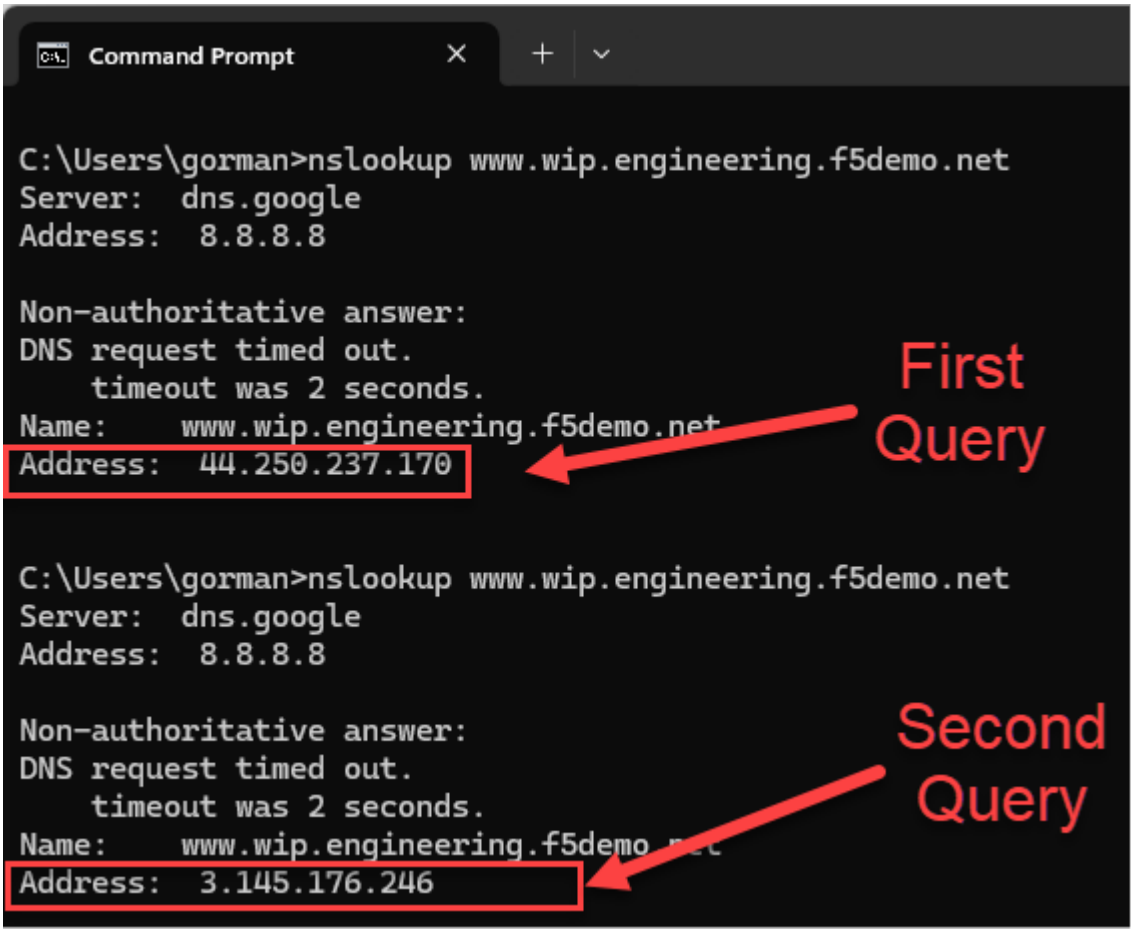
ここでは例として、BIG-IP DNS にワイド IP (WIP) を設定します。DNS はグループ同期を使用するため、1 つのアプライアンスの GUI を使用して調整するだけで済みます。BIG-IP DNS GUI 内で、**DNS > GSLB >** ワイド **IP >** ワイド **IP** リスト **(+)** に移動します。従来の DNS FQDN 設定では 1 つ以上の IPv4 アドレスを入力しますが、この場合は、 StorageGRID仮想サーバーの 1 つ以上のプールを指定するだけです。



この例では、オハイオ州とオレゴン州の両方のサイトに汎用 Web HTTPS サーバーが配置されています。単純な「ラウンドロビン」アプローチを使用すると、グローバル DNS が両方の仮想サーバー IP を使用して *www.wip.engineering.f5demo.net* の A リソース レコード マッピングのクエリに応答することがわかります。

簡単なテストは Web ブラウザで実行できます。また、 StorageGRIDを使用する S3 の場合は、S3Browser などのグラフィカル ツールを使用することもできます。各 DNS クエリでは、プール内でラウンドロビンが選択されているため、後続のトラフィックのターゲットとして使用されるプール内の次のデータセンター サイトが表示されます。

このサンプル設定では、dig または nslookup を使用して、一連の 2 つの DNS クエリをすばやく生成し、BIG-IP DNS が実際にラウンドロビン ロード バランシングを実行していることを確認して、時間の経過とともに両方のサイトがトラフィックを受信できるようにします。

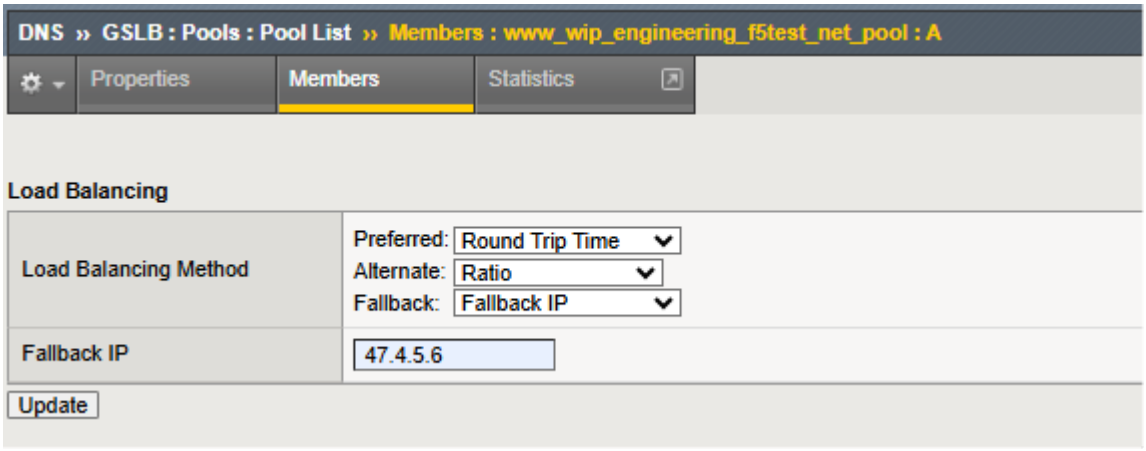


より高度な技術の探求の提案

多くの可能なアプローチの 1 つは、上記の単純な「ラウンドロビン」の例ではなく、「グローバル可用性」

モードを使用することです。グローバル可用性を使用すると、プールの順序、または単一のプール内の仮想サーバーにトラフィックを送信できます。この方法では、すべての S3 トラフィックを、たとえばニューヨーク市のサイトにデフォルトで送信することができます。

ヘルス チェックによってこのサイトのStorageGRIDノードの可用性に問題があることが示された場合、その時点でトラフィックはセントルイスに送信される可能性があります。セントルイスで健康上の懸念が生じた場合、フランクフルトのサイトが S3 の読み取りまたは書き込みトランザクションの受信を開始する可能性があります。したがって、グローバルな可用性は、S3 StorageGRIDソリューション全体の回復力に対する 1 つのアプローチです。もう 1 つのアプローチは、階層型アプローチを使用して負荷分散アプローチを組み合わせることです。



この例では、「動的」オプションが、構成されたプール内のサイトの最初の負荷分散の選択肢になります。示されている例では、ローカル DNS リゾルバのパフォーマンスのアクティブ プロービングを使用した継続的な測定アプローチが維持され、サイト選択のきっかけとなっています。この方法が利用できない場合は、各サイトに割り当てられた比率によって個々のサイトを選択できます。比率により、大規模で高帯域幅のStorageGRIDサイトは、小規模なサイトよりも多くの S3 トランザクションを受信できます。最後に、おそらく災害復旧シナリオとして、プール内のすべてのサイトが正常でなくなった場合、指定されたフォールバック IP が最後の手段としてサイトとして使用されます。BIG-IP DNS の興味深い負荷分散方法の 1 つは「トポロジ」です。これは、DNS クエリの受信ソースである S3 ユーザーのローカル DNS リゾルバを監視し、インターネット トポロジ情報を使用して、プールから一見「最も近い」サイトを選択するものです。

最後に、サイトが地球全体に広がっている場合は、F5 BIG-IP DNS マニュアルで詳細に説明されている動的「プローブ」テクノロジの使用を検討する価値があるかもしれません。プローブを使用すると、頻繁に発生する DNS クエリのソースを監視できます。たとえば、トラフィックで通常同じローカル DNS リゾルバを使用する B2B パートナーなどが挙げられます。BIG-IP DNS プローブは、世界中の各サイトの BIG-IP LTM から起動して、S3 トランザクションのレイテンシが最も低くなる可能性のあるサイトを大まかに判断できます。そのため、アジアからのトラフィックは、北米やヨーロッパにあるサイトよりもアジアのStorageGRIDサイトの方が適切に処理される可能性があります。

まとめ

F5 BIG-IP とNetApp StorageGRID を統合することで、複数のサイト間でのデータの可用性と一貫性、および S3 トランザクション ルーティングの最適化に関連する技術的な課題に対処します。このソリューションを導入すると、ストレージの復元力、パフォーマンス、信頼性が向上し、堅牢でスケーラブルかつ柔軟なストレージ インフラストラクチャを求める企業に最適です。

詳細については、BIG-IP DNSの公式F5ドキュメントをご覧ください。 "リンク"。セットアップ例を段階的に説明するガイド付き教室形式のガイドも用意されています。 "こちらをご覧ください"。

Datadog SNMP構成

アロンクライン著

StorageGRID SNMPメトリクスとトラップを収集するようにDatadogを構成します。

Datadogを構成します

Datadogは、メトリクス、ビジュアライゼーション、アラートを提供する監視解決策 です。次の構成は、StorageGRID システムのローカルに配置されたUbuntu 22.04.1ホスト上のLinuxエージェントバージョン7.43.1で実装されました。

StorageGRID MIBファイルから生成されたDatadogプロファイルおよびトラップファイル

Datadogは、製品MIBファイルをSNMPメッセージのマッピングに必要なdatadog参照ファイルに変換する方法を提供します。

見つかった命令に従って生成されたDatadogトラップ解決マッピング用のこのStorageGRID YAMLファイル "こちらをご覧ください"。+このファイルを/etc/datadog-agent/conf.d/snmp.d/traps_db/+に配置します

- "トラップYAMLファイルをダウンロードします" [+]
  - * MD5チェックサム* 42e27e4210719945a46172b98c379517以降
  - * SHA256チェックサム* d0fe5c8e6ca3c902d054f854b70a85f928cba8b7c76391d356f05d2cf73b6887以降

見つかった命令に従って生成されたDatadogメトリクスマッピング用のこのStorageGRID プロファイルYAMLファイル "こちらをご覧ください"。+このファイルを/etc/datadog-agent/conf.d/snmp.d/profiles/+に配置します

- "プロファイルYAMLファイルをダウンロードします" [+]
  - * MD5チェックサム* 72bb7784f4801adda4e0c3ea77df19aa+
  - * SHA256チェックサム* b6b7fadd33063422a8bb8e39b3ead8ab349ee0229926eadc8585f0087b8cee+

メトリクスのSNMP Datadog構成

メトリックのSNMPの設定は、2つの方法で管理できます。自動検出を設定するには、StorageGRID システムを含むネットワークアドレス範囲を指定するか、個 々 のデバイスのIPを定義します。設定の場所は、決定内容によって異なります。自動検出は、datadogエージェントのYAMLファイルで定義されます。明示的なデバイス定義は、SNMP設定YAMLファイルで設定されます。以下に、同じStorageGRID システムのそれぞれの例を示します。

自動検出

設定は/etc/datadog-agent/datadog.yamlにあります

```
listeners:
  - name: snmp
snmp_listener:
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

個々のデバイス

/etc/datadog-agent/conf.d/snmp.d/conf.yaml

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

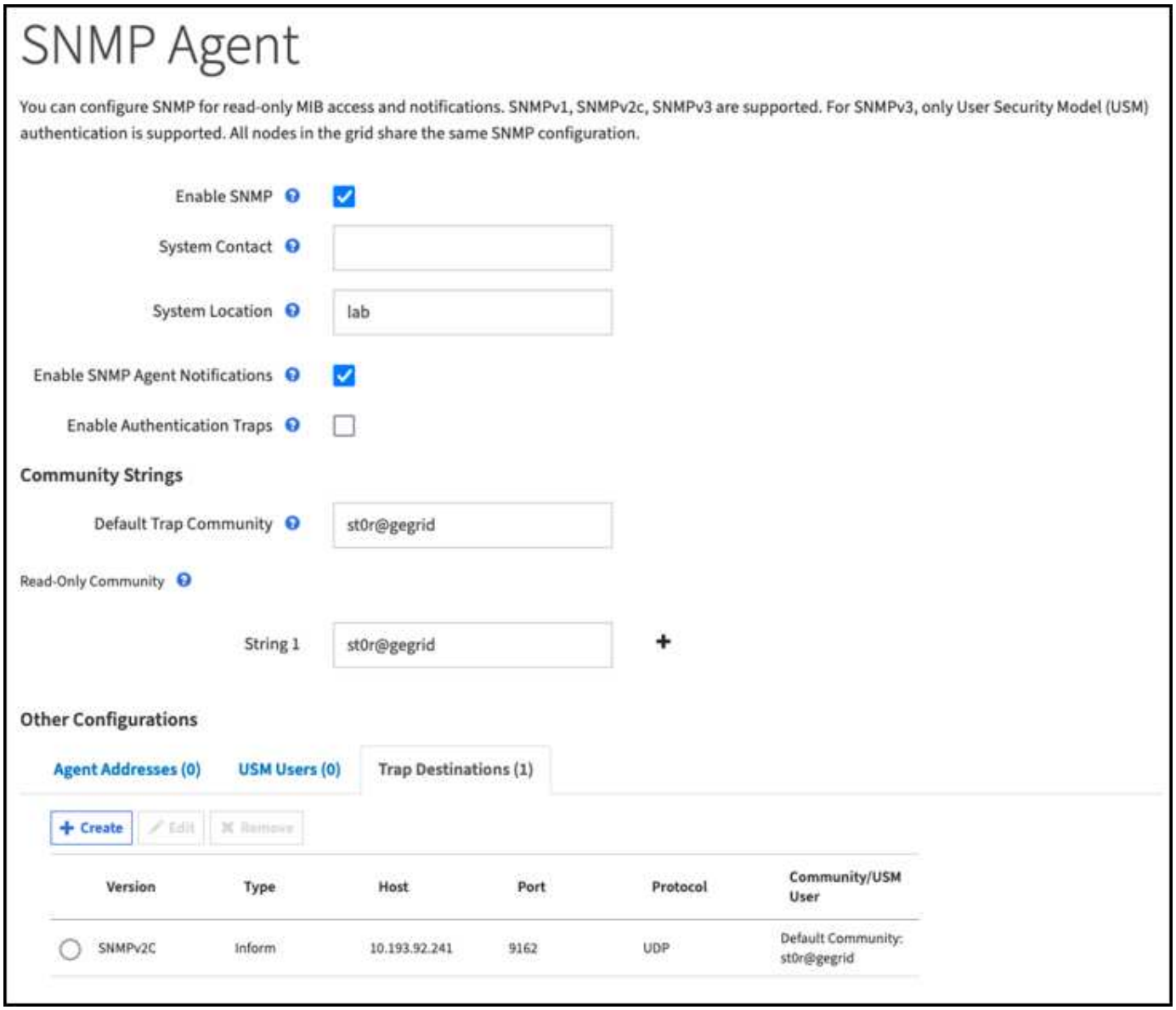
トラップの**SNMP**設定

SNMPトラップの構成は、datadog構成YAMLファイル/etc/datadog-agent/datadog.yamlで定義されています

```
network_devices:
  namespace:  # optional, defaults to "default".
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

StorageGRID のSNMP設定例

StorageGRID システムのSNMPエージェントは、[Configuration]タブの[Monitoring]列にあります。SNMPを有効にし、必要な情報を入力します。トラップを構成する場合は、[Traps Destinations]を選択し、トラップ構成を含むDatadogエージェントホストの宛先を作成します。



rcloneを使用して、StorageGRID 上のオブジェクトを移行、PUT、および削除します

ジークフリート・ヘップとアロン・クライン著_

rcloneは、S3処理用の無料のコマンドラインツールでクライアントです。rcloneを使用して、StorageGRID 上のオブジェクトデータを移行、コピー、および削除できます。rcloneには、次の例に示すように、「purge」機能を使用して空でなくてもバケットを削除する機能が含まれています。

rcloneをインストールして設定します

rcloneをワークステーションまたはサーバにインストールするには、からダウンロードします "rclone.org"。

初期設定手順

1. 設定スクリプトを実行するか、ファイルを手動で作成して、rclone構成ファイルを作成します。
2. この例では、rclone構成のリモートStorageGRID S3エンドポイントの名前にsgdemoを使用します。
   a. 設定ファイル~/.config/rclone/rclone.confを作成します

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

   b. rclone configを実行します

#rclone設定

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
```

```
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
```

```
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

基本的なコマンドの例

- バケットを作成：

  `rclone mkdir remote:bucket`

  #rclone mkdir sgdemo：test01

  SSL証明書を無視する必要がある場合は、--no-check-certificateを使用します。

- すべてのバケットを表示：

```
rclone lsd remote:
```

#rclone lsd sgdemo：

- 特定のバケット内のオブジェクトをリストします。

```
rclone ls remote:bucket
```

rclone ls sgdemo：test01

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- バケットを削除：

```
rclone rmdir remote:bucket
```

#rclone rmdir sgdemo：test02

- オブジェクトを置きなさい:

```
rclone copy filename remote:bucket
```

#rclone copy ~/test/ testfile.txt sgdemo：test01

- オブジェクトを取得：

```
rclone copy remote:bucket/objectname filename
```

#rclone copy sgdemo：test01 / testfile.txt ~/test/ testfileS3.txt

- オブジェクトを削除：

```
rclone delete remote:bucket/objectname
```

#rclone delete sgdemo：test01 / testfile.txt

- バケット内のオブジェクトの移行

```
rclone sync source:bucket destination:bucket --progress

rclone sync source_directory destination:bucket --progress
```

#rclone sync sgdemo：test01 sgdemo：clone01 — progress

```
Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

— progressまたは- Pを使用して、タスクの進行状況を表示します。それ以外の場合、出力はありません。

- バケットとすべてのオブジェクトコンテンツを削除する

```
rclone purge remote:bucket --progress
```

#rclone purge sgdemo：test01 — progress

```
Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
Elapsed time:        10.2s
```

rclone ls sgdemo：test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

Veeam Backup & Replicationを使用した導入に関するStorageGRIDのベストプラクティス

_ Oliver HaenselとAron Klein著_

このガイドでは、NetApp StorageGRIDの構成と、Veeam Backup & Replicationの一部を中心に説明します。本ドキュメントは、Linuxシステムに精通し、Veeam Backup & Replicationと組み合わせてNetApp StorageGRIDシステムの保守または実装を担当するストレージ管理者およびネットワーク管理者を対象としています。

概要

ストレージ管理者は、可用性、迅速なリカバリの目標を達成し、ニーズに合わせて拡張し、データの長期保存に関するポリシーを自動化するソリューションを使用して、データの増加を管理したいと考えています。これらのソリューションは、損失や悪意のある攻撃からも保護する必要があります。VeeamとNetAppは提携して、オンプレミスのオブジェクトストレージ向けのVeeam Backup & RecoveryとNetApp StorageGRIDを組み合わせたデータ保護解決策を作成しました。

VeeamとNetApp StorageGRIDが連携して動作する使いやすい解決策を提供することで、急速なデータ量の増大や世界的な規制強化のニーズに対応できます。クラウドベースのオブジェクトストレージは、耐障害性、拡張性、運用効率、コスト効率に優れていることで知られており、バックアップのターゲットとして最適です。本ドキュメントでは、Veeam Backup解決策およびStorageGRIDシステムの構成に関するガイダンスと推奨事項を提供します。

Veeamのオブジェクトワークロードによって、小規模オブジェクトのPUT、DELETE、LIST処理が同時に多数作成されます。書き換えや削除の防止を有効にすると、保持期間の設定やバージョンの表示に関する要求がオブジェクトストアに追加されます。バックアップジョブのプロセスでは、日次変更のためにオブジェクトが書き込まれます。その後、新しい書き込みが完了すると、バックアップの保持ポリシーに基づいてオブジェクトが削除されます。バックアップジョブのスケジュールは、ほとんどの場合重複します。その結果、バックアップウィンドウの大部分がオブジェクトストアに50分の50のPUT / DELETEワークロードで構成されます。タスクスロットの設定を使用して同時処理数をVeeamで調整し、バックアップジョブのブロックサイズを増やしてオブジェクトサイズを増やし、複数オブジェクトの削除要求に含まれるオブジェクト数を減らします。また、ジョブを完了する最大期間を選択することで、解決策のパフォーマンスとコストが最適化されます。

必ず製品ドキュメントをお読みください "Veeam Backup Replication"そして "StorageGRID"始める前に。Veeam は、 StorageGRIDソリューションのサイズを決定する前に使用する必要がある、Veeam インフラストラクチャのサイズと容量要件を理解するための計算ツールを提供しています。 Veeam Ready ProgramのWebサイトでVeeam- NetApp検証済み構成を常に確認してください。 "Veeam Readyのオブジェクト、オブジェクトの変更不可、リポジトリ" 。

Veeam構成

推奨バージョン

常に最新の状態に保ち、Veeam Backup & Replication 12または12.1システムの最新の修正プログラムを適用することをお勧めします。現在、少なくともVeeam 12パッチP20230718のインストールを推奨しています。

S3リポジトリ設定

スケールアウトバックアップリポジトリ（SOBR）は、S3オブジェクトストレージの大容量階層です。大容量階層はプライマリリポジトリを拡張したもので、データ保持期間が長くなり、ストレージ解決策が低コストになります。Veeamには、S3 Object Lock APIを通じて不変性を提供する機能があります。Veeam 12では、スケールアウトリポジトリで複数のバケットを使用できます。StorageGRIDでは、1つのバケット内のオブジェクト数や容量に制限はありません。複数のバケットを使用すると、オブジェクトのバックアップデータがペタバイト規模になる可能性がある非常に大規模なデータセットをバックアップする際のパフォーマンスが向上する可能性があります。

特定の解決策のサイジングと要件によっては、同時に実行できるタスクを制限する必要があります。デフォルト設定では、CPUコアごとに1つのリポジトリタスクスロットを指定し、タスクスロットごとに最大64の同時タスクスロットを指定します。たとえば、サーバに2つのCPUコアがある場合、オブジェクトストアには合計128個の同時スレッドが使用されます。これには、PUT、GET、およびBATCH Deleteが含まれます。タスクスロットに控えめな制限を選択して開始し、Veeamバックアップが新しいバックアップの安定した状態と期限切れになるバックアップ・データに達したら、この値を調整することをお勧めします。NetAppアカウントチームと協力して、希望する時間枠とパフォーマンスに合わせてStorageGRIDシステムを適切にサイジングしてください。最適な解決策を提供するには、タスクスロットの数とスロットあたりのタスクの制限を調整する必要がある場合があります。

バックアップジョブの設定

Veeamバックアップジョブでは、さまざまなブロックサイズオプションを設定できますが、これらは慎重に検討する必要があります。デフォルトのブロックサイズは1MBで、Veeamの圧縮機能と重複排除機能を使用すると、最初のフルバックアップでは約500KB、増分ジョブでは100$_{200KB}$のオブジェクトが作成されます。バックアップブロックサイズを大きくすることで、パフォーマンスを大幅に向上し、オブジェクトストレージの要件を縮小できます。ブロックサイズが大きいほどオブジェクトストアのパフォーマンスは大幅に向上しますが、ストレージ効率のパフォーマンスが低下するため、プライマリストレージの容量要件が増大する可能性があります。バックアップジョブのブロックサイズを4MBに設定することを推奨します。この場合、フルバックアップ用に約2MBのオブジェクトが作成され、増分バックアップ用に700KB1MBのオブジェクトサイズが作成されます。お客様は、8 MBのブロックサイズを使用してバックアップジョブを構成することも検討できます。これは、Veeamサポートの支援を受けて有効にすることができます。

変更不可のバックアップの実装では、オブジェクトストアのS3オブジェクトロックが使用されます。immutabilityオプションを指定すると、オブジェクトに対するリストおよび保持の更新要求がオブジェクトストアに対して生成される回数が増加します。

バックアップの保持期間が終了すると、バックアップジョブによってオブジェクトの削除が処理されます。Veeamは、1回の要求につき1、000個のオブジェクトを含む複数のオブジェクトの削除要求で、オブジェクトストアに削除要求を送信します。小規模なソリューションの場合は、リクエストあたりのオブジェクト数を減らすために調整が必要になることがあります。この値を小さくすると、削除要求がStorageGRIDシステム内のノードに均等に分散されるというメリットもあります。複数オブジェクトの削除制限を設定する場合は、次の表の値を開始点として使用することをお勧めします。表の値に選択したアプライアンスタイプのノード数

を掛けて、Veeamの設定値を取得します。この値が1000以上の場合、デフォルト値を調整する必要はありません。この値を調整する必要がある場合は、Veeamサポートに連絡して変更を行ってください。

アプライアンスモデル	ノードあたりの**S3MultiObjectDeleteLimit**
SG5712	34
SG5760	七五
SG6060 の設計	200です

お客様固有のニーズに基づいた推奨構成については、NetAppアカウントチームにお問い合わせください。Veeamの設定に関する推奨事項は次のとおりです。

- バックアップジョブのブロックサイズ= 4MB
- SOBRタスクスロット制限=2-16
- 複数オブジェクトの削除制限= 34-1000

StorageGRID構成

推奨バージョン

Veeam の導入に推奨されるバージョンは、最新のホットフィックスを適用したNetApp StorageGRID 11.9 または 12.0 です。常に最新の状態を維持し、 StorageGRIDシステムに最新の修正プログラムを適用することをお勧めします。

ロードバランサと**S3**エンドポイントの設定

Veeamでは、エンドポイントの接続にHTTPSのみを使用する必要があります。暗号化されていない接続はVeeamではサポートされていません。SSL証明書には、自己署名証明書、信頼されたプライベート認証局、または信頼されたパブリック認証局を使用できます。S3リポジトリへの継続的なアクセスを確保するために、HA構成で少なくとも2つのロードバランサを使用することを推奨します。ロードバランサには、すべての管理ノードとゲートウェイノードに配置されるStorageGRID提供の統合ロードバランササービス、またはF5、Kemp、HAProxy、Loadbalancer.orgなどのサードパーティの解決策を使用できます。 StorageGRIDロードバランサを使用すると、Veeamのワークロードに優先順位を付けたり、StorageGRIDシステムの優先順位の高いワークロードに影響しないようにVeeamを制限したりできるトラフィック分類機能（QoSルール）を設定できます。

S3 バケット

StorageGRIDは、安全なマルチテナント ストレージ システムです。 Veeam ワークロード専用のテナントを作成することをお勧めします。オプションでストレージ クォータを割り当てることができます。ベストプラクティスとして、「独自の ID ソースを使用する」を有効にします。適切なパスワードを使用してテナント ルート管理ユーザーを保護します。 Veeam Backup 12 では、S3 バケットに強力な一貫性が必要です。 StorageGRID は、バケット レベルで構成された複数の整合性オプションを提供します。 Veeam が複数の場所からデータにアクセスするマルチサイト展開の場合は、「strong-global」を選択します。 Veeam のバックアップと復元が単一のサイトでのみ行われる場合、一貫性レベルは「strong-site」に設定する必要があります。バケットの一貫性レベルの詳細については、 "ドキュメント" 。 Veeam 不変バックアップにStorageGRIDを使用するには、S3 オブジェクト ロックをグローバルに有効にして、バケットの作成時にバケット上で設定する必要があります。

ライフサイクル管理

StorageGRIDは、レプリケーションとイレイジャーコーディングをサポートして、StorageGRIDのノードとサイト全体でオブジェクトレベルの保護を実現します。イレイジャーコーディングには、オブジェクトサイズが200KB以上必要です。Veeamのデフォルトのブロックサイズである1MBで作成されるオブジェクトサイズは、VeeamのStorage Efficiency機能と比較して、この200KBの推奨最小サイズよりも小さくなることがあります。解決策のパフォーマンスを高めるために、サイト間の接続が十分でない場合やStorageGRIDシステムの帯域幅が制限されない場合を除き、複数のサイトにまたがるイレイジャーコーディングプロファイルを使用することは推奨されません。マルチサイトStorageGRIDシステムでは、各サイトにコピーを1つ格納するようにILMルールを設定できます。データの保持性を最大限に高めるために、各サイトにイレイジャーコーディングコピーを格納するルールを設定できます。このワークロードには、Veeam Backupサーバのローカルコピーを2つ使用することを推奨します。

パフォーマンスを削除

Veeam は、削除要求レートの調整とバックアップ削除プロセスのスケジュール設定を提供します。削除のパフォーマンスをさらに調整するには、同期削除を無効にして、ILM スキャナーにオブジェクトの最終的な削除を管理させることができます。

同期削除を無効にする手順

1. StorageGRIDグリッド マネージャーを開きます。
2. 右上隅で疑問符を選択し、次に API ドキュメントを選択します。
3. 右上隅にあるプライベート API ドキュメント ページ リンクをクリックします。
4. ilm-advancedを展開します。
5. GET ilm-advancedを選択します。
6. 「試してみる」を選択し、「実行」を選択します。
7. 応答結果を確認します。

    a. 値が null の場合、デフォルトの ilm-advanced 値が使用中であることを意味します。

    b. 値が null でない場合は、カスタム ILM の詳細値が使用中であることを意味します。 「data」: の後のすべての出力を、{ から最後から 2 番目の } までコピーします。

        i. テキストエディタで保存します。

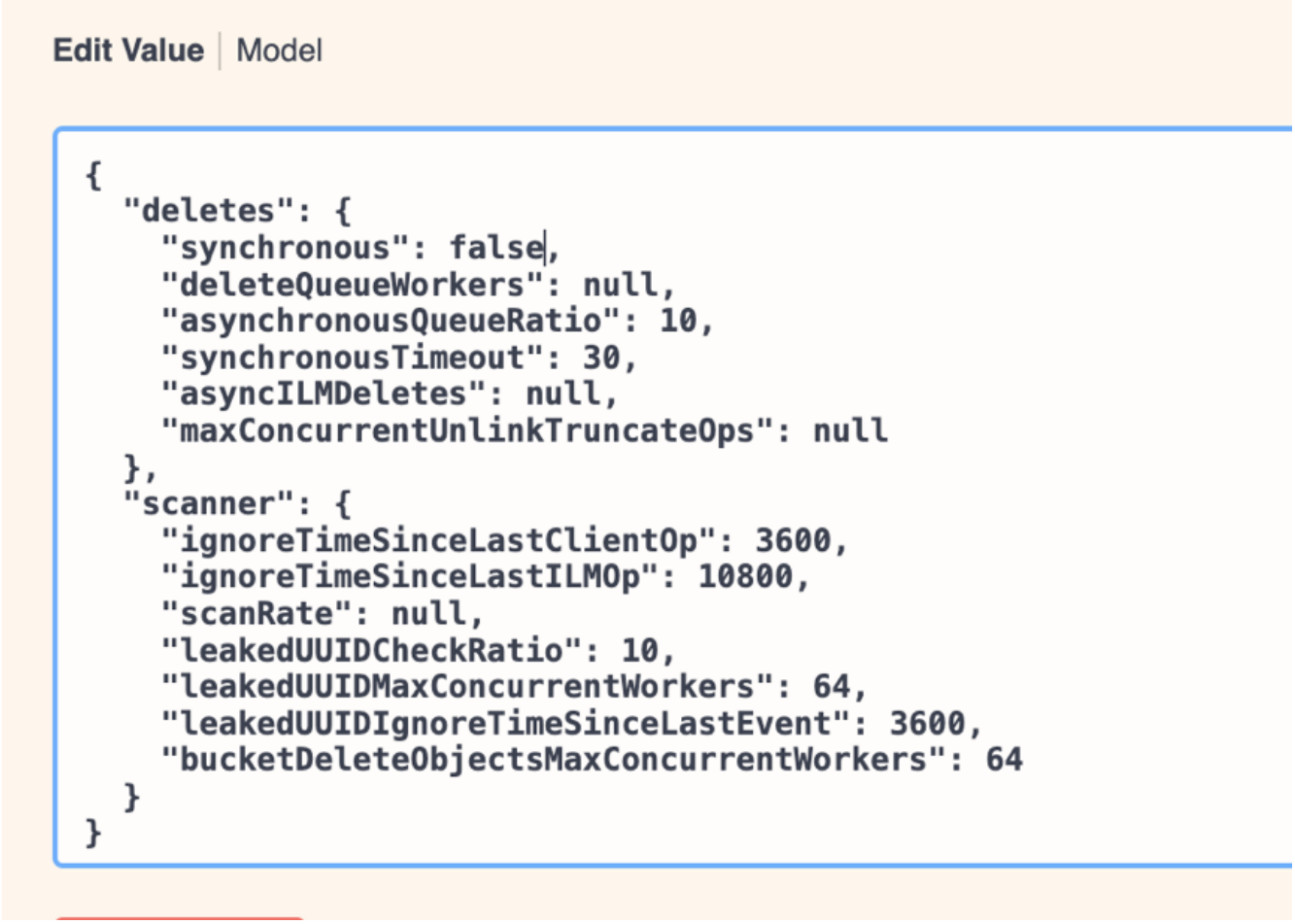
        応答例:

Response body


```
{
  "responseTime": "2025-09-19T15:01:28.142Z",
  "status": "success",
  "apiVersion": "4.2",
  "data": {
    "deletes": {
      "synchronous": null,
      "deleteQueueWorkers": null,
      "asynchronousQueueRatio": null,
      "synchronousTimeout": null,
      "asyncILMDeletes": null,
      "maxConcurrentUnlinkTruncateOps": null
    },
    "scanner": {
      "ignoreTimeSinceLastClientOp": null,
      "ignoreTimeSinceLastILMOp": null,
      "scanRate": null,
      "leakedUUIDCheckRatio": null,
      "leakedUUIDMaxConcurrentWorkers": null,
      "leakedUUIDIgnoreTimeSinceLastEvent": null,
      "bucketDeleteObjectsMaxConcurrentWorkers": null
    }
  }
}
```


8. PUT ilm-advancedを選択します。
9. 「試してみる」を選択して、API 本体の編集を開始します。
   a. デフォルトでは、API 本体にはデフォルト値が含まれ、以前に構成されたカスタム値は含まれません。これが、手順 5 ～ 7 を実行することが非常に重要である理由です。
10. 手順 5 ～ 7 でデフォルト以外の値が見つかった場合は、API 本体を手順 7 で保存した出力に置き換えます。 。それ以外の場合、手順 5 ～ 7 で値が null だった場合は、API 本体はそのままにしておきます。
11. API 本体ボックスで次のパラメータを調整します。
    a. 同期値を false に設定します。

       API 本文の例:

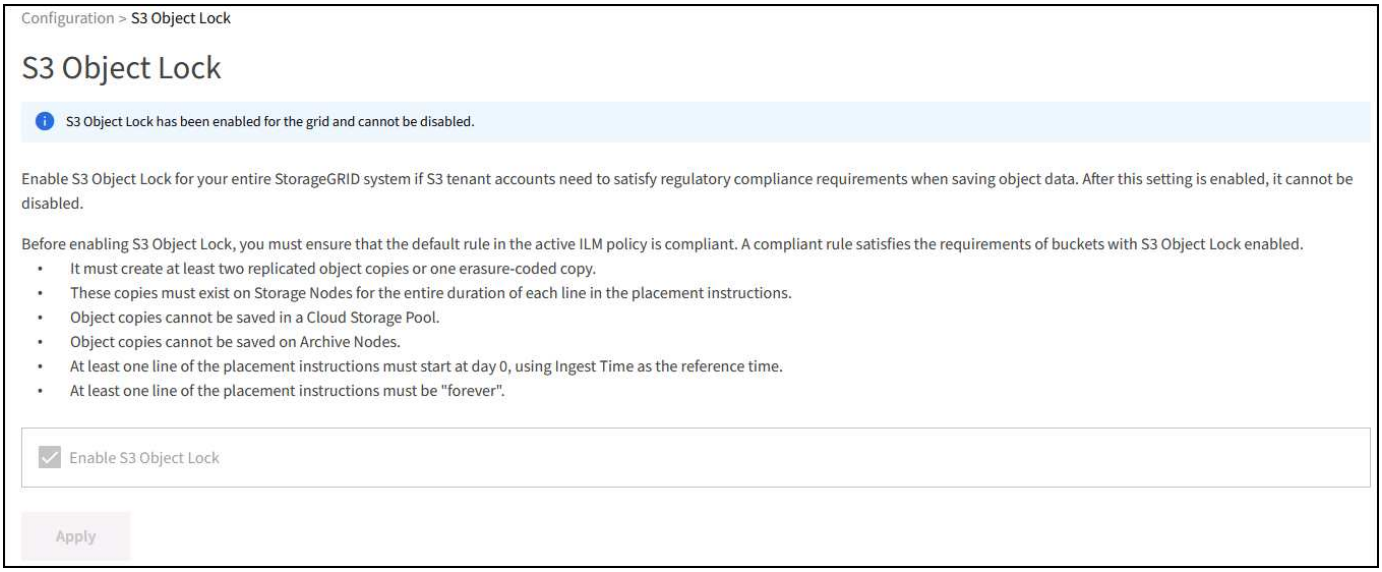


12. 完了したら、「実行」を選択します

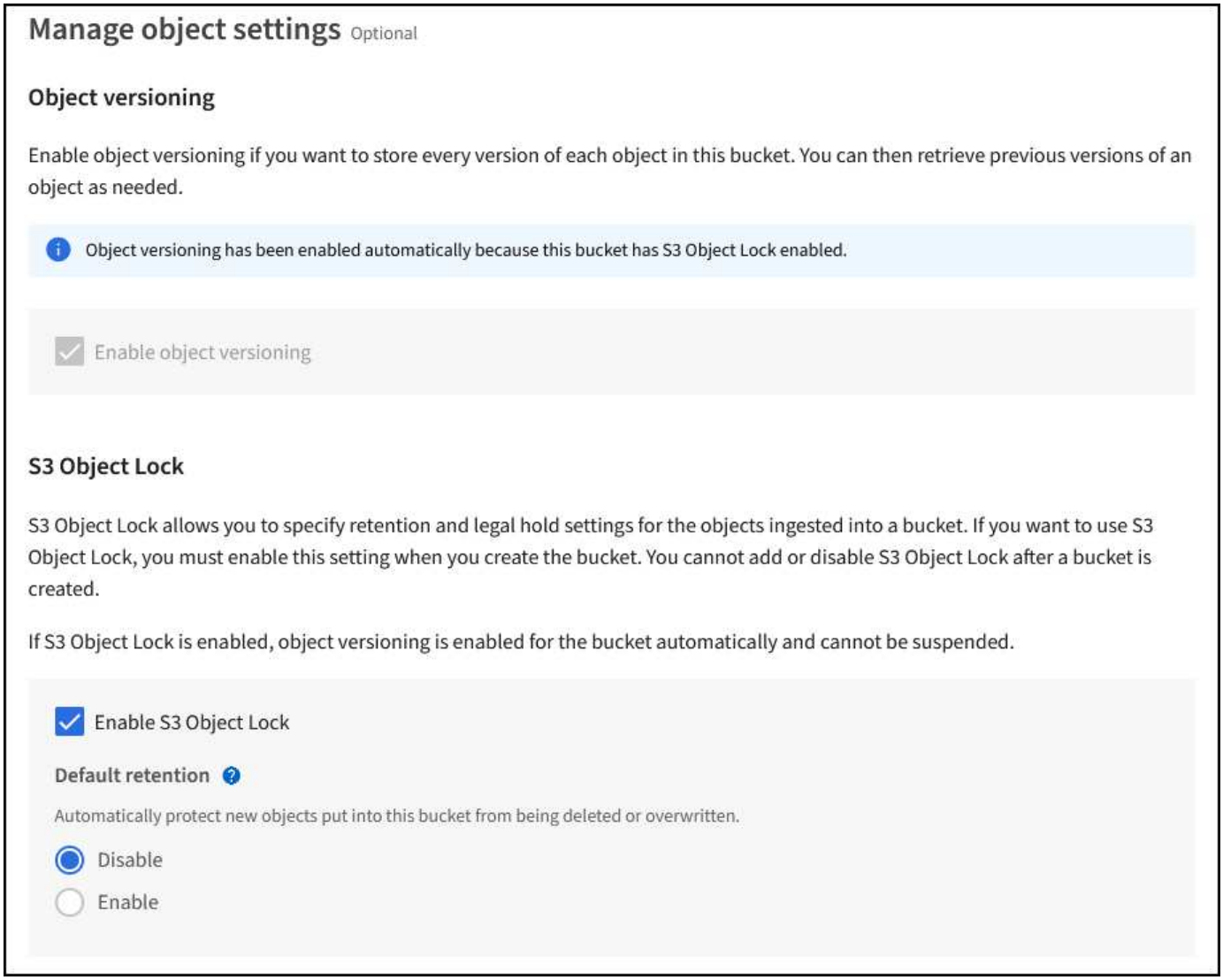
導入のキーポイント

StorageGRID

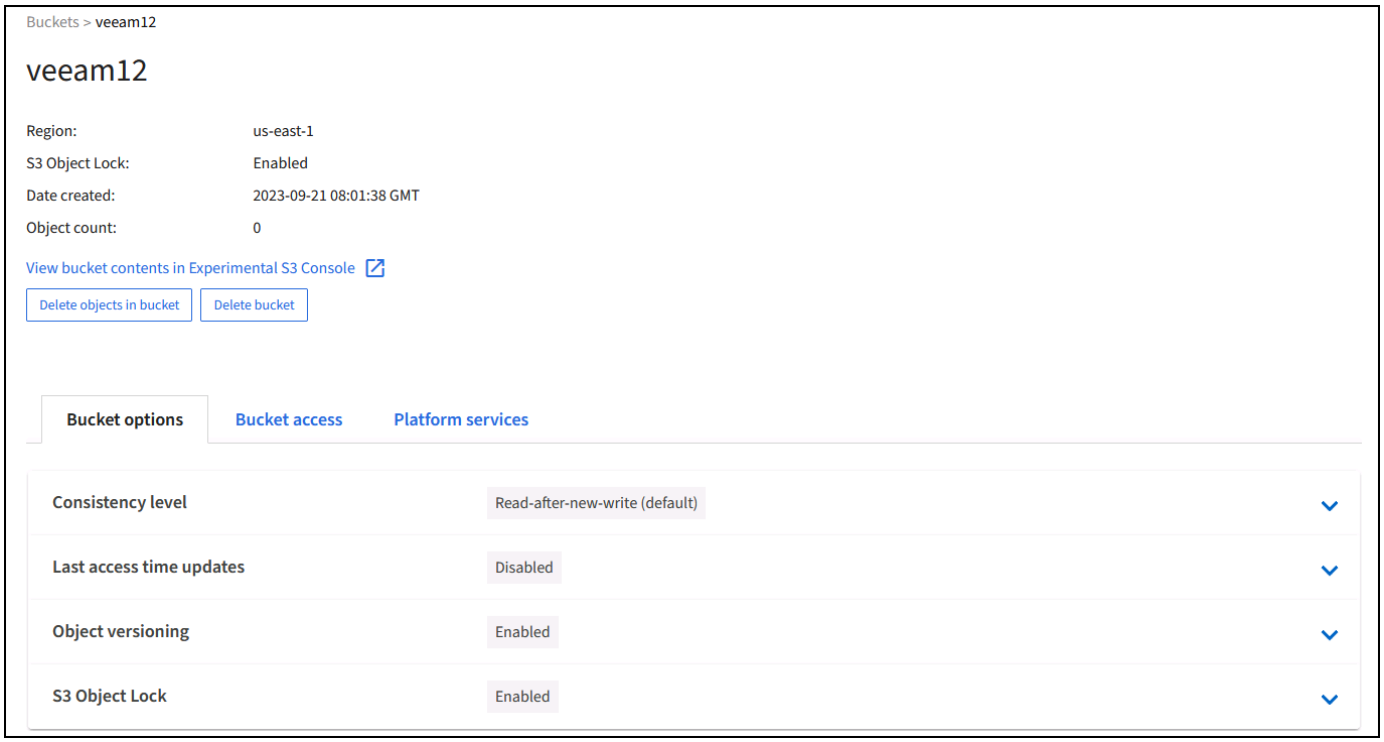
不変性が必要な場合は、StorageGRIDシステムでオブジェクトロックが有効になっていることを確認します。管理UIの[Configuration]/[S3][Object Lock]にあるオプションを選択します。



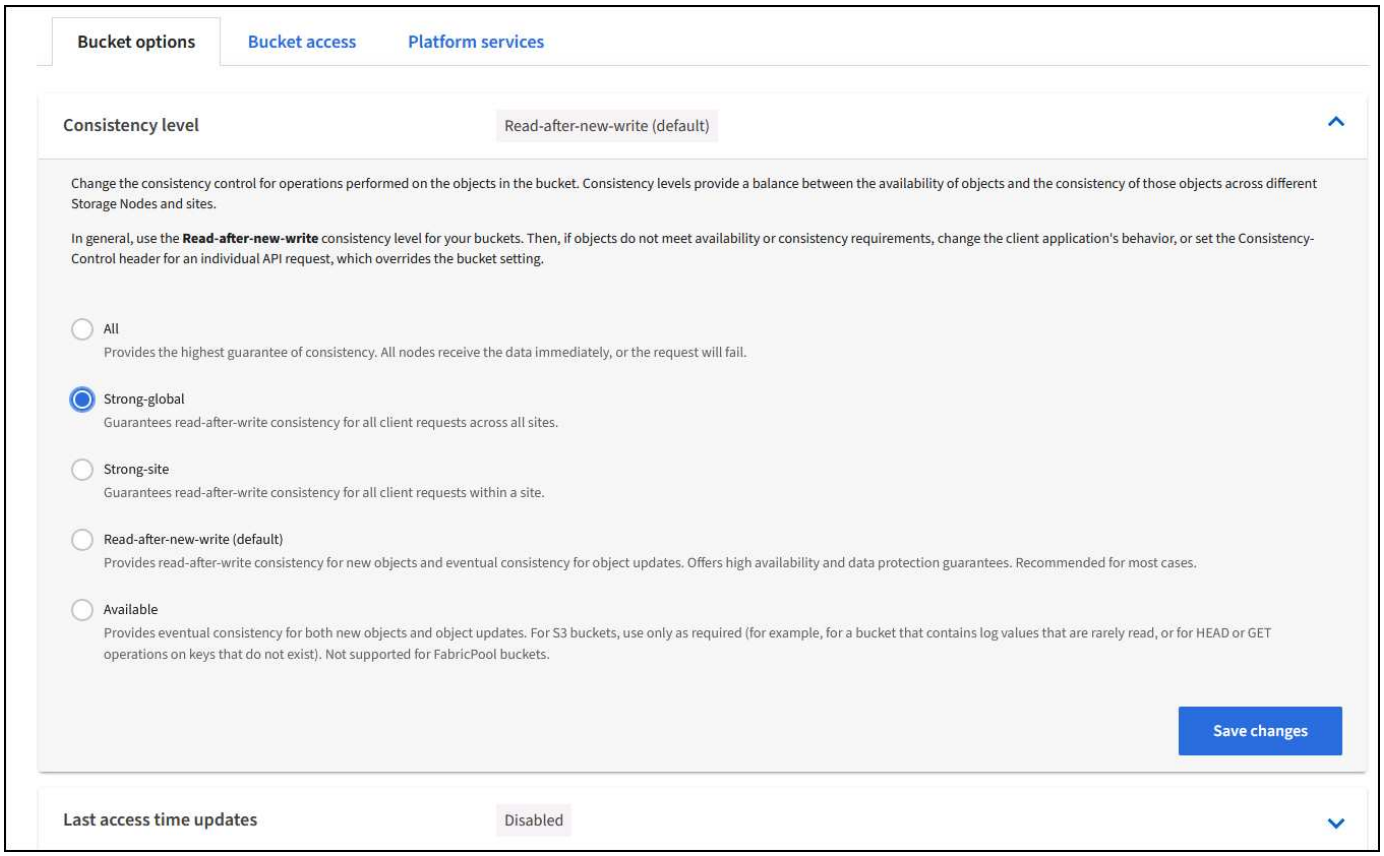
バケットを変更不可のバックアップに使用する場合は、バケットの作成時に[Enable S3 Object Lock]を選択します。これにより、バケットのバージョン管理が自動的に有効になります。オブジェクト保持期間はVeeamによって明示的に設定されるため、デフォルトの保持期間は無効のままにします。Veeamで変更不可のバックアップが作成されていない場合は、[Versioning]と[S3 Object Lock]を選択しないでください。



バケットが作成されたら、作成したバケットの詳細ページに移動します。整合性レベルを選択します。



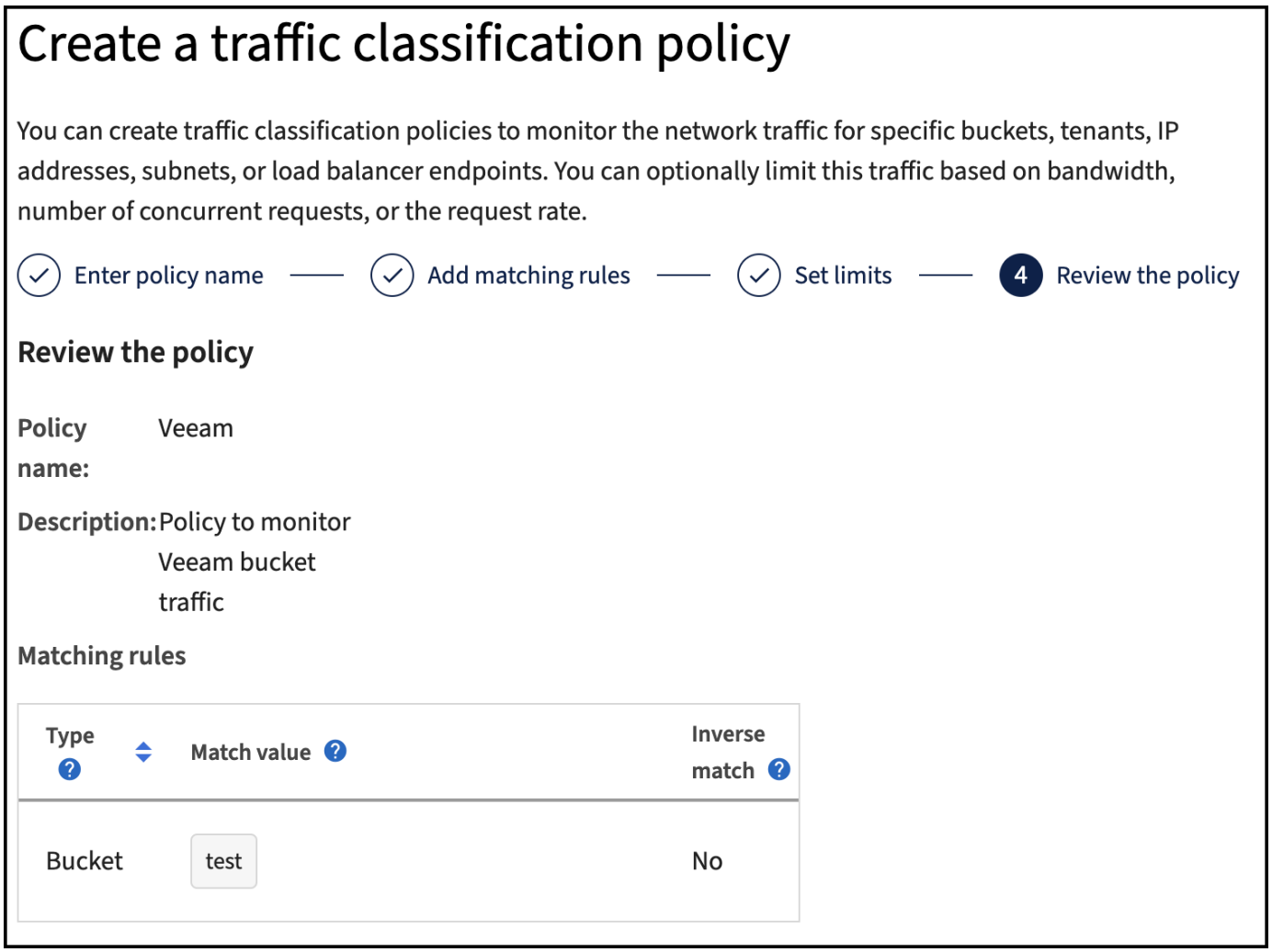
Veeamでは、S3バケットに対して強力な整合性が必要です。そのため、Veeamが複数の場所からデータにアクセスするマルチサイト環境の場合は、「strong-global」を選択します。Veeamのバックアップとリストアを単一サイトでのみ実行する場合は、整合性レベルを「strong-site」に設定する必要があります。変更を保存します。



StorageGRIDは、すべての管理ノードおよび専用のゲートウェイノードで統合されたロードバランササービス

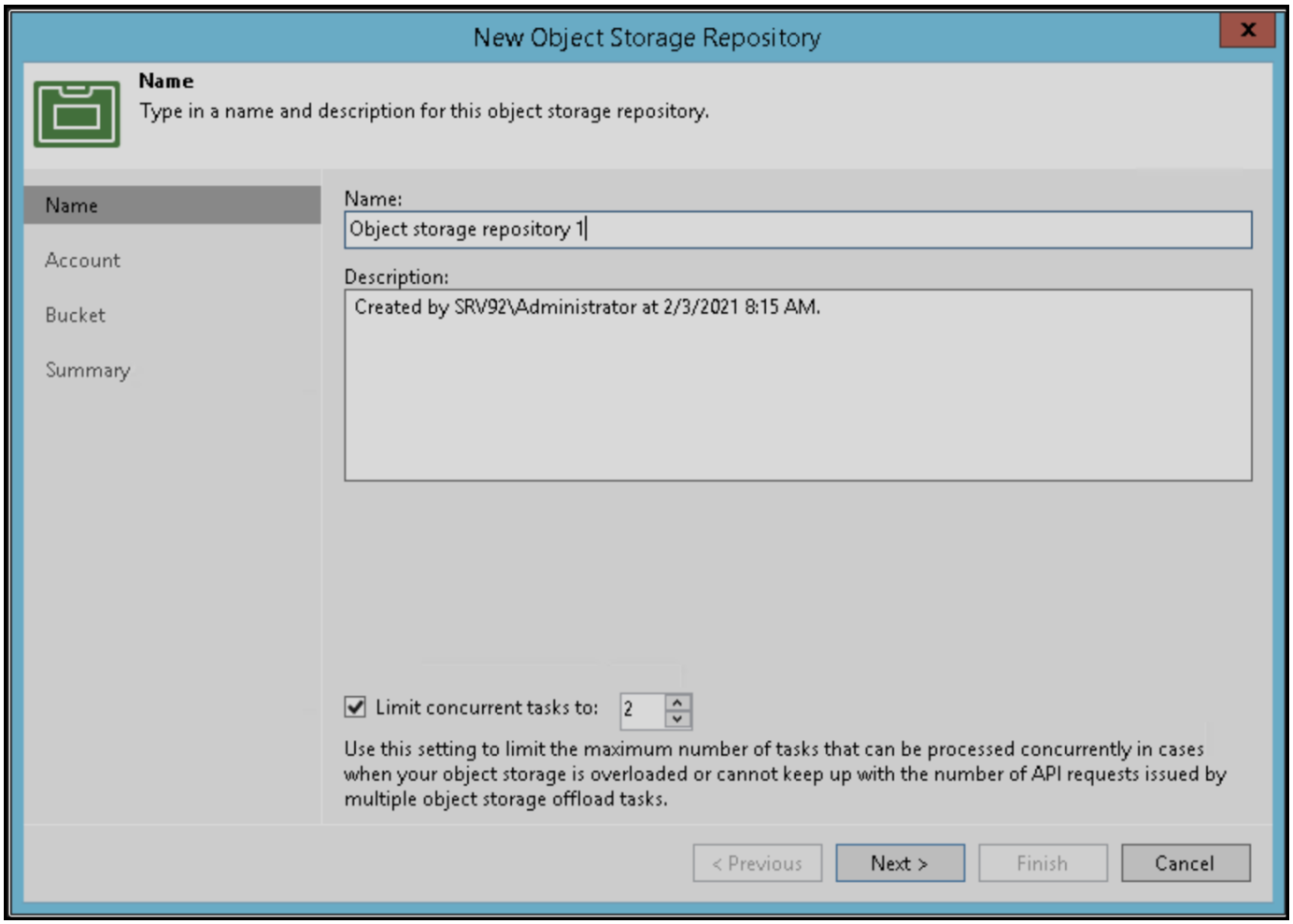
を提供します。このロードバランサを使用する多くの利点の1つは、トラフィック分類ポリシー（QoS）を設定できることです。主に、他のクライアントワークロードへのアプリケーションの影響を制限したり、他のクライアントワークロードよりもワークロードを優先したりするために使用されますが、監視に役立つ追加の指標収集のボーナスも提供します。

[Configuration]タブで、[Traffic Classification]を選択し、新しいポリシーを作成します。ルールに名前を付け、タイプとしてバケットまたはテナントを選択します。バケットまたはテナントの名前を入力します。QoSが必要な場合は制限を設定しますが、ほとんどの実装では、制限を設定しないでください。

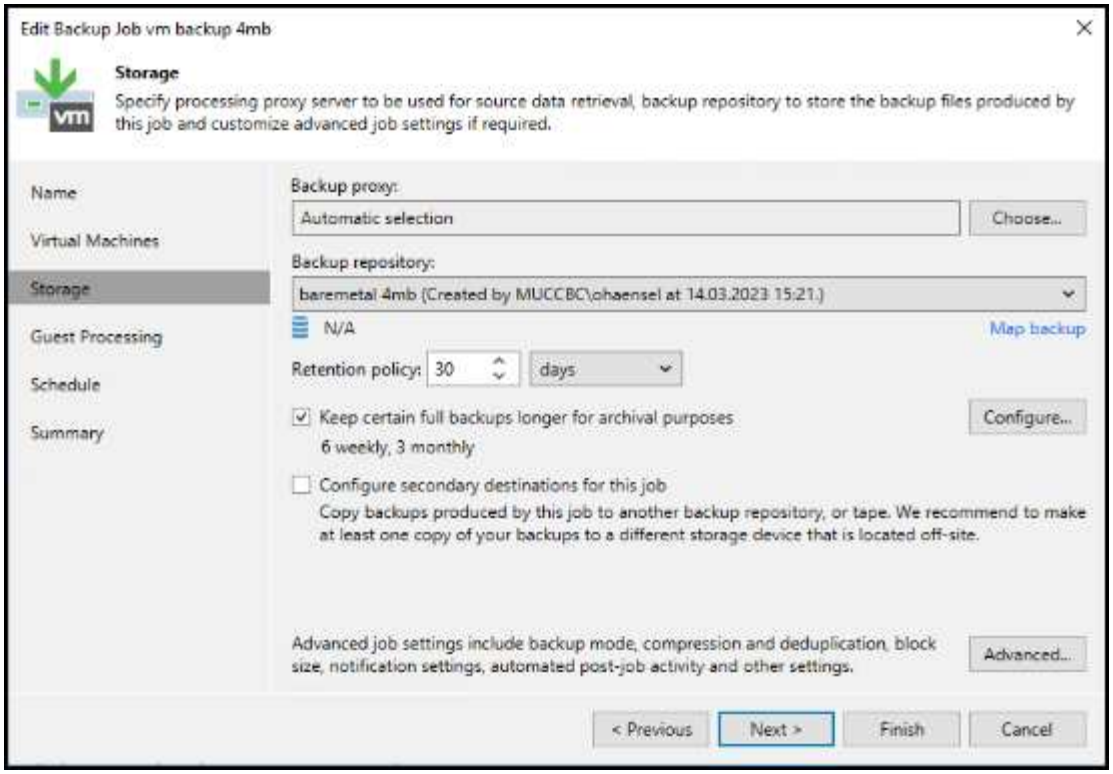


Veeamの統合によって

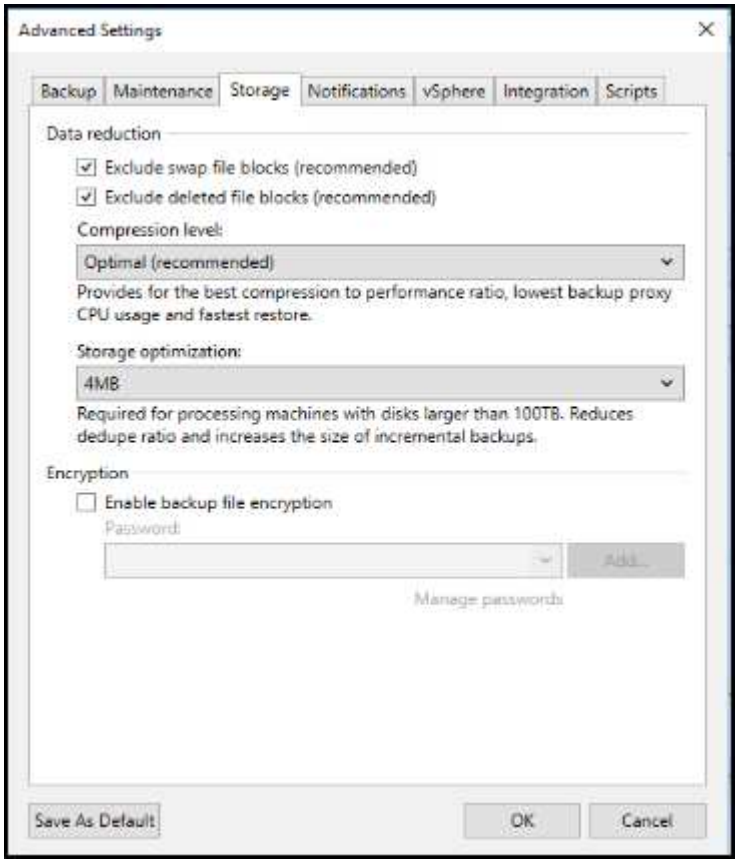
StorageGRIDアプライアンスのモデルと数によっては、バケットで同時に実行できる処理数の制限を選択して設定する必要があります。



Veeamコンソールのバックアップジョブ設定に関するVeeamのドキュメントに従って、ウィザードを開始します。VMを追加したら、SOBRリポジトリを選択します。



[詳細設定]をクリックし、ストレージ最適化設定を4 MB以上に変更します。圧縮機能と重複排除機能を有効にします。要件に応じてゲスト設定を変更し、バックアップジョブのスケジュールを設定します。



StorageGRID の監視

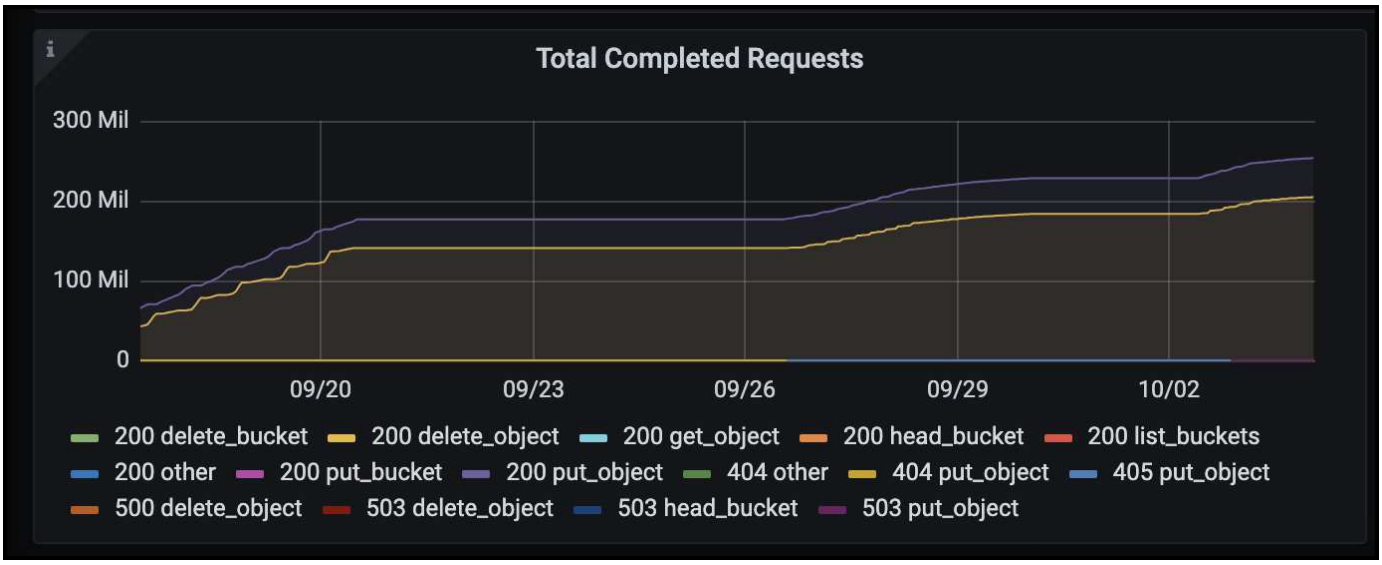
VeeamとStorageGRIDの連携によるパフォーマンスの全体像を把握するには、最初のバックアップの保持期限が切れるまで待つ必要があります。これまで、Veeamのワークロードは主にPUT処理で構成され、削除は行われていませんでした。バックアップデータの有効期限が近づいてクリーンアップを実行すると、オブジェクトストアに一貫した使用状況が表示され、必要に応じてVeeamで設定を調整できます。

StorageGRIDには、[Support]タブの[Metrics]ページにあるシステムの動作を監視するための便利なチャートが用意されています。主にS3の[Overview]、[ILM]、[Traffic Classification Policy]（ポリシーが作成されている場合）の各ダッシュボードを確認します。S3の[Overview]ダッシュボードには、S3の処理率、レイテンシ、要求応答に関する情報が表示されます。

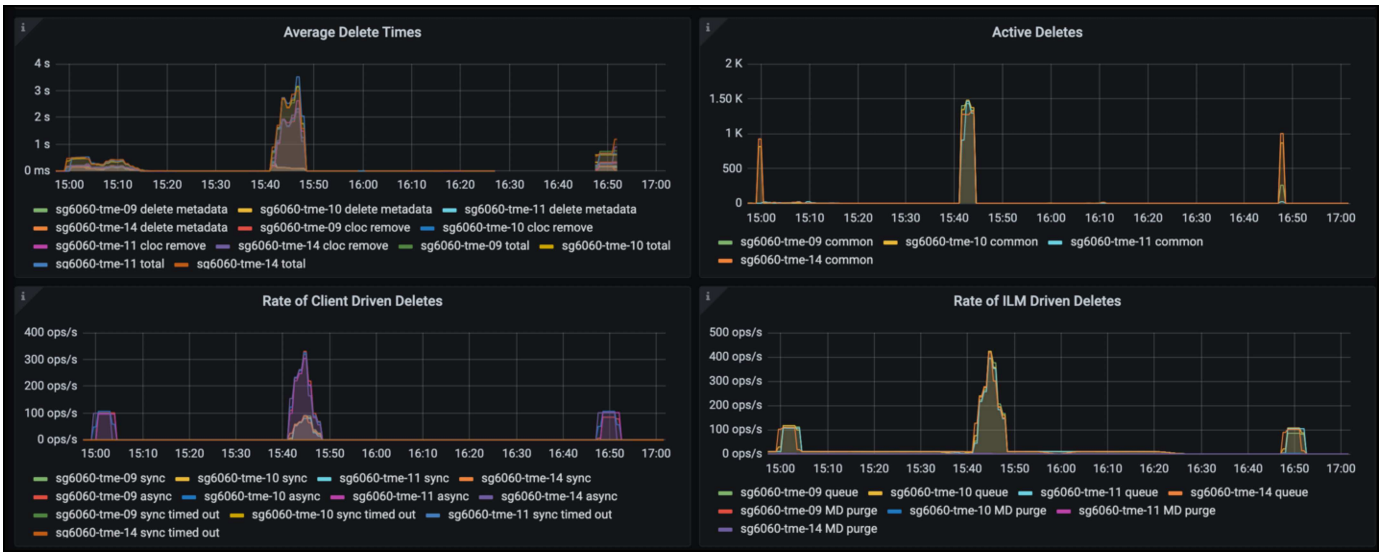
S3の速度とアクティブな要求を確認すると、各ノードで処理されている負荷の量と、タイプ別の要求の総数を確認できます。

[Average Duration]チャートには、各ノードの要求タイプごとの平均所要時間が表示されます。これはリクエストの平均遅延で、追加の調整が必要か、StorageGRIDシステムがより多くの負荷を引き受ける余地があることを示しているかもしれません。

[Total Completed Requests]チャートでは、リクエストをタイプコードと応答コード別に表示できます。応答に200（OK）以外の応答が表示された場合、これは、StorageGRIDシステムのような問題が503（スローダウン）応答を送信しており、追加の調整が必要になるか、負荷が増加するためにシステムを拡張する時間が来たことを示している可能性があります。



[ILM]ダッシュボードでは、StorageGRIDシステムの削除のパフォーマンスを監視できます。StorageGRIDでは、各ノードで同期削除と非同期削除を組み合わせて使用し、すべての要求の全体的なパフォーマンスを最適化しようとします。



トラフィック分類ポリシーを使用すると、ロードバランサ要求のスループット、レート、期間、およびVeeamが送受信するオブジェクトサイズに関するメトリックを表示できます。

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製品ドキュメント"
- "Veeam Backup Replication"

StorageGRIDを使用したDremioデータソースの設定

Angela Cheng著_

Dremioは、クラウドベースやオンプレミスのオブジェクトストレージなど、多様なデータソースをサポートしています。 StorageGRIDをオブジェクトストレージデータソースとして使用するようにDremioを設定できます。

Dremioデータソースの設定

前提条件

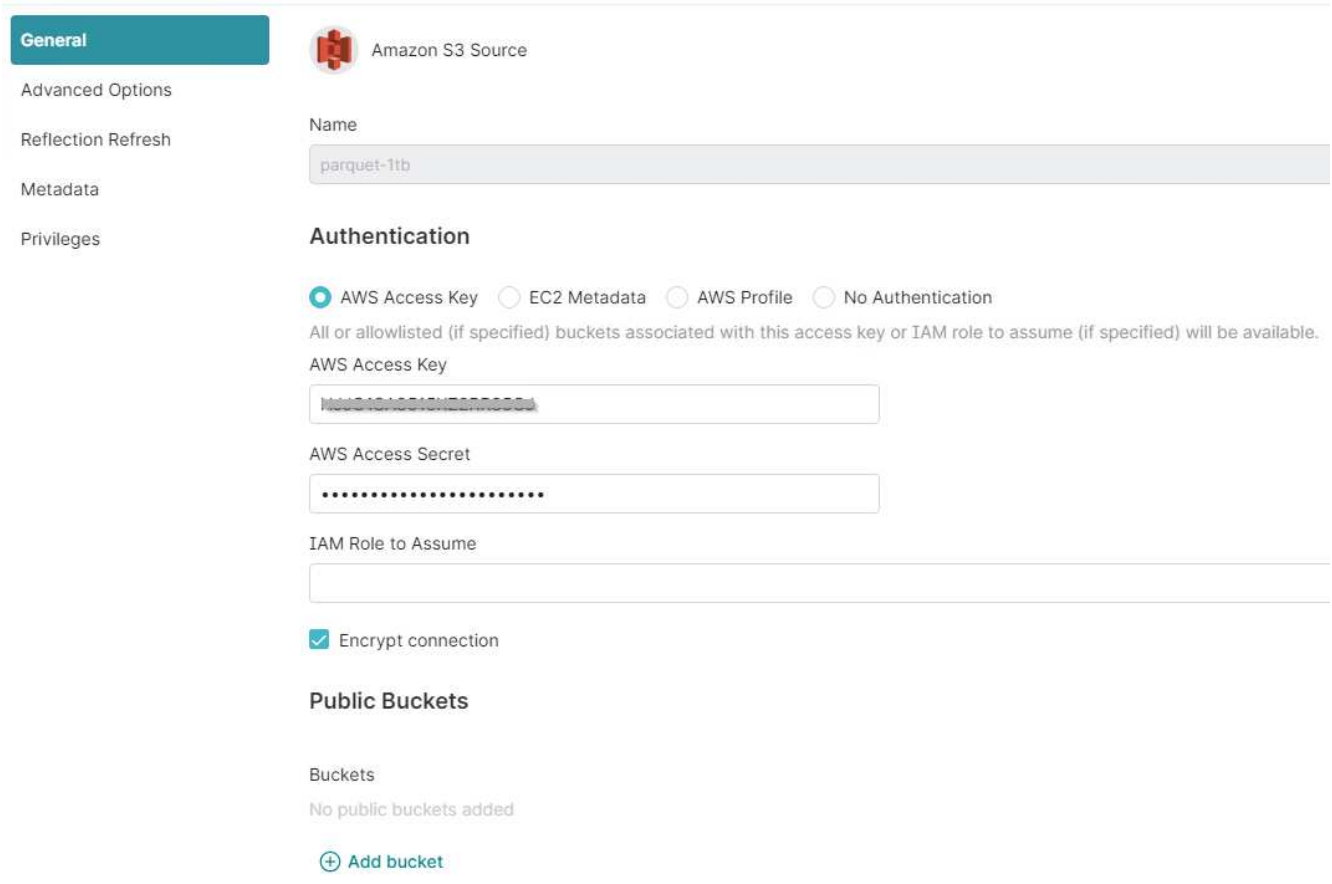
- StorageGRID S3エンドポイントURL、テナントs3アクセスキーID、シークレットアクセスキー。
- StorageGRID構成の推奨事項：圧縮を無効にします（デフォルトでは無効）。 [+]
  Dremioは、Byte range GETを使用して、クエリ中に同じオブジェクト内から異なるバイト範囲を同時に取得します。 バイト範囲要求の一般的なサイズは1MBです。圧縮オブジェクトを使用すると、バイト範囲GETのパフォーマンスが低下します。

Dremioガイド

"Amazon S3への接続- S3互換ストレージの設定"。

指示

1. [Dremio Datasets]ページで、[+]をクリックしてソースを追加し、[Amazon S3]を選択します。
2. この新しいデータソースの名前（StorageGRID S3のテナントアクセスキーIDとシークレットアクセスキー）を入力します。
3. StorageGRID S3エンドポイントへの接続にhttpsを使用する場合は、[Encrypt connection]チェックボックスをオンにします。[+]
   このs3エンドポイントで自己署名CA証明書を使用する場合は、Dremioのガイド手順に従って、このCA証明書をDremioサーバの<JAVA_HOME>/jre/lib/security+に追加します。
   サンプルスクリーンショット

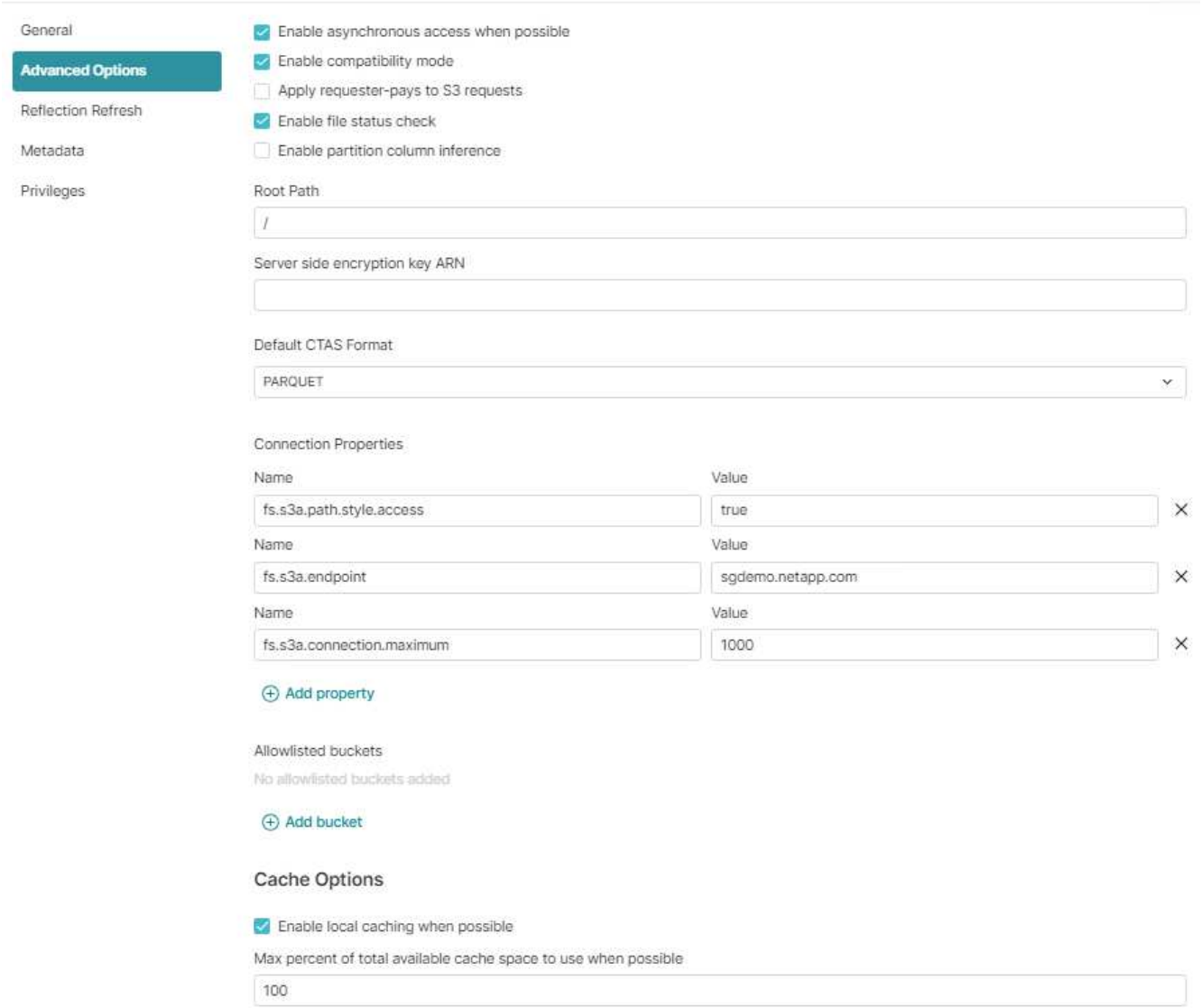


4. [詳細オプション]をクリックし、[互換モードを有効にする]をオンにします。

5. [Connection properties]で、[+ Add Properties]をクリックして、これらのs3aプロパティを追加します。
6. fs.s3a.connection.maximumデフォルトは100です。 s3データセットに100列以上の大きな寄木細工ファイルが含まれている場合は、100より大きい値を入力する必要があります。 この設定については、Dremioのガイドを参照してください。

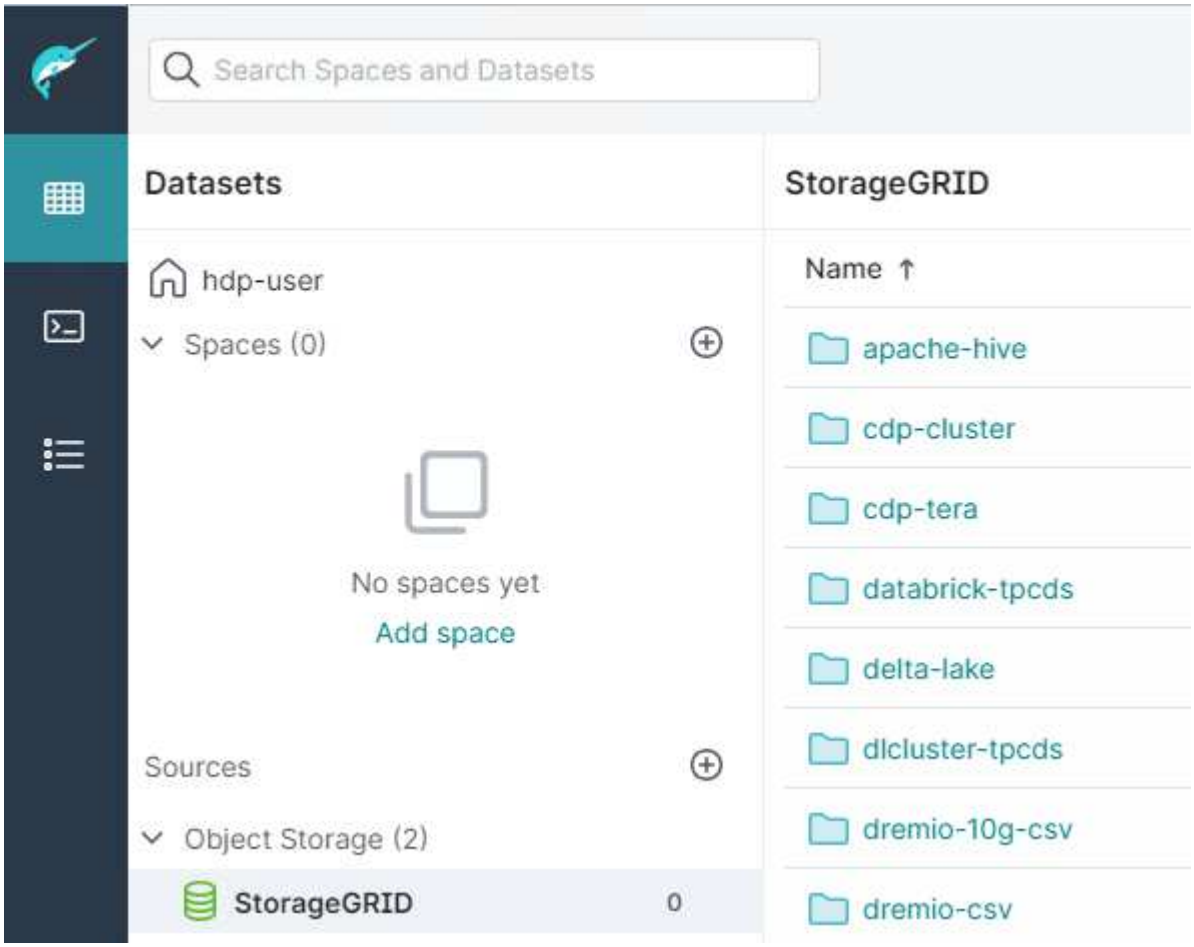
名前	価値
FS.s3a.endpoint	_ StorageGRID S3エンドポイント：port>_
FS.s3a.path.style.access	正しいです
fs.s3a.connection.maximum	< *100*より大きい値>

サンプルスクリーンショット



7. 組織またはアプリケーションの要件に応じて、その他のDremioオプションを設定します。

8. [Save]ボタンをクリックして新しいデータソースを作成します。
9. StorageGRIDデータソースが正常に追加されると、バケットのリストが左側のパネルに表示されます。[+]
サンプルスクリーンショット



NetApp StorageGRIDとGitLab

Angela Cheng著_

NetAppはStorageGRIDをGitLabでテストしました。以下のGitLabの設定例を参照してください。 を参照してください "GitLabオブジェクトストレージ構成ガイド" を参照してください。

オブジェクトストレージの接続例

Linuxパッケージのインストールの場合は、次の例を参照してください。 `connection` 統合フォームでの設定。編集 `/etc/gitlab/gitlab.rb` 次の行を追加し、必要な値を置き換えます。

```
# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

手順とAPIの例

StorageGRID でS3暗号化オプションをテストして実証

アロンクライン著

StorageGRID とS3 APIには、保存データを暗号化するためのさまざまな方法が用意されています。詳細については、を参照してください "StorageGRID の暗号化方式を確認します"。

このガイドでは、S3 APIの暗号化メソッドについて説明します。

サーバー側の暗号化（SSE）

SSEを使用すると、クライアントがオブジェクトを格納し、StorageGRID で管理される一意のキーで暗号化できます。オブジェクトが要求されると、StorageGRID に格納されたキーによってオブジェクトが復号化されます。

SSEの例

- SSEを持つオブジェクトを配置します

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- オブジェクトのヘッダーで暗号化を確認します

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- オブジェクトを取得します

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

ユーザ指定のキーによるサーバ側の暗号化（SSE-C）

SSEを使用すると、クライアントがオブジェクトを格納し、クライアントがオブジェクトで提供する一意のキーでオブジェクトを暗号化できます。オブジェクトが要求されたときに、オブジェクトを復号化して返すために同じキーを指定する必要があります。

SSE-Cの例

- テストまたはデモ目的で暗号化キーを作成できます
  - 暗号化キーを作成します

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- 生成されたキーを持つオブジェクトを配置します

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- オブジェクトの先頭に追加します

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:20:02+00:00",
    "ContentLength": 47,
    "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
    "ContentType": "binary/octet-stream",
    "Metadata": {},
    "SSECustomerAlgorithm": "AES256",
    "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
}
```

暗号化キーを指定しないと、「The error occurred (404) when calling the HeadObject operation: not found"」(ヘッダオブジェクト操作:見つかりません)というエラーが表示されます。

- オブジェクトを取得します

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

暗号化キーを指定しないと、「An error occurred（InvalidRequest）when calling the GetObject operation：the object was stored using a form of Server Side Encryption」というエラーが表示されます。オブジェクトを読み出すには、正しいパラメータを指定する必要があります。"

バケットサーバ側の暗号化（SSE-C）

SSE-Cを使用すると、バケットに格納されているすべてのオブジェクトのデフォルトの暗号化動作をクライアントで定義できます。オブジェクトはStorageGRID で管理される一意のキーで暗号化されます。オブジェクトが要求されると、StorageGRID に格納されているキーによってオブジェクトが復号化されます。

バケット**SSE-C**の例

- 新しいバケットを作成し、デフォルトの暗号化ポリシーを設定
  - 新しいバケットを作成する

```
aws s3api create-bucket --bucket <bucket> --region us-east-1
--endpoint-url https://s3.example.com
```

  - PUT Bucket encryptionの設定

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- オブジェクトをバケットに配置します

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- オブジェクトの先頭に追加します

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- オブジェクトを取得します

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

StorageGRID でS3オブジェクトロックをテストして実証

アロンクライン著

Object Lockは、オブジェクトが削除または上書きされないようにWORMモデルを提供します。StorageGRIDによるオブジェクトロックの実装では、規制要件を満たし、オブジェクト保持のリーガルホールドとコンプライアンスモードをサポートし、バケットのデフォルト保持ポリシーをサポートするように、Cohassetが評価されます。

このガイドでは、S3オブジェクトロックAPIについて説明します。

リーガルホールド

- オブジェクトロックリーガルホールドは、オブジェクトに適用される単純なオン/オフステータスです。

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- GET処理で検証します。

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- リーガルホールドをオフにします

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- GET処理で検証します。

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Complianceモード

- オブジェクトの保持には、タイムスタンプがretain untilを使用します。

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- 保持ステータスを確認

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

デフォルトの保持

- オブジェクト単位のAPIで定義された保持期限を日数と年数で設定します。

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- 保持ステータスを確認

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- オブジェクトをバケットに配置します

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- バケットで設定された保持期間がオブジェクトの保持タイムスタンプに変換されます。

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

保持期間が定義されているオブジェクトの削除をテストします

オブジェクトロックは、バージョン管理の上に構築されます。保持期間はオブジェクトのバージョンで定義されます。保持が定義されているオブジェクトを削除しようとしたときに、バージョンが指定されていない場合は、削除マーカーがオブジェクトの現在のバージョンとして作成されます。

- 保持期間が定義されたオブジェクトを削除します

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- バケット内のオブジェクトをリストします

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

◦ オブジェクトがリストされていないことに注意してください。

- 削除マーカーとロックされた元のバージョンを表示するには、バージョンをリストします

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- ロックされているオブジェクトのバージョンを削除します

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

StorageGRIDのポリシーと権限

ここでは、StorageGRID S3のポリシーと権限の例を示します。

ポリシーの構造

StorageGRIDでは、グループポリシーはAWSユーザ（IAM）のS3サービスポリシーと同じです。

StorageGRIDではグループポリシーが必要です。S3アクセスキーを持っていてユーザグループに割り当てられていないユーザや、一部の権限を許可するポリシーが設定されていないグループに割り当てられているユーザは、データにアクセスできません。

バケットポリシーとグループポリシーは、ほとんどの要素を共有します。ポリシーはJSON形式で作成され、"AWSポリシージェネレータ"

すべてのポリシーで、効果、アクション、リソースが定義されます。バケットポリシーではプリンシパルも定義されます。

Effect*はリクエストを許可するか拒否するかのどちらかになります。

プリンシパル

- バケットポリシーにのみ適用されます。
- プリンシパルは、権限を付与または拒否するアカウント/ユーザです。
- 次のように定義できます。
  - ワイルドカード"+*"

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

  - テナント内のすべてのユーザのテナントID（AWSアカウントに相当）

```
"Principal": { "AWS": "27233906934684427525" }
```

- ユーザ（バケットが存在するテナント内からのローカルまたはフェデレーテッド、またはグリッド内の別のテナント）

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

- グループ（バケットが配置されているテナント内からのローカルまたはフェデレーテッド、またはグリッド内の別のテナント）。

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

Action *は、ユーザに許可または拒否される一連のS3処理です。

グループポリシーの場合、S3操作を実行するには、許可されているs3：ListBucket操作が必要です。

Resource *は、プリンシパルに対してアクションの実行を許可または拒否するバケットです。必要に応じて、ポリシーアクションが有効な場合の*条件*を指定できます。

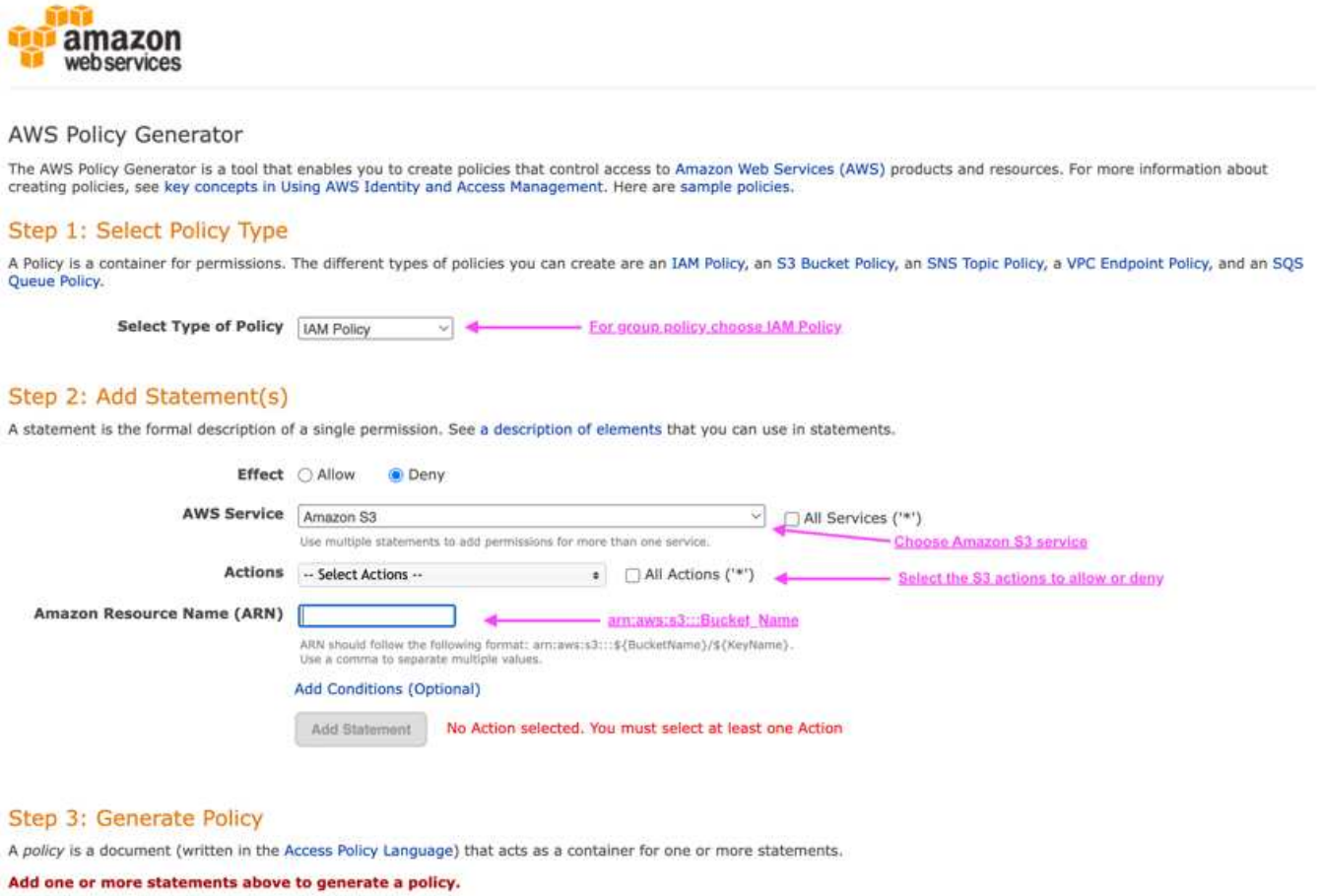
JSONポリシーの形式は次のようになります。

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

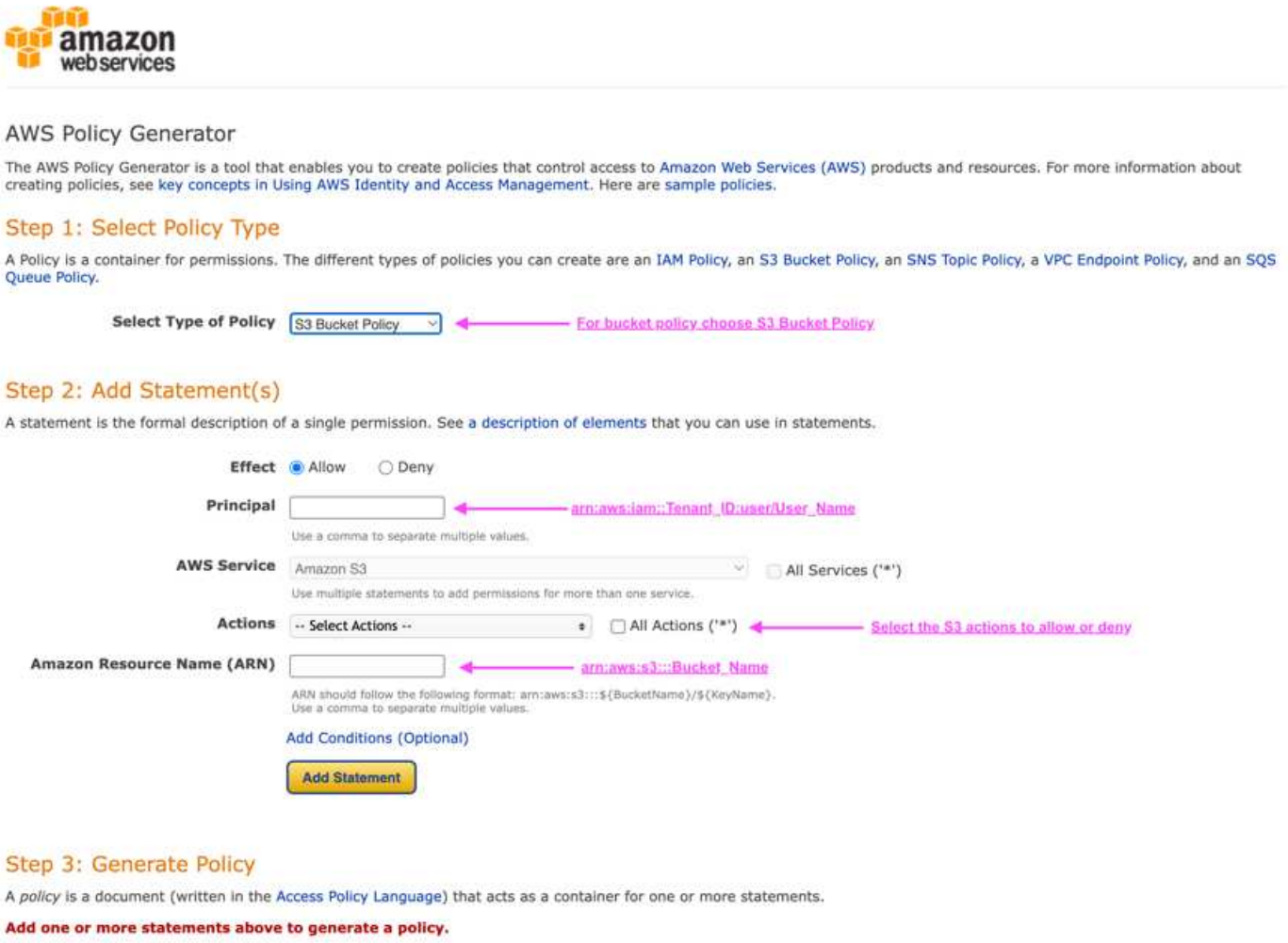
AWSポリシージェネレータの使用

AWSポリシージェネレータは、実装しようとしている正しい形式と情報でJSONコードを取得するのに役立つ優れたツールです。

StorageGRIDグループポリシーの権限を生成するには、次の手順を実行します。ポリシーのタイプに応じた**IAM**ポリシーを選択します。*希望する効果のボタンを選択します。「許可」または「拒否」です。ポリシーで**deny**権限を指定して開始し、アクションドロップダウンに**Allow**権限*を追加することを推奨します。この権限または**[**すべての操作**]**ボックスに含める**S3**操作の横にあるボックスをクリックします。[Amazon Resource Name（ARN）]ボックスにバケットパスを入力します。バケット名の前に「arn：aws：s3：：：」を含めます。ex."arn：aws：s3：：：example_bucket"

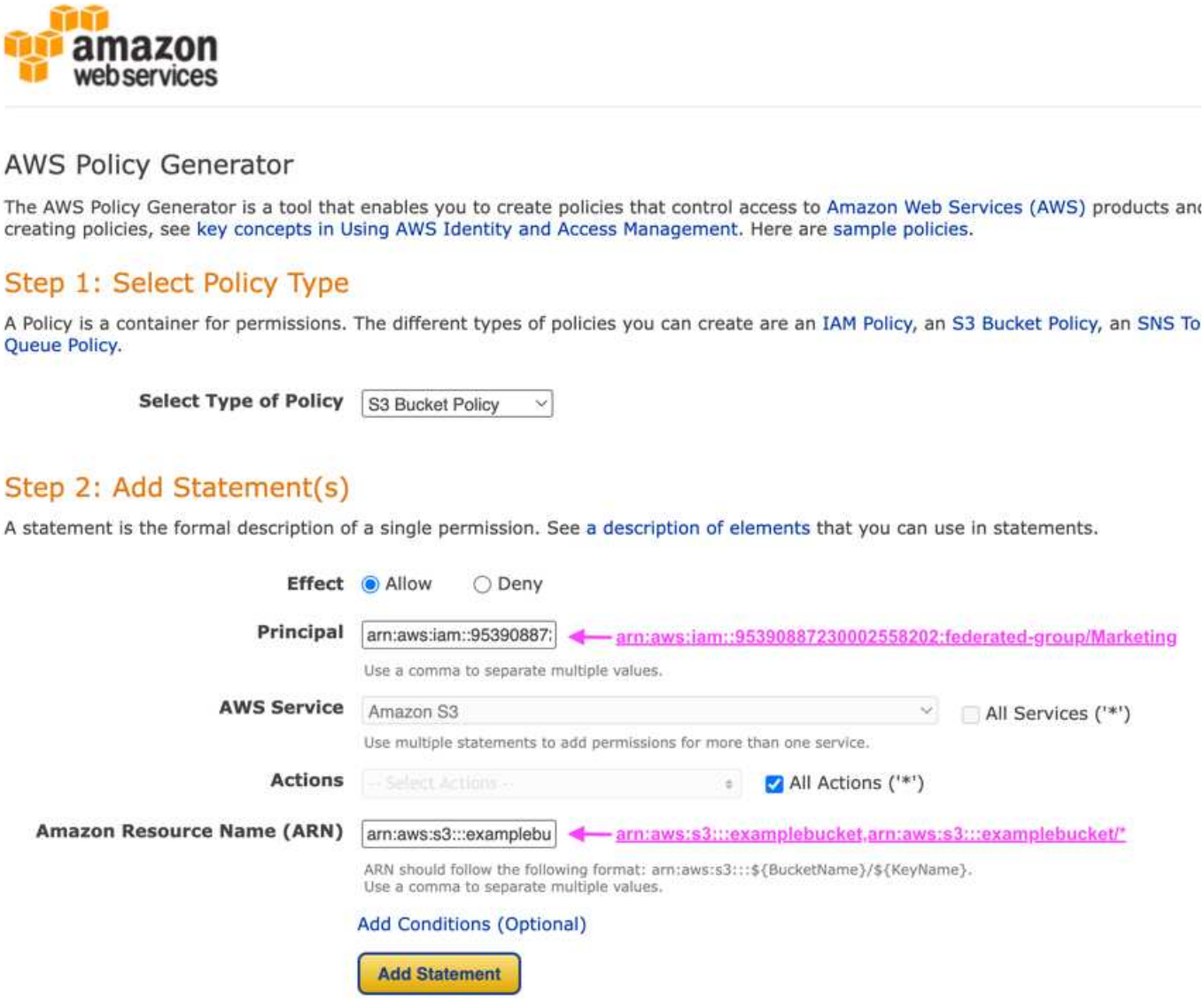


バケットポリシーの権限を生成するには：ポリシーのタイプに**[S3 Bucket Policy]**を選択します。*希望する効果のボタンを選択します。「許可」または「拒否」です。ポリシーを**deny**権限で開始し、**Principal**のユーザまたはグループ情報に**Allow permissions * Type**を追加することを推奨します。[Actions]ドロップダウンで、この権限または[All Actions]ボックスに含めるS3アクションの横にあるボックスをクリックします。*[Amazon Resource Name（ARN）]ボックスにバケットパスを入力します。バケット名の前に「arn：aws：s3：：：」を含めます。ex."arn：aws：s3：：：example_bucket"



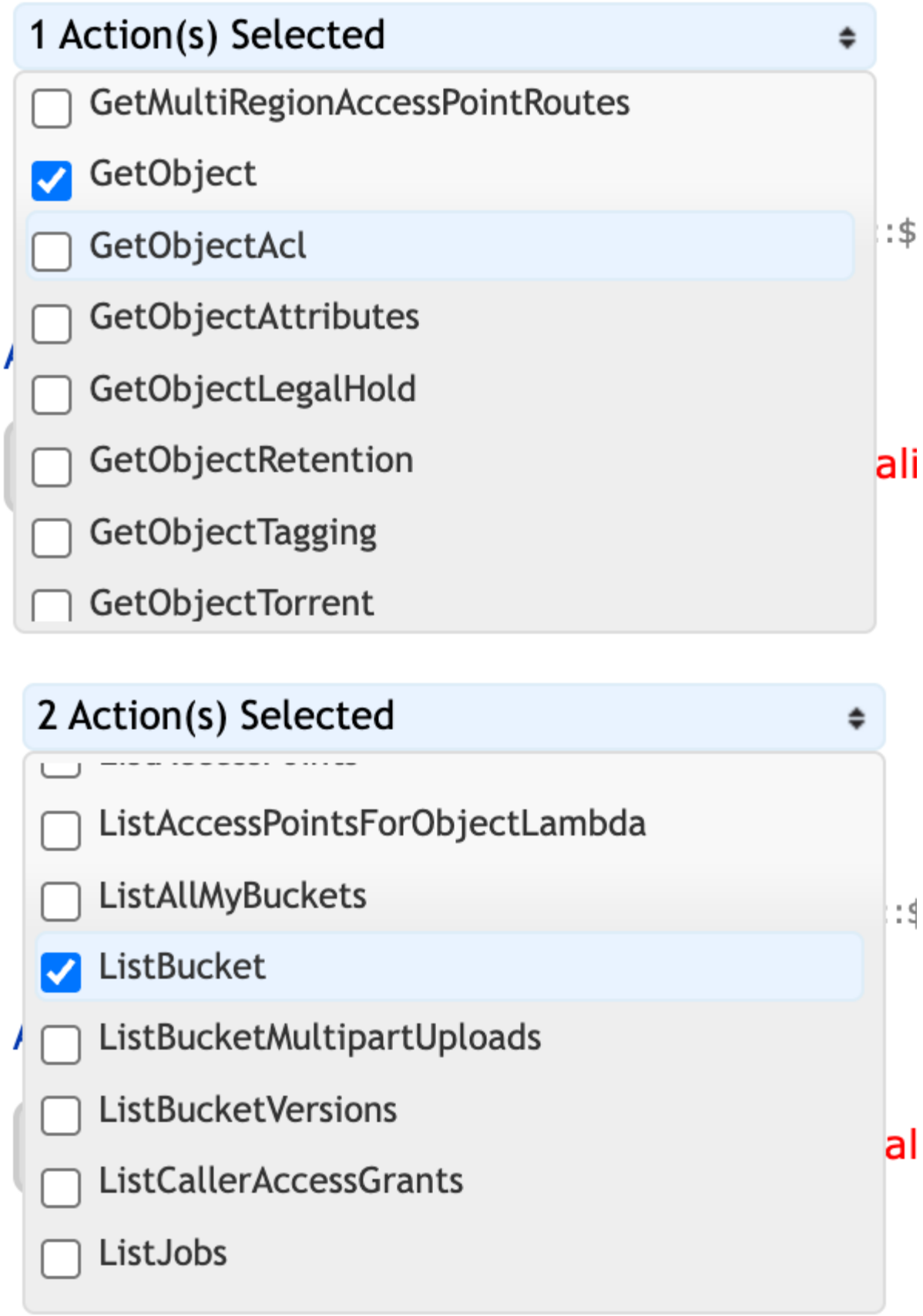
たとえば、すべてのユーザにバケット内のすべてのオブジェクトに対するGetObject処理の実行を許可するバケットポリシーを生成し、指定したアカウントの「Marketing」グループに属するユーザにのみフルアクセスを許可するとします。

- ポリシータイプとして[S3][Bucket Policy]を選択します。
- 「許可」エフェクトを選択します。
- マーケティンググループの情報を入力します。arn：aws：iam：：95390887230002558202：federated-group/Marketing
- [すべてのアクション]のボックスをクリックします。
- バケット情報を入力します。arn：aws：s3：：：example_bucket、arn：aws：s3：：：example_bucket/*



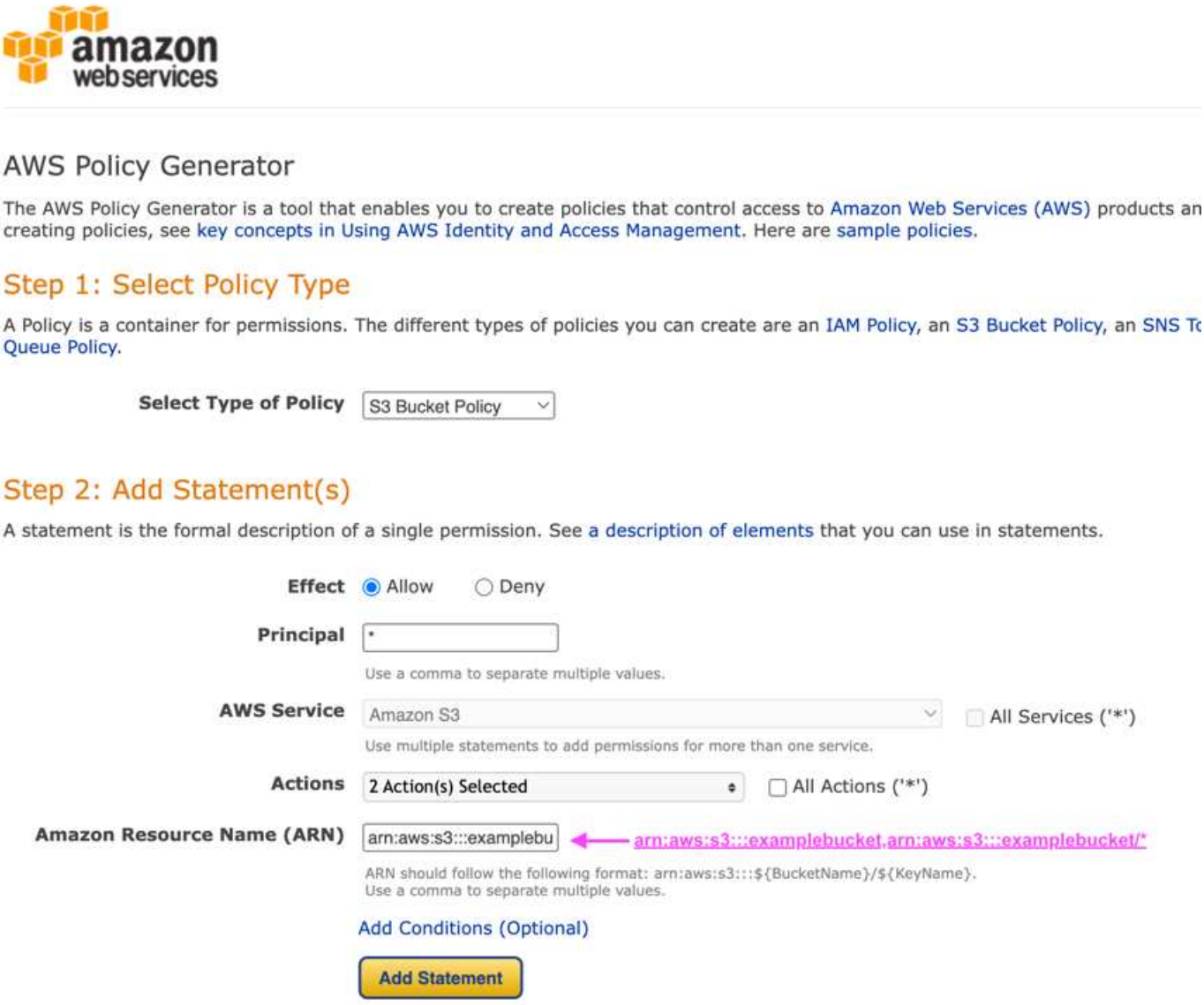
- [Add Statement]ボタンをクリックします。

- 「許可」エフェクトを選択します。
- すべてのユーザのアスタリスク「*」を入力します。
- [GetObject actions]と[ListBucket actions]の横にあるボックスをクリックします。

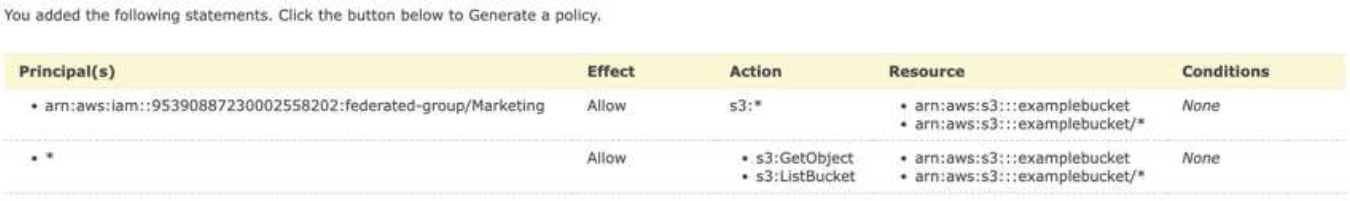


- バケット情報を入力します。arn：aws：s3：：：example_bucket、arn：aws：s3：：：example_bucket

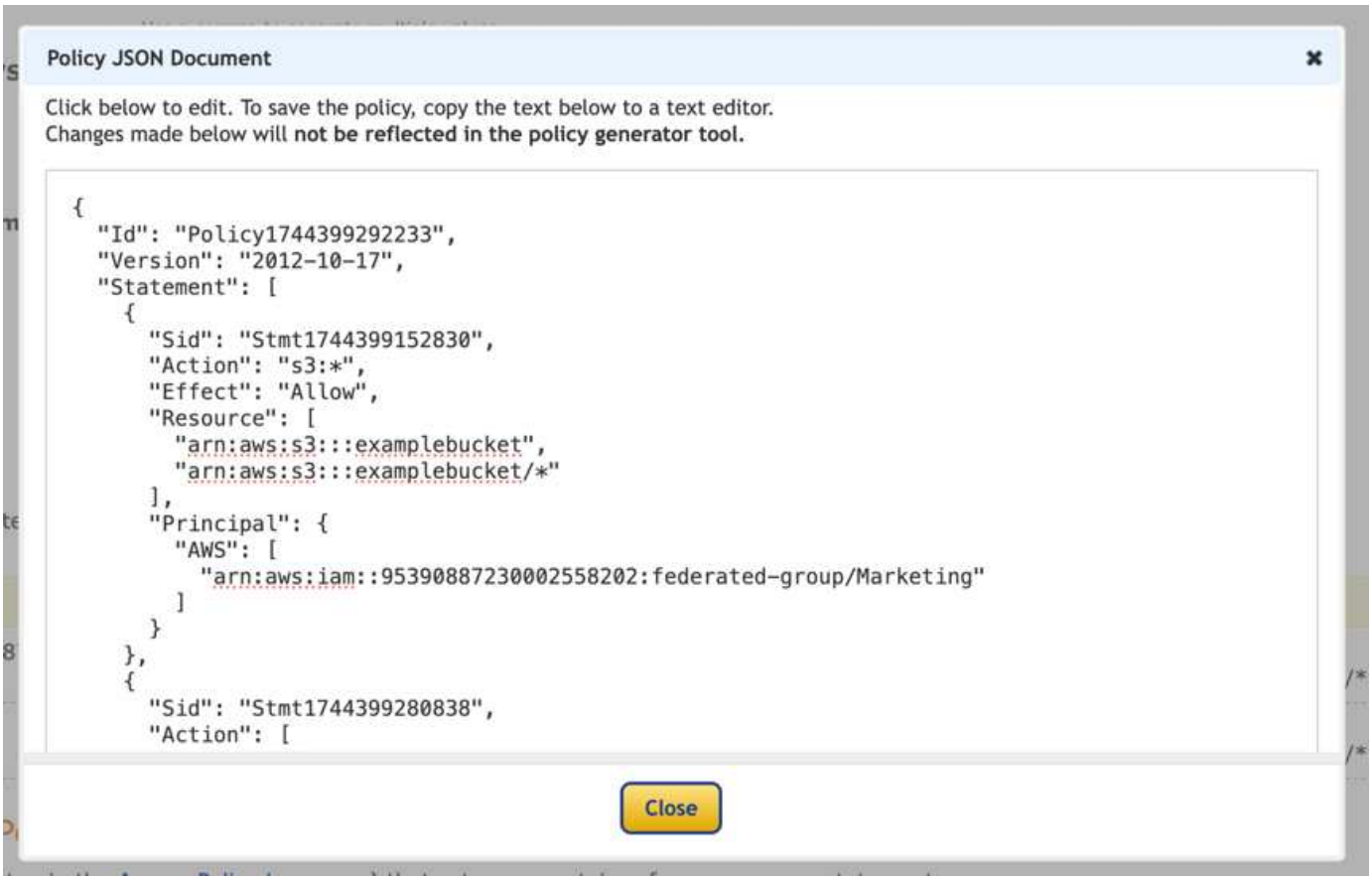
/*



- [Add Statement]ボタンをクリックします。



- 「ポリシーの生成」ボタンをクリックすると、生成されたポリシーを含むポップアップウィンドウが表示されます。



- 次のような完全なJSONテキストをコピーします。

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

このJSONはそのまま使用することも、"Statement"行の上にあるIDとバージョンの行を削除することもできます。また、アクセス許可ごとに、より意味のあるタイトルでSIDをカスタマイズしたり、削除したりすることもできます。

例：

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

グループポリシー（IAM）

ホームディレクトリ形式のバケットアクセス

このグループポリシーでは、users usernameという名前のバケット内のオブジェクトへのアクセスのみがユーザに許可されます。

```
{
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

オブジェクトロックバケットの作成を拒否します

このグループポリシーでは、ユーザがバケットを作成してそのバケットでオブジェクトロックを有効にすることはできません。

> このポリシーはStorageGRID UIでは適用されず、S3 APIでのみ適用されます。

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

オブジェクトロックの保持制限

このバケットポリシーでは、Object-Lockの保持期間が10日以下に制限されます

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

ユーザーによるオブジェクトの削除を**versionId**で制限します

このグループポリシーは、versionIdでバージョン管理オブジェクトを削除することをユーザに制限します

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

グループを読み取り専用アクセスで単一のサブディレクトリ（プレフィックス）に制限する

このポリシーでは、グループのメンバーにバケット内のサブディレクトリ（プレフィックス）への読み取り専用アクセスを許可します。バケット名は「study」、サブディレクトリは「study01」です。

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:s3::: study"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

バケットポリシー

バケットを読み取り専用アクセス権を持つ単一ユーザに制限します

このポリシーでは、1人のユーザにバケットへの読み取り専用アクセスを許可し、他のすべてのユーザへのアクセスを明示的に拒否します。評価を迅速に行うには、ポリシーの先頭にDenyステートメントをグループ化することを推奨します。

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

バケットを読み取り専用アクセス権を持つ少数のユーザに制限する。

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

バケット内のバージョン管理オブジェクトのユーザによる削除を制限する

このバケットポリシーは、ユーザ（ユーザID「56622399308951294926」で識別）がversionIdでバージョン管理オブジェクトを削除することを制限します

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

StorageGRIDのバケットライフサイクル

S3 ライフサイクル設定を作成して、特定のオブジェクトが StorageGRID システムから削除されるタイミングを制御できます。

ライフサイクル構成とは

ライフサイクル設定は、特定の S3 バケット内のオブジェクトに適用される一連のルールです。各ルールは、影響を受けるオブジェクトと、それらのオブジェクトの有効期限（特定の日付または日数後）を指定します。

各オブジェクトは、S3バケットライフサイクルまたはILMポリシーの保持設定に従います。S3バケットライフサイクルが設定されている場合は、バケットライフサイクルフィルタに一致するオブジェクトのILMポリシーがライフサイクル有効期限のアクションで上書きされます。バケットライフサイクルフィルタに一致しないオブジェクトには、ILMポリシーの保持設定が使用されます。オブジェクトがバケットライフサイクルフィル

タに一致し、有効期限の操作が明示的に指定されていない場合、ILMポリシーの保持設定は使用されず、オブジェクトのバージョンが無期限に保持されることが暗黙的に示されます。

そのため、 ILM ルールの配置手順がオブジェクトに引き続き適用されていても、オブジェクトがグリッドから削除されることがあります。あるいは、オブジェクトに対するILM配置指示が失効した後でも、オブジェクトがグリッド上に保持される可能性がある。

StorageGRID では、 1 つのライフサイクル設定で最大 1 、 000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。

- Expiration ：指定した日付に達した場合、またはオブジェクトが取り込まれたときから指定した日数に達した場合にオブジェクトを削除します。
- NoncurrentVersionExpiration ：指定した日数に達したオブジェクトを削除します。これは、オブジェクトが最新でなくなったときからです。
- フィルタ（プレフィックス、タグ）
- ステータス *ID

StorageGRID では、次のバケット処理を使用してライフサイクル設定を管理できます。

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ライフサイクルポリシーの構造

ライフサイクル設定を作成するための最初の手順として、 1 つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の 3 つのルールが含まれています。

1. *ルール1*は、プレフィックス「category1/」に一致し、key2の値が「tag2」であるオブジェクトにのみ適用されます。Expirationパラメータは、フィルターに一致するオブジェクトが2020年8月22日の午前0時に期限切れになることを指定します。
2. *ルール2*は、プレフィックス「category2/」に一致するオブジェクトにのみ適用されます。Expirationパラメータは、フィルターに一致するオブジェクトが取り込まれてから100日後に有効期限切れになることを指定します。

   日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. *ルール3*は、プレフィックス「category3/」に一致するオブジェクトにのみ適用されます。Expirationパラメータは、一致するオブジェクトの非現行バージョンが、非現行バージョンになってから50日後に期限切れになることを指定します。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

バケットにライフサイクル設定を適用

ライフサイクル設定ファイルを作成したら、PutBucketLifecycleConfiguration要求を発行してバケットに適用します。

この要求は、サンプルファイルのライフサイクル設定をという名前のバケット内のオブジェクトに適用し`testbucket`ます。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを確認するには、GetBucketLifecycleConfiguration要求を問題します。例えば：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

標準（バージョン管理されていない）バケットのライフサイクル ポリシーの例

90日後にオブジェクトを削除する

ユースケース：このポリシーは、一時ファイル、ログ、中間処理データなど、限られた期間のみ関連するデータの管理に最適です。メリット：ストレージコストを削減し、バケットを整理整頓できます。

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

バージョン管理されたバケットのライフサイクル ポリシーの例

10日後に非最新版を削除する

ユースケース：このポリシーは、時間の経過とともに蓄積され、大量のスペースを消費する可能性のある、最

新バージョンではないオブジェクトのストレージ管理に役立ちます。メリット：最新バージョンのみを保持することで、ストレージ使用量を最適化します。

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled",
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

5つの非最新バージョンを保持する

使用例: 回復または監査の目的で、限られた数の以前のバージョンを保持する場合に便利です。利点: 十分な履歴と回復ポイントを確保するために、十分な数の非最新バージョンを保持します。

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled",
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

他のバージョンが存在しない場合は削除マーカーを削除します

ユースケース：このポリシーは、すべての非最新バージョンを削除した後に残る削除マーカーを管理するのに役立ちます。これらのマーカーは時間の経過とともに蓄積される可能性があります。メリット：不要な混乱を軽減します。

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled",
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

現在のバージョンは **30** 日後に削除され、現在のバージョン以外のバージョンは **60** 日後に削除され、他のバージョンが存在しなくなったら現在のバージョンの削除によって作成された削除マーカーが削除されます。

ユースケース：削除マーカーを含む、現在のバージョンと非現在のバージョンの完全なライフサイクルを提供します。メリット：十分なリカバリポイントと履歴を保持しながら、ストレージコストを削減し、バケットを整理された状態に保ちます。

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

他のバージョンがない削除マーカーを削除し、「**accounts_** プレフィックス」を持つオブジェクトについては **4** つの非最新バージョンと少なくとも **30** 日分の履歴を保持し、他のすべてのオブジェクト バージョンについては **2** つのバージョンと少なくとも **10** 日分の履歴を保持します。

ユースケース：特定のオブジェクトと他のオブジェクトに固有のルールを適用し、削除マーカーを含む現在のバージョンと非現在のバージョンのライフサイクル全体を管理します。メリット：ストレージコストを削減し、バケットを整理しながら、十分なリカバリポイントと履歴を保持することで、多様なクライアント要件に対応できます。

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    },
    {
      "ID": "accounts version retention",
      "Filter": {"Prefix":"account_"},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

まとめ

- ライフサイクル ポリシーを定期的に確認および更新し、ILM およびデータ管理の目標に合わせて調整します。
- ポリシーを広範囲に適用する前に、非本番環境またはバケットでテストして、意図したとおりに機能することを確認します。
- ロジック構造が複雑になる可能性があるため、ルールをより直感的にするために説明的なIDを使用します。
- これらのバケット ライフサイクル ポリシーがストレージの使用状況とパフォーマンスに与える影響を監視し、必要な調整を行います。

テクニカルレポート

StorageGRIDテクニカルレポートの概要

NetApp StorageGRID は、ソフトウェアで定義されるオブジェクトストレージスイートで、パブリック、プライベート、ハイブリッドのマルチクラウド環境での幅広いユースケースに対応します。StorageGRID はAmazon S3 APIをネイティブでサポートし、自動化されたライフサイクル管理などの業界をリードする革新的なテクノロジを提供して、非構造化データを長期にわたってコスト効率よく格納、保護、保持します。

StorageGRIDには、StorageGRIDのいくつかの機能と統合に関するベストプラクティスと推奨事項が記載されたドキュメントが用意されています。

NetApp StorageGRIDとビッグデータ分析

NetApp StorageGRIDのユースケース

NetApp StorageGRIDオブジェクトストレージ解決策は、拡張性、データ可用性、セキュリティ、ハイパフォーマンスを提供します。StorageGRID S3は、あらゆる規模のさまざまな業界の組織で幅広いユースケースに使用されています。典型的なシナリオをいくつか見てみましょう。

ビッグデータ分析： StorageGRID S3はデータレイクとしてよく使用されています。企業は、Apache Spark、Splunk Smartstore、Dremioなどのツールを使用して、分析用に大量の構造化データと非構造化データを保存します。

データ階層化： NetAppのお客様は、ONTAPのFabricPool機能を使用して、ハイパフォーマンスなローカル階層間でStorageGRIDにデータを自動的に移動します。階層化することで、高価なフラッシュストレージをホットデータ用に解放し、コールドデータを低コストのオブジェクトストレージでいつでも利用できる状態に維持できます。これにより、パフォーマンスとコスト削減が最大化されます。

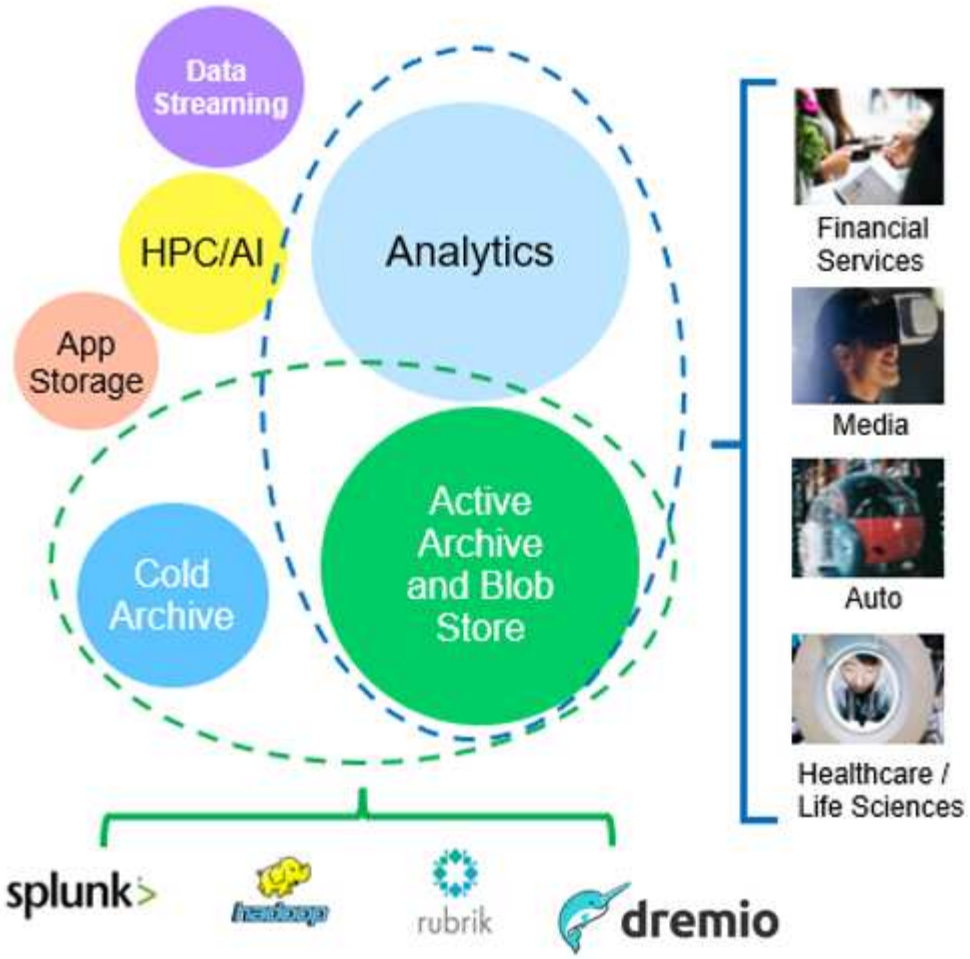
*データのバックアップとディザスタリカバリ：*企業は、StorageGRID S3を信頼性とコスト効率に優れた解決策として使用して、重要なデータのバックアップと災害時のリカバリを実行できます。

アプリケーション用のデータストレージ： StorageGRID S3はアプリケーションのストレージバックエンドとして使用できるため、開発者はファイル、画像、ビデオ、その他の種類のデータを簡単に保存および取得できます。

コンテンツ配信： StorageGRID S3を使用すると、静的なWebサイトコンテンツ、メディアファイル、ソフトウェアダウンロードを世界中のユーザに保存して配信できます。StorageGRIDの地理的な配信とグローバルネームスペースを活用して、高速で信頼性の高いコンテンツ配信を実現できます。

データアーカイブ： StorageGRIDは、さまざまな種類のストレージを提供し、パブリックな長期低コストストレージオプションへの階層化をサポートします。コンプライアンスや履歴目的で保持する必要があるデータのアーカイブや長期保存に最適な解決策です。

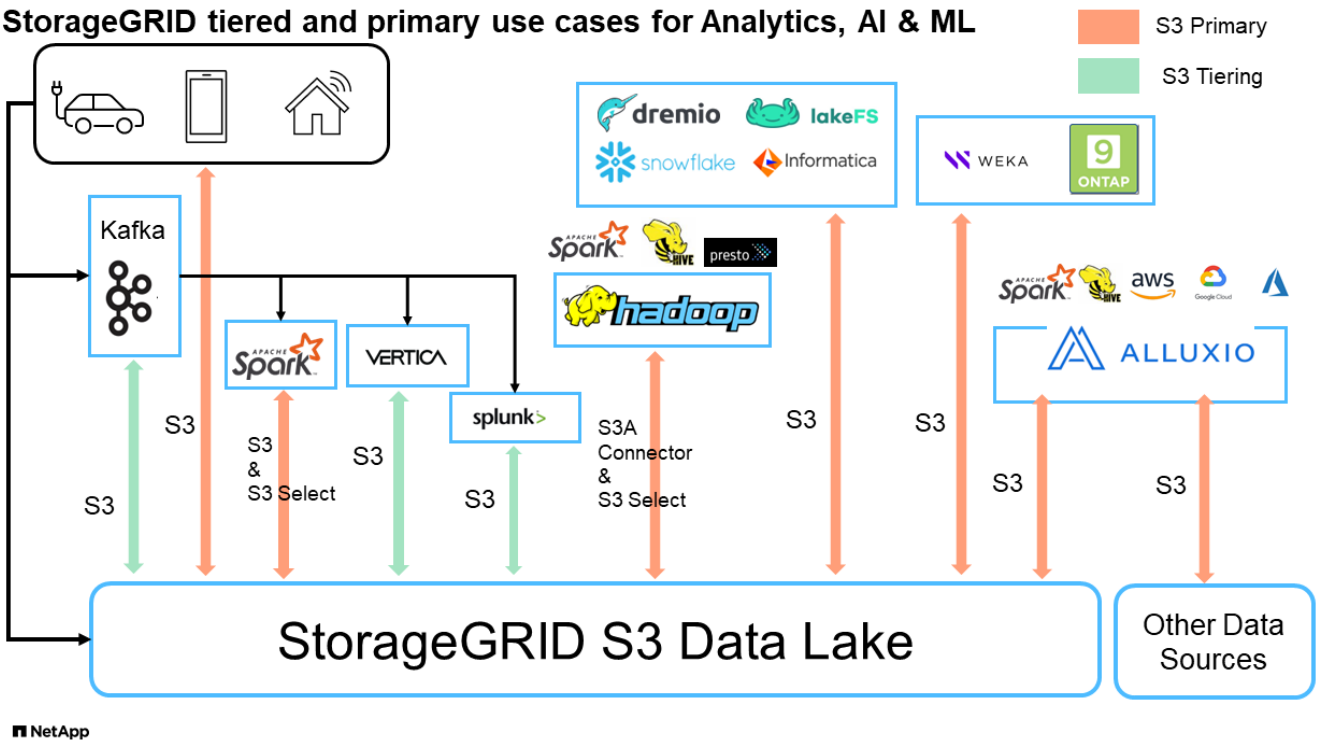
オブジェクトストレージのユースケース



上記の中で、ビッグデータ分析は最も多くのユースケースの1つであり、その使用量は増加傾向にあります。

データレイクにStorageGRIDを選ぶ理由

- コラボレーションの強化-業界標準のAPIアクセスによる大規模な共有マルチサイト、マルチテナンシー
- 運用コストの削減-単一の自己回復型自動スケールアウトアーキテクチャによる運用の簡易化
- 拡張性-従来のHadoopやデータウェアハウスソリューションとは異なり、StorageGRID S3オブジェクトストレージはコンピューティングやデータからストレージを切り離し、ビジネスの成長に合わせてストレージニーズを拡張できます。
- 耐久性と信頼性- StorageGRIDは99.999999999%の耐久性を提供し、保存されたデータはデータ損失に対して非常に耐性があります。また、高可用性を提供し、データへの常時アクセスを保証します。
- セキュリティ- StorageGRIDは、暗号化、アクセス制御ポリシー、データライフサイクル管理、オブジェクトロック、S3バケットに格納されたデータを保護するバージョン管理など、さまざまなセキュリティ機能を提供します。
- StorageGRID S3データレイク*



S3オブジェクトストレージを使用したデータウェアハウスとレイクハウスのベンチマーク比較調査

この記事では、NetApp StorageGRIDを使用したさまざまなデータウェアハウスとLakehouseエコシステムの包括的なベンチマークを紹介します。目的は、S3オブジェクトストレージでパフォーマンスが最も優れたシステムを特定することです。データウェアハウス/レイクハウスアーキテクチャとテーブルフォーマット(寄木細工と氷山)の詳細については、こちらを参照してhttps://www.dremio.com/wp-content/uploads/2023/02/apache-iceberg-TDG_ER1.pdf?aliId=eyJpIjoieDRUYjFKN2ZMbXhTRnFRWCIsInQiOiJIUUw0djJsWnlJa21iNUsyQURRalNnPT0ifQ%253D%253D["『Apache Iceberg: The Definitive Guide』"]ください。

- ベンチマークツール- TPC-DS- https://www.tpc.org/tpcds/
- ビッグデータエコシステム
  - VMのクラスタ（それぞれ128G RAM、24 vCPU、システムディスク用SSDストレージ）
  - Hadoop 3.3.5とHive 3.1.3（1つのネームノード+ 4つのデータノード）
  - Delta LakeとSpark 3.2.0（1マスター+ 4ワーカー）およびHadoop 3.3.5
  - Dremio v25.2（コーディネータ1名+執行者5名）
  - Trino v438（コーディネータ1名+作業者5名）
  - Starburst v453（コーディネータ1名+ワーカー5名）
- オブジェクトストレージ
  - SG6060を3台+ SG1000ロードバランサを1台搭載した場合、SG®SG®11.8 NetApp StorageGRID
  - オブジェクト保護-コピー×2（EC 2+1と同様の結果）
- データベースサイズ1000GB

- Parquet形式を使用したクエリテストごとに、すべてのエコシステムでキャッシュが無効になりました。Iceberg形式では、S3 GET要求の数と、キャッシュが無効なシナリオとキャッシュが有効なシナリオの間の合計クエリ時間を比較しました。

TPC-DSには、ベンチマーク用に設計された99の複雑なSQLクエリが含まれています。99個すべてのクエリの実行にかかった合計時間を測定し、S3要求のタイプと数を調べて詳細な分析を行いました。私たちのテストでは、寄木細工とアイスバーグという2つの一般的なテーブル形式の効率を比較しました。

寄木細工テーブル形式の**TPC-DS**クエリ結果

エコシステム	ハイブ	デルタレイク"	デレミオ	トリノ	スターバースト
TPCDS 99クエリ+ 合計分数	1084 ^ 1 ^	55	36	32	28
S3要求の内訳	取得	一、一一七、一八四	2、074、610	3,939,690	1,504,212
1,495,039	観察：+ すべての範囲GET	80%のGET ：32MBオブジェクトから2KB ～2MB、50~100要求/秒	73%の範囲は、32MBオブジェクトから100KB未満、1 、000~1400要求/秒	90% 1Mバイト範囲は256MBのオブジェクトから取得、2500~3000の要求/秒	範囲GETサイズ ：100KB未満50%、1MB前後16%、2MB ～9MB 27% 、3500~4000要求/秒
範囲GETサイズ ：100KB未満50%、1MB前後16%、2MB ～9MB 27%、4000-5000要求/秒	オブジェクトをリスト表示	三一二、〇 五三	二四、一五八	120	509
512	頭部+ （存在しないオブジェクト）	156、027	一二、一 〇 三	96	0
0	頭部+ （既存のオブジェクト）	982、126	922、732	0	0
0	リクエスト総数	二、五六七、三九〇	3、033、603	3,939.906	1,504,721

[1]Hiveクエリー番号72を完了できません

氷山表形式の**TPC-DS**クエリ結果

エコシステム	デレミオ	トリノ	スターバースト
TPCDS 99クエリ+合計分（キャッシュ無効）	22	28	22
TPCDS 99クエリ+合計分[2]（キャッシュ有効）	16	28	21.5
S3要求の内訳	GET（キャッシュ無効）	1,985,922	938,639
931,582	GET（キャッシュ有効）	611,347	30,158
3,281	観察：+ すべての範囲GET	範囲GETサイズ： 67%1MB、15% 100KB 、10% 500KB、3500 ～4500リクエスト/秒	範囲GETサイズ：100KB未満42%、1MB前後17% 、2MB～9MB 33%、3500 ～4000要求/秒
範囲GETサイズ ：100KB未満43% 、1MB前後17%、2MB ～9MB 33%、4000- 5000要求/秒	オブジェクトをリスト表示	1465	0
0	頭部+ （存在しないオブジェクト）	1464	0
0	頭部+ （既存のオブジェクト）	3,702	509
509	合計要求数（キャッシュ無効）	1,992,553	939,148

[2]トリノ/スターバーストのパフォーマンスは、コンピューティングリソースによってボトルネックになっています。クラスタにRAMを追加すると、合計クエリ時間が短縮されます。

最初の表に示すように、Hiveは他の最新のデータLakehouseエコシステムよりも大幅に低速です。Hiveが大量のS3リストオブジェクト要求を送信したことがわかりましたが、すべてのオブジェクトストレージプラットフォーム（特に多数のオブジェクトを含むバケットを扱う場合）では通常処理が遅くなります。これにより、全体的なクエリ時間が大幅に長くなります。さらに、現代のLakehouseエコシステムは、Hiveの毎秒50~100の要求に対して、毎秒2,000から5,000の要求までの多数のGET要求を並行して送信することができます。HiveとHadoop S3Aによる標準的なファイルシステムの模倣により、S3オブジェクトストレージとのやり取りが遅くなっています。

HiveまたはSparkでHadoop（HDFSまたはS3オブジェクトストレージ）を使用するには、HadoopとHive/Sparkの両方に関する広範な知識と、各サービスの設定がどのように連動するかを理解している必要があります。合計で1,000を超える設定があり、その多くは相互に関連しており、独立して変更することはできません。設定と値の最適な組み合わせを見つけるには、膨大な時間と労力が必要です。

寄木細工とアイスバーグの結果を比較すると、表形式が主要なパフォーマンス要因であることがわかります。Icebergテーブル形式は、S3要求の数に関して寄木細工よりも効率的であり、寄木細工形式と比較して35%~50%少ない要求です。

Dremio、Trino、Starburstのパフォーマンスは、主にクラスタのコンピューティング能力によって駆動されます。3つともS3オブジェクトストレージ接続にS3Aコネクタを使用しますが、Hadoopは必要なく、Hadoop

のfs.s3a設定のほとんどはこれらのシステムでは使用されません。これにより、パフォーマンスの調整が簡易化され、Hadoop S3Aのさまざまな設定を学習してテストする必要がなくなります。

このベンチマーク結果から、S3ベースのワークロード向けに最適化されたビッグデータ分析システムが大きなパフォーマンス要因であることがわかります。最新のレイクハウスでは、クエリの実行が最適化され、メタデータが効率的に利用され、S3データへのシームレスなアクセスが提供されるため、S3ストレージを使用する場合にHiveよりもパフォーマンスが向上します。

StorageGRIDでDremio S3データソースを設定するには、こちらを参照し "ページ"てください。

StorageGRIDとDremioが連携して最新の効率的なデータレイクインフラを提供する方法や、NetAppがHive + HDFSからDremio + StorageGRIDに移行してビッグデータ分析の効率を劇的に向上させる方法については、以下のリンクをご覧ください。

- "NetApp StorageGRIDでビッグデータのパフォーマンスを向上"
- "StorageGRIDとDremioによる、パワフルで効率性に優れた最新のデータレイクインフラ"
- "NetAppが製品分析でカスタマーエクスペリエンスを再定義する方法"

Hadoop S3Aの調整

Angela Cheng著_

Hadoop S3Aコネクタは、HadoopベースのアプリケーションとS3オブジェクトストレージ間のシームレスなやり取りを容易にします。S3オブジェクトストレージを使用する際のパフォーマンスを最適化するには、Hadoop S3Aコネクタの調整が不可欠です。調整の詳細に進む前に、Hadoopとそのコンポーネントの基本を理解しておきましょう。

Hadoopとは

- Hadoop * は、大規模なデータ処理とストレージを処理するために設計された強力なオープンソース・フレームワークです。これにより、コンピュータのクラスタ間で分散ストレージと並列処理が可能になります。

Hadoopの3つのコアコンポーネントは次のとおりです。

- * Hadoop HDFS（Hadoop分散ファイルシステム）*：ストレージを処理し、データをブロックに分割してノード間で分散します。
- * Hadoop MapReduce *：タスクを小さなチャンクに分割し、並行して実行することでデータを処理します。
- * Hadoop YARN（Yet Another Resource Negotiator）：* "リソースの管理とタスクのスケジュール設定を効率的に行う"

Hadoop HDFSおよびS3Aコネクタ

HDFSはHadoopエコシステムの重要なコンポーネントであり、効率的なビッグデータ処理において重要な役割を果たします。HDFSは信頼性の高いストレージと管理を実現します。並列処理と最適化されたデータストレージを実現し、データアクセスと分析を高速化します。

ビッグデータ処理では、HDFSは大規模データセットにフォールトトレラントなストレージを提供することに優れています。これは、データレプリケーションによって実現されます。IT部門は、データウェアハウス環境

に大量の構造化データと非構造化データを格納して管理できます。さらに、Apache Spark、Hive、Pig、Flinkなどの主要なビッグデータ処理フレームワークとシームレスに統合し、スケーラブルで効率的なデータ処理を可能にします。UNIXベース(Linux)オペレーティングシステムと互換性があり、ビッグデータ処理にLinuxベースの環境を使用することを好む組織にとって理想的な選択肢です。

時間の経過とともにデータ量が増大するにつれて、独自のコンピューティングとストレージを使用してHadoopクラスタに新しいマシンを追加するアプローチは非効率的になります。リニアに拡張すると、リソースの効率的な使用やインフラの管理が難しくなります。

これらの課題に対処するために、Hadoop S3AコネクタはS3オブジェクトストレージに対するハイパフォーマンスI/Oを提供します。S3Aを使用してHadoopワークフローを実装することで、オブジェクトストレージをデータリポジトリとして活用でき、コンピューティングとストレージを分離することができます。これにより、コンピューティングとストレージを別々に拡張できます。コンピューティングとストレージを分離することで、コンピューティングジョブ専用のリソースを確保し、データセットのサイズに基づいて容量を提供することもできます。そのため、Hadoopワークフローの総所有コストを削減することができます。

Hadoop S3Aコネクタの調整

S3の動作はHDFSとは異なり、ファイルシステムの外観を維持しようとすると積極的に最適化されません。S3リソースを最も効率的に使用するには、慎重な調整、テスト、実験が必要です。

本ドキュメントのHadoopオプションはHadoop 3.3.5に基づいています。を参照してください。 "Hadoop 3.3.5 core-site.xml" 使用可能なすべてのオプションについて。

注–一部のHadoop fs.s3a設定のデフォルト値は、Hadoopのバージョンによって異なります。現在のHadoopバージョンに固有のデフォルト値を確認してください。これらの設定がHadoop core-site.xmlに指定されていない場合は、デフォルト値が使用されます。SparkまたはHive構成オプションを使用して、実行時に値を上書きできます。

これに行く必要があります。 "Apache Hadoopページ" 各fs.s3aオプションを理解するため。可能であれば、非本番環境のHadoopクラスタでテストして最適な値を特定します。

お読みください "S3Aコネクタでの作業時のパフォーマンスの最大化" その他のチューニングの推奨事項については、

主な考慮事項をいくつか見ていきましょう。

- 1 。データ圧縮*

StorageGRID圧縮を有効にしないでください。ほとんどのビッグデータシステムでは、オブジェクト全体を読み出す代わりにバイト範囲GETを使用します。圧縮オブジェクトにbyte range getを使用すると、GETのパフォーマンスが大幅に低下します。

※ 2S3Aコミッタ*

一般的には、マジックs3aコミッターをお勧めします。これを参照してください "共通のS3Aコミッタオプションページ" マジックコミッタとそれに関連するs3a設定をよりよく理解するため。

マジックコミッター：

Magic Committerは、特にS3Guardを使用して、S3オブジェクトストアで一貫したディレクトリリストを提供します。

整合性のあるS3（現在はそうなっています）を使用すると、Magic Committerは任意のS3バケットで安全に使用できます。

選択と実験：

ユースケースに応じて、Staging Committer（クラスタHDFSファイルシステムに依存）とMagic Committerのどちらかを選択できます。

両方を試して、ワークロードと要件に最適なものを判断してください。

要約すると、S3Aコミッタは、S3への一貫した、高性能で信頼性の高い出力コミットメントという基本的な課題に対する解決策を提供します。内部設計により、データの整合性を維持しながら効率的なデータ転送を実現します。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable “magic committer” support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

3.スレッド、接続プールサイズ、ブロックサイズ

- 1つのバケットとやり取りする各* S3A *クライアントには、アップロードおよびコピー処理用のオープンHTTP 1.1接続とスレッドの専用プールがあります。
- "これらのプールサイズを調整して、パフォーマンスとメモリ/スレッド使用量のバランスをとることができます。"。
- S3にデータをアップロードする場合、データはブロックに分割されます。デフォルトのブロックサイズは32MBです。この値をカスタマイズするには、fs.s3a.block.sizeプロパティを設定します。
- ブロックサイズを大きくすると、アップロード中にマルチパートパートパートを管理するオーバーヘッドが軽減されるため、大規模なデータアップロードのパフォーマンスが向上します。大規模なデータセットの場合、推奨値は256 MB以上です。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

4.マルチパートアップロード

s3aコミッタ*常に* MPU（マルチパートアップロード）を使用してデータをs3バケットにアップロードします。これは、タスクの失敗、タスクの投機的な実行、およびコミット前のジョブの中止を可能にするために必要です。マルチパートアップロードに関連する主な仕様を次に示します。

- 最大オブジェクトサイズ：5TiB（テラバイト）。
- アップロードあたりの最大パーツ数：10、000
- パーツ番号：1～10,000（含む）。
- パーツサイズ：5MiB~5GiB。特に、マルチパートアップロードの最後のパートには最小サイズの制限はありません。

S3マルチパートアップロードに小さいパートサイズを使用すると、メリットとデメリットの両方があります。

利点：

- ネットワークの問題からのクイックリカバリ:小さなパーツをアップロードすると、ネットワークエラーによるアップロードの再開による影響が最小限に抑えられます。パーツに障害が発生した場合は、オブジェ

クト全体ではなく、その特定のパーツのみを再アップロードする必要があります。

- 並列化の向上:マルチスレッディングまたは同時接続を利用して、より多くのパーツを並行してアップロードできます。この並列化により、特に大きなファイルを処理する場合のパフォーマンスが向上します。

欠点：

- ネットワークオーバーヘッド:部品サイズが小さいほど、アップロードする部品が増えます。各部品には独自のHTTPリクエストが必要です。HTTP要求が増えると、個 々 の要求の開始と完了のオーバーヘッドが増加します。多数の小さなパーツを管理すると、パフォーマンスに影響を与える可能性があります。
- 複雑さ：注文の管理、パーツの追跡、アップロードの成功の確認は面倒です。アップロードを中止する必要がある場合は、すでにアップロードされているすべてのパーツを追跡してパージする必要があります。

Hadoopの場合、fs.s3a.multipart.sizeには256MB以上のパーツサイズを推奨します。fs.s3a.mutlipart.threshold値は常に2 x fs.s3a.multipart.size値に設定します。たとえば、fs.s3a.multipart.size=256Mの場合、fs.s3a.mutlipart.thresholdは512Mにする必要があります。

大きなデータセットには大きなパーツサイズを使用してください。特定のユースケースとネットワーク条件に基づいて、これらの要因のバランスを取る部品サイズを選択することが重要です。

マルチパートアップロードは "3段階のプロセス"：

1. アップロードが開始され、StorageGRIDはupload-idを返します。
2. オブジェクトパーツはupload-idを使用してアップロードされます。
3. すべてのオブジェクトパートがアップロードされると、は、upload-idを指定して完全なマルチパートアップロード要求を送信します。StorageGRIDは、アップロードされたパーツからオブジェクトを構築し、クライアントがオブジェクトにアクセスできるようにします。

Complete multipart upload要求が正常に送信されなかった場合、パーツはStorageGRIDに残り、オブジェクトは作成されません。これは、ジョブが中断、失敗、または中止された場合に発生します。マルチパートアップロードが完了するか中止されるか、アップロードが開始されてから15日が経過するとStorageGRIDがそれらのパートをパージするまで、パートはグリッドに残ります。バケット内で実行中のマルチパートアップロードが多数（数十万から数百万）ある場合、Hadoopが「list-multipart-uploads」を送信すると（この要求はアップロードIDでフィルタリングされません）、要求の完了に時間がかかるか、最終的にタイムアウトになることがあります。fs.s3a.mutlipart.purgeをtrueに設定し、適切なfs.s3a.multipart.purge.ageの値を設定することを検討してください（例：5〜7日、デフォルト値の86400、つまり1日は使用しないでください）。または、NetAppサポートに状況を調査してください。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

5.メモリ内のバッファ書き込みデータ

パフォーマンスを向上させるには、書き込みデータをS3にアップロードする前にメモリにバッファします。これにより、少量の書き込み数が削減され、効率が向上します。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

S3とHDFSは別 々 の方法で機能することに注意してください。S3リソースを最も効率的に使用するには、慎

重な調整/テスト/実験が必要です。

TR-4871：『Configure StorageGRID for backup and recovery with Commvault』

StorageGRIDとCommvaultを使用したデータのバックアップとリカバリ

CommvaultとNetAppは提携して、Commvault Complete Backup and Recovery for NetAppソフトウェアとクラウドストレージ向けのNetApp StorageGRIDソフトウェアを組み合わせた共同データ保護解決策を作成しました。Commvault Complete Backup and RecoveryとNetApp StorageGRIDは、相互に連携して機能する独自の使いやすいソリューションを提供し、急速なデータ量の増大や世界各地の規制への対応を支援します。

多くの組織は、ストレージをクラウドに移行し、システムを拡張し、データの長期保持に関するポリシーを自動化したいと考えています。クラウドベースのオブジェクトストレージは、耐障害性、拡張性、運用効率とコスト効率に優れていることで知られており、バックアップのターゲットとして最適です。CommvaultとNetAppは、2014年に解決策の統合を共同で認定し、それ以来、両社のソリューション間の緊密な統合を設計してきました。世界中のあらゆるタイプのお客様が、Commvault Complete Backup and RecoveryとStorageGRID Combined解決策を採用しています。

CommvaultとStorageGRIDについて

Commvault Complete Backup and Recoveryソフトウェアは、エンタープライズレベルの統合データおよび情報管理解決策で、単一プラットフォーム上に一から構築され、統合コードベースを備えています。すべての機能がバックエンドテクノロジを共有し、データの保護、管理、アクセスに完全に統合されたアプローチによる比類のないメリットとメリットをもたらします。このソフトウェアには、データを保護、アーカイブ、分析、複製、検索するためのモジュールが含まれています。これらのモジュールは、相互にシームレスに連携する、共通のバックエンドサービスと高度な機能セットを共有しています。解決策は、企業のデータ管理のあらゆる側面に対応しながら、無限の拡張性とかつてないデータと情報の制御を提供します。

CommvaultクラウドとしてのNetApp StorageGRIDは、エンタープライズハイブリッドクラウドのオブジェクトストレージ解決策です。専用アプライアンスまたはSoftware-Defined環境のいずれかを使用して、多数のサイトに導入できます。StorageGRIDを使用すると、データの格納方法と保護方法を決定するデータ管理ポリシーを確立できます。StorageGRIDは、ポリシーの開発と実施に必要な情報を収集します。パフォーマンス、耐久性、可用性、地理的な場所、 長寿とコスト。データは、サイト間や古くなっても、完全に維持され、保護されます。

StorageGRIDインテリジェントポリシーエンジンを使用すると、次のいずれかのオプションを選択できます。

- イレイジャーコーディングを使用して複数のサイトにデータをバックアップし、耐障害性を確保するため。
- オブジェクトをリモートサイトにコピーしてWANのレイテンシとコストを最小限に抑えること。

StorageGRIDにオブジェクトが格納されると、その場所やコピーの数に関係なく、オブジェクトに1つのオブジェクトとしてアクセスできます。この動作はディザスタリカバリに不可欠です。ディザスタリカバリでは、データの1つのバックアップコピーが破損しても、StorageGRIDはデータをリストアできます。

バックアップデータをプライマリストレージに保持すると、コストがかかる場合があります。NetApp StorageGRIDを使用すると、使用頻度の低いバックアップデータをStorageGRIDに移行してプライマリストレージのスペースを解放しながら、StorageGRIDのさまざまな機能を活用できます。バックアップデータの価値

は時間の経過とともに変化し、保存コストも変化します。StorageGRIDを使用すると、データの保持性を高めながら、プライマリストレージのコストを最小限に抑えることができます。

主な特長

Commvaultソフトウェアプラットフォームの主な機能は次のとおりです。

- 仮想サーバと物理サーバ、NASシステム、クラウドベースのインフラ、モバイルデバイス上のすべての主要なオペレーティングシステム、アプリケーション、データベースをサポートする完全なデータ保護解決策。
- 単一のコンソールによるシンプルな管理：企業全体のすべての機能とすべてのデータと情報を表示、管理、アクセスできます。
- データのバックアップとアーカイブ、Snapshot管理、データレプリケーション、eディスカバリ向けのコンテンツインデックス作成など、さまざまな保護方法が用意されています。
- ディスクストレージとクラウドストレージの重複排除による効率的なストレージ管理
- AFF、FAS、NetApp HCI、Eシリーズアレイ、NetApp SolidFire ®スケールアウトストレージシステムなどのNetAppストレージアレイとの統合また、NetApp Cloud Volumes ONTAPソフトウェアとの統合により、NetAppストレージポートフォリオ全体で、インデックス付きのアプリケーション対応NetApp Snapshot™コピーの作成を自動化できます。
- 業界をリードするオンプレミスの仮想ハイパーバイザーとパブリッククラウドハイパースケーラプラットフォームをサポートする包括的な仮想インフラ管理
- 重要なデータへのアクセスを制限し、きめ細かな管理機能を提供し、Active Directoryユーザにシングルサインオンアクセスを提供する高度なセキュリティ機能。
- ポリシーベースのデータ管理により、物理的な場所ではなく、ビジネスニーズに基づいてデータを管理できます。
- 最先端のエンドユーザエクスペリエンスで、ユーザが自身のデータを保護、検索、リカバリできるようにします。
- APIベースの自動化：vRealize AutomationやService Nowなどのサードパーティ製ツールを使用してデータ保護とリカバリの処理を管理できます。

サポートされるワークロードの詳細については、を参照してください "Commvaultがサポートするテクノロジ"。

バックアップオプション

Commvault Complete Backup and Recoveryソフトウェアをクラウドストレージに実装する場合は、次の2つのバックアップオプションがあります。

- プライマリディスクターゲットにバックアップし、補助コピーをクラウドストレージにバックアップします。
- プライマリターゲットとしてクラウドストレージにバックアップします。

これまで、クラウドやオブジェクトストレージは、プライマリバックアップに使用するにはパフォーマンスが低すぎると考えられていました。プライマリディスクターゲットを使用することで、バックアップとリストアのプロセスを高速化し、コールドバックアップとしてクラウドに補助コピーを保持することができました。StorageGRIDは次世代のオブジェクトストレージです。StorageGRIDは、他のオブジェクトストレージベンダーが提供するよりも優れたパフォーマンスと優れたスループットに加え、優れたパフォーマンスと柔軟性を備えています。

次の表に、StorageGRIDを使用した各バックアップオプションの利点を示します。

	ディスクへのプライマリ・バックアップと**StorageGRID**への補助コピー	**StorageGRID**へのプライマリバックアップ
パフォーマンス	ライブマウントまたはライブリカバリを使用した最速のリカバリ時間：Tier0/Tier1ワークロードに最適	ライブマウントまたはライブリカバリ処理には使用できません。ストリーミングリストア処理や長期保持に最適です。
導入アーキテクチャ	オールフラッシュまたは回転式ディスクを第1のバックアップランディング層として使用StorageGRIDはセカンダリ階層として使用されます。	包括的なバックアップターゲットとしてStorageGRIDを使用することで、導入を簡易化します。
高度な機能（ライブリストア）	サポートされます	サポート対象外

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。

- StorageGRID 11.9ドキュメントセンター+https://docs.netapp.com/us-en/storagegrid-119/[]
- NetApp製品ドキュメント+ https://docs.netapp.com
- Commvaultのドキュメント+ https://documentation.commvault.com/2024/essential/index.html

テスト済みソリューションの概要

テスト済みの解決策は、CommvaultとNetAppのソリューションを組み合わせて、強力な共同解決策を構築しました。

ソリューションのセットアップ

このラボStorageGRID環境は、4台のNetApp StorageGRID SG5712アプライアンス、1台の仮想プライマリ管理ノード、1台の仮想ゲートウェイノードで構成されています。SG5712アプライアンスは、ベースライン構成であるエントリレベルオプションです。NetApp StorageGRID SG5760やSG6060などの高パフォーマンスアプライアンスを選択すると、パフォーマンスが大幅に向上します。サイジングの支援については、NetApp StorageGRID 解決策 アーキテクトにお問い合わせください。

StorageGRIDのデータ保護ポリシーでは、統合ライフサイクル管理（ILM）ポリシーを使用してデータを管理および保護します。ILMルールはポリシー内で上から下に評価されます。次の表に示すILMポリシーを実装しました。

ILMルール	絞り込み	取り込み動作
イレイジャーコーディング2+1	200KBを超えるオブジェクト	中間（ Balanced ）
2コピー	すべてのオブジェクト	デュアルコミット

デフォルトルールはILM 2 Copyルールです。このテストでは、200KB以上のすべてのオブジェクトにイレイジャーコーディング2+1ルールを適用しました。デフォルトルールは200KB未満のオブジェクトに適用されました。このようにルールを適用することは、StorageGRIDのベストプラクティスです。

このテスト環境の技術的な詳細については解決策、 "CommvaultによるNetAppスケールアウトデータ保護" テクニカルレポート：

StorageGRIDハードウェア

次の表に、このテストで使用したNetApp StorageGRIDハードウェアを示します。10Gbpsネットワークを備えたStorageGRID SG5712アプライアンスはエントリレベルのオプションで、ベースライン構成です。必要に応じて、25Gbpsネットワーク用にSG5712を設定できます。

ハードウェア	数量	ディスク	使用可能容量	ネットワーク
StorageGRID SG5712アプライアンス	4.	4TB×48（ニアラインSAS HDD）	136TB	10Gbps

NetApp StorageGRID SG5760、SG6060、オールフラッシュSGF6112アプライアンスなどのハイパフォーマンスアプライアンスオプションを選択すると、パフォーマンスが大幅に向上します。サイジングの支援については、NetApp StorageGRID 解決策 アーキテクトにお問い合わせください。

Commvaultと**StorageGRID**のソフトウェア要件

次の表に、テスト用にVMwareソフトウェアにインストールしたCommvaultおよびNetApp StorageGRIDソフトウェアのソフトウェア要件を示します。4つのMediaAgentデータ転送マネージャと1つのCommServeサーバがインストールされました。このテストでは、VMwareインフラ用に10Gbpsネットワークを実装しました。次の表

次の表に、Commvaultソフトウェアの総システム要件を示します。

コンポーネント	数量	データストア	サイズ	合計	合計必要**IOPS**
CommServeサーバ	1.	OS	500 GB	500 GB	n/a
		SQL>	500 GB	500 GB	n/a
MediaAgent	4.	仮想CPU（vCPU）	16	64歳	n/a
		RAM	128 GB	512	n/a

コンポーネント	数量	データストア	サイズ	合計	合計必要**IOPS**
		OS	500 GB	2TB	n/a
		インデックスキャッシュ	2TB	8TB	200以上
		DDB	2TB	8TB	200 ~ 80、000 K

このテスト環境では、NetApp EシリーズE2812ストレージアレイ上のVMwareに、1つの仮想プライマリ管理ノードと1つの仮想ゲートウェイノードを導入しました。各ノードを別 々 のサーバに配置し、本番環境の最小要件を次の表に示します。

次の表に、StorageGRIDの仮想管理ノードとゲートウェイノードの要件を示します。

ノードタイプ	数量	**vCPU**	**RAM**	ストレージ
ゲートウェイノード	1.	8	24 GB	OS用に100GBのLUN
管理ノード	1.	8	24 GB	OS用に100GBのLUN 管理ノードのテーブル用に200GBのLUN 管理ノードの監査ログ用に200GBのLUN

StorageGRIDのサイジングガイダンス

お客様の環境に合わせた具体的なサイジングについては、NetAppデータ保護のスペシャリストにお問い合わせください。NetAppのデータ保護スペシャリストは、Commvault Total Backup Storage Calculatorツールを使用して、バックアップインフラの要件を見積もることができます。このツールにはCommvaultパートナーポータルへのアクセスが必要です。必要に応じてアクセスにサインアップします。

Commvaultのサイジング情報

次のタスクを使用して、データ保護解決策のサイジングに関する検出を実行できます。

- 保護が必要なシステムまたはアプリケーション/データベースのワークロードと、対応するフロントエンドの容量（テラバイト[TB]）を特定します。
- 保護が必要なVM /ファイルワークロードと同様のフロントエンド容量（TB）を特定します。
- 短期および長期の保持要件を特定します。
- 特定したデータセット/ワークロードの1日あたりの変更率を特定します。

- 今後12カ月、24カ月、36カ月間のデータ増加予測を特定します。
- ビジネスニーズに応じて、データ保護/リカバリのRTOとRPOを定義します。

この情報が入手可能になったら、バックアップインフラのサイジングを実行し、必要なストレージ容量の内訳を表示できます。

StorageGRIDのサイジングガイダンス

NetApp StorageGRIDサイジングを実行する前に、ワークロードについて次の点を考慮してください。

- 使用可能容量
- WORMモード
- 平均オブジェクトサイズ
- パフォーマンス要件
- 適用されたILMポリシー

StorageGRIDに階層化したバックアップワークロードのサイズと保持スケジュールに対応するために必要な使用可能容量。

WORMモードは有効になるかどうかCommvaultでWORMを有効にすると、StorageGRIDでオブジェクトロックが設定されます。これにより、必要なオブジェクトストレージ容量が増加します。必要な容量は、保持期間および各バックアップで変更されるオブジェクトの数によって異なります。

平均オブジェクトサイズは、StorageGRID環境でのパフォーマンスのサイジングに役立つ入力パラメータです。Commvaultワークロードに使用される平均オブジェクトサイズは、バックアップのタイプによって異なります。

次の表に、バックアップタイプ別の平均オブジェクトサイズと、リストアプロセスでオブジェクトストアから読み取られる内容を示します。

バックアップタイプ	平均オブジェクトサイズ	リストア動作
StorageGRIDで補助コピーを作成する	32 MB	32MBオブジェクトのフル読み取り
バックアップをStorageGRIDに転送する（重複排除が有効）	8 MB	1MBのランダムレンジ読み取り
バックアップをStorageGRIDに転送する（重複排除は無効）	32 MB	32MBオブジェクトのフル読み取り

また、フルバックアップと増分バックアップのパフォーマンス要件を理解しておくと、StorageGRIDストレージノードのサイズを決定する際に役立ちます。StorageGRIDの情報ライフサイクル管理（ILM）ポリシーのデータ保護方式は、Commvaultバックアップの格納に必要な容量を決定し、グリッドのサイジングに影響します。

StorageGRID ILMレプリケーションは、オブジェクトデータを格納するためにStorageGRIDで使用される2つのメカニズムの1つです。データをレプリケートするILMルールにStorageGRIDがオブジェクトを割り当てると、オブジェクトのデータの完全なコピーが作成されてストレージノードに格納されます。

イレイジャーコーディングは、オブジェクトデータを格納するために StorageGRID で使用される 2 つ目の方法です。イレイジャーコーディングコピーを作成するように設定されたILMルールにStorageGRIDがオブジェクトを割り当てると、オブジェクトデータが複数のデータフラグメントに分割されます。その後、追加のパリティフラグメントを計算し、各フラグメントを別 々 のストレージノードに格納します。アクセスされたオブジェクトは、格納されたフラグメントを使用して再アセンブルされます。データフラグメントまたはパリティフラグメントが破損したり失われたりした場合、イレイジャーコーディングアルゴリズムで残りのデータフラグメントとパリティフラグメントのサブセットを使用してそのフラグメントを再作成できます。

次の例に示すように、2つのメカニズムで必要なストレージ容量は異なります。

- レプリケートコピーを2つ格納すると、ストレージのオーバーヘッドが2倍になります。
- 2+1のイレイジャーコーディングコピーを格納すると、ストレージのオーバーヘッドが1.5倍に増加します。

テストした解決策では、単一サイトのエントリレベルのStorageGRID環境を使用しました。

- 管理ノード：VMware仮想マシン（VM）
- ロードバランサ：VMware VM
- ストレージノード：SG5712（4TBドライブ搭載）×4
- プライマリ管理ノードとゲートウェイノード：本番環境のワークロードの最小要件を満たすVMware VM

StorageGRIDは、サードパーティのロードバランサもサポートしています。

StorageGRIDは通常、ノードレベルやサイトレベルの障害から保護するためにデータをレプリケートするデータ保護ポリシーを使用して、2つ以上のサイトに導入されます。データをStorageGRIDにバックアップすることで、複数のコピーまたはイレイジャーコーディングによってデータを保護します。イレイジャーコーディングは、アルゴリズムによってデータを確実に分離して再構成します。

サイジングツールを使用できます。 "Fusion" グリッドのサイズを調整します。

拡張性

NetApp StorageGRIDシステムを拡張するには、ストレージノードにストレージを追加するか、既存のサイトに新しいグリッドノードを追加するか、新しいデータセンターサイトを追加します。拡張は現在のシステムの処理を中断せずに実行できます。
StorageGRIDでは、ストレージノードのパフォーマンスが高いノード、またはロードバランサと管理ノードを実行する物理アプライアンスを使用するか、ノードを追加するだけでパフォーマンスを拡張できます。

StorageGRIDシステムの拡張の詳細については、を参照してください "StorageGRID 11.9拡張ガイド"。

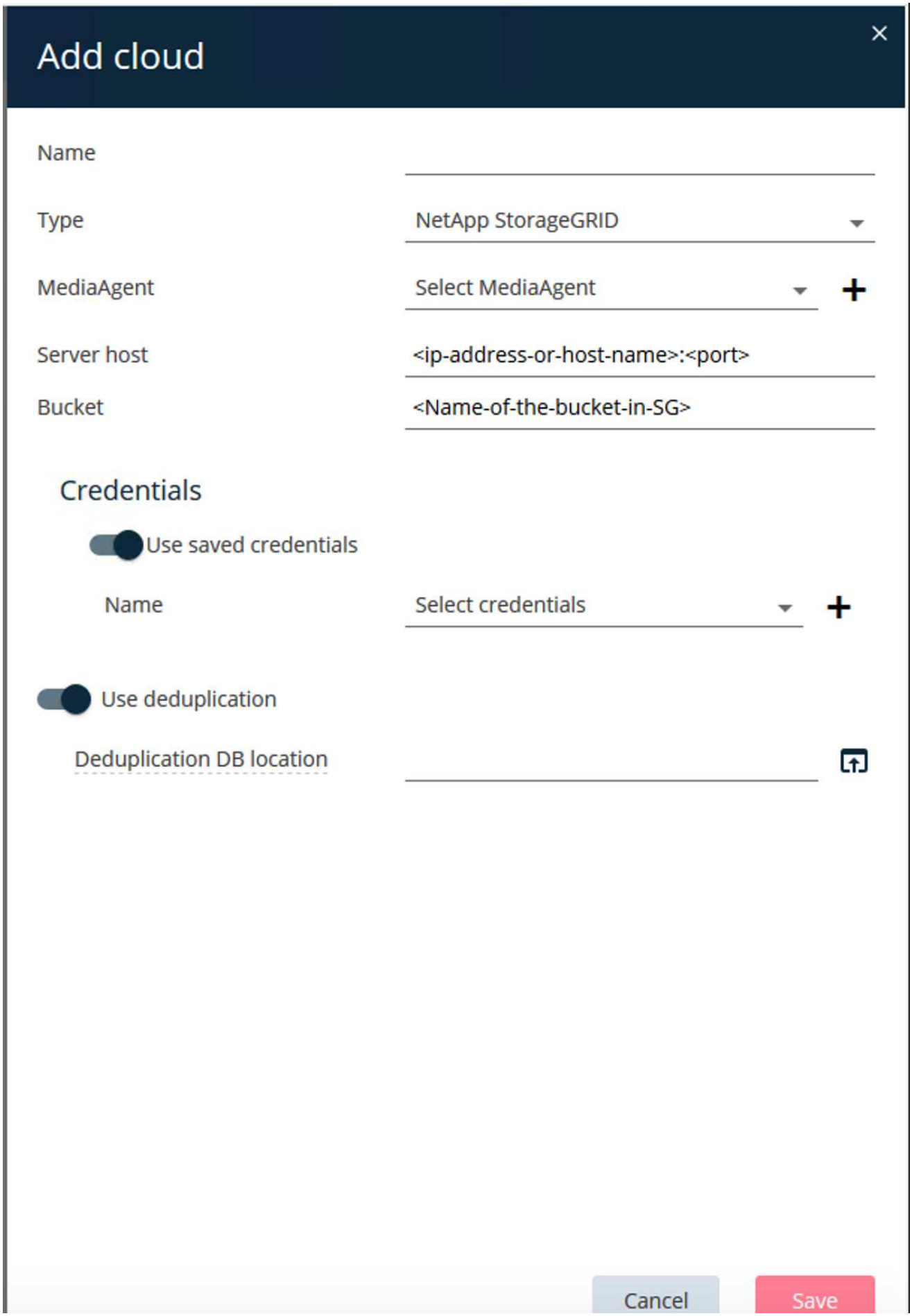
データ保護ジョブを実行する

Commvault Complete Backup and Recovery for NetAppを使用してStorageGRIDを設定するには、次の手順を実行してStorageGRIDをCommvaultソフトウェア内のクラウドライブラリとして追加しました。

ステップ**1**：**Commvault**と**StorageGRID**を設定する

手順

1. CommVault Command Centerにログインします。左側のパネルで、[Storage]>[Cloud]>[Add]をクリックし、[Add Cloud]ダイアログボックスを確認して応答します。


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. タイプ（Type）で、NetApp StorageGRIDを選択します。
3. MediaAgentの場合は、クラウドライブラリに関連付けられているものをすべて選択します。
4. [Server Host]に、StorageGRIDエンドポイントのIPアドレスまたはホスト名とポート番号を入力します。

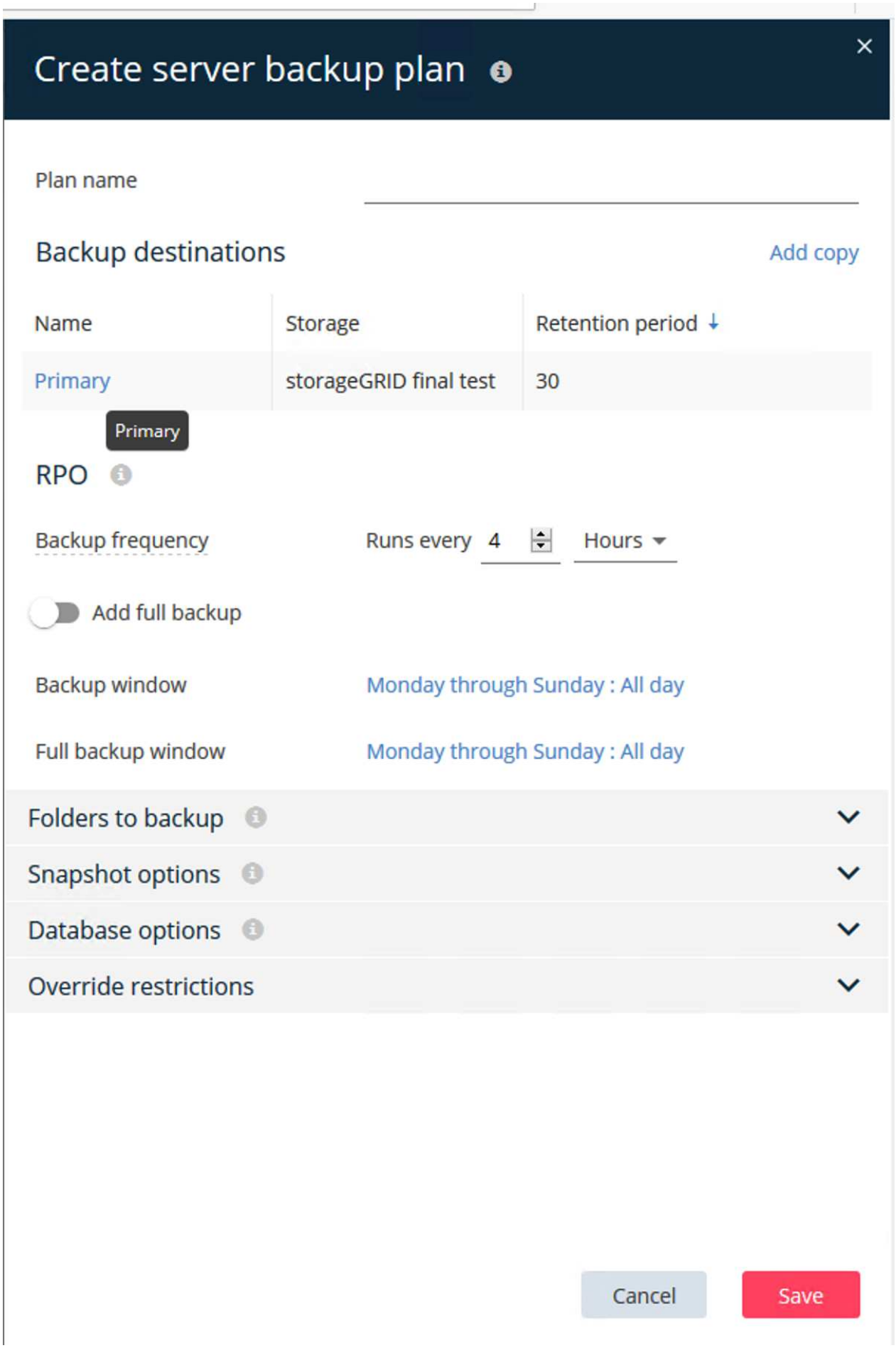
   StorageGRIDのドキュメントに記載されている手順に従います。 "ロードバランサエンドポイント（ポート）の設定方法"。自己署名証明書とStorageGRIDエンドポイントのIPアドレスまたはドメイン名を含むHTTPSポートがあることを確認します。

5. 重複排除を使用する場合は、このオプションをオンにして、重複排除データベースの場所へのパスを指定します。
6. [保存] をクリックします .

手順2：StorageGRIDをプライマリターゲットとしてバックアップ計画を作成する

手順

1. 左側のパネルで、[Manage]>[Plans]を選択し、[Create Server Backup Plan]ダイアログボックスを表示して応答します。

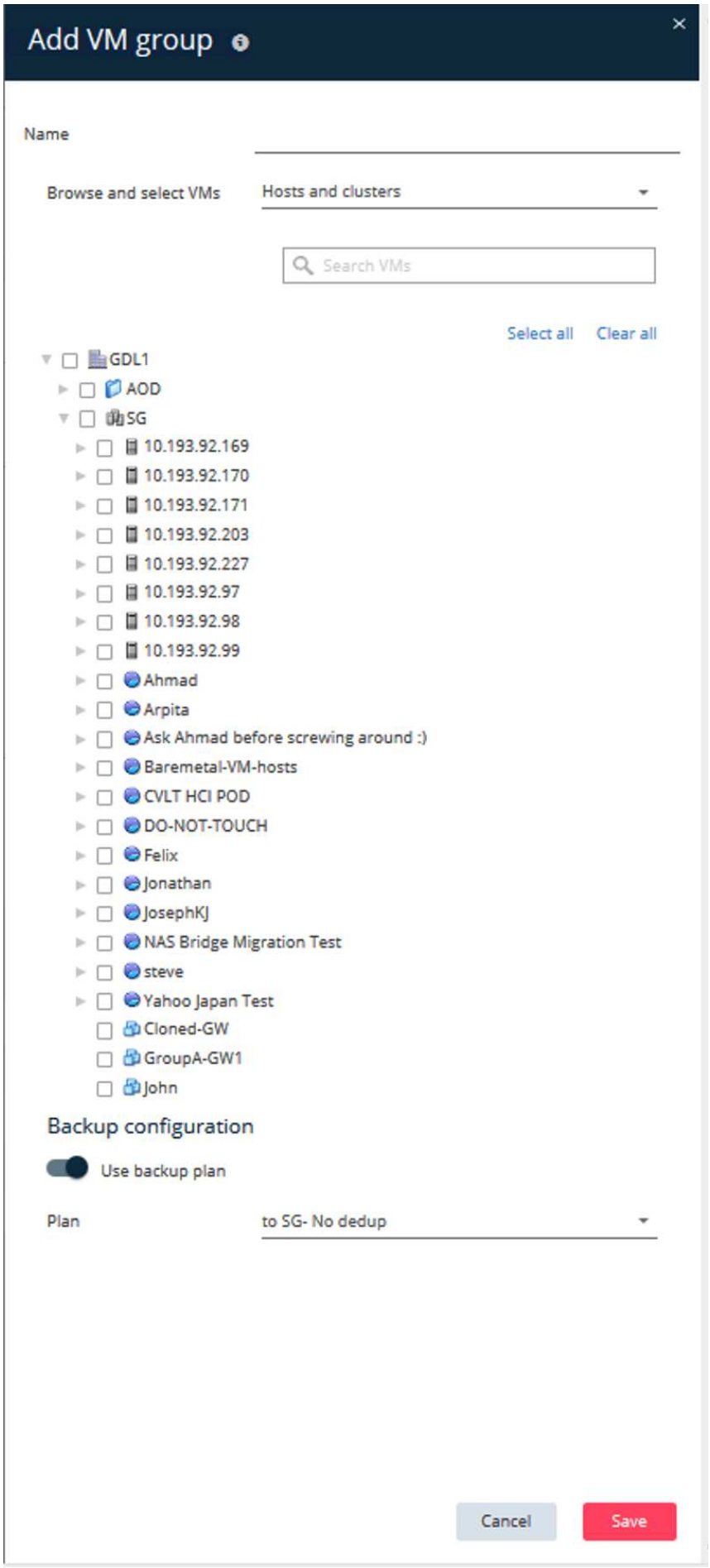

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. 計画名を入力します。
3. 前の手順で作成したStorageGRID Simple Storage Service（S3）ストレージのバックアップ先を選択します。
4. バックアップの保持期間と目標復旧時点（RPO）を入力します。
5. [保存] をクリックします .

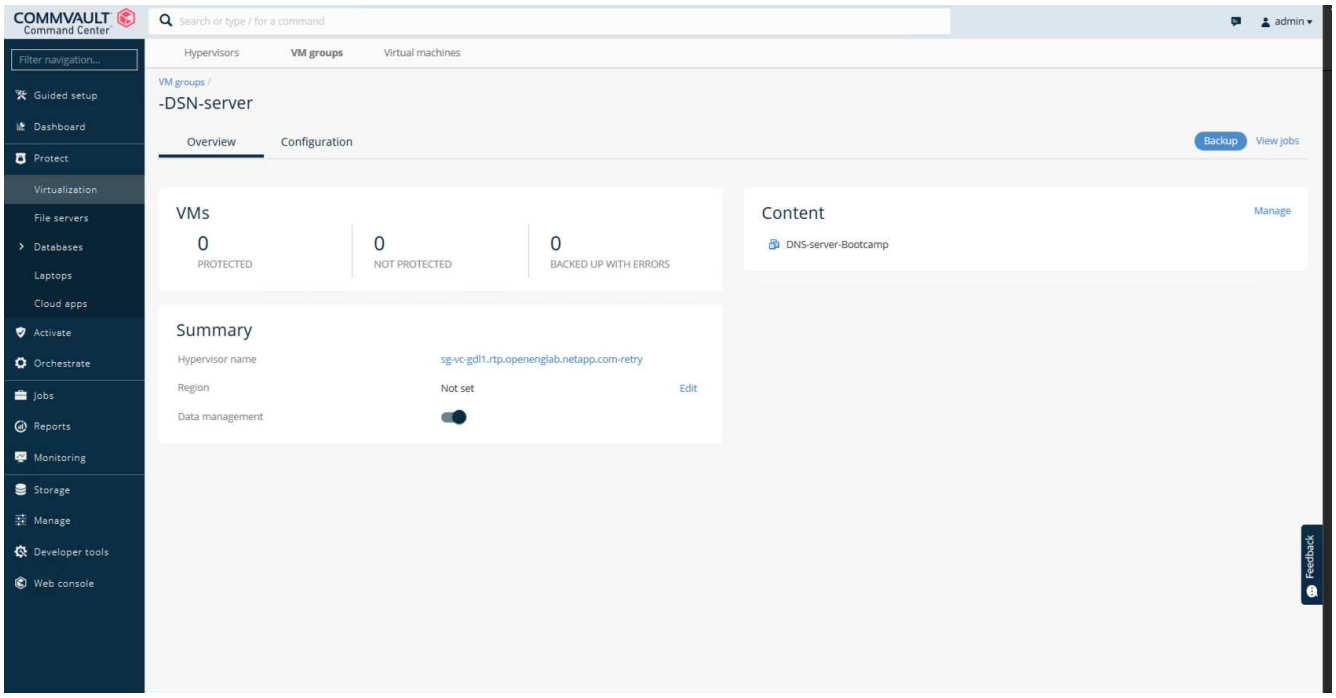
ステップ**3**：バックアップジョブを開始してワークロードを保護する

手順

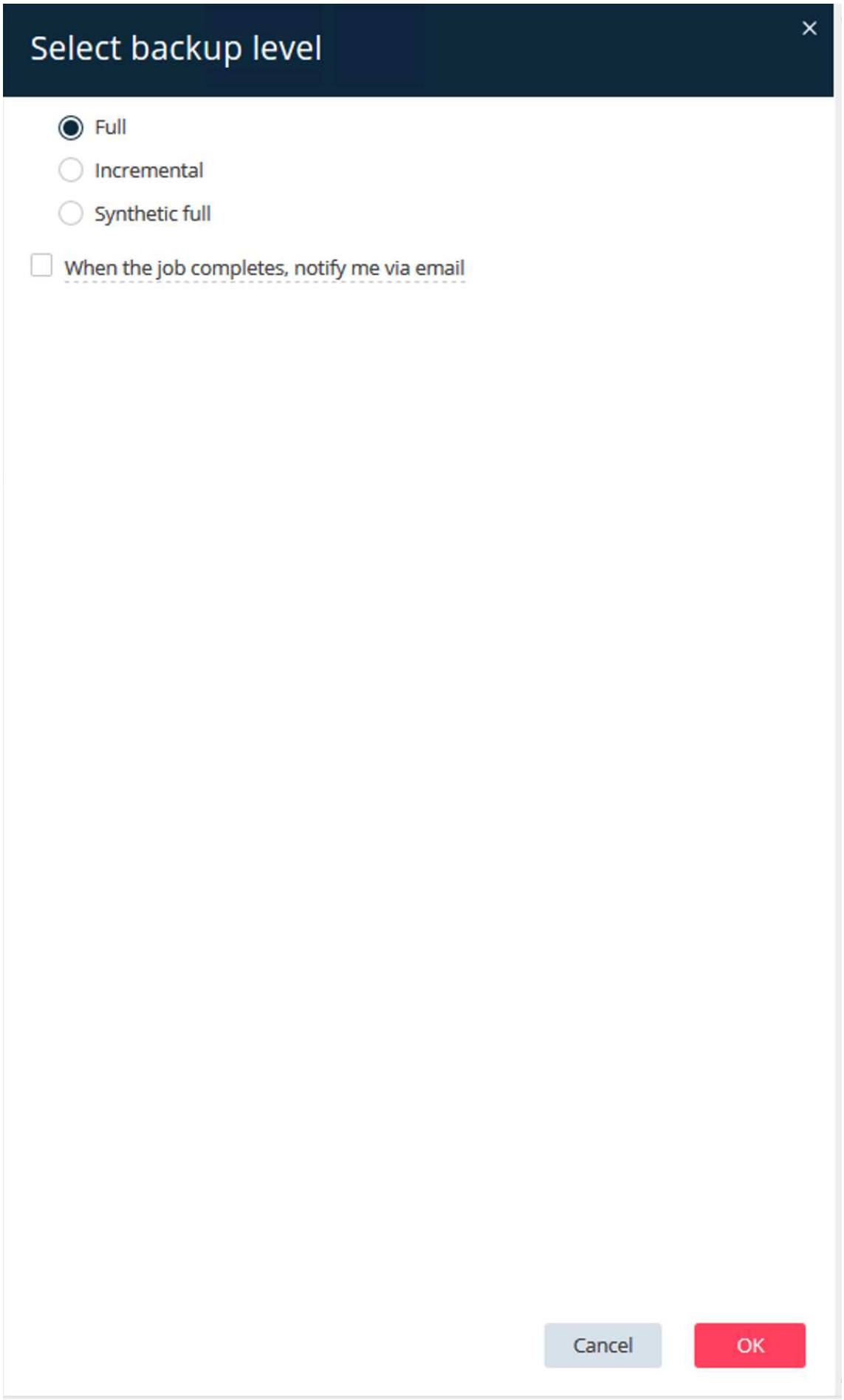
1. CommVault Command Centerで、[Protect]>[Virtualization]の順に選択します。
2. VMware vCenter Serverハイパーバイザーを追加します。
3. 追加したハイパーバイザーをクリックします。
4. [Add VM group]をクリックして[Add VM Group]ダイアログボックスに応答し、保護するvCenter環境を確認します。


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

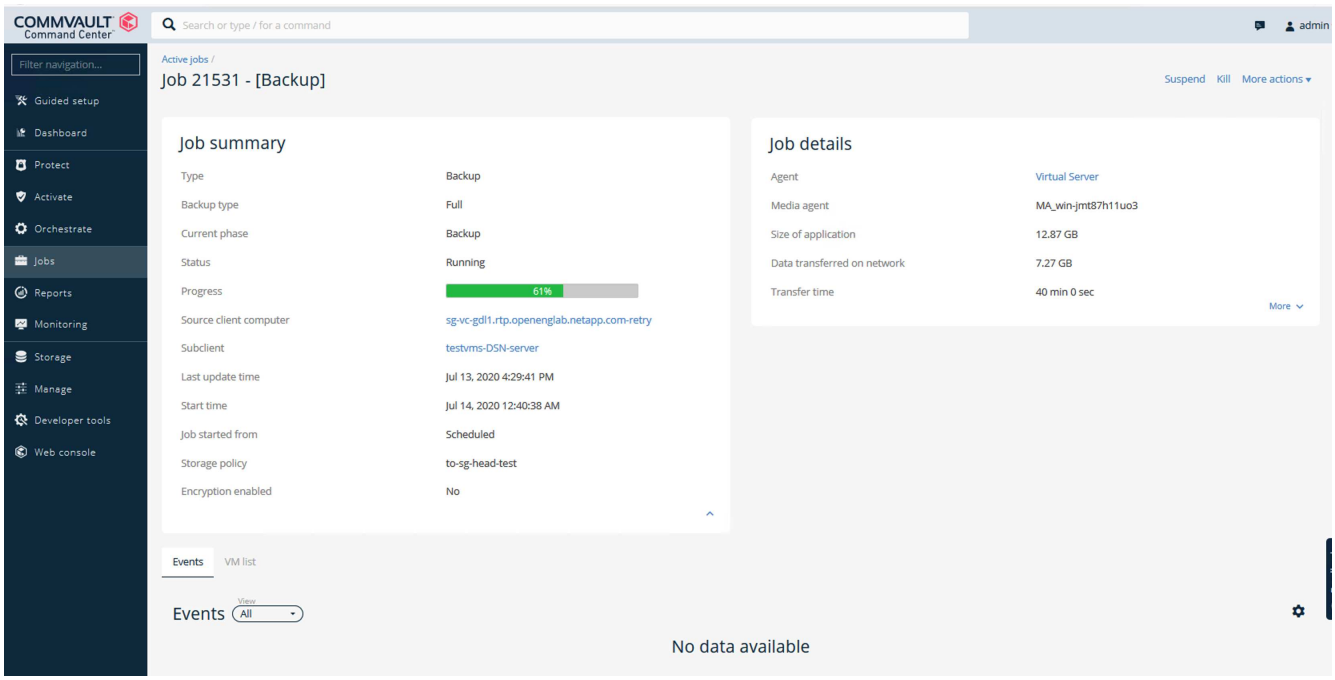
5. データストア、VM、またはVMの集合を選択し、名前を入力します。
6. 前のタスクで作成したバックアップ計画を選択します。
7. [Save]をクリックして、作成したVMグループを確認します。
8. [VM group]ウィンドウの右上にある[Backup]を選択します。



9. バックアップ・レベルとして[Full]を選択し、バックアップが完了したら（オプションで）Eメールを要求し、[OK]をクリックしてバックアップ・ジョブを開始します。


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. ジョブの概要ページに移動して、ジョブの指標を確認します。



ベースラインパフォーマンステストのレビュー

Aux Copy操作では、4つのCommvault MediaAgentがNetApp AFF A300システムにデータをバックアップし、NetApp StorageGRID上に補助コピーを作成しました。テストセットアップ環境の詳細については、テクニカルレポートの「ソリューションの設計とベストプラクティス」セクションを参照して "CommvaultによるNetAppスケールアウトデータ保護" ください。

このテストは、100台のVMと1、000台のVMを使用して実施しました。どちらのテストも、Windows VMとCentOS VMが50対50で混在した環境で実施しました。次の表に、ベースラインパフォーマンステストの結果を示します。

操作	バックアップ速度	リストア速度
AUXコピー	2TB/時	1.27TB/時間
オブジェクトとの直接やり取り（重複排除オン）	2.2 TB/時間	1.22TB/時間

エージングオフパフォーマンスをテストするために、250万個のオブジェクトが削除されました。図2と図3に示すように、削除の実行は3時間以内に完了し、80TB以上のスペースが解放されました。削除の実行は午前10時30分に開始されました。

図**1**：**250**万（**80TB**）のオブジェクトを**3**時間未満で削除

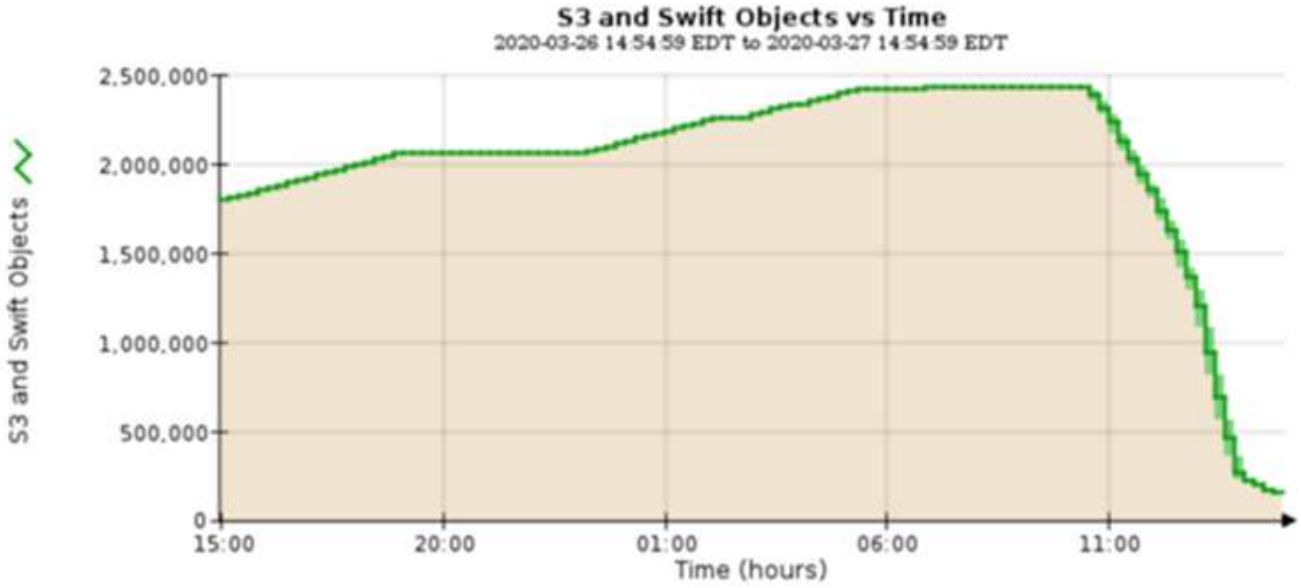
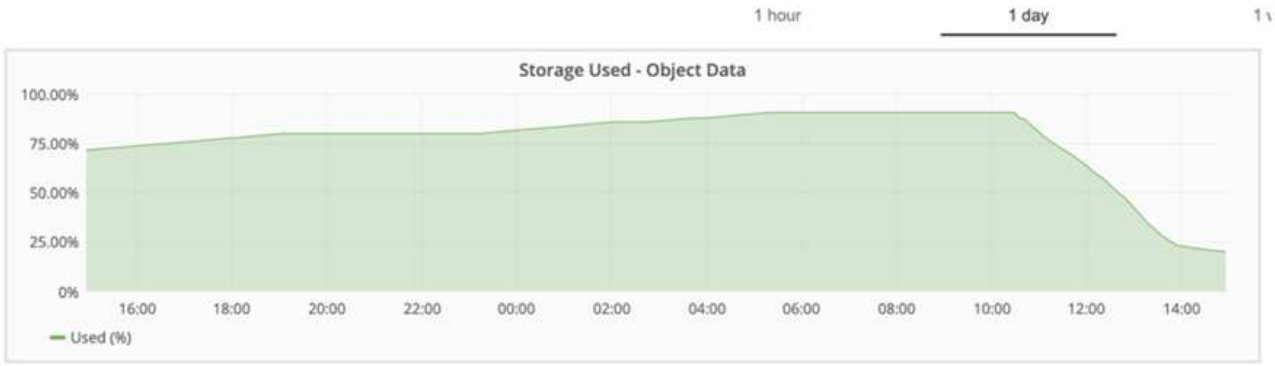


図**2**：**80TB**のストレージを**3**時間未満で解放



バケット整合性レベルの推奨事項

NetApp StorageGRIDを使用すると、エンドユーザは、Simple Storage Service（S3）バケット内のオブジェクトに対して実行される処理の整合性レベルを選択できます。

CommVault MediaAgentは、CommVault環境のデータムーバーです。ほとんどの場合、MediaAgentはプライマリStorageGRIDサイトにローカルで書き込むように設定されています。そのため、ローカルのプライマリサイト内で高い整合性レベルを維持することを推奨します。StorageGRIDで作成したCommvaultバケットに整合性レベルを設定する場合は、次のガイドラインに従ってください。

> 11.0.0-Service Pack 16より前のバージョンのCommVaultを使用している場合は、CommVaultを最新バージョンにアップグレードすることを検討してください。これがオプションでない場合は、使用しているバージョンのガイドラインに従ってください。

- 11.0.0より前のバージョンのCommVault - Service Pack 16。* 11.0.0より前のバージョンのService Pack 16では、CommVaultはリストアおよび削除処理の一環として、存在しないオブジェクトに対してS3 HEADおよびGET処理を実行します。バケットの整合性レベルをstrong-siteに設定して、StorageGRIDへのCommvaultバックアップに最適な整合性レベルを実現します。
- CommVaultバージョン11.0.0 - Service Pack 16以降。*バージョン11.0.0 - Service Pack 16以降では、存在

しないオブジェクトに対して実行されるS3 HEAD処理とGET処理の数が最小限に抑えられます。CommvaultおよびStorageGRID環境で高い整合性レベルを確保するには、バケットのdefault整合性レベルをRead-after-new-writeに設定します。

TR-4626：ロードバランサ

StorageGRIDで他社製ロードバランサを使用する

StorageGRIDなどのオブジェクトストレージシステムにおける、サードパーティおよびグローバルロードバランサの役割について説明します。

サードパーティ製ロードバランサを使用してNetApp®StorageGRID®を実装するための一般的なガイダンス。

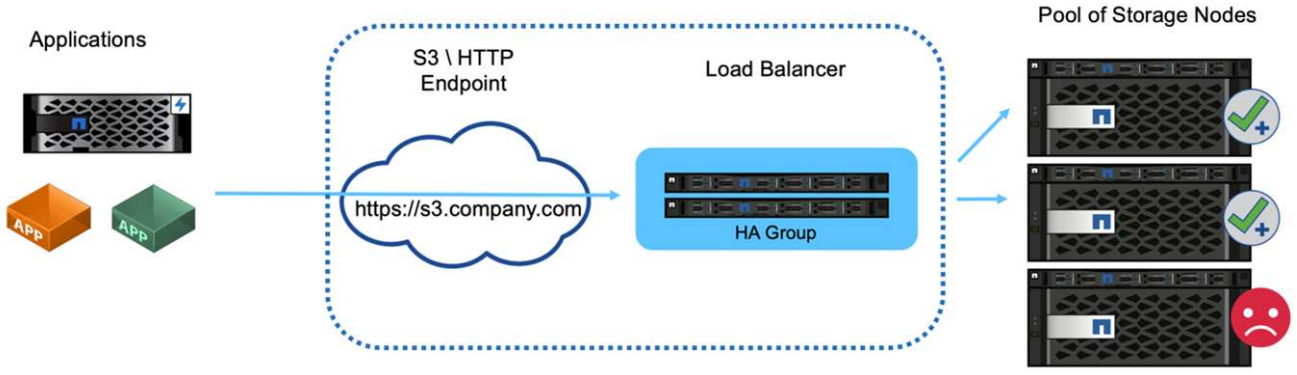
オブジェクトストレージはクラウドストレージと同義です。クラウドストレージを利用するアプリケーションは、予想どおりURLを介してストレージに対応します。StorageGRIDは、このシンプルなURLを使用して、単一サイトまたは地理的に分散したサイト全体で容量、パフォーマンス、データ保持性を拡張できます。この簡易性を実現するコンポーネントは、ロードバランサです。

このドキュメントの目的は、StorageGRIDのお客様にロードバランサのオプションについて説明し、サードパーティ製ロードバランサの設定に関する一般的なガイダンスを提供することです。

ロードバランサの基本

ロードバランサは、StorageGRIDなどのエンタープライズクラスのオブジェクトストレージシステムに欠かせないコンポーネントです。StorageGRIDは複数のストレージノードで構成され、各ストレージノードは特定のStorageGRIDインスタンスのSimple Storage Service（S3）ネームスペース全体を提供できます。ロードバランサは可用性の高いエンドポイントを作成し、その背後にStorageGRIDノードを配置します。StorageGRIDは、S3互換オブジェクトストレージシステムの中で独自のロードバランサを提供するだけでなく、F5、Citrix NetScaler、HAプロキシ、NGINXなどのサードパーティまたは汎用のロードバランサもサポートしています。

次の図では、例としてURL/完全修飾ドメイン名（FQDN）「s3.company.com”」を使用しています。ロードバランサは、DNSを介してFQDNに解決される仮想IP（VIP）を作成し、アプリケーションからの要求をすべてStorageGRIDノードのプールに転送します。ロードバランサは各ノードで健全性チェックを実行し、正常なノードへの接続のみを確立します。



次の図はStorageGRIDが提供するロードバランサを示していますが、概念はサードパーティのロードバランサでも同じです。アプリケーションはロードバランサのVIPを使用してHTTPセッションを確立し、トラフィックはロードバランサを経由してストレージノードに送信されます。デフォルトでは、アプリケーションからロードバランサ、およびロードバランサからストレージノードへのすべてのトラフィックがHTTPSを介して暗号化されます。HTTPはサポートされているオプションです。

ローカルおよびグローバルのロードバランサ

ロードバランサには次の2種類があります。

- ローカルトラフィックマネージャ（**LTM**）。単一サイト内のノードのプール全体に接続を分散します。
- グローバルサービスロードバランサ（**GSLB**）。複数のサイトに接続を分散し、LTMロードバランサを効果的にロードバランシングします。GSLBは、インテリジェントDNSサーバと考えてください。クライアントがStorageGRIDエンドポイントURLを要求すると、GSLBは可用性またはその他の要因（アプリケーションの遅延を低減できるサイトなど）に基づいて、そのURLをLTMのVIPに解決します。LTMは常に必要ですが、StorageGRIDサイトの数とアプリケーションの要件に応じて、GSLBはオプションです。

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/[]
- NetApp StorageGRIDイネーブルメント https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRID F5ロードバランサの設計に関する考慮事項 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load Balancing NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp：ロードバランシングNetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

StorageGRIDロードバランサーを使用する

StorageGRIDゲートウェイ ノード ロード バランサーの役割について学習します。

NetApp® StorageGRID® ゲートウェイ ノードを実装するための一般的なガイダンス。

StorageGRIDゲートウェイノードロードバランサと他社製ロードバランサの比較

StorageGRIDは、S3と互換性のあるオブジェクトストレージベンダーの中で唯一、専用のアプライアンス、VM、コンテナとして使用できる標準のロードバランサを提供します。StorageGRIDが提供するロードバランサは、ゲートウェイノードとも呼ばれます。

F5やCitrixなどのロードバランサをまだ所有していないお客様の場合、サードパーティのロードバランサの実装は非常に複雑になる可能性があります。StorageGRIDロードバランサは、ロードバランサの処理を大幅に簡易化します。

ゲートウェイノードは、可用性とパフォーマンスに優れたエンタープライズクラスのロードバランサです。ゲートウェイノード、サードパーティ製ロードバランサ、またはその両方を同じグリッドに実装することもできます。ゲートウェイノードはローカルトラフィックマネージャであり、GSLBではありません。

StorageGRIDロードバランサには、次の利点があります。

- 簡易性。リソースプール、健全性チェック、パッチ適用、メンテナンスの自動構成をすべてStorageGRIDで管理

- パフォーマンス。 StorageGRIDロード バランサはStorageGRID専用であり、高パフォーマンスのキャッシュを提供でき、帯域幅をめぐって他のアプリケーションと競合することはありません。
- コスト。仮想マシン（VM）とコンテナのバージョンは追加コストなしで提供されます。
- トラフィック分類。高度なトラフィック分類機能を使用すると、StorageGRID固有のQoSルールとワークロード分析を実行できます。
- 今後の**StorageGRID**固有の機能。StorageGRIDは、今後のリリースで引き続き最適化を行い、ロードバランサに革新的な機能を追加していきます。

StorageGRIDの統合ノードとして、ローカル トラフィック マネージャーは、高度なヘルス チェックを使用して、ストレージ ノードのヘルス、負荷、およびリソースの可用性に基づいて要求を分散する機能を備えています。さらに、サイト間のStorageGRIDリンク コストが「0」に設定されている場合は、複数のサイトにわたって負荷を分散する機能もあります。ストレージ ノードが使用できないが、サイト内のゲートウェイ ノードが使用できる場合、負荷はグリッド内の別のサイトに自動的に送信されます。

ゲートウェイ ノードのロード バランサ キャッシュ機能は、データ処理の一環としてデータ セットを複数回再読み取りする特定のワークロード (AI トレーニングなど) のパフォーマンスを大幅に向上させることを目的としています。キャッシュ ゲートウェイ ノードは、グリッドの残りの部分から物理的に離れた場所に展開することも可能で、これにより、一部のワークロードでパフォーマンスが向上し、WAN ネットワークの使用率が低下します。キャッシュはリードバック モードで動作し、書き込みはキャッシュされず、キャッシュの状態は変更されません。各キャッシング ゲートウェイ ノードは、他のキャッシング ゲートウェイ ノードとは独立して動作します。

StorageGRID Gatewayノードの導入の詳細については、 "StorageGRID のドキュメント" 。

HTTPS用のSSL証明書をStorageGRIDに実装する方法

StorageGRIDにSSL証明書を実装するための重要性と手順を理解します。

HTTPSを使用する場合は、Secure Sockets Layer（SSL）証明書が必要です。SSLプロトコルはクライアントとエンドポイントを識別し、信頼できるものとして検証します。SSLは、トラフィックの暗号化も提供します。SSL証明書はクライアントから信頼されている必要があります。これを実現するには、DigiCertなどのグローバルに信頼された認証局（CA）からのSSL証明書、インフラストラクチャで実行されているプライベートCA、またはホストによって生成された自己署名証明書を使用します。

クライアント側での追加のアクションが不要なため、グローバルに信頼されたCA証明書の使用が推奨されます。証明書がロードバランサまたはStorageGRIDにロードされ、クライアントはエンドポイントを信頼して接続します。

プライベートCAを使用するには、ルート証明書とすべての下位証明書をクライアントに追加する必要があります。プライベートCA証明書を信頼するプロセスは、クライアントのオペレーティングシステムとアプリケーションによって異なります。たとえば、ONTAP for FabricPoolでは、チェーン内の各証明書（ルート証明書、下位証明書、エンドポイント証明書）をONTAPクラスタに個別にアップロードする必要があります。

自己署名証明書を使用するには、クライアントがCAなしで提供された証明書を信頼して信頼性を検証する必要があります。一部のアプリケーションでは、自己署名証明書が受け入れられず、検証を無視できない場合があります。

クライアントロードバランサのStorageGRIDパスへのSSL証明書の配置は、SSLターミネーションが必要な場所によって異なります。ロードバランサをクライアントの終端エンドポイントとして設定し、ロードバランサからStorageGRIDへの接続用の新しいSSL証明書を使用して再暗号化またはホット暗号化することができます。または、トラフィックを通過させ、StorageGRIDをSSL終端エンドポイントにすることもできます。ロー

ドバランサがSSLターミネーションエンドポイントの場合、証明書はロードバランサにインストールされ、DNS名/URLのサブジェクト名、およびロードバランサを介してStorageGRIDターゲットに接続するようにクライアントが設定されている代替URL/DNS名が含まれています。 ワイルドカード名を含む。ロードバランサがパススルー用に設定されている場合は、StorageGRIDにSSL証明書をインストールする必要があります。証明書には、DNS名/URLのサブジェクト名と、ロードバランサを介してStorageGRIDターゲットに接続するようにクライアントが設定されている代替URL/DNS名（ワイルドカード名を含む）が含まれている必要があります。個 々 のストレージノード名を証明書に含める必要はなく、エンドポイントのURLのみを含める必要があります。

StorageGRIDでの信頼できるサードパーティ製ロードバランサの設定

StorageGRIDで信頼できるサードパーティ製ロードバランサを設定する方法について説明します。

1つ以上の外部レイヤ7ロードバランサと、IPベースのS3バケットまたはグループポリシーを使用している場合、StorageGRIDは実際の送信者のIPアドレスを特定する必要があります。これは、ロードバランサによって要求に挿入されるX-Forwarded-For（XFF）ヘッダーを調べることによって行われます。ストレージノードに直接送信された要求でXFFヘッダーが簡単にスプーフィングされる可能性があるため、StorageGRIDでは、各要求が信頼されたレイヤ7ロードバランサによってルーティングされていることを確認する必要があります。StorageGRIDがリクエストの送信元を信頼できない場合は、XFFヘッダを無視します。グリッド管理APIを使用して、信頼された外部レイヤ7ロードバランサのリストを設定できます。この新しいAPIはプライベートAPIであり、今後のStorageGRIDリリースで変更される可能性があります。最新の情報については、技術情報アーティクルを参照してください "サードパーティのレイヤ7ロードバランサと連携するようにStorageGRIDを設定する方法"。

ローカルトラフィックマネージャロードバランサの詳細

ローカルトラフィックマネージャロードバランサのガイダンスを確認し、最適な設定を決定します。

以下は、サードパーティ製ロードバランサの設定に関する一般的なガイダンスです。お使いの環境に最適な構成を決定するには、ロードバランサ管理者にお問い合わせください。

ストレージノードのリソースグループを作成

StorageGRIDストレージノードをリソースプールまたはサービスグループにグループ化します（用語は特定のロードバランサによって異なる場合があります）。StorageGRIDストレージノードは次のポートにS3 APIを提供します。

- S3 HTTPS：18082
- S3 HTTP：18084

ほとんどのお客様は、標準のHTTPSポートとHTTPポート（443および80）を使用してAPIを仮想サーバに提供することを選択しています。

> 各StorageGRIDサイトにはデフォルトで3つのストレージノードが必要で、そのうち2つは正常な状態である必要があります。

健全性チェック

サードパーティのロードバランサには、各ノードの健常性とトラフィックを受信できるかどうかを確認する方法が必要です。NetAppでは、健全性チェックの実行にHTTP方式を使用することを推奨しています `OPTIONS` 。ロードバランサは個 々 のストレージノードにHTTP要求を発行し `OPTIONS` 、ステータス応答を期待します。 `200`

応答を返さないストレージノードがあると `200` 、そのノードはストレージ要求を処理できません。アプリケーションとビジネスの要件によって、これらのチェックのタイムアウトと、ロードバランサが実行するアクションを決定する必要があります。

たとえば、データセンター1の4つのストレージノードのうち3つが停止している場合は、すべてのトラフィックをデータセンター2に転送できます。

推奨されるポーリング間隔は1秒に1回で、チェックに3回失敗したあとにノードをオフラインにします。

S3の健全性チェックの例

次の例では、を送信し `OPTIONS` て確認し `200 OK` ます。`Amazon S3`が許可されていない要求をサポートしていないため、を使用して `OPTIONS` います。

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

ファイルベースまたはコンテンツベースの健全性チェック

一般に、NetAppではファイルベースの健全性チェックは推奨されません。通常、読み取り専用ポリシーが設定されたバケットには、たとえば小さなファイル —`healthcheck.htm`が作成されます。このファイルがフェッチされ、ロードバランサによって評価されます。この方法にはいくつかの欠点があります。

- * 1つのアカウントに依存します。*ファイルを所有するアカウントが無効になると、健全性チェックは失敗し、ストレージ要求は処理されません。
- *データ保護ルール。*デフォルトのデータ保護方式は2コピー方式です。このシナリオでは、健全性チェックファイルをホストしている2つのストレージノードを使用できない場合、健全性チェックは失敗し、ストレージ要求が正常なストレージノードに送信されず、グリッドがオフラインになります。
- *監査ログの肥大化。*ロードバランサは各ストレージノードからファイルをX分ごとにフェッチし、多数の監査ログエントリを作成します。
- *大量のリソースを必要とします。*健全性チェックファイルをすべてのノードから数秒おきにフェッチすると、グリッドリソースとネットワークリソースが消費されます。

コンテンツベースの健全性チェックが必要な場合は、専用のS3バケットで専用テナントを使用します。

セッションの永続性

セッションの持続性（スティッキ性）とは、特定のHTTPセッションの持続が許可される時間のことです。デフォルトでは、ストレージノードは10分後にセッションを破棄します。持続性が長くなると、すべてのアクションでアプリケーションがセッションを再確立する必要がなくなるため、パフォーマンスが向上しますが、セッションを開いたままにするとリソースが消費されます。ワークロードにメリットがあると判断した場合は、サードパーティのロードバランサでのセッションの永続性を減らすことができます。

仮想ホスト形式のアドレス指定

AWS S3のデフォルトの方法が仮想ホスト形式になりました。StorageGRIDや多くのアプリケーションでは引き続きパス形式がサポートされますが、仮想ホスト形式のサポートを実装することを推奨します。仮想ホスト形式の要求では、ホスト名の一部にバケットが含まれます。

仮想ホスト形式をサポートするには、次の手順を実行します。

- サポートされるワイルドカードDNSルックアップ：*.s3.company.com
- ワイルドカードをサポートするには、サブジェクトalt名を含むSSL証明書を使用してください。*.s3.company.com一部のお客様から、ワイルドカード証明書の使用に関するセキュリティ上の懸念が表明されています。StorageGRIDは、FabricPoolなどの主要なアプリケーションと同様に、パス形式のアクセスを引き続きサポートします。とはいえ、仮想ホストがサポートされていないと、一部のS3 API呼び出しが失敗したり、正常に動作しなくなったりします。

SSLターミネーション

サードパーティのロードバランサでのSSLターミネーションには、セキュリティ上の利点があります。ロードバランサが危険にさらされると、グリッドは分離されます。

サポートされる構成は次の3つです。

- * SSLパススルー*SSL証明書は、カスタムサーバ証明書としてStorageGRIDにインストールされます。
- * SSLターミネーションと再暗号化（推奨）*これは、SSL証明書をStorageGRIDにインストールするのではなく、ロードバランサでSSL証明書管理をすでに実行している場合に便利です。この構成では、攻撃対象をロードバランサに限定することで、セキュリティ上のメリットが追加されます。
- * HTTPによるSSL終了*この構成では、SSLはサードパーティのロードバランサで終端され、ロードバランサからStorageGRIDへの通信はSSLオフロードを利用するために非暗号化されます（最新のプロセッサに組み込まれたSSLライブラリを使用すると、メリットは限られています）。

パススルー構成

ロードバランサをパススルー用に設定する場合は、StorageGRIDに証明書をインストールする必要があります。メニューの[Configuration][Server Certificates]>[Object Storage API Service Endpoints Server Certificate]に移動します。

ソースクライアントの**IP**可視性

StorageGRID 11.4では、信頼できるサードパーティ製ロードバランサの概念が導入されました。クライアントアプリケーションIPをStorageGRIDに転送するには、この機能を設定する必要があります。詳細については、を参照してください。 "サードパーティのレイヤ7ロードバランサと連携するようにStorageGRIDを設定する方法。"

XFFヘッダーを使用してクライアントアプリケーションのIPを表示できるようにするには、次の手順を実行します。

手順

1. 監査ログにクライアントIPを記録します。
2. S3バケットまたはグループポリシーを使用する `aws:SourceIp` 。

ロードバランシング戦略

ほとんどのロードバランシングソリューションには、ロードバランシングに関する複数の戦略が用意されています。一般的な戦略は次のとおりです。

- *ラウンドロビン*ユニバーサルフィットですが、少数のノードと大規模な転送で単一のノードを詰まらせることに苦しんでいます。
- *最小接続。*すべてのノードへの接続が均等に分散される、小規模なオブジェクトワークロードや混在オブジェクトワークロードに適しています。

選択するストレージノードの数が増えるにつれて、アルゴリズムの選択はそれほど重要ではありません。

データパス

すべてのデータは、ローカルトラフィックマネージャロードバランサを経由します。StorageGRIDは、Direct Server Routing（DSR；直接サーバールーティング）をサポートしていません。

セツゾクノフンサンノカクニン

負荷を複数のストレージノードに均等に分散していることを確認するには、特定のサイトの各ノードで確立されたセッションを確認します。

- * UIメソッド。*メニューの[Support][Metrics]>[S3][Overview]>[LDR HTTP Sessions]に移動します。
- *メトリクスAPI。*使用 `storagegrid_http_sessions_incoming_currently_established`

StorageGRID構成のユースケースをご紹介します

お客様とNetApp ITによって実装されたStorageGRID構成のユースケースをご紹介します。

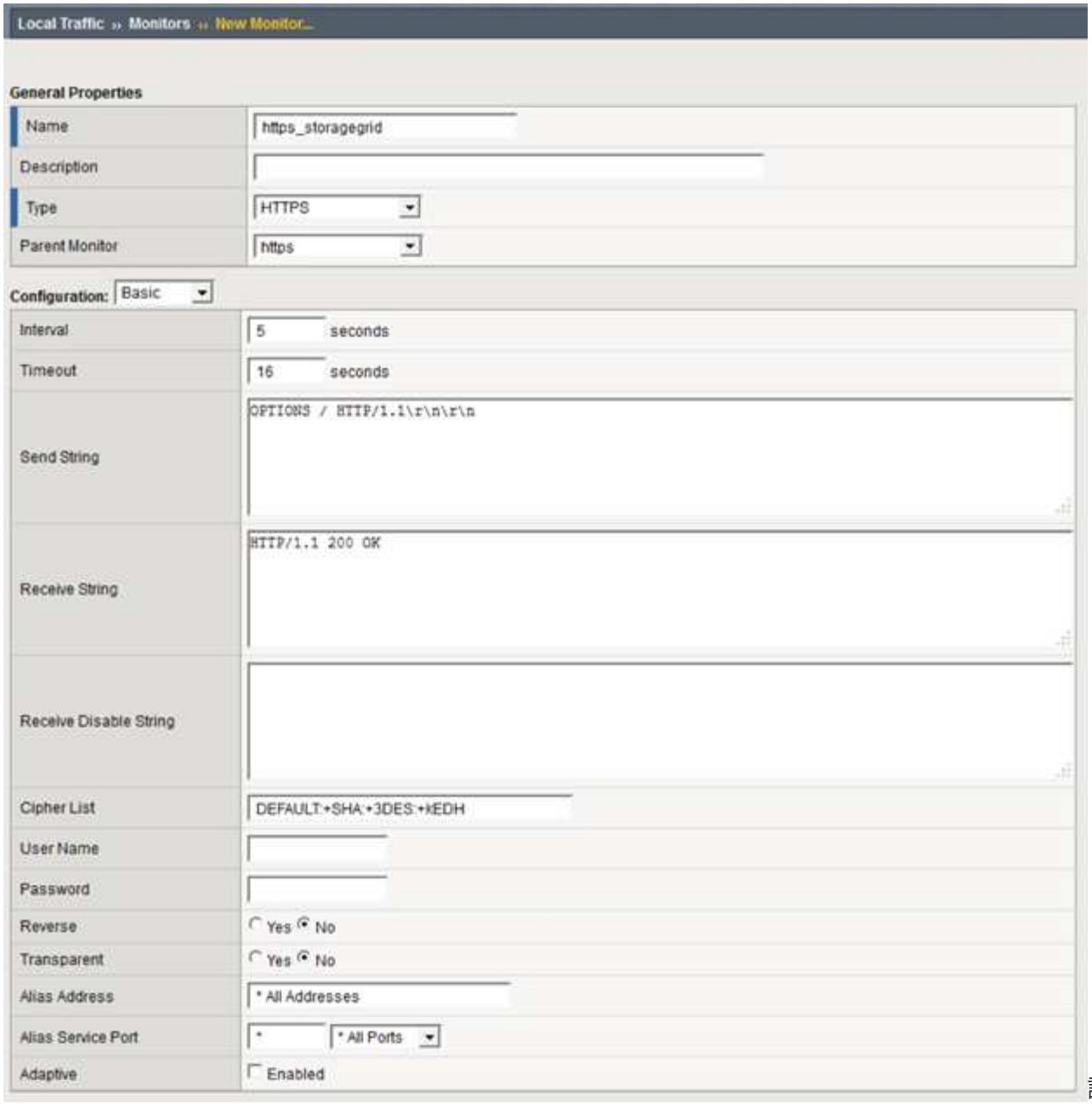
次の例は、StorageGRIDのお客様（NetApp ITを含む）が実装した構成を示しています。

S3バケット用のF5 BIG-IP Local Traffic Manager健全性チェックモニタ

F5 BIG-IPローカルトラフィックマネージャヘルスチェックモニタを設定する手順は、次のとおりです。

手順

1. 新しいモニタを作成します。
   a. [Type]フィールドにと入力します `HTTPS`。
   b. 必要に応じて、間隔とタイムアウトを設定します。
   c. Send Stringフィールドに、 `OPTIONS / HTTP/1.1\r\n\r\n`. \r\nはキャリッジリターンです。異なるバージョンのBIG-IPソフトウェアでは、0、1、または2セットの\r\nシーケンスが必要です。詳細については、を参照してください https://support.f5.com/csp/article/K10655。
   d. [Receive String]フィールドに、次のように入力します。 `HTTP/1.1 200 OK`



設定ページ"]

2. [Create Pool]で、必要なポートごとにプールを1つ作成します。
   a. 前の手順で作成したヘルスモニタを割り当てます。
   b. ロードバランシング方式を選択します。
   c. サービスポート18082（S3）を選択します。
   d. ノードを追加します。

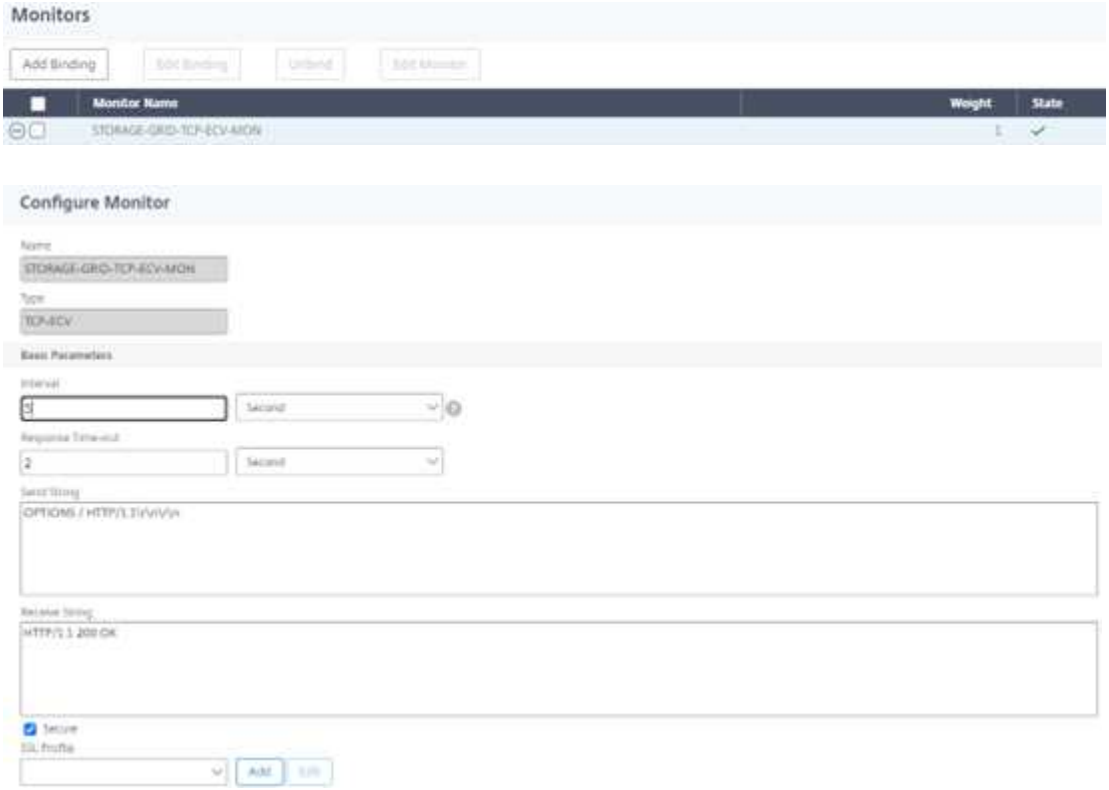
Citrix NetScaler

Citrix NetScalerは、ストレージエンドポイント用の仮想サーバーを作成し、StorageGRIDストレージノードをアプリケーションサーバーとして参照してから、サービスにグループ化します。

HTTPS-ECV健全性チェックモニタを使用してカスタムモニタを作成し、OPTIONS要求と受信を使用して推奨される健全性チェックを実行し `200`ます。HTTP-ECVは送信文字列を使用して設定され、受信文字列を検

証します。

詳細については、Citrixのドキュメントを参照してください "HTTP-ECVヘルスチェックモニタの設定例"。



Loadbalancer.org

Loadbalancer.orgは、独自のStorageGRIDとの統合テストを実施し、広範な構成ガイドを用意しています。
https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf

ケンプ

KempはStorageGRIDとの統合テストを独自に実施し、広範な構成ガイドを用意しています。
https://kemptechnologies.com/solutions/netapp/

HAProxy

OPTIONS要求を使用するようにHAProxyを設定し、haproxy.cfgでヘルスチェックの200ステータス応答を確認します。フロントエンドのバインドポートを別のポート（443など）に変更できます。

次に、HAProxyでのSSL終端の例を示します。

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

次に、SSLパススルーの例を示します。

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

StorageGRIDの設定の完全な例については、GitHubのを参照してください "HAProxy設定の例" 。

StorageGRIDでのSSL接続の検証

StorageGRIDでSSL接続を検証する方法について説明します。

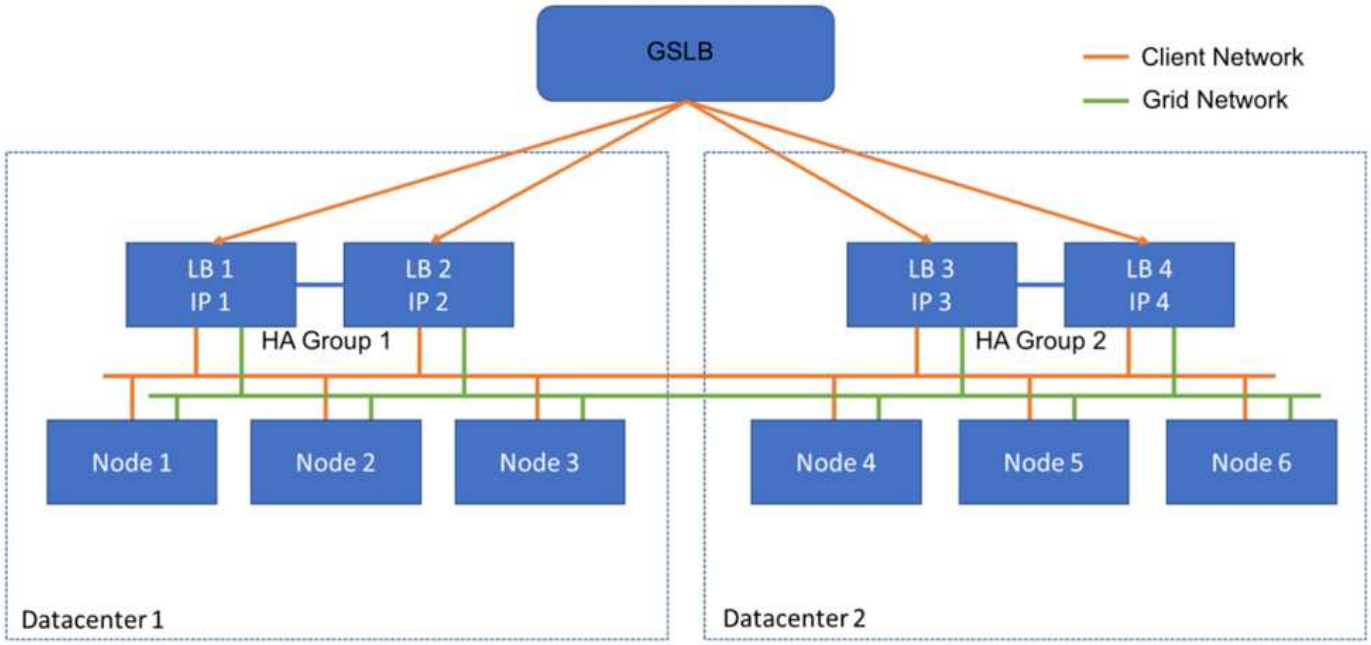
ロードバランサを設定したら、OpenSSLやAWS CLIなどのツールを使用して接続を検証する必要があります。S3 Browserなどの他のアプリケーションでは、SSLの設定ミスが無視される可能性があります。

StorageGRIDのグローバルロードバランシング要件を理解する

StorageGRIDでのグローバルロードバランシングの設計上の考慮事項と要件を確認します。

グローバルなロードバランシングでは、複数のStorageGRIDサイトにインテリジェントなルーティングを提供するために、DNSと統合する必要があります。この機能はStorageGRIDドメインの外部にあり、前述のロードバランサ製品などのサードパーティのソリューションや、InfobloxなどのDNSトラフィック制御ソリューションによって提供される必要があります。このトップレベルのロードバランシングは、ネームスペース内の最も近い宛先サイトへのスマートルーティング、および停止の検出とネームスペース内の次のサイトへのリダイ

レクションを提供します。一般的なGSLBの実装は、サイトローカルのロードバランサを含むサイトプールを含むトップレベルのGSLBで構成されます。サイトロードバランサには、ローカルサイトのストレージノードのプールが含まれています。これには、GSLB機能用のサードパーティ製ロードバランサとサイトローカルロードバランシングを提供するStorageGRIDの組み合わせ、またはサードパーティの組み合わせが含まれます。または、前述したサードパーティの多くが、GSLBとサイトローカルロードバランシングの両方を提供できます。



TR-4645：『Security features』

オブジェクトストア内の**StorageGRID**データとメタデータを保護

StorageGRIDオブジェクトストレージソリューションに組み込まれているセキュリティ機能をご確認ください。

これは、データ アクセス、オブジェクトとメタデータ、管理アクセス、プラットフォーム セキュリティを網羅した、 NetApp® StorageGRID® のさまざまなセキュリティ機能の概要です。 StorageGRID 12.0 でリリースされた最新の機能が含まれるように更新されました。

セキュリティは、NetApp StorageGRIDオブジェクトストレージソリューションに不可欠な要素です。オブジェクトストレージに適した多くのタイプのリッチコンテンツデータも機密性が高く、規制やコンプライアンスの対象となるため、セキュリティは特に重要です。StorageGRIDの機能が進化し続ける中で、このソフトウェアは、組織のセキュリティ体制を保護し、業界のベストプラクティスに準拠するのに役立つ多くのセキュリティ機能を利用できるようにします。

このホワイト ペーパーでは、 StorageGRID 12.0 のさまざまなセキュリティ機能の概要を 5 つのカテゴリに分けて説明します。

- データアクセスセキュリティ機能
- オブジェクトとメタデータのセキュリティ機能
- 管理セキュリティ機能

- プラットフォームのセキュリティ機能
- クラウドとの統合

このホワイト ペーパーはセキュリティ データシートとして作成されており、デフォルトでは構成されていない、本書に記載されているセキュリティ機能をサポートするようにシステムを構成する方法については詳しく説明していません。その "StorageGRIDセキュリティガイド"公式ウェブサイトで入手可能 "StorageGRID のドキュメント"ページ。

このレポートで説明する機能に加えて、StorageGRIDはにも準拠して "NetApp製品セキュリティ脆弱性対応および通知ポリシー"います。報告された脆弱性は、製品のセキュリティインシデント対応プロセスに従って検証され、対応されます。

NetApp StorageGRIDは、要件の厳しいエンタープライズオブジェクトストレージのユースケースに対応する高度なセキュリティ機能を提供します。

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：SEC 17a-4（f）、FINRA 4511（c）、CFTC 1.31（c）-（d）コンプライアンス評価 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 カーネル暗号化認定 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B エントロピー認定 https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRIDカナダサイバーセキュリティセンター コモンクライテリア認定 https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRIDドキュメントページhttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp製品ドキュメント https://www.netapp.com/support-and-training/documentation/

用語と略語

このセクションでは、ドキュメントで使用される用語の定義について説明します。

用語または頭字語	定義
S3	Simple Storage Serviceの略。
クライアント	データアクセス用にS3プロトコルを使用するか、管理用にHTTPプロトコルを使用してStorageGRIDと連携できるアプリケーション。
テナント管理者	StorageGRIDテナントアカウントの管理者
テナントユーザ	StorageGRIDテナントアカウント内のユーザ
TLS	トランスポート層セキュリティ
ILM	情報ライフサイクル管理
LAN	ローカルエリアネットワーク

用語または頭字語	定義
グリッド管理者	StorageGRIDシステムの管理者
グリッド	StorageGRIDシステム
バケット	S3に格納されたオブジェクトのコンテナ
LDAP	Lightweight Directory Access Protocolの略
秒	証券取引委員会（取引所メンバー、ブローカー、ディーラーを規制）
フィンラ	金融業界規制当局（SEC Rule 17a-4（f）のフォーマットおよびメディア要件を延期）
CFTC	商品先物取引委員会、商品先物取引の規制
NIST	米国標準技術研究所

データアクセスセキュリティ機能

StorageGRIDのデータアクセスセキュリティ機能について説明します。

機能	機能	影響	コンプライアンス
設定可能なTransport Layer Security（TLS）	TLSは、クライアントとStorageGRIDゲートウェイノード、ストレージノード、またはロードバランサエンドポイント間の通信用にハンドシェイクプロトコルを確立します。 StorageGRIDでは、TLSで次の暗号スイートがサポートされています。 • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 TLS v1.2および1.3をサポート。 SSLv3、TLS v1.1 以前はサポートされていません。	クライアントとStorageGRIDがお互いを識別して認証し、機密性とデータ整合性を維持して通信できるようにします。最新のTLSバージョンを確実に使用します。[設定/セキュリティ]設定で暗号を設定できるようになりました。	—

機能	機能	影響	コンプライアンス
設定可能なサーバ証明書（ロードバランサエンドポイント）	グリッド管理者は、サーバ証明書を生成または使用するようにロードバランサエンドポイントを設定できます。	標準の信頼された認証局（CA）によって署名されたデジタル証明書を使用して、ロードバランサエンドポイントごとにグリッドとクライアント間のオブジェクトAPI処理を認証できるようにします。	—
設定可能なサーバ証明書（APIエンドポイント）	グリッド管理者は、組織の信頼されたCAによって署名されたサーバ証明書を使用するように、すべてのStorageGRID APIエンドポイントを一元的に設定できます。	標準の信頼されたCAによって署名されたデジタル証明書を使用して、クライアントとグリッドの間のオブジェクトAPI処理を認証できます。	—

機能	機能	影響	コンプライアンス
マルチテナンシー	StorageGRIDでは、グリッドごとに複数のテナントがサポートされ、各テナントに独自のネームスペースがあります。テナントはS3プロトコルを提供します。デフォルトでは、バケット/コンテナおよびオブジェクトへのアクセスはアカウント内のユーザに制限されます。テナントには、1人のユーザ（各ユーザが独自のアカウントを持つエンタープライズ環境など）または複数のユーザ（サービスプロバイダ環境など、各アカウントがサービスプロバイダの企業および顧客であるサービスプロバイダ環境など）を設定できます。ユーザはローカルまたはフェデレーテッドにすることができます。フェデレーテッドユーザは、Active DirectoryまたはLightweight Directory Access Protocol（LDAP）によって定義されます。StorageGRIDには、ユーザがローカルまたはフェデレーテッドアカウントのクレデンシャルを使用してログインするテナントごとのダッシュボードが用意されています。ユーザは、バケットに格納されているデータ内の使用状況やオブジェクトの使用状況など、グリッド管理者によって割り当てられたクォータに対するテナント使用状況に関する可視化されたレポートにアクセスできます。管理権限を持つユーザは、ユーザ、グループ、アクセスキーの管理など、テナントレベルのシステム管理タスクを実行できます。	StorageGRID管理者は、テナントアクセスを分離しながら複数のテナントのデータをホストできます。また、Active DirectoryやLDAPなどの外部のアイデンティティプロバイダとユーザをフェデレーションすることでユーザIDを確立できます。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
アクセスクレデンシャルの否認防止	すべてのS3処理は、一意のテナントアカウント、ユーザ、およびアクセスキーで識別され、ログに記録されます。	Grid管理者は、どのAPIアクションをどのユーザが実行するかを設定できます。	—

機能	機能	影響	コンプライアンス
匿名アクセスの無効化	デフォルトでは、S3アカウントに対して匿名アクセスは無効になっています。テナントアカウント内のバケット、コンテナ、またはオブジェクトにアクセスするには、要求者がテナントアカウント内の有効なユーザの有効なアクセスクレデンシャルを持っている必要があります。明示的なIAMポリシーを使用して、S3バケットまたはオブジェクトへの匿名アクセスを有効にできます。	グリッド管理者がバケット/コンテナおよびオブジェクトへの匿名アクセスを無効化または制御できるようにします。	—
コンプライアンスWORM	SEC Rule 17a-4（f）の要件を満たすように設計され、Cohassetによって検証されています。バケットレベルでの準拠を有効にできます。保持期間は延長できますが、短縮することはできません。 情報ライフサイクル管理（ILM）ルールでは、最小限のデータ保護レベルが適用されます。	規制上のデータ保持要件があるテナントで、格納オブジェクトとオブジェクトメタデータのWORM保護を実現できます。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
WORM	グリッド管理者は、[Disable Client Modify]オプションを有効にすることで、グリッド全体のWORMを有効にできます。これにより、クライアントがすべてのテナントアカウントのオブジェクトまたはオブジェクトメタデータを上書きまたは削除できなくなります。 S3テナント管理者は、IAMポリシーを指定して、テナント、バケット、またはオブジェクトプレフィックスでWORMを有効にすることもできます。このポリシーには、オブジェクトおよびメタデータの上書きに関するカスタムのS3：PutOverwriteObject権限が含まれています。	グリッド管理者とテナント管理者は、格納オブジェクトとオブジェクトメタデータに対するWORM保護を制御できます。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）

機能	機能	影響	コンプライアンス
KMSホストサーバ暗号化キー管理	グリッド管理者は、Grid Managerで1つ以上の外部キー管理サーバ（KMS）を設定して、StorageGRIDサービスとストレージアプライアンスに暗号化キーを提供できます。各KMSホストサーバまたはKMSホストサーバクラスタは、Key Management Interoperability Protocol（KMIP）を使用して、関連付けられたStorageGRIDサイトのアプライアンスノードに暗号化キーを提供します。	保存データの暗号化が実現されます。アプライアンスボリュームが暗号化されると、ノードがKMSホストサーバと通信できる場合を除き、アプライアンス上のデータにアクセスすることはできません。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
自動フェイルオーバー	StorageGRIDは、あらかじめ組み込まれた冗長性と自動フェイルオーバー機能を提供します。ディスクまたはノードからサイト全体に至るまで、複数の障害が発生しても、テナントアカウント、バケット、オブジェクトへのアクセスを継続できます。StorageGRIDはリソースを認識し、使用可能なノードとデータの場所に要求を自動的にリダイレクトします。StorageGRIDサイトは、孤立モードでも動作できます。WANが停止してサイトがシステムの残りの部分から切断された場合、ローカルリソースで読み取りと書き込みを続行でき、WANがリストアされるとレプリケーションが自動的に再開されます。	グリッド管理者は、アップタイムやSLAなどの契約上の義務に対処し、ビジネス継続性計画を実装できます。	—
• S3固有のデータアクセスセキュリティ機能*	AWS署名バージョン2およびバージョン4	API要求の署名は、S3 API処理の認証を提供します。AmazonはSignature Version 2とVersion 4の2つのバージョンをサポートしている。署名プロセスは、要求者の身元を確認し、転送中のデータを保護し、潜在的なリプレイ攻撃から保護します。	シグネチャバージョン4に関するAWSの推奨事項に準拠し、シグネチャバージョン2を使用する古いアプリケーションとの下位互換性を有効にします。

機能	機能	影響	コンプライアンス
—	S3 オブジェクトのロック	StorageGRIDのS3オブジェクトロック機能は、Amazon S3のS3オブジェクトロックに相当するオブジェクト保護ソリューションです。	テナントは、特定のオブジェクトを一定期間または無期限に保持することを求める規制に準拠するために、S3オブジェクトロックを有効にしたバケットを作成できます。
SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）	S3クレデンシャルのセキュアなストレージ	S3アクセスキーは、パスワードハッシュ関数（SHA-2）で保護された形式で格納されます。	キーの長さ（10^{31}ランダムに生成された数字）とパスワードハッシュアルゴリズムを組み合わせて、アクセスキーのセキュアな格納をイネーブルにします。
—	タイムバウンドのS3アクセスキー	ユーザのS3アクセスキーを作成するときに、アクセスキーに有効期限の日時を設定できます。	グリッド管理者は、一時的なS3アクセスキーをプロビジョニングできます。
—	ユーザアカウントごとに複数のアクセスキー	StorageGRIDを使用すると、1つのユーザアカウントに対して複数のアクセスキーを作成し、同時にアクティブにすることができます。各APIアクションはテナントユーザアカウントとアクセスキーを使用してログに記録されるため、複数のキーがアクティブであっても拒否されません。	クライアントがアクセスキーを無停止でローテーションできるようにします。また、各クライアントに独自のキーを割り当てることができるため、クライアント間でのキー共有が不要になります。
—	S3 IAMアクセスポリシー	StorageGRIDはS3 IAMポリシーをサポートしているため、グリッド管理者はテナント、バケット、またはオブジェクトプレフィックスごとに詳細なアクセス制御を指定できます。StorageGRIDでは、IAMポリシーの条件と変数もサポートしているため、より動的なアクセス制御ポリシーを使用できます。	グリッド管理者がテナント全体に対してユーザグループ別にアクセス制御を指定できるようにします。また、テナントユーザが自身のバケットとオブジェクトに対してアクセス制御を指定できるようにします。

機能	機能	影響	コンプライアンス
—	S3 セキュリティトークンサービス API AssumeRole	StorageGRID は、S3 STS API AssumeRole をサポートし、権限の範囲が狭められ、有効期間が制限された一時的なセキュリティ認証情報 (アクセス キー ID、シークレット アクセス キー、セッション トークン) を提供します。セッション中に権限をさらに制限するインライン セッション ポリシーは、AssumeRole API の一部としてサポートされています。	テナント管理者がオブジェクト データへの安全な一時アクセスを提供できるようにします。
—	シンプルな通知サービス	StorageGRID は、オブジェクト アクセスに関する通知の送信をサポートしています。次のイベント タイプがサポートされています。 • s3:オブジェクトが作成されました: • s3:オブジェクト作成:配置 • s3:オブジェクト作成:投稿 • s3:オブジェクト作成:コピー • s3:ObjectCreated:CompleteMultipartUpload • s3:オブジェクトが削除されました: • s3:オブジェクトが削除されました:削除 • s3:オブジェクトが削除されました:削除マーカーが作成されました • s3:オブジェクトの復元:投稿	テナント管理者がオブジェクトへのアクセスを監視できるようにする
—	StorageGRIDで管理されるキー（SSE）によるサーバ側の暗号化	StorageGRIDはSSEをサポートしているため、StorageGRIDで管理される暗号化キーを使用して保管データをマルチテナントで保護できます。	テナントでオブジェクトを暗号化できます。これらのオブジェクトの書き込みと読み出しには暗号化キーが必要です。

機能	機能	影響	コンプライアンス
SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）	ユーザ指定の暗号化キーによるサーバ側の暗号化（SSE-C）	StorageGRIDはSSE-Cをサポートしており、クライアントが管理する暗号化キーを使用して保管データをマルチテナントで保護できます。 StorageGRIDはすべてのオブジェクトの暗号化および復号化処理を管理しますが、SSE-Cを使用する場合、クライアントは暗号化キーを自身で管理する必要があります。	クライアントが制御するキーを使用してオブジェクトを暗号化できます。これらのオブジェクトの書き込みと読み出しには暗号化キーが必要です。

オブジェクトとメタデータのセキュリティ

StorageGRIDのオブジェクトとメタデータのセキュリティ機能を確認します。

機能	機能	影響	コンプライアンス
Advanced Encryption Standard（AES）サーバ側オブジェクト暗号化	StorageGRIDは、AES 128およびAES 256ベースのサーバ側オブジェクト暗号化を提供します。グリッド管理者は、暗号化をグローバルなデフォルト設定として有効にすることができます。StorageGRIDはS3のx-amz-server-side-encryptionヘッダーもサポートしており、オブジェクト単位で暗号化を有効または無効にできます。有効にすると、グリッドノード間で格納または転送中のオブジェクトが暗号化されます。	基盤となるストレージハードウェアに依存せずに、ストレージやオブジェクトの転送を保護します。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
組み込みのキー管理機能	暗号化を有効にすると、各オブジェクトがランダムに生成された一意の対称キーで暗号化され、外部アクセスなしでStorageGRID内に格納されます。	外部キー管理を必要とせずにオブジェクトを暗号化できます。	
Federal Information Processing Standard（FIPS）140-2準拠の暗号化ディスク	SG5812、SG5860、SG6160、およびSGF6024 StorageGRIDアプライアンスには、FIPS 140-2準拠の暗号化ディスクをオプションで選択できます。必要に応じて、外部KMIPサーバでディスクの暗号化キーを管理できます。	システムデータ、メタデータ、オブジェクトのセキュアなストレージを実現します。また、StorageGRIDソフトウェアベースのオブジェクト暗号化を提供し、オブジェクトのストレージと転送を保護します。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）

機能	機能	影響	コンプライアンス
ノード向け連邦情報処理規格（FIPS）140-3準拠の暗号化	SG5812、SG5860、SG6160、SGF6112、SG1100、およびSG110 StorageGRIDアプライアンスは、FIPS 140-3 準拠のノード暗号化オプションを提供します。ノードの暗号化キーは外部の KMIP サーバーによって管理されます。	システムデータ、メタデータ、オブジェクトのセキュアなストレージを実現します。また、StorageGRIDソフトウェアベースのオブジェクト暗号化を提供し、オブジェクトのストレージと転送を保護します。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
バックグラウンド整合性スキャンと自己回復	StorageGRIDでは、オブジェクトレベルとサブオブジェクトレベルでハッシュ、チェックサム、巡回冗長検査（CRC）のインターロックメカニズムを使用して、オブジェクトが格納中と転送中の両方でデータの不整合、改ざん、変更から保護します。StorageGRIDは、破損したオブジェクトや改ざんされたオブジェクトを自動的に検出して置換し、変更されたデータを隔離して管理者に警告します。	グリッド管理者は、SLA、規制、データ保持に関するその他の義務を満たすことができます。データの暗号化、改ざん、変更を試みるランサムウェアやウイルスの検出を支援します。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
ポリシーベースのオブジェクトの配置と保持	StorageGRIDを使用すると、グリッド管理者はILMルールを設定して、オブジェクトの保持、配置、保護、移行、有効期限を指定できます。グリッド管理者はStorageGRID、メタデータでオブジェクトをフィルタリングし、グリッド全体、テナント、バケット、キープレフィックス、 およびユーザ定義のメタデータのキーと値のペア。StorageGRIDを使用すると、クライアントによって明示的に削除されないかぎり、ライフサイクル全体を通じてオブジェクトがILMルールに従って格納されるようになります。	データの配置、保護、保持を徹底データ保持性、可用性、パフォーマンスに関するSLAの達成を支援	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
バックグラウンドメタデータスキャン	StorageGRIDは、オブジェクトメタデータをバックグラウンドで定期的にスキャンし、オブジェクトデータの配置または保護の変更をILMの指定に従って適用します。	破損したオブジェクトの検出に役立ちます。	

機能	機能	影響	コンプライアンス
調整可能な整合性	テナントはバケットレベルで整合性レベルを選択して、マルチサイト接続などのリソースを利用できるようにすることができます。	必要な数のサイトまたはリソースが使用可能な場合にのみ、グリッドへの書き込みをコミットするオプションを提供します。	

管理セキュリティ機能

StorageGRIDの管理セキュリティ機能を確認します。

機能	機能	影響	コンプライアンス
サーバ証明書（Grid管理インターフェイス）	グリッド管理者は、組織の信頼されたCAによって署名されたサーバ証明書を使用するようにグリッド管理インターフェイスを設定できます。	標準の信頼されたCAによって署名されたデジタル証明書を使用して、管理クライアントとグリッドの間の管理UIおよびAPIアクセスを認証できます。	—
管理ユーザ認証	管理ユーザは、ユーザ名とパスワードを使用して認証されます。管理ユーザと管理グループは、ローカルまたはフェデレーテッド、お客様のActive DirectoryまたはLDAPからインポートできます。ローカルアカウントパスワードはbcryptで保護された形式で保存され、コマンドラインパスワードはSHA-2で保護された形式で保存されます。	管理UIおよびAPIへの管理アクセスを認証します。	—
SAMLノサホオト	StorageGRIDは、Security Assertion Markup Language 2.0（SAML 2.0）標準を使用したシングルサインオン（SSO）をサポートしています。SSOが有効な場合は、 Grid Manager 、 Tenant Manager 、 Grid 管理 API 、またはテナント管理 API にアクセスするすべてのユーザを外部のアイデンティティプロバイダによって認証する必要があります。ローカルユーザは StorageGRID にサインインできません。	グリッド管理者やテナント管理者向けに、SSOや多要素認証（MFA）などのセキュリティレベルを強化できます。	NIST SP800-63

機能	機能	影響	コンプライアンス
権限のきめ細かな制御	グリッド管理者は、ロールに権限を割り当てたり、管理ユーザグループにロールを割り当てたりできます。これにより、管理クライアントが管理UIとAPIの両方を使用して実行できるタスクを適用できます。	Grid管理者が管理者ユーザと管理者グループのアクセス制御を管理できるようにします。	—
分散監査ログ	StorageGRIDは、組み込みの分散監査ログインフラを提供し、最大16のサイトにまたがる数百のノードに拡張できます。StorageGRIDソフトウェアノードは監査メッセージを生成します。このメッセージは冗長な監査リレーシステムを介して送信され、最終的に1つ以上の監査ログリポジトリにキャプチャされます。監査メッセージには、クライアントが開始したS3 API処理、ILM別のオブジェクトライフサイクルイベント、バックグラウンドのオブジェクト健全性チェック、管理UIまたはAPIからの設定変更など、オブジェクトレベルのきめ細かなイベントが記録されます。 監査ログは syslog によってエクスポートできるため、Splunk や ELK などのツールで監査メッセージをマイニングできます。監査メッセージには次の 4 つの種類があります。 • システム監査メッセージ • オブジェクトストレージ監査メッセージ • HTTPプロトコル監査メッセージ • 管理監査メッセージ 監査ログは、長期保存とアプリケーション アクセスのために S3 バケットに保存できます。	Grid管理者は、実績と拡張性に優れた監査サービスを利用して、さまざまな目的の監査データをマイニングできます。その目的には、トラブルシューティング、SLAパフォーマンスの監査、クライアントデータアクセスAPI処理、管理設定の変更などがあります。	—

機能	機能	影響	コンプライアンス
システム監査	システム監査メッセージには、グリッドノードの状態、破損オブジェクトの検出、ILMルールで指定されたすべての場所でコミットされたオブジェクト、システム全体のメンテナンスタスク（グリッドタスク）の進捗状況など、システム関連のイベントが記録されます。	システムの問題のトラブルシューティングを支援し、オブジェクトがSLAに従って格納されていることを証明します。SLAはStorageGRIDのILMルールによって実装され、整合性が保護されます。	—
オブジェクトストレージの監査	オブジェクトストレージ監査メッセージには、オブジェクトAPIトランザクションとライフサイクル関連のイベントがキャプチャされます。これらのイベントには、オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、および検証が含まれます。	システム内のデータの進捗状況と、StorageGRID ILMとして指定されたSLAが提供されているかどうかをお客様が監査できるようにします。	—
HTTPプロトコルの監査	HTTPプロトコル監査メッセージには、クライアントアプリケーションとStorageGRIDノードに関連するHTTPプロトコルのやり取りがキャプチャされます。さらに、特定のHTTP要求ヘッダー（X-Forwarded-Forやユーザメタデータ[x-amz-meta-*]など）を監査に取り込むこともできます。	クライアントとStorageGRIDの間のデータアクセスAPI処理を監査し、個 々 のユーザアカウントとアクセスキーまでのアクションをトレースできるようにします。ユーザメタデータを監査に記録し、SplunkやELKなどのログマイニングツールを使用してオブジェクトメタデータで検索することもできます。	—
管理監査	管理監査メッセージには、管理UI（Grid管理インターフェイス）またはAPIへの管理ユーザ要求が記録されます。API に対する GET または HEAD 以外のすべての要求は、応答に加えて要求のユーザ名、 IP 、およびタイプをログに記録します。	グリッド管理者は、どのユーザがどのソースIPから、どのデスティネーションIPから何時に行ったシステム設定変更の記録を作成できるようになります。	—
管理UIおよびAPIアクセスでのTLS 1.3のサポート	TLSは、管理クライアントとStorageGRID管理ノードの間の通信用にハンドシェイクプロトコルを確立します。	管理クライアントとStorageGRIDが相互に識別および認証し、機密性とデータ整合性を維持して通信できるようにします。	—

機能	機能	影響	コンプライアンス
SNMPv3によるStorageGRID監視	SNMPv3は、プライバシーのために強力な認証とデータ暗号化の両方を提供することでセキュリティを提供します。v3では、プロトコルデータユニットは暗号化プロトコルにCBC-DESを使用して暗号化されます。 プロトコルデータユニットを送信したユーザ認証は、HMAC-SHAまたはHMAC-MD5認証プロトコルによって提供されます。 SNMPv2とv1は引き続きサポートされます。	管理ノードでSNMPエージェントを有効にすることで、グリッド管理者がStorageGRIDシステムを監視できるようにします。	—
Prometheus指標エクスポート用のクライアント証明書	グリッド管理者は、クライアント証明書をアップロードまたは生成して、StorageGRID Prometheusデータベースへのセキュアな認証されたアクセスを提供できます。	グリッド管理者は、クライアント証明書を使用して、Grafanaなどのアプリケーションを使用してStorageGRIDを外部から監視できます。	—

プラットフォームのセキュリティ機能

StorageGRIDのプラットフォームセキュリティ機能について説明します。

機能	機能	影響	コンプライアンス
内部公開鍵インフラ（PKI）、ノード証明書、TLS	StorageGRIDは、内部PKIおよびノード証明書を使用して、ノード間通信を認証および暗号化します。ノード間通信はTLSで保護されます。	特にマルチサイト展開では、LANまたはWAN経由のシステムトラフィックの保護に役立ちます。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
ノードのファイアウォール	StorageGRIDは、IPテーブルとファイアウォールルールを自動的に設定して、送受信ネットワークトラフィックを制御し、未使用のポートを閉じます。	StorageGRIDシステム、データ、メタデータを未承諾のネットワークトラフィックから保護します。	—
OSのセキュリティ強化	StorageGRID物理アプライアンスと仮想ノードのベースオペレーティングシステムが強化され、関連のないソフトウェアパッケージが削除されます。	潜在的な攻撃対象領域を最小限に抑えます。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）

機能	機能	影響	コンプライアンス
プラットフォームとソフトウェアの定期的な更新	StorageGRIDでは、オペレーティングシステム、アプリケーションバイナリ、ソフトウェアアップデートなどのソフトウェアリリースを定期的に提供しています。	StorageGRIDシステムを最新のソフトウェアとアプリケーションバイナリで更新するのに役立ちます。	—
Secure Shell（SSH）を使用したルートログインの無効化	SSH経由のrootログインは、すべてのStorageGRIDノードで無効になっています。SSHアクセスでは証明書認証が使用されます。	rootログインの潜在的なリモートパスワードクラックからお客様を保護するのに役立ちます。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
自動時刻同期	StorageGRIDは、各ノードのシステムクロックを複数の外部タイムネットワークタイムプロトコル（NTP）サーバと自動的に同期します。Stratum 3以降のNTPサーバが少なくとも4台必要です。	すべてのノードで時刻参照が同じになるようにします。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
クライアント、管理者、内部のグリッドトラフィック用に別々 のネットワークを使用	StorageGRIDソフトウェアノードとハードウェアアプライアンスは、複数の仮想ネットワークインターフェイスと物理ネットワークインターフェイスをサポートしているため、クライアントトラフィック、管理トラフィック、内部グリッドトラフィックを別 々 のネットワーク経由で分離できます。	グリッド管理者は、内部と外部のネットワークトラフィックを分離して、SLAの異なるネットワーク経由でトラフィックを配信できます。	—
複数の仮想LAN（VLAN）インターフェイス	StorageGRIDでは、StorageGRIDクライアントネットワークおよびグリッドネットワークにVLANインターフェイスを設定できます。	グリッド管理者はアプリケーショントラフィックをパーティショニングして分離し、セキュリティ、柔軟性、パフォーマンスを確保できます。	
Untrusted Client Networkの略	信頼されていないクライアントネットワークインターフェイスは、ロードバランサエンドポイントとして明示的に設定されたポートでのみインバウンド接続を受け入れます。	信頼されていないネットワークに公開されているインターフェイスのセキュリティが確保されます。	—

機能	機能	影響	コンプライアンス
設定可能なファイアウォール	管理、グリッド、クライアントの各ネットワークの開いているポートと閉じているポートを管理します。	グリッド管理者がポートでのアクセスを制御し、ポートへの承認済みデバイスアクセスを管理できるようにします。	
SSH動作の強化	インストール前にデフォルトでSSH を無効にします。デフォルト状態では、SSH アクセスはリンクローカル管理ポートアドレスでのみ有効になります。管理者およびルート ユーザーのパスワードは、アプライアンスのコンピューティング コントローラーのシリアル番号に設定されます。ログインはシリアル コンソールとグラフィカル コンソール (BMC KVM) でのみ許可されます。すべてのネットワーク ポート上の SSH が無効になっています。	ネットワーク アクセス保護を強化します。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）
ノード暗号化	新しいKMSホストサーバ暗号化機能の一部として、StorageGRIDアプライアンスインストーラに新しいノード暗号化設定が追加されます。	この設定は、アプライアンスの設置のハードウェア構成段階で有効にする必要があります。	SECルール17a-4（f）CTFC 1.31（c）-（d）（FINRA）ルール4511（c）

クラウドとの統合

StorageGRIDとクラウドサービスの統合方法をご紹介します。

機能	機能	影響
通知ベースのウィルススキャン	StorageGRIDプラットフォームサービスでは、イベント通知がサポートされます。外部のクラウドコンピューティングサービスでイベント通知を使用すると、データに対してウィルススキャンワークフローをトリガーできます。	テナント管理者は、外部のクラウドコンピューティングサービスを使用してデータのウィルススキャンをトリガーできます。

TR-4921：『Ransomware Defense』

StorageGRID S3オブジェクトをランサムウェアから保護

ランサムウェア攻撃と、StorageGRIDのセキュリティに関するベストプラクティスでデータを保護する方法をご紹介します。

ランサムウェア攻撃が増加しています。このドキュメントでは、StorageGRIDでオブジェクトデータを保護する方法について、いくつかの推奨事項を示します。

ランサムウェアは今日、データセンターに常に存在する危険です。ランサムウェアは、データを暗号化し、データに依存するユーザやアプリケーションがデータを使用できないようにするように設計されています。保護は、強化されたネットワーキングと強固なユーザーセキュリティプラクティスの通常の防御から始まります。そして、データアクセスセキュリティプラクティスに従う必要があります。

ランサムウェアは、今日の最大級のセキュリティ脅威の1つです。NetApp StorageGRIDチームは、これらの脅威に先手を打つためにお客様と協力しています。オブジェクトロックとバージョン管理を使用すると、不要な変更から保護し、悪意のある攻撃からリカバリできます。データセキュリティは多層的な取り組みであり、オブジェクトストレージはデータセンターの一部にすぎません。

StorageGRIDのベストプラクティス

StorageGRIDのセキュリティのベストプラクティスとして、管理アクセスとオブジェクトアクセスの両方に、署名済み証明書を使用したHTTPSの使用を推奨します。アプリケーションと個人用に専用のユーザアカウントを作成し、アプリケーションアクセスやユーザデータアクセスにテナントrootアカウントを使用しないでください。言い換えれば、最小特権の原則に従ってください。IDおよびアクセス管理（IAM）ポリシーが定義されたセキュリティグループを使用して、ユーザ権限を管理し、アプリケーションおよびユーザに固有のアカウントにアクセスします。これらの対策を実施した場合でも、データを確実に保護する必要があります。Simple Storage Service（S3）では、オブジェクトが暗号化するように変更されると、元のオブジェクトが上書きされます。

防御方法

S3 APIの主なランサムウェア対策メカニズムは、オブジェクトロックの実装です。すべてのアプリケーションがオブジェクトロックと互換性があるわけではありません。そのため、このレポートでは、バージョン管理が有効な別のバケットへのレプリケーションと、IAMポリシーによるバージョン管理の2つのオプションについて説明します。

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/[]
- NetApp StorageGRIDイネーブルメント https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp製品ドキュメント https://www.netapp.com/support-and-training/documentation/

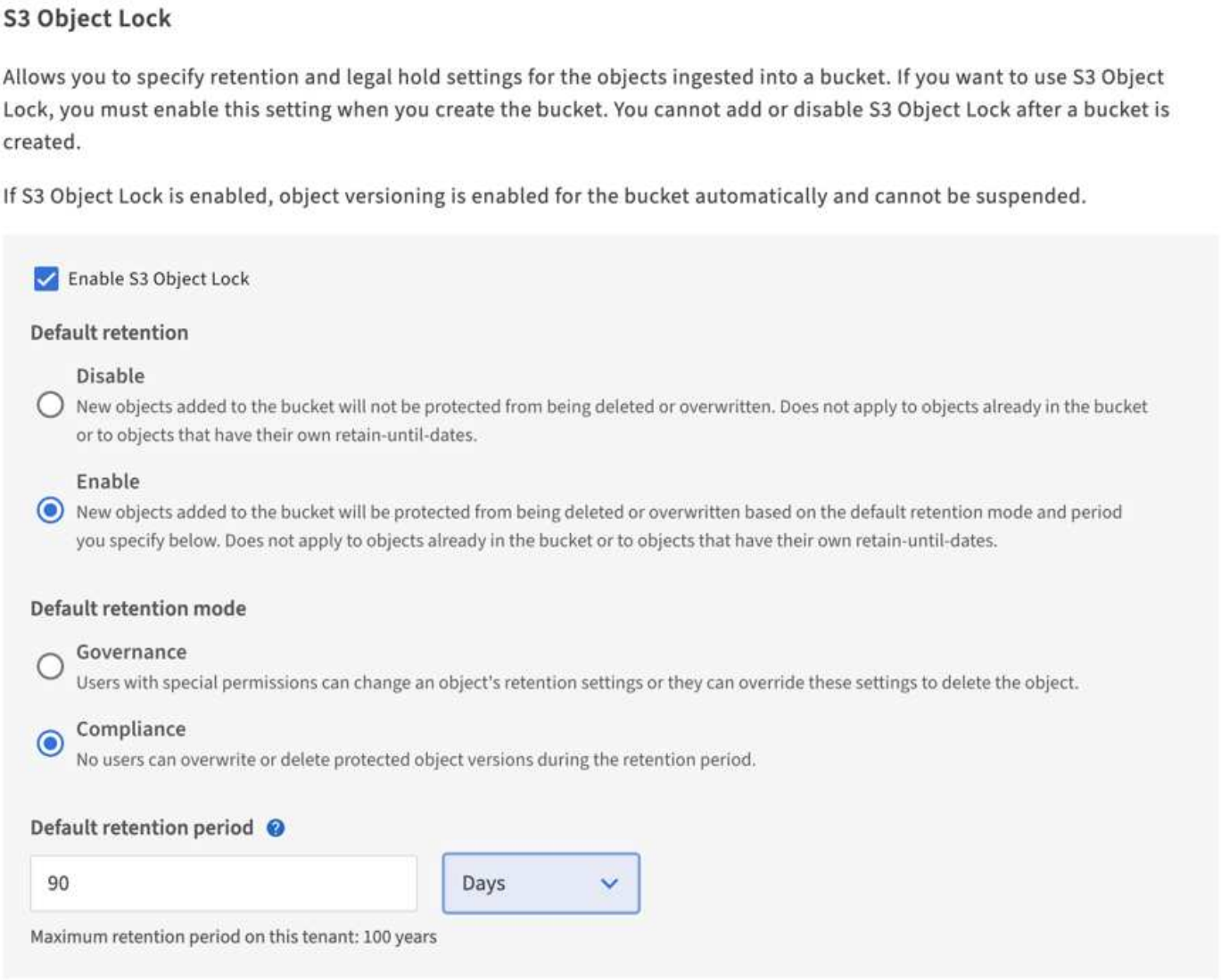
オブジェクトロックを使用したランサムウェア対策

StorageGRIDのオブジェクトロックがWORMモデルを提供してデータの削除や上書きを防止する方法や、それが規制要件をどのように満たしているかをご紹介します。

オブジェクトロックは、オブジェクトが削除または上書きされないようにするWORMモデルを提供します。StorageGRIDではオブジェクトロックを実装すること "Cohasset評価済み" で、規制要件への対応を支援し、オブジェクト保持のリーガルホールド、コンプライアンスモード、ガバナンスモード、およびデフォルトのバケット保持ポリシーをサポートします。オブジェクトロックは、バケットの作成およびバージョン管理の一環として有効にする必要があります。オブジェクトの特定のバージョンがロックされ'バージョンIDが定義されていない場合は'オブジェクトの現在のバージョンに保持が適用されます現在のバージョンに保持が設定

されていて、オブジェクトを削除、変更、または上書きしようとすると、削除マーカーまたはオブジェクトの新しいリビジョンを現在のバージョンとして使用して新しいバージョンが作成されます。 ロックされたバージョンは、最新でないバージョンとして保持されます。まだ互換性がないアプリケーションでは、オブジェクトロックとバケットに配置されたデフォルトの保持設定を使用できます。設定の定義が完了すると、バケットに追加される新しいオブジェクトごとにオブジェクト保持期間が適用されます。これは、保持期間が経過する前にオブジェクトを削除または上書きしないようにアプリケーションが設定されているかぎり機能します。

テナント管理 UI でバケットを作成するときに、オブジェクト ロックを有効にし、デフォルトの保持モードと保持期間を設定できます。これを構成すると、そのバケットに取り込まれるすべてのオブジェクトに対して最小オブジェクト ロック保持が設定されます。



オブジェクトロックAPIの使用例を次に示します。

オブジェクトロックリーガルホールドは、オブジェクトに適用される単純なオン/オフステータスです。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

リーガルホールドステータスを設定しても値は返されないため、GET処理で確認できます。

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

リーガルホールドをオフにするには、オフステータスを適用します。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

オブジェクトの保持期間の設定には、タイムスタンプまで保持が適用されます。

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

繰り返しになりますが、成功した場合も戻り値はありません。そのため、GET呼び出しを使用して保持ステータスを同様に確認できます。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

オブジェクトロックが有効なバケットにデフォルトの保持期間を設定すると、保持期間（日と年）が使用されます。

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

これらの処理のほとんどと同様に、成功した場合も応答が返されないため、設定を検証するGETを実行できます。

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

次に、保持設定を適用した状態でバケットにオブジェクトを配置します。

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

PUT処理で応答が返されます。

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

保持オブジェクトでは、上記の例でバケットに設定されている保持期間がオブジェクトの保持タイムスタンプに変換されます。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

レプリケートされたバケットを使用したバージョン管理によるランサムウェア対策

StorageGRID CloudMirrorを使用してセカンダリバケットにオブジェクトをレプリケートする方法について説明します。

すべてのアプリケーションとワークロードがオブジェクトロックと互換性があるわけではありません。もう1つの方法は、同じグリッド内（アクセスが制限された別のテナントを推奨）、またはStorageGRIDプラットフォームサービスCloudMirrorを使用する他のS3エンドポイントのいずれかのセカンダリバケットにオブジェクトをレプリケートする方法です。

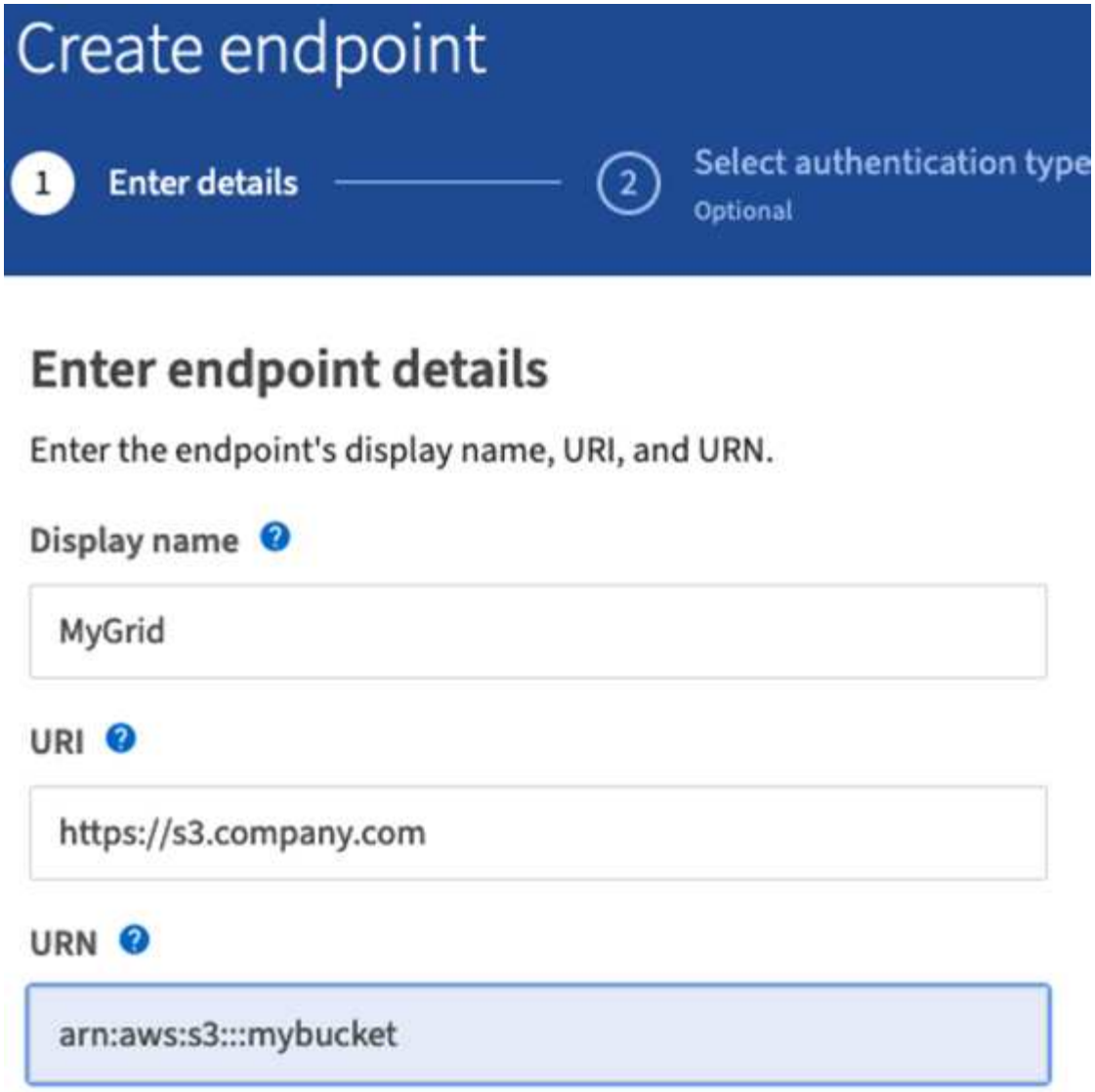
StorageGRID CloudMirrorはStorageGRIDのコンポーネントです。定義されたデスティネーションにバケットのオブジェクトがソースバケットに取り込まれたときにレプリケートされ、削除はレプリケートされません。CloudMirrorはStorageGRIDに統合されたコンポーネントであるため、S3 APIベースの攻撃によって無効にしたり操作したりすることはできません。このレプリケートされたバケットは、バージョン管理を有効にして設定できます。このシナリオでは、レプリケートされたバケットの古いバージョンを破棄しても安全な自動クリーンアップが必要です。そのためには、StorageGRID ILMポリシーエンジンを使用できます。最新でない時間に基づいてオブジェクトの配置を管理するルールを作成し、攻撃を特定してリカバリします。

このアプローチの欠点は、バケットの完全な2つ目のコピーを作成し、オブジェクトの複数のバージョンをしばらくの間保持することで、より多くのストレージを消費することです。また、プライマリバケットから意図的に削除されたオブジェクトは、レプリケートされたバケットから手動で削除する必要があります。NetApp CloudSyncなど、製品以外にも、同様のソリューションで削除をレプリケートできるレプリケーションオプションがあります。セカンダリバケットのバージョン管理が有効でオブジェクトロックが有効でない場合のもう1つの欠点は、セカンダリの場所に損傷を与える可能性がある特権アカウントが多数存在することです。長所は、そのエンドポイントまたはテナントバケットに対して一意のアカウントである必要があり、プライマリロケーションのアカウントへのアクセスやプライマリロケーションのアカウントへのアクセスが侵害されない可能性があることです。

ソースバケットとデスティネーションバケットが作成され、デスティネーションでバージョン管理が設定されたら、次のようにレプリケーションを設定して有効にすることができます。

手順

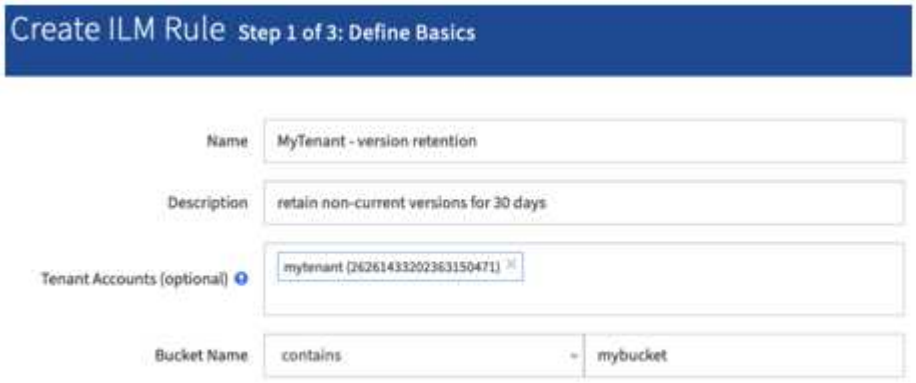
1. CloudMirrorを設定するには、S3デスティネーション用のプラットフォームサービスエンドポイントを作成します。

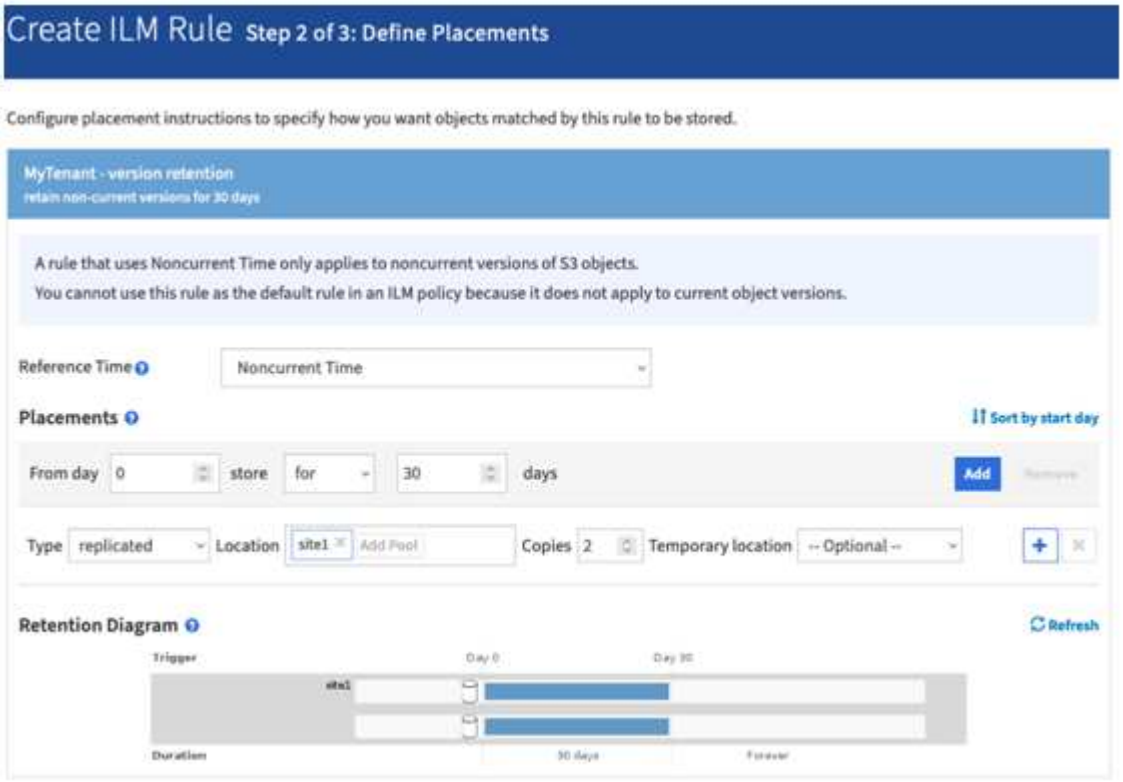


2. ソースバケットで、設定されているエンドポイントを使用するようにレプリケーションを設定します。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. ストレージの配置とバージョンのストレージ期間を管理するILMルールを作成します。この例では、格納するオブジェクトの最新でないバージョンが設定されています。





サイト1にコピーが2つあり、30日間保持されます。また、ILMルールの取り込み時間をソースバケットのストレージ期間に一致させるための参照時間として使用することに基づいて、オブジェクトの現在のバージョンのルールを設定します。オブジェクトバージョンのストレージ配置は、イレイジャーコーディングまたはレプリケートが可能です。

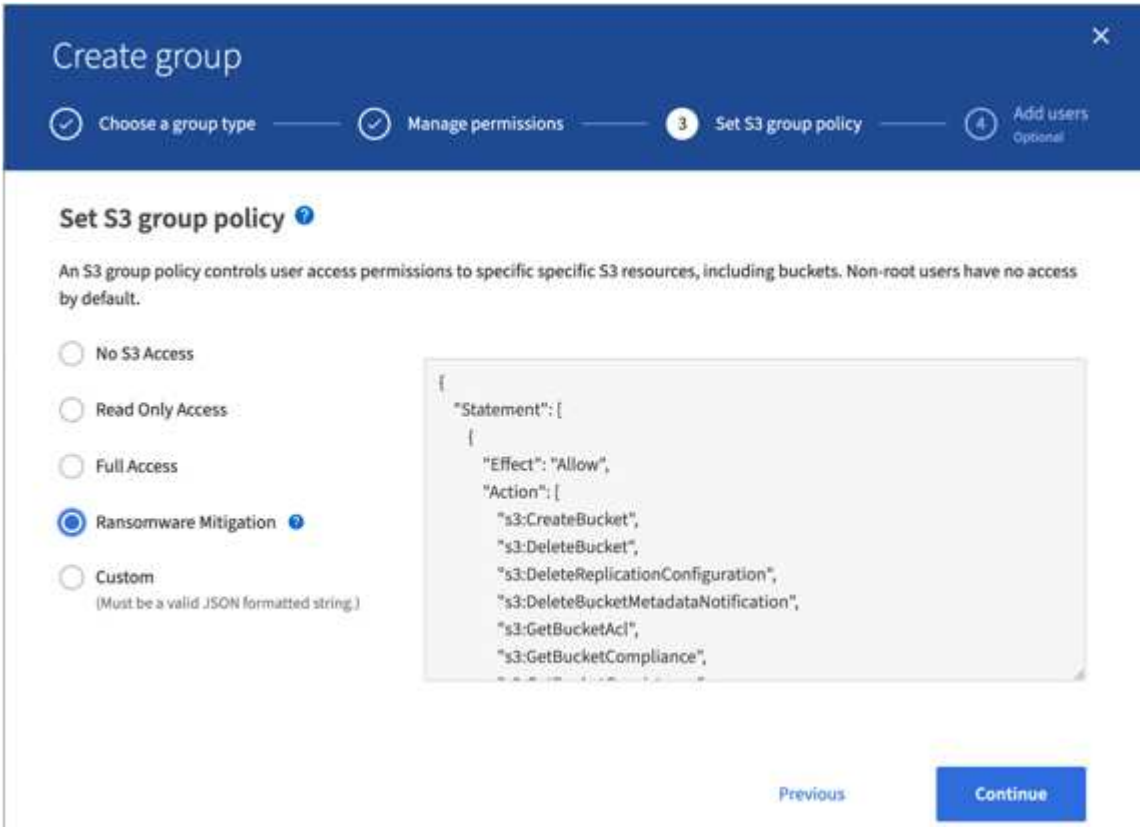
保護**IAM**ポリシーを使用したバージョン管理を使用したランサムウェア防御

バケットのバージョン管理を有効にし、StorageGRIDのユーザセキュリティグループにIAMポリシーを実装して、データを保護する方法について説明します。

オブジェクトロックやレプリケーションを使用せずにデータを保護するには、バケットでバージョン管理を有効にし、ユーザセキュリティグループにIAMポリシーを実装して、ユーザによるオブジェクトのバージョン管理を制限します。攻撃が発生した場合、データの新しい不正なバージョンが現在のバージョンとして作成され、最新でないバージョンが安全なクリーンデータになります。データにアクセスするために侵害されたアカ

ウントは、削除したり、最新でないバージョンを変更したりすることができず、以降のリストア処理のために保護されています。前のシナリオと同様に、最新でないバージョンの保持期間を選択してILMルールによって管理されます。欠点は、不正なアクター攻撃のために特権アカウントが存在する可能性がまだあることですが、すべてのアプリケーションサービスアカウントとユーザーは、より制限的なアクセスを設定する必要があります。制限付きグループポリシーでは、ユーザまたはアプリケーションに許可する各アクションを明示的に許可し、許可しないアクションを明示的に拒否する必要があります。NetAppでは、今後新しいアクションが導入される可能性があり、許可するか拒否するかを制御する必要があるため、ワイルドカードAllowの使用は推奨されていません。このソリューションでは、ユーザによる変更やプログラムによる変更からバケットとオブジェクトのバージョン設定を保護するために、拒否リストにDeleteObjectVersion、PutBucketPolicy、DeleteBucketPolicy、PutLifecycleConfiguration、およびPutBucketVersioningを含める必要があります。

StorageGRIDでは、S3 グループ ポリシー オプション「ランサムウェア軽減」により、このソリューションの実装が容易になります。テナントにユーザー グループを作成するときに、グループ権限を選択すると、このオプション ポリシーが表示されます。



次に、グループポリシーの内容を示します。このグループポリシーには、明示的に許可された処理と、最低限必要な処理が含まれています。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
```

```
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

ランサムウェアの調査と修復

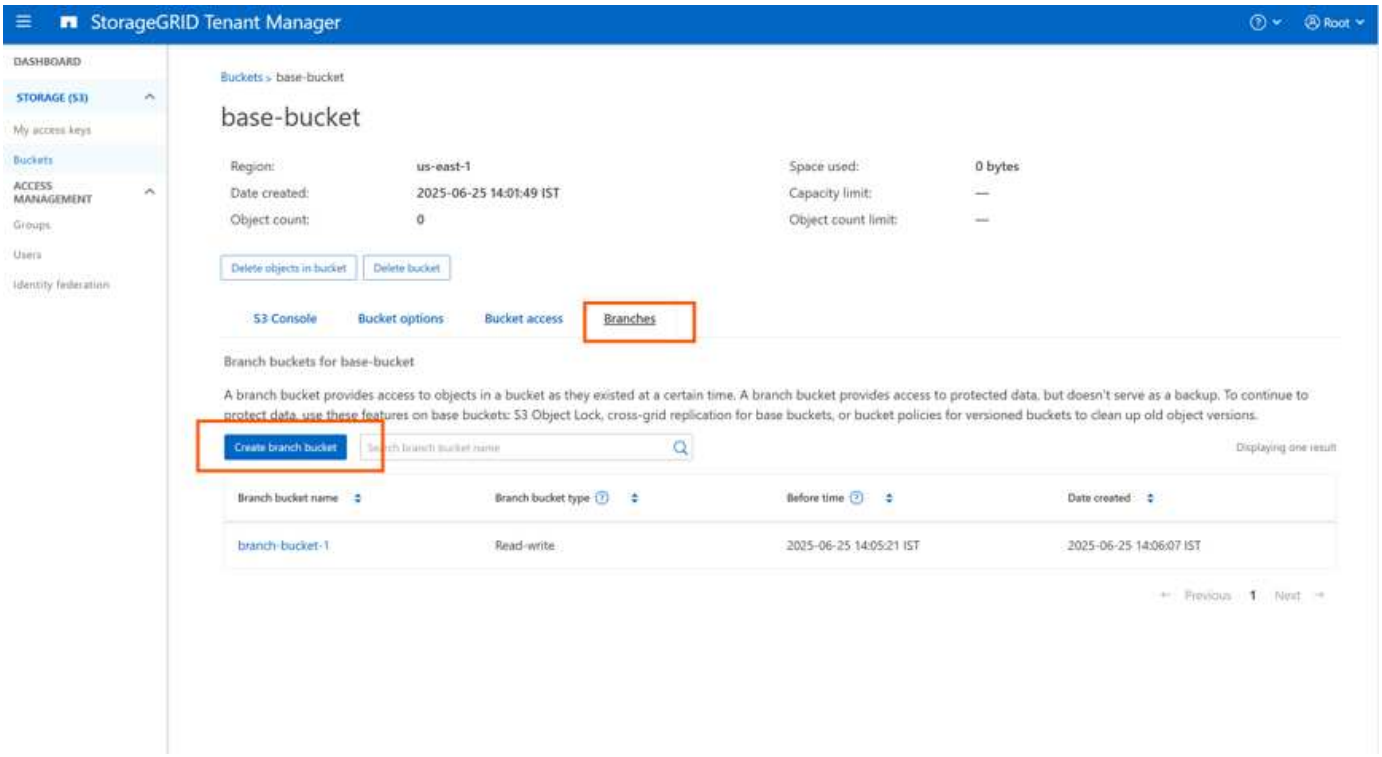
StorageGRIDを使用して、ランサムウェア攻撃の可能性があった場合にバケットを調査して修復する方法を学びます。

StorageGRID 12.0 では、ランサムウェア防御におけるバージョン管理の有用性を拡張するために、新しいブランチ バケット機能が追加されました。ブランチ バケットは、バケット内にまだ存在するオブジェクトに対して、特定の時点におけるそのオブジェクトへのアクセスを提供します。ブランチ バケットは、バージョン管理が有効なベース バケットに対してのみ作成できます。

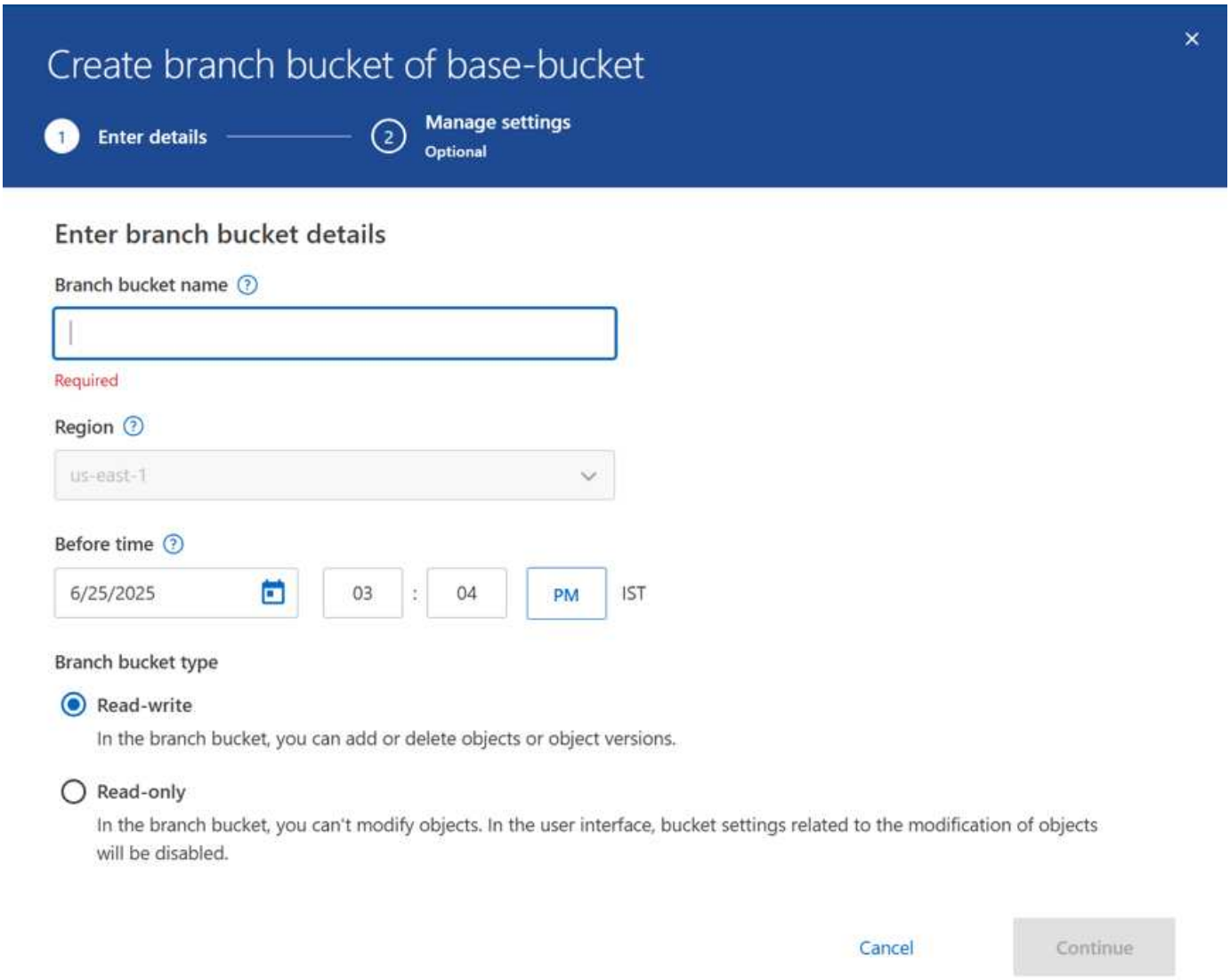
つまり、ランサムウェア攻撃が発生した疑いがある場合は、最初の攻撃時以前に存在していたすべてのオブジェクトとバージョンを含む読み取り/書き込みまたは読み取り専用のブランチ バケットを作成できます。このブランチ バケットを使用してベース バケットの内容と比較し、どのオブジェクトが変更されたか、その変更が攻撃の一部であったかどうかを判断できます。ブランチ バケットを使用すると、攻撃を調査しながらクリーンなブランチを使用してクライアント操作を続行することもできます。

ブランチバケットの作成

- ブランチ バケットを作成するには、ベース バケットの詳細ページと [ブランチ] タブに移動します。



- [ブランチ バケットの作成] ボタンをクリックすると、ベース バケットに関連付けられたリージョンの詳細が事前に入力されたポップアップが開きます。
- 時間の前にブランチ バケット名を指定し、作成するブランチ バケットのタイプを選択します。



TR-4765：『Monitor StorageGRID』

StorageGRID監視の概要

Splunkなどの外部アプリケーションを使用してStorageGRIDシステムを監視する方法について説明します。

NetApp StorageGRIDオブジェクトベースストレージを効果的に監視することで、管理者は緊急の問題に迅速に対応し、リソースをプロアクティブに追加してワークロードの増大に対処できます。このレポートでは、主要な指標を監視する方法と、外部の監視アプリケーションを活用する方法について、一般的なガイダンスを提供します。これは、既存の『Monitoring and Troubleshooting Guide』を補足することを目的としています。

通常、NetApp StorageGRID環境は、分散型のフォールトトレランスに優れたオブジェクトストレージシステムを構築するために複数のサイトと多数のノードで構成されます。StorageGRIDのような分散型で耐障害性に優れたストレージシステムでは、エラー状態が発生してもグリッドは正常に動作し続けます。管理者にとっての課題は、エラー状態（ノードの停止など）ですぐに対処する必要のある問題が発生し、分析する必要のある情報が発生するしきい値を把握することです。StorageGRIDが提供するデータを分析することで、ワークロードを把握し、リソースをいつ追加すべきかなど、十分な情報に基づく意思決定を行うことができます。

StorageGRIDは、監視の主題を深く掘り下げる優れたドキュメントを提供します。本レポートは、に関する十分な知識があり、StorageGRIDに関するドキュメントを確認済みであることを前提としています。この情報を繰り返すのではなく、このガイド全体を通して製品ドキュメントを参照しています。StorageGRID製品マニュアルは、オンラインでPDF形式で入手できます。

本ドキュメントの目的は、製品ドキュメントを補完し、Splunkなどの外部アプリケーションを使用してStorageGRIDシステムを監視する方法について説明することです。

データソース

NetApp StorageGRIDを正常に監視するには、StorageGRIDシステムの健全性と運用に関するデータを収集する場所を把握することが重要です。

- * Web UIとダッシュボード*StorageGRIDグリッドマネージャには、管理者が論理プレゼンテーションで確認する必要がある情報の最上位レベルのビューが表示されます。管理者は、トラブルシューティングやログ収集のためにサービスレベル情報をさらに掘り下げることもできます。
- *監査ログ。*StorageGRIDは、PUT、GET、DELETEなどのテナント操作の詳細な監査ログを保持します。また、オブジェクトの取り込みからデータ管理ルールの適用までのライフサイクルをトレースすることもできます。
- *メトリクスAPI。*StorageGRID GMIの基盤となるのは、APIベースのUIであるため、オープンAPIです。このアプローチでは、外部の監視ツールや分析ツールを使用してデータを抽出できます。

追加情報の参照先

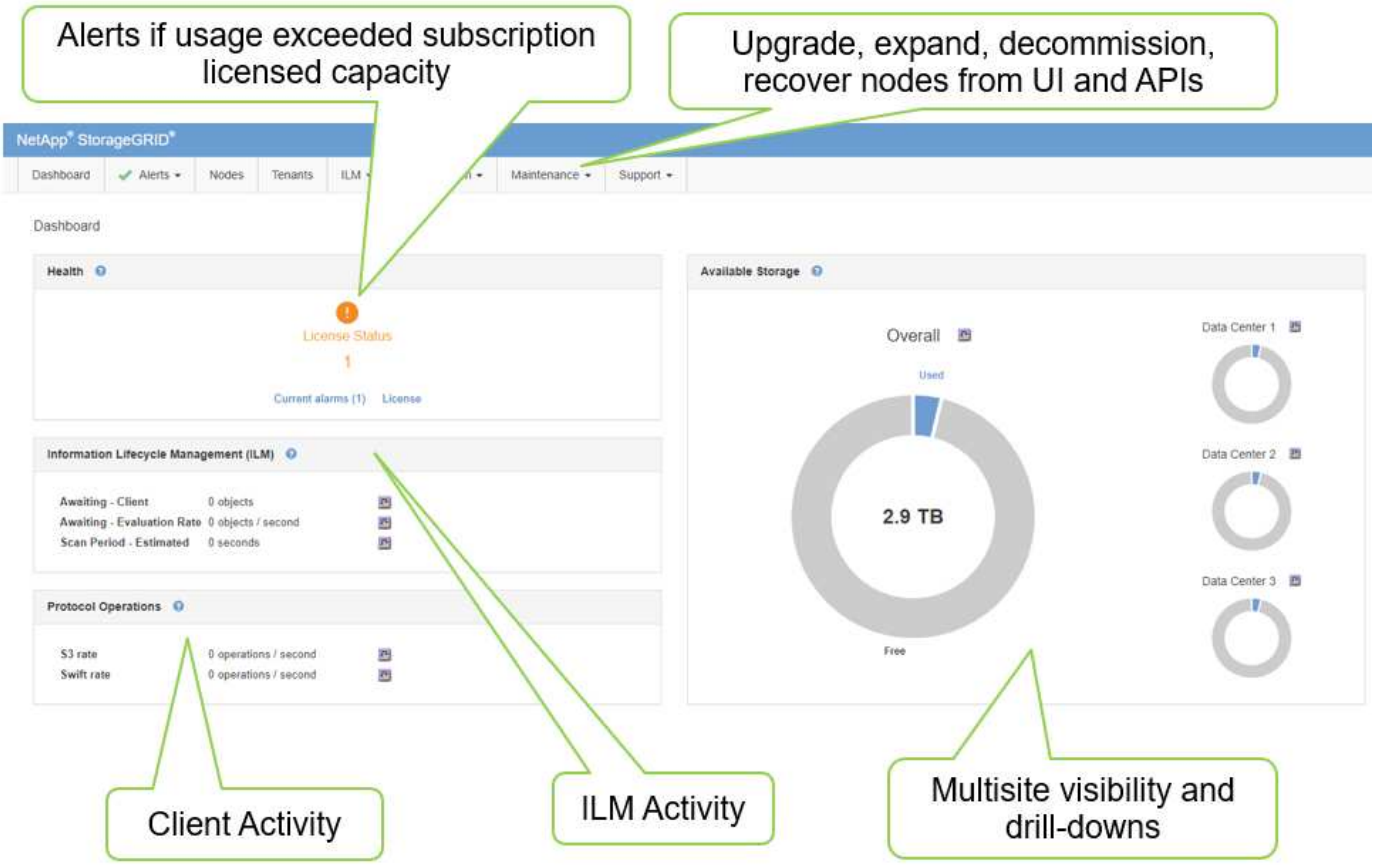
このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- 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/
- NetApp製品ドキュメント https://www.netapp.com/support-and-training/documentation/
- Splunk向けNetApp StorageGRIDアプリケーション https://splunkbase.splunk.com/app/3898/#/details

GMIダッシュボードを使用して**StorageGRID**を監視する

StorageGRIDのグリッド管理インターフェイス（GMI）ダッシュボードでは、StorageGRIDインフラを一元的に表示して、グリッド全体の健全性、パフォーマンス、容量を監視できます。

GMIダッシュボードを使用して、グリッドの各コアコンポーネントを確認します。



定期的に監視する必要がある情報

このテクニカルレポートの以前のバージョンでは、定期的に確認する指標と傾向が表示されていました。この情報がに含まれるようになりまし "監視およびトラブルシューティングガイド"た。

ストレージの監視

このテクニカルレポートの以前のバージョンでは、オブジェクトストレージスペース、メタデータスペース、ネットワークリソースなどの重要な指標の監視場所が記載されていました。この情報がに含まれるようになりまし "監視およびトラブルシューティングガイド"た。

アラートを使用したStorageGRIDの監視

StorageGRIDのアラートシステムを使用して、問題の監視、カスタムアラートの管理、SNMPやEメールを使用したアラート通知の拡張を行う方法について説明します。

アラートは、StorageGRIDシステム内のさまざまなイベントや状態を監視するための重要な情報を提供します。

アラートシステムは、StorageGRIDシステムで発生する可能性のある問題を監視するための主要なツールとして設計されています。アラートシステムは、システム内の実行可能な問題に焦点を当て、使いやすいインターフェイスを提供します。

システムの監視とトラブルシューティングに役立つさまざまなデフォルトアラートルールを提供しています。カスタムアラートの作成、デフォルトアラートの編集または無効化、アラート通知のサイレント化により、アラートの詳細な管理を行うことができます。

アラートは、SNMPまたはEメール通知を通じて拡張することもできます。

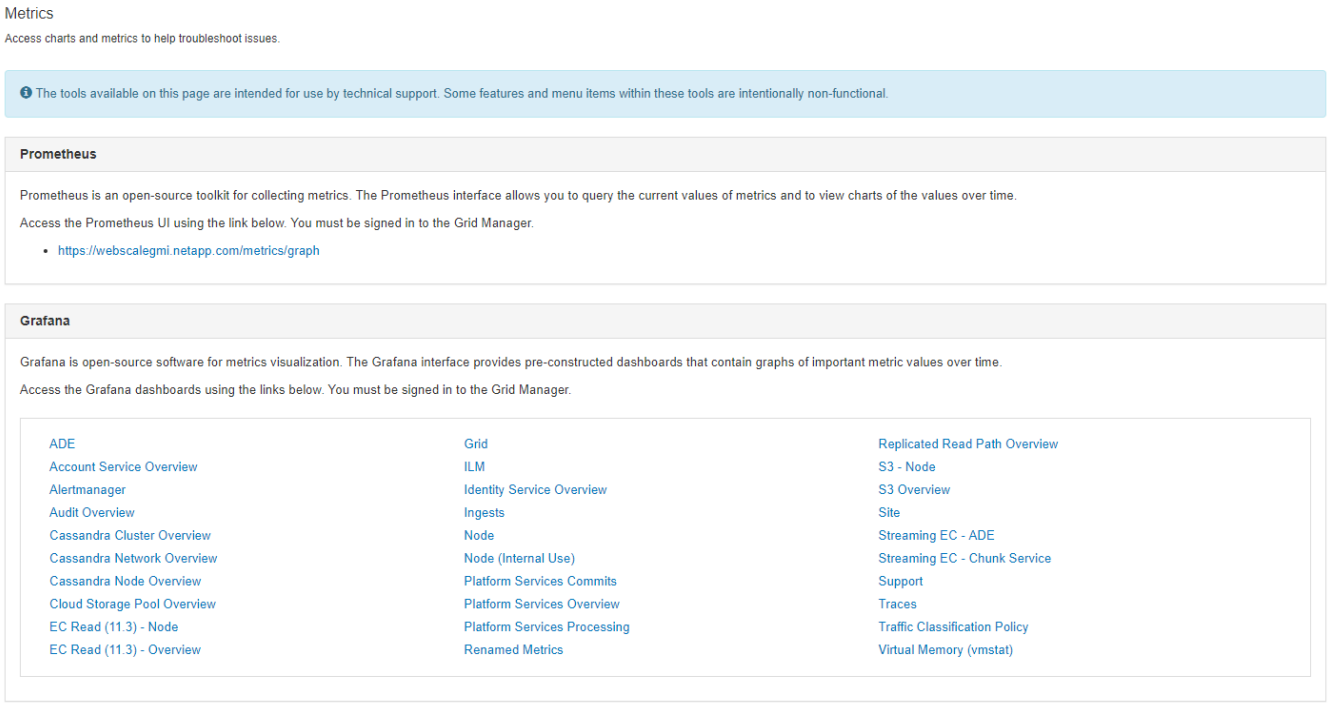
アラートの詳細については、オンラインでPDF形式のを参照してください "製品ドキュメント" 。

StorageGRIDの高度な監視

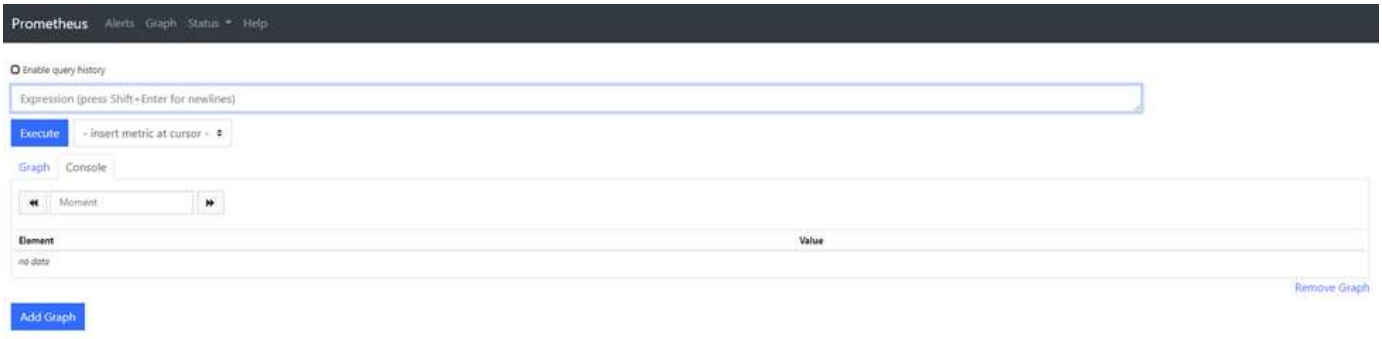
問題のトラブルシューティングに役立つ指標にアクセスしてエクスポートする方法について説明します。

Prometheusクエリを使用した指標APIの表示

Prometheusは指標を収集するためのオープンソースソフトウェアです。GMIを使用してStorageGRIDに組み込まれているPrometheusにアクセスするには、メニューの[Support][Metrics]に移動します。



または、リンクに直接移動することもできます。

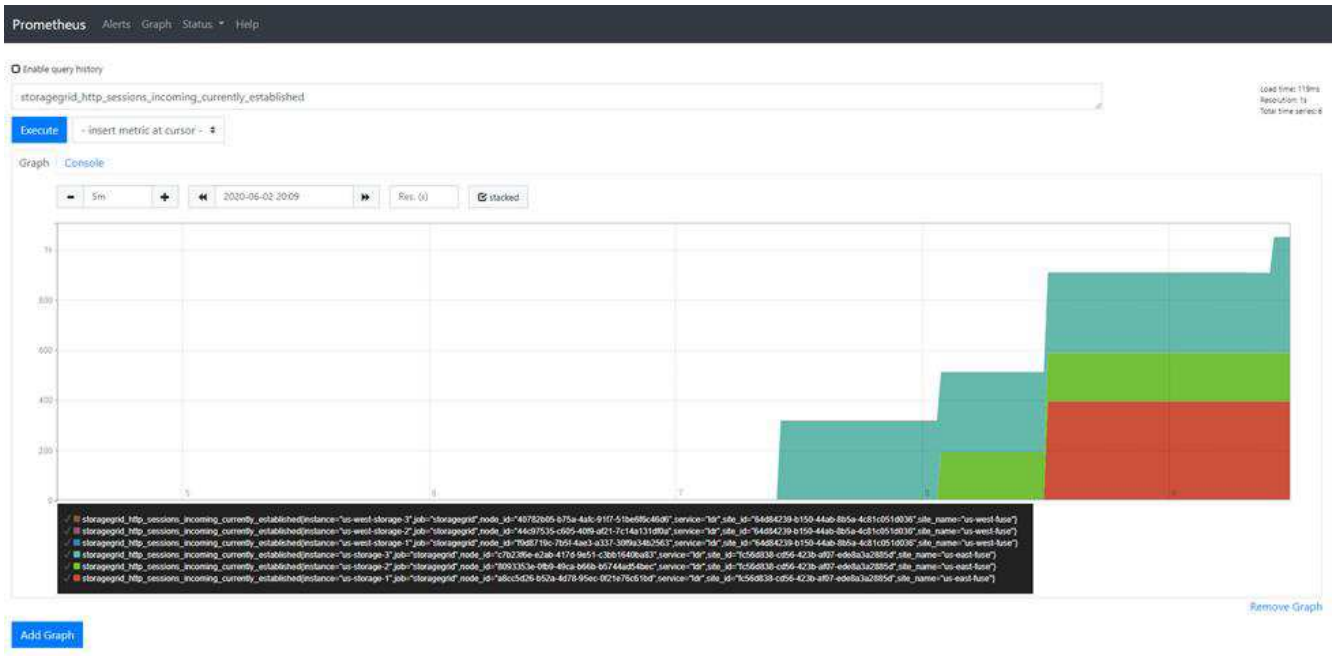


このビューからPrometheusインターフェイスにアクセスできます。そこから、利用可能な指標を検索したり、クエリを試したりすることができます。

Prometheus URLクエリを作成するには、次の手順を実行します。

手順

1. クエリテキストボックスに入力を開始します。入力すると、指標が表示されます。ここで重要なのは、StorageGRIDとNodeで始まる指標だけです。
2. 各ノードのHTTPセッションの数を確認するには、と入力し `storagegrid_http` て選択します `storagegrid_http_sessions_incoming_currently_established`。[Execute]をクリックし、グラフ形式またはコンソール形式で情報を表示します。



このURLを使用して作成したクエリとグラフは維持されません。複雑なクエリは管理ノードのリソースを消費します。NetAppでは、このビューを使用して使用可能な指標を確認することをお勧めします。

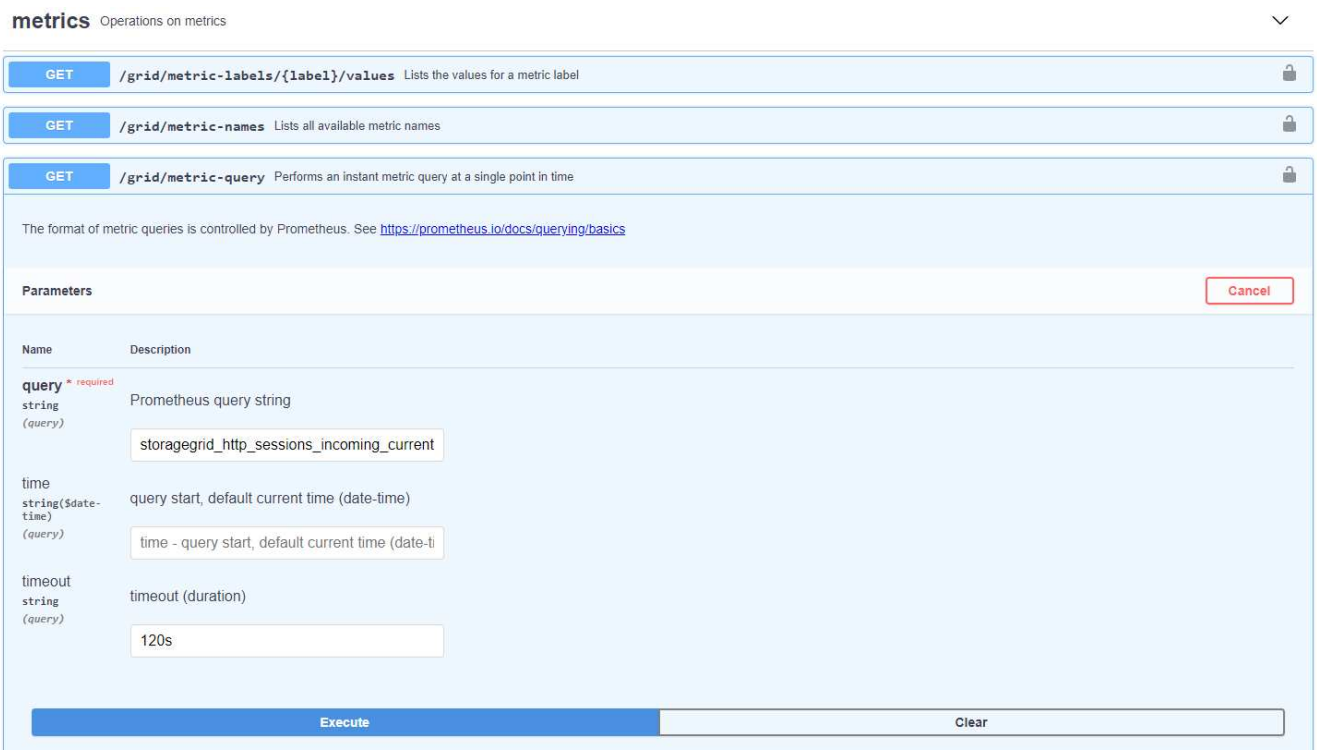
追加のポートを開く必要があるため、Prometheusインスタンスに直接接続することは推奨されません。APIを介して指標にアクセスすることは、推奨される安全な方法です。

APIを使用した指標のエクスポート

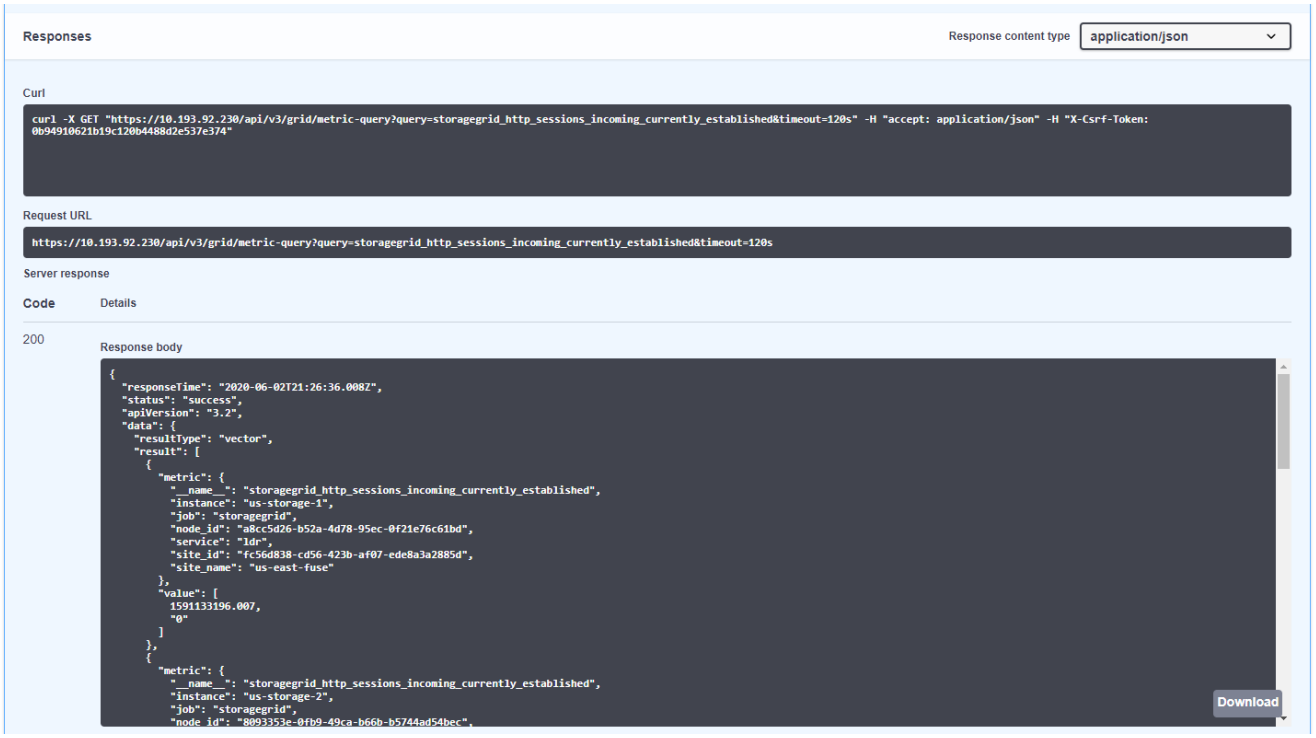
StorageGRID管理APIを使用して同じデータにアクセスすることもできます。

APIを使用して指標をエクスポートするには、次の手順を実行します。

1. GMIで、[Help][API Documentation]の順に選択します。
2. [Metrics]まで下にスクロールし、[GET /grid/metric-query]を選択します。



応答には、Prometheus URLクエリで取得できる情報と同じ情報が含まれます。各ストレージノードで現在確立されているHTTPセッションの数をもう一度確認できます。応答をJSON形式でダウンロードして読みやすくすることもできます。次の図は、Prometheusクエリ応答の例を示しています。



APIを使用する利点は、認証されたクエリを実行できることです。

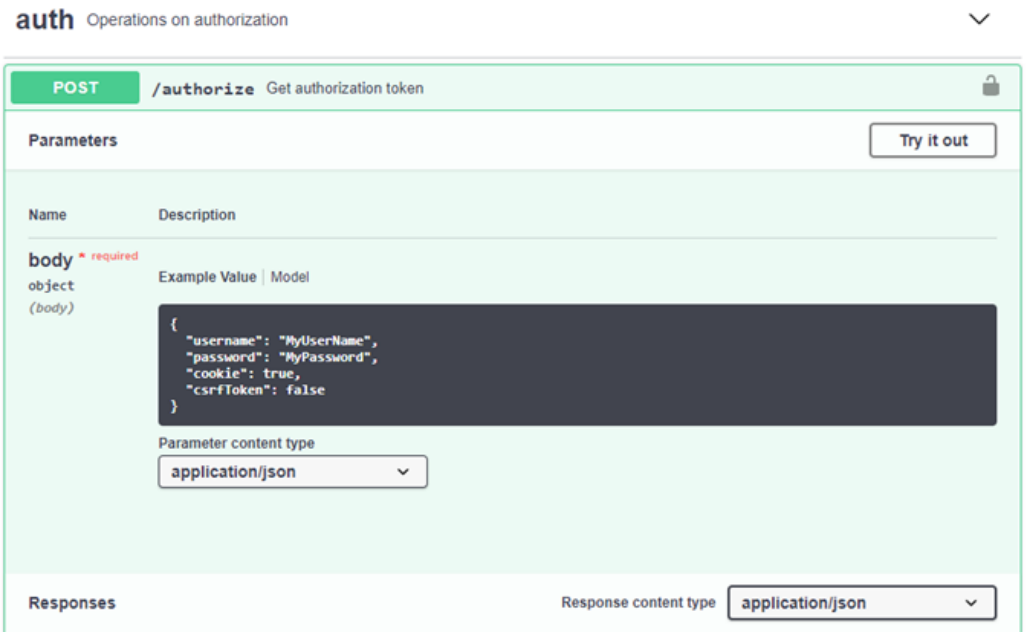
StorageGRIDでcURLを使用してメトリクスにアクセスする

cURLを使用してCLIから指標にアクセスする方法について説明します。

この操作を実行するには、最初に認証トークンを取得する必要があります。トークンを要求するには、次の手順を実行します。

手順

1. GMIで、[Help][API Documentation]の順に選択します。
2. [Auth]まで下にスクロールして、許可に関する操作を検索します。次のスクリーンショットは、POSTメソッドのパラメータを示しています。



3. [Try it out]をクリックし、GMIのユーザー名とパスワードで本文を編集します。
4. Executeをクリックします。
5. cURLセクションにあるcURLコマンドをコピーし、ターミナルウィンドウに貼り付けます。コマンドは次のようになります。

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

GMIパスワードに特殊文字が含まれている場合は、必ず\を使用して特殊文字をエスケープしてください。たとえば、置き換えます。

6. 上記のcURLコマンドを実行すると、次の例のような認証トークンが出力に表示されます。

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

これで、認証トークン文字列を使用して、cURLを介してメトリックにアクセスできるようになりました。指標にアクセスするプロセスは、セクションの手順と似てい "StorageGRIDの高度な監視"ます。ただし、デモ用として、[Metrics]カテゴリで[GET /grid/metric-labels/｛label｝/values]を選択した例を示します。

7. たとえば、次のcURLコマンドに先行する認証トークンを指定すると、StorageGRID内のサイト名が一覧表示されます。

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

cURLコマンドは、次の出力を生成します。

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

StorageGRIDのGrafanaダッシュボードを使用した指標の表示

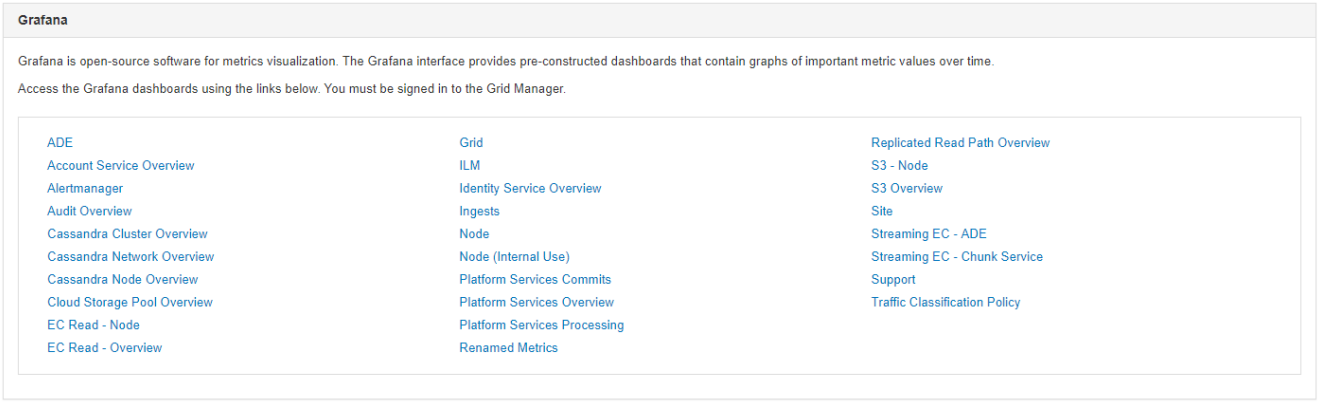
Grafanaインターフェイスを使用してStorageGRIDデータを可視化および監視する方法について説明します。

Grafanaは、メートル法を視覚化するためのオープンソースソフトウェアです。デフォルトでは、StorageGRIDシステムに関する有用で強力な情報を提供するダッシュボードが事前に構築されています。

事前構築されたダッシュボードは、監視だけでなく、問題のトラブルシューティングにも役立ちます。一部はテクニカルサポートが使用することを目的としています。たとえば、ストレージノードの指標を表示するには、次の手順を実行します。

手順

1. GMIのメニューから、[Support][Metrics]を選択します。
2. [Grafana]セクションで、[Node]ダッシュボードを選択します。



3. Grafanaで、指標を表示するノードにホストを設定します。この例では、ストレージノードが選択されています。以下のスクリーンショットよりも詳細な情報が表示されます。

StorageGRIDでトラフィック分類ポリシーを使用する

StorageGRIDでネットワークトラフィックを管理および最適化するためのトラフィック分類ポリシーをセットアップおよび設定する方法について説明します。

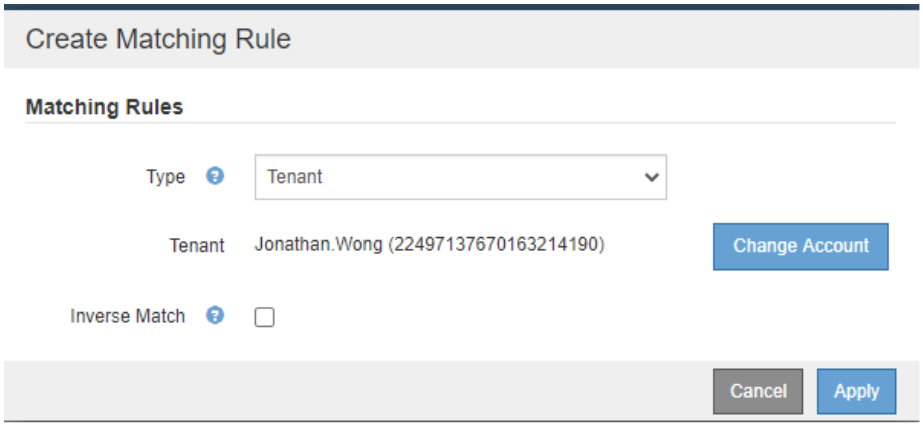
トラフィック分類ポリシーは、特定のテナント、バケット、IPサブネット、またはロードバランサエンドポイントに基づいてトラフィックを監視または制限する方法を提供します。ネットワーク接続と帯域幅は、StorageGRIDにとって特に重要な指標です。

トラフィック分類ポリシーを設定する手順は、次のとおりです。

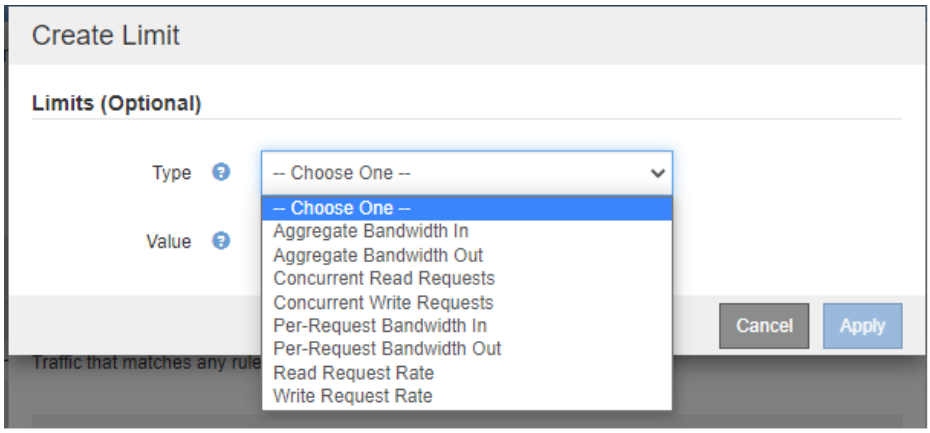
手順

1. GMIで、メニュー[Configuration][System Settings]>[Traffic Classification]に移動します。
2. [Create]をクリック+
3. ポリシーの名前と説明を入力します。

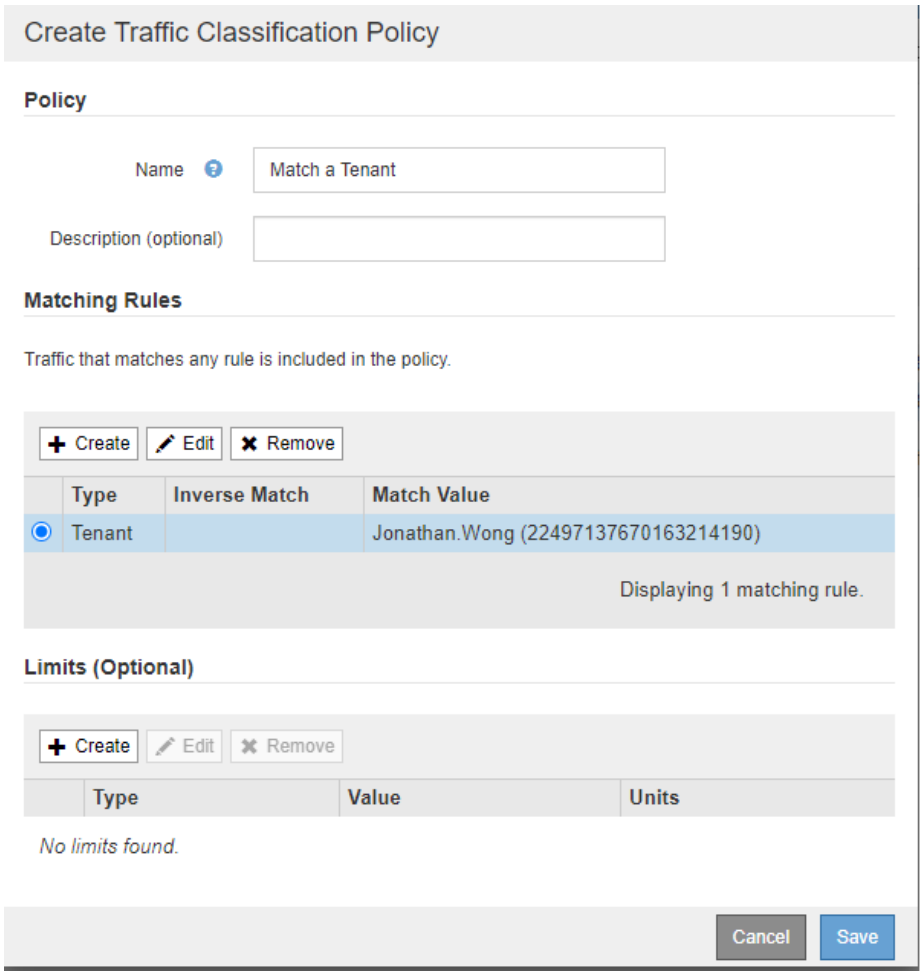
4. 一致ルールを作成します。



5. 制限を設定します（オプション）。



6. ポリシーを保存する



トラフィック分類ポリシーに関連付けられているメトリックを表示するには、ポリシーを選択して[Metrics]をクリックします。ロードバランサ要求トラフィックや平均要求期間などの情報を表示するGrafanaダッシュボードが生成されます。

監査ログを使用したStorageGRIDの監視

StorageGRID監査ログを使用してテナントやグリッドのアクティビティを詳細に分析する方法や、Splunkなどのツールをログ分析に活用する方法について説明します。

StorageGRID監査ログを使用して、テナントとグリッドのアクティビティに関する詳細情報を収集できます。監査ログは、NFS経由で分析用に公開できます。監査ログのエクスポート方法の詳細については、『管理者ガイド』を参照してください。

監査がエクスポートされたら、SplunkやLogstash+Elasticsearchなどのログ分析ツールを使用してテナントのアクティビティを把握したり、詳細な課金レポートやチャージバックレポートを作成したりできます。

監査メッセージの詳細については、StorageGRIDのドキュメントを参照してください。を参照して "監査メッセージ"

Splunk向けStorageGRIDアプリケーションを使用

SplunkプラットフォームでStorageGRID環境を監視、分析できるNetApp StorageGRID for Splunkの詳細をご確認ください。

Splunkは、マシンデータのインポートとインデックス付けを行うソフトウェアプラットフォームで、強力な検索と分析機能を提供します。NetApp StorageGRIDアプリは、StorageGRIDから活用されるデータをインポートしてエンリッチ化するSplunk向けのアドオンです。

StorageGRIDアドオンのインストール、アップグレード、および設定の方法については、次のサイトを参照してください。 https://splunkbase.splunk.com/app/3895/#/details

TR-4882：『Install a StorageGRID bare metal grid』

StorageGRIDノインストールノガイヨウ

ベアメタルホストにStorageGRIDをインストールする方法について説明します。

TR-4882には、NetApp StorageGRIDの実際的なインストール手順が記載されています。ベアメタルまたはRed Hat Enterprise Linux（RHEL）で実行されている仮想マシン（VM）にインストールできます。このアプローチでは、StorageGRIDコンテナ化された6つのサービスを、推奨されるレイアウトとストレージ構成で、3台の物理（または仮想）マシンに「独自の」インストールを実行します。お客様によっては、このTRに記載されている導入例に従うことで、導入プロセスを理解しやすくなる場合があります。

StorageGRIDとインストールプロセスの詳細については、製品ドキュメントの[Install、upgrade、and hotfix（インストール、アップグレード、およびホットフィックスのStorageGRID）]を参照して https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html ください。

導入を開始する前に、NetApp StorageGRIDソフトウェアのコンピューティング、ストレージ、ネットワークの要件を確認してみましょう。StorageGRIDは、PodmanまたはDocker内でコンテナ化されたサービスとして実行されます。このモデルでは、一部の要件はホストオペレーティングシステム（StorageGRIDソフトウェアを実行しているDockerをホストするOS）を参照しています。また、リソースの一部は、各ホスト内で実行されているDockerコンテナに直接割り当てられます。この導入では、ハードウェアの使用率を最大化するために、物理ホストごとに2つのサービスを導入します。詳細については、次のセクションに進んでください "StorageGRIDをインストールするための前提条件"。

このTRで説明した手順を実行すると、6台のベアメタルホストにStorageGRIDのインストールが完了します。これでグリッドネットワークとクライアントネットワークが正常に機能し、ほとんどのテストシナリオで役立ちます。

追加情報の参照先

このTRに記載されている情報の詳細については、次のドキュメントリソース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/
- NetApp製品ドキュメント https://www.netapp.com/support-and-training/documentation/

StorageGRIDをインストールするための前提条件

StorageGRIDを導入するためのコンピューティング、ストレージ、ネットワーク、Docker、ノードの要件について説明します。

コンピューティング要件

次の表に、StorageGRIDノードのタイプごとにサポートされる最小リソース要件を示します。これらは、StorageGRIDノードに必要な最小限のリソースです。

ノードのタイプ	CPUコア数	RAM
管理者	8	24 GB
ストレージ	8	24 GB
ゲートウェイ	8	24 GB

また、適切に動作するためには、各物理Dockerホストに16GB以上のRAMを割り当てる必要があります。たとえば、表に記載されている2つのサービスを1つの物理Dockerホストで一緒にホストするには、次の計算を行います。

24 + 24 + 16 = 64GB RAM、8 + 8 = 16コア

最新のサーバの多くはこれらの要件を超えているため、6つのサービス（StorageGRIDコンテナ）を3台の物理サーバに統合しました。

ネットワーク要件

StorageGRIDトラフィックには、次の3種類があります。

- *グリッドトラフィック（必須）。*グリッド内のすべてのノードの間で伝送される、内部 StorageGRID トラフィック。
- *管理トラフィック（オプション）。*システムの管理とメンテナンスに使用されるトラフィック。
- *クライアントトラフィック（オプション）。*S3 および Swift クライアントからのオブジェクトストレージ要求をすべて含む、外部のクライアントアプリケーションとグリッドの間で伝送されるトラフィック。

StorageGRIDシステムで使用するネットワークを3つまで設定できます。各ネットワークタイプは、重複のない別 々 のサブネット上に存在する必要があります。すべてのノードが同じサブネット上にある場合、ゲート

ウェイアドレスは必要ありません。

この評価では、グリッドトラフィックとクライアントトラフィックを含む2つのネットワークにを導入します。あとで管理ネットワークを追加して、その機能を利用することもできます。

すべてのホストのインターフェイスにネットワークを一貫してマッピングすることが非常に重要です。たとえば、各ノードにens192とens224の2つのインターフェイスがある場合は、すべてのホストで同じネットワークまたはVLANにマッピングする必要があります。このインストールでは、インストーラはこれらをeth0@if2およびeth2@if3としてDockerコンテナにマッピングします（ループバックはコンテナ内のIf1であるため）。したがって、一貫したモデルが非常に重要です。

Dockerネットワークに関する注意事項

StorageGRIDでは、一部のDockerコンテナ実装とは異なるネットワークを使用します。Docker（Kubernetes、Swarm）が提供するネットワークは使用しません。代わりに、StorageGRIDは実際には--net=noneとしてコンテナを生成し、Dockerはコンテナのネットワーク化に何もしないようにします。StorageGRIDサービスによってコンテナが生成されると、ノード構成ファイルに定義されているインターフェイスから新しいmacvlanデバイスが作成されます。このデバイスは新しいMACアドレスを持ち、物理インターフェイスからパケットを受信できる別個のネットワークデバイスとして機能します。macvlanデバイスはコンテナネームスペースに移動され、コンテナ内のeth0、eth1、またはeth2のいずれかに名前が変更されます。この時点で、ネットワークデバイスはホストOSに表示されなくなります。この例では、Dockerコンテナ内のグリッドネットワークデバイスはeth0で、クライアントネットワークはeth2です。管理ネットワークがある場合、デバイスはコンテナ内のeth1になります。

> ⓘ コンテナネットワークデバイスの新しいMACアドレスでは、一部のネットワーク環境および仮想環境で無差別モードを有効にする必要がある場合があります。このモードでは、物理デバイスは既知の物理MACアドレスとは異なるMACアドレスのパケットを送受信できます。 VMware vSphereで実行している場合は、RHELの実行時にStorageGRIDトラフィックを処理するポートグループで、プロミスキャスモード、MACアドレスの変更、および偽装送信を受け入れる必要があります。UbuntuまたはDebianはほとんどの状況でこれらの変更なしに動作します。+

ストレージ要件

各ノードには、次の表に示すサイズのSANベースまたはローカルディスクデバイスが必要です。

> ⓘ 表内の数値はStorageGRIDサービスタイプごとのものであり、グリッド全体や物理ホストごとの数値ではありません。導入の選択肢に基づいて、このドキュメントで後述するでの各物理ホストの数を計算します "物理ホストのレイアウトと要件"。アスタリスクが付いているパスまたはファイルシステムは、インストーラによってStorageGRIDコンテナ自体に作成されます。管理者による手動での設定やファイルシステムの作成は必要ありませんが、これらの要件を満たすためにはホストにブロックデバイスが必要です。つまり、ブロックデバイスはコマンドを使用して表示され `lsblk` ますが、ホストOS内でフォーマットまたはマウントされていません。+

ノードタイプ	LUNの用途	LUN数	LUNの最小サイズ	手動ファイルシステムが必要	推奨されるノード設定エントリ
すべて	管理ノードのシステムスペース `/var/local` （SSDが有用）	管理ノードごとに1つ	90GB	いいえ	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`

ノードタイプ	LUNの用途	LUN数	LUNの最小サイズ	手動ファイルシステムが必要	推奨されるノード設定エントリ
すべてのノード	Dockerストレージプール：`/var/lib/docker for container pool`	ホスト（物理またはVM）ごとに1つ	コンテナあたり100GB	○–etx4	NA–フォーマットしてホストファイルシステムとしてマウント（コンテナにマッピングされていない）
管理者	管理ノードの監査ログ（管理コンテナ内のシステムデータ）`/var/local/audit/export`	管理ノードごとに1つ	200GB	いいえ	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
管理者	管理ノードのテーブル（管理コンテナ内のシステムデータ）`/var/local/mysql_ibdata`	管理ノードごとに1つ	200GB	いいえ	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
ストレージノード	オブジェクトストレージ（ブロックデバイス）`/var/local/rangedb0` （SSDが役立つ）`/var/local/rangedb1` `/var/local/rangedb2`	ストレージコンテナごとに3つ	4000GB	いいえ	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

この例では、コンテナタイプごとに必要なディスクサイズを次の表に示します。物理ホストごとの要件については、このドキュメントの後半で説明し "物理ホストのレイアウトと要件"ます。

コンテナタイプ別のディスクサイズ

Adminコンテナ

名前	サイズ（**GiB**）
Dockerストア	100（コンテナあたり）
ADM-OS	90
ADM -監査	200です
ADM - MySQL	200です

ストレージコンテナ

名前	サイズ（**GiB**）
Dockerストア	100（コンテナあたり）
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

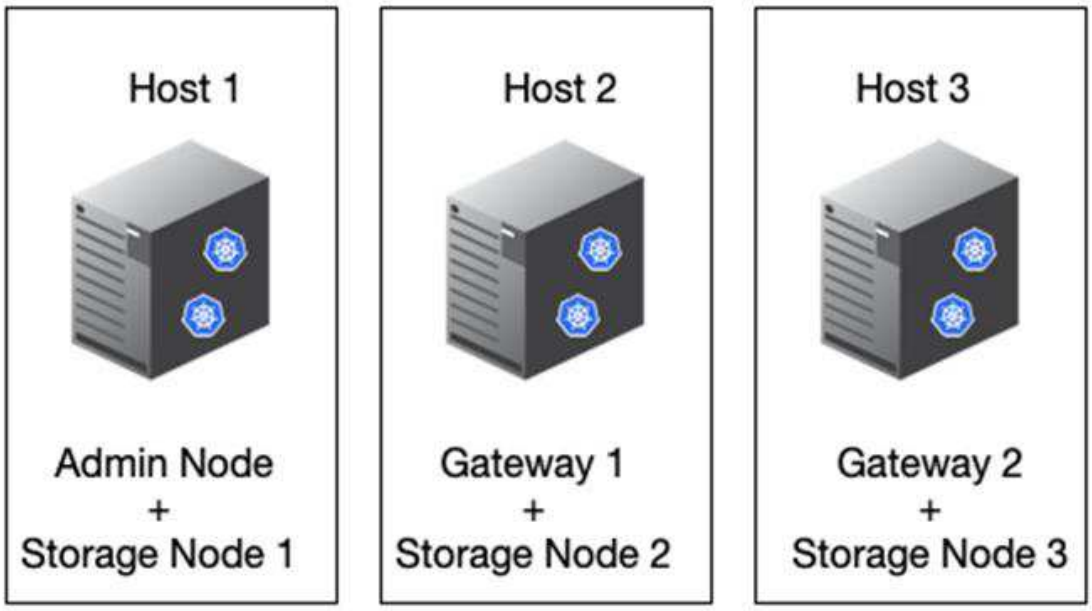
ゲートウェイコンテナ

名前	サイズ（**GiB**）
Dockerストア	100（コンテナあたり）
/var/local	90

物理ホストのレイアウトと要件

上記の表に示すコンピューティング要件とネットワーク要件を組み合わせることで、16コア、64GBのRAM、2つのネットワークインターフェイスを備えた3台の物理（または仮想）サーバに必要な基本的なハードウェアセットを入手できます。より高いスループットが必要な場合は、グリッドネットワークまたはクライアントネットワーク上の複数のインターフェイスをボンディングし、ノード構成ファイルでbond0.520などのVLANタグ付きインターフェイスを使用できます。負荷の高いワークロードが必要な場合は、ホストとコンテナの両方のメモリを増やす方が効果的です。

次の図に示すように、これらのサーバは6つのDockerコンテナ（ホストごとに2つ）をホストします。RAMはコンテナあたり24GB、ホストOS自体に16GBを提供することで計算されます。



物理ホスト（VM）あたりに必要な合計RAMは、24 x 2 + 16 = 64GBです。次の表に、ホスト1、2、3に必要なディスクストレージを示します。

ホスト**1**	サイズ（**GiB**）
• Dockerストア*	`/var/lib/docker` （ファイルシステム）
200（100 x 2）	管理コンテナ
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200です
`BLOCK_DEVICE_TABLES`	200です
ストレージコンテナ	SN-OS `/var/local` （デバイス）
90	Rangedb-0（デバイス）
4096	Rangedb-1（デバイス）
4096	Rangedb-2（デバイス）

ホスト**2**	サイズ（**GiB**）
• Dockerストア*	`/var/lib/docker` （共有）
200（100 x 2）	ゲートウェイコンテナ
GW-OS */`var/local`	100

ホスト**2**	サイズ（**GiB**）
ストレージコンテナ	*/var/local*
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

ホスト**3**	サイズ（**GiB**）
• Dockerストア*	*/var/lib/docker* （共有）
200（100 x 2）	ゲートウェイコンテナ
/var/local	100
ストレージコンテナ	*/var/local*
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Docker Storeの計算では、/var/localあたり100GB（コンテナあたり）x 2つのコンテナが200GBであるとしました。

ノードの準備

StorageGRIDの初期インストールの準備として、まずRHELバージョン9.2をインストールし、SSHを有効にします。ベストプラクティスに従って、ネットワークインターフェイス、ネットワークタイムプロトコル（NTP）、DNS、およびホスト名を設定します。グリッドネットワークでとクライアントネットワーク用に少なくとも1つのネットワークインターフェイスが有効になっている必要があります。VLANタグ付きインターフェイスを使用している場合は、次の例に従って設定します。それ以外の場合は、シンプルな標準ネットワークインターフェイス設定で十分です。

グリッドネットワークインターフェイスでVLANタグを使用する必要がある場合は、次の形式の2つのファイルが構成に含まれている必要があります */etc/sysconfig/network-scripts/* 。

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

この例では、グリッドネットワークの物理ネットワークデバイスがenp67s0であると想定しています。また、bond0などの結合デバイスにすることもできます。ネットワークポートにデフォルトのVLANがない場合やデフォルトのVLANがグリッドネットワークに関連付けられていない場合は、ボンディングを使用するか標準のネットワークインターフェイスを使用する必要があります。StorageGRIDコンテナ自体はイーサネットフレームのタグを解除しないため、親OSで処理する必要があります。

iSCSIを使用したストレージセットアップ（オプション）

iSCSIストレージを使用しない場合は、host1、host2、およびhost3に、要件を満たす十分なサイズのブロックデバイスが含まれていることを確認する必要があります。host1、host2、およびhost3のストレージ要件については、を参照してください "コンテナタイプ別のディスクサイズ" 。

iSCSIを使用してストレージをセットアップするには、次の手順を実行します。

手順

1. NetApp EシリーズやNetApp ONTAP®データ管理ソフトウェアなどの外部iSCSIストレージを使用する場合は、次のパッケージをインストールします。

```
sudo yum install iscsi-initiator-utils
sudo yum install device-mapper-multipath
```

2. 各ホストでイニシエータIDを確認します。

```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2006-04.com.example.node1
```

3. 手順2のイニシエータ名を使用して、ストレージデバイス上のLUN（表に示されている数とサイズ）を各ストレージノードにマッピングし "ストレージ要件" ます。

4. で新しく作成したLUNを検出し `iscsiadm` 、ログインします。

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

詳細については、Red Hatカスタマーポータルのを参照してください "iSCSIイニシエータの作成" 。

5. マルチパスデバイスとそれに関連付けられたLUN WWIDを表示するには、次のコマンドを実行します。

```
# multipath -ll
```

iSCSIをマルチパスデバイスで使用していない場合は、一意のパス名を使用してデバイスをマウントするだけで、デバイスの変更やリブートが同じように維持されます。

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

デバイス名を使用するだけで、 `/dev/sdx` デバイスが削除または追加された場合に問題が発生する可能性があります。マルチパスデバイスを使用している場合は、次のようにエイリアスを使用するようにファイルを変更します `/etc/multipath.conf` 。+

レイアウトによっては、これらのデバイスがすべてのノードに存在する場合とない場合があります。

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

ホストOSにDockerをインストールする前に、LUNまたはディスクのバッキングをフォーマットしてマウントし `/var/lib/docker`ます。他のLUNはノード構成ファイルに定義され、StorageGRIDコンテナによって直接使用されます。つまり、これらのファイルシステムはホストOSには表示されず、コンテナ自体に表示され、インストーラによって処理されます。

iSCSIベースのLUNを使用している場合は、fstabファイルに次のような行を追加します。前述のように、他

のLUNはホストOSにマウントする必要はありませんが、使用可能なブロックデバイスとして表示される必要があります。

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Dockerのインストールの準備

Dockerのインストールを準備するには、次の手順を実行します。

手順

1. 3つのホストすべてのDockerストレージボリュームにファイルシステムを作成します。

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   iSCSIデバイスをマルチパスで使用している場合は、を使用し `/dev/mapper/Docker-Store`ます。

2. Dockerストレージボリュームマウントポイントを作成します。

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. 同様のエントリをdocker-storage-volume-deviceに追加します `/etc/fstab`。

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   次の `_netdev` オプションは、iSCSIデバイスを使用している場合にのみ推奨されます。ローカルのブロックデバイスを使用する場合は `_netdev` 必要ないため、を推奨します。 `defaults`

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. 新しいファイルシステムをマウントし、ディスクの使用状況を表示します。

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. パフォーマンス上の理由から、スワップをオフにして無効にします。

   ```
   $ sudo swapoff --all
   ```

6. 設定を維持するには、次のようなすべてのスワップエントリを/etc/fstabから削除します。

```
/dev/mapper/rhel-swap swap defaults 0 0
```

スワップを完全に無効にできないと、パフォーマンスが大幅に低下する可能性があります

7. ノードのテストリブートを実行して、ボリュームが永続的であり、すべてのディスクデバイスが戻ってくることを確認し `/var/lib/docker` ます。

Docker for StorageGRIDのインストール

Docker for StorageGRIDのインストール方法について説明します。

Dockerをインストールするには、次の手順を実行します。

手順

1. Docker用のyumリポジトリを設定します。

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. 必要なパッケージをインストールします。

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Dockerを起動します。

```
sudo systemctl start docker
```

4. Dockerをテストします。

```
sudo docker run hello-world
```

5. Dockerがシステム起動時に実行されていることを確認します。

```
sudo systemctl enable docker
```

StorageGRIDのノード構成ファイルを準備

StorageGRID用のノード構成ファイルを準備する方法について説明します。

ノード設定プロセスの大まかな手順は次のとおりです。

手順

1. すべてのホストにディレクトリを作成し `/etc/storagegrid/nodes` ます。

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. コンテナ/ノードタイプのレイアウトに合わせて、物理ホストごとに必要なファイルを作成します。この例では、各ホストマシンの物理ホストごとに2つのファイルを作成しました。

> ファイルの名前は、インストールの実際のノード名を定義します。たとえば、は `dc1-adm1.conf` という名前のノードになり `dc1-adm1`ます。

--ホスト1：
`dc1-adm1.conf`
`dc1-sn1.conf`

--ホスト2:
`dc1-gw1.conf`
`dc1-sn2.conf`

--ホスト3:
`dc1-gw2.conf`
`dc1-sn3.conf`

ノード構成ファイルの準備

次の例では、という形式を使用し `/dev/disk/by-path` ます。次のコマンドを実行して、正しいパスを確認できます。

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

コマンドは次のとおりです。

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

プライマリ管理ノードの例

ファイル名の例：

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

ファイルの内容の例：

> ディスクパスの例を次に示します。または、形式の名前を使用できます `/dev/mapper/alias` 。などのブロックデバイス名は使用しないでください。ブロックデバイス名は `/dev/sdb` リブート時に変更され、グリッドに大きな損傷を与える可能性があります。

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

ストレージノードの例

ファイル名の例：

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

ファイルの内容の例：

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

ゲートウェイノードの例

ファイル名の例：

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

ファイルの内容の例：

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

StorageGRIDの依存関係とパッケージのインストール

StorageGRIDの依存関係とパッケージをインストールする方法について説明します。

StorageGRIDの依存関係とパッケージをインストールするには、次のコマンドを実行します。

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

StorageGRID構成ファイルの検証

StorageGRIDの構成ファイルの内容を検証する方法について説明します。

各StorageGRIDノードのに構成ファイルを作成したら `/etc/storagegrid/nodes` 、それらのファイルの内容を検証する必要があります。

構成ファイルの内容を検証するには、各ホストで次のコマンドを実行します。

```
sudo storagegrid node validate all
```

ファイルが正しい場合は、各構成ファイルについてPASSEDと表示されます。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

構成ファイルが正しくない場合は、警告およびエラーとして問題が表示されます。構成エラーが見つかった場合は、インストールを続行する前に修正する必要があります。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

StorageGRID ホストサービスを開始します

StorageGRIDホストサービスを開始する方法について説明します。

StorageGRIDノードを開始し、ホストのリブート後にノードが再起動されるようにするには、StorageGRIDホストサービスを有効にして開始する必要があります。

StorageGRIDホストサービスを開始するには、次の手順を実行します。

手順

1. 各ホストで次のコマンドを実行します。

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

> 最初の実行では、開始プロセスに時間がかかることがあります。

2. 次のコマンドを実行して、導入の進行状況を確認します。

```
sudo storagegrid node status node-name
```

3. またはのステータスを返すノードに対して、 `Not-Running` `Stopped`次のコマンドを実行します。

```
sudo storagegrid node start node-name
```

たとえば、次の出力からノードを起動するとし `dc1-adm1` ます。

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. StorageGRIDホストサービスを以前に有効にして開始したことがある場合（またはサービスが有効になって開始されたかどうかが不明な場合）は、次のコマンドも実行します。

```
sudo systemctl reload-or-restart storagegrid
```

StorageGRIDでのGrid Managerの設定

プライマリ管理ノードのStorageGRIDでグリッドマネージャを設定する方法について説明します。

プライマリ管理ノードのGrid Managerユーザインターフェイスから StorageGRIDシステムを設定して、インストールを完了します。

手順の概要

グリッドを設定してインストールを完了するには、次のタスクを実行します。

手順

1. Grid Managerに移動
2. "StorageGRID ライセンス情報を指定します"
3. "StorageGRIDへのサイトの追加"
4. "グリッドネットワークサブネットの指定"
5. "保留中のグリッドノードを承認します"
6. "NTPサーバ情報の指定"
7. "ドメインネームシステムサーバ情報の指定"
8. "StorageGRID システムのパスワードを指定します"
9. "構成を確認し、インストールを完了します"

Grid Managerに移動

グリッドマネージャを使用して、StorageGRIDシステムの設定に必要なすべての情報を定義します。

作業を開始する前に、プライマリ管理ノードを導入し、最初の起動シーケンスを完了しておく必要があります。

Grid Managerを使用して情報を定義するには、次の手順を実行します。

手順

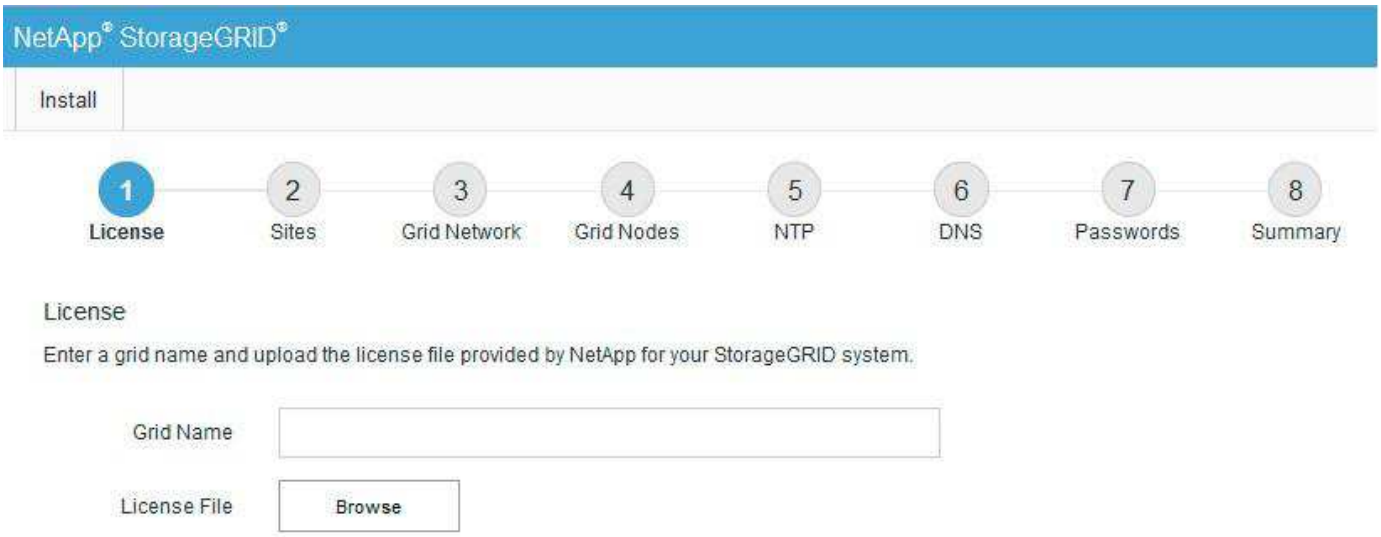
1. 次のアドレスでGrid Managerにアクセスします。

   ```
   https://primary_admin_node_grid_ip
   ```

   または、ポート8443でGrid Managerにアクセスできます。

   ```
   https://primary_admin_node_ip:8443
   ```

2. [Install a StorageGRID System]をクリックします。StorageGRIDグリッドの設定に使用するページが表示されます。



StorageGRIDライセンスの詳細を追加

StorageGRIDライセンスファイルをアップロードする方法について説明します。

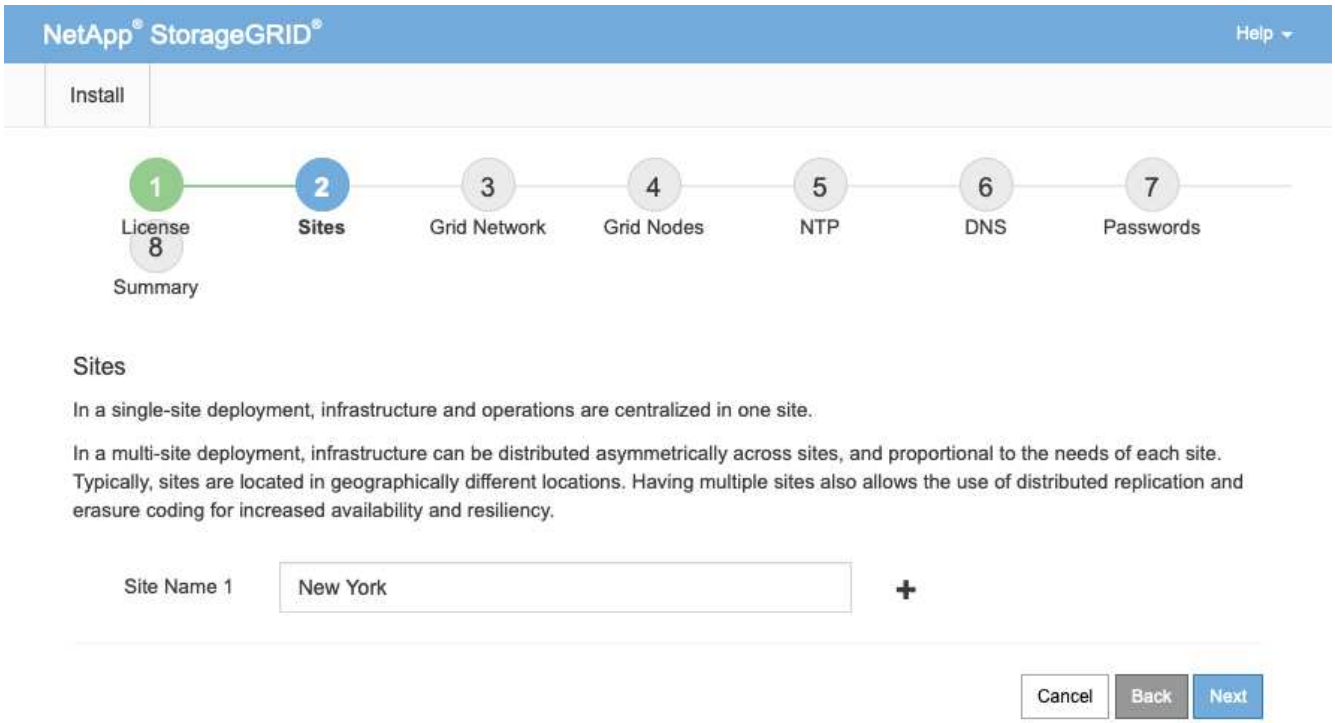
StorageGRID システムの名前を指定し、ネットアップから提供されたライセンスファイルをアップロードする必要があります。

StorageGRIDライセンス情報を指定するには、次の手順を実行します。

手順

1. [License]ページの[Grid Name]フィールドに、StorageGRIDシステムの名前を入力します。インストール後、その名前がグリッドトポロジツリーの最上位レベルとして表示されます。
2. [Browse]をクリックし、NetAppライセンスファイルを検索し (`NLF-*unique-id*.txt`ます）、[Open]をクリックします。ライセンスファイルが検証され、シリアル番号とライセンスされたストレージ容量が表示されます。

> StorageGRID インストールアーカイブには、製品サポートのない無償ライセンスが含まれています。インストール後に、サポートを提供するライセンスに更新できます。



3. [Next]をクリックします。

StorageGRIDへのサイトの追加

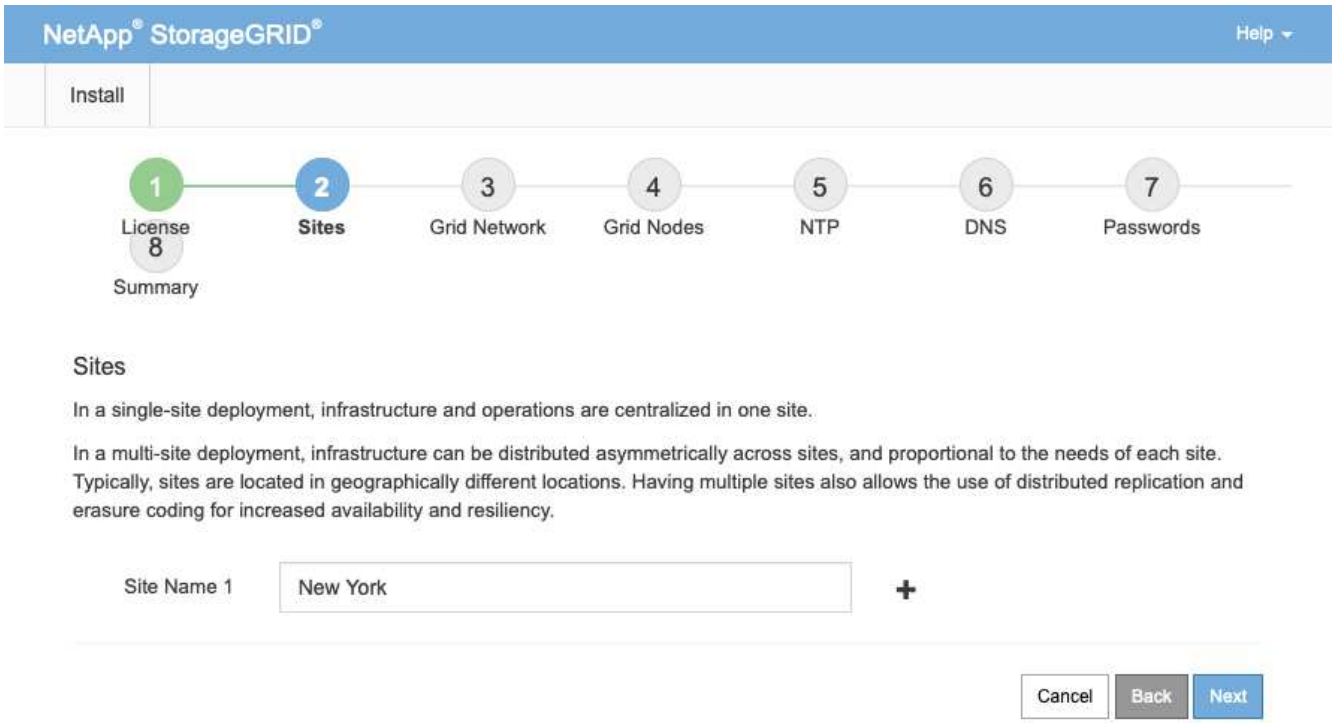
StorageGRIDにサイトを追加して信頼性とストレージ容量を向上させる方法について説明します。

StorageGRIDをインストールする場合は、サイトを少なくとも1つ作成する必要があります。StorageGRID システムの信頼性を高め、ストレージ容量を増やすために、追加のサイトを作成することができます。

サイトを追加するには、次の手順を実行します。

手順

1. [サイト]ページで、サイト名を入力します。
2. サイトを追加するには、最後のサイトエントリの横にあるプラス記号をクリックし、新しい[サイト名]テキストボックスに名前を入力します。グリッドトポロジに必要な数のサイトを追加します。サイトは最大16 個まで追加できます。



3. [Next]をクリックします。

StorageGRIDのグリッドネットワークサブネットの指定

StorageGRID用のグリッドネットワークサブネットの設定方法について説明します。

グリッドネットワークで使用されるサブネットを指定する必要があります。

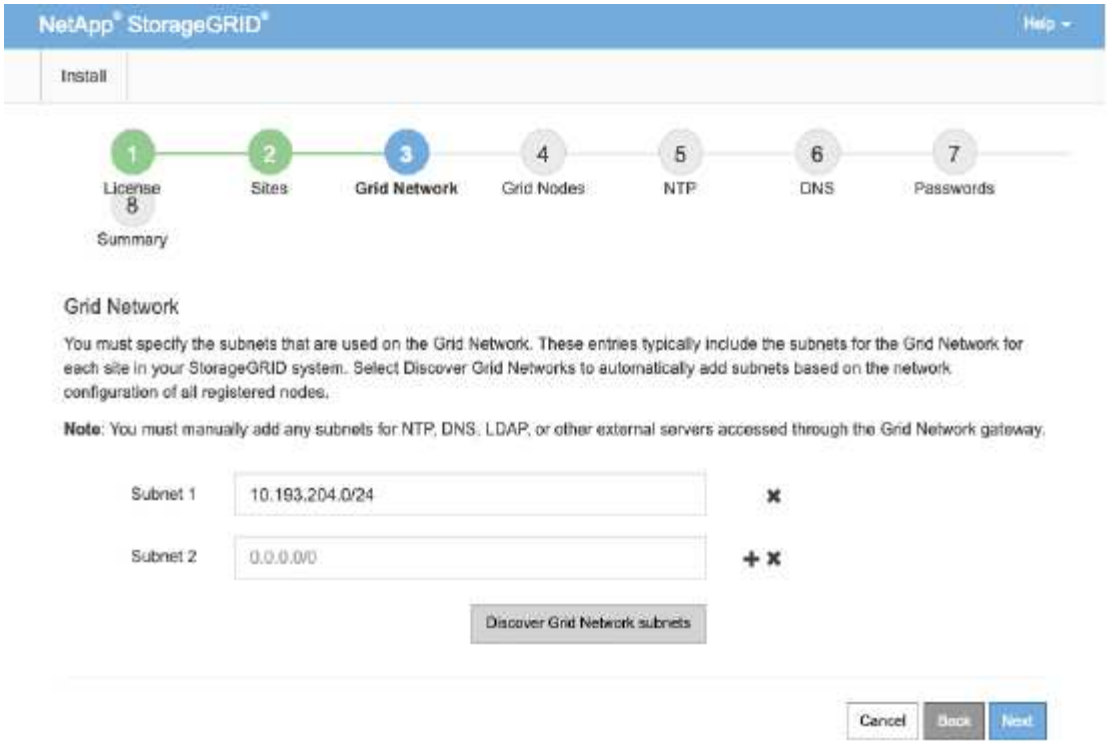
サブネットエントリには、StorageGRIDシステム内の各サイトのグリッドネットワークのサブネット、およびグリッドネットワーク経由で到達できる必要があるサブネット（NTPサーバをホストするサブネットなど）が含まれます。

グリッドサブネットが複数ある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。

グリッドネットワークのサブネットを指定するには、次の手順を実行します。

手順

1. [Subnet 1]テキストボックスで、少なくとも1つのグリッドネットワークのCIDRネットワークアドレスを指定します。
2. 最後のエントリの横にあるプラス記号をクリックして、追加のネットワークエントリを追加します。少なくとも1つのノードをすでに導入している場合は、[Discover Grid Networks Subnets]をクリックして、Grid Managerに登録されているグリッドノードから報告されるサブネットをグリッドネットワークサブネットリストに自動的に追加します。



3. [Next]をクリックします。

StorageGRIDのグリッドノードの承認

StorageGRIDシステムに追加されている保留中のグリッドノードを確認して承認する方法について説明します。

各グリッドノードは、StorageGRIDシステムに追加する前に承認する必要があります。

作業を開始する前に、仮想アプライアンスとStorageGRIDアプライアンスのグリッドノードをすべて導入しておく必要があります。

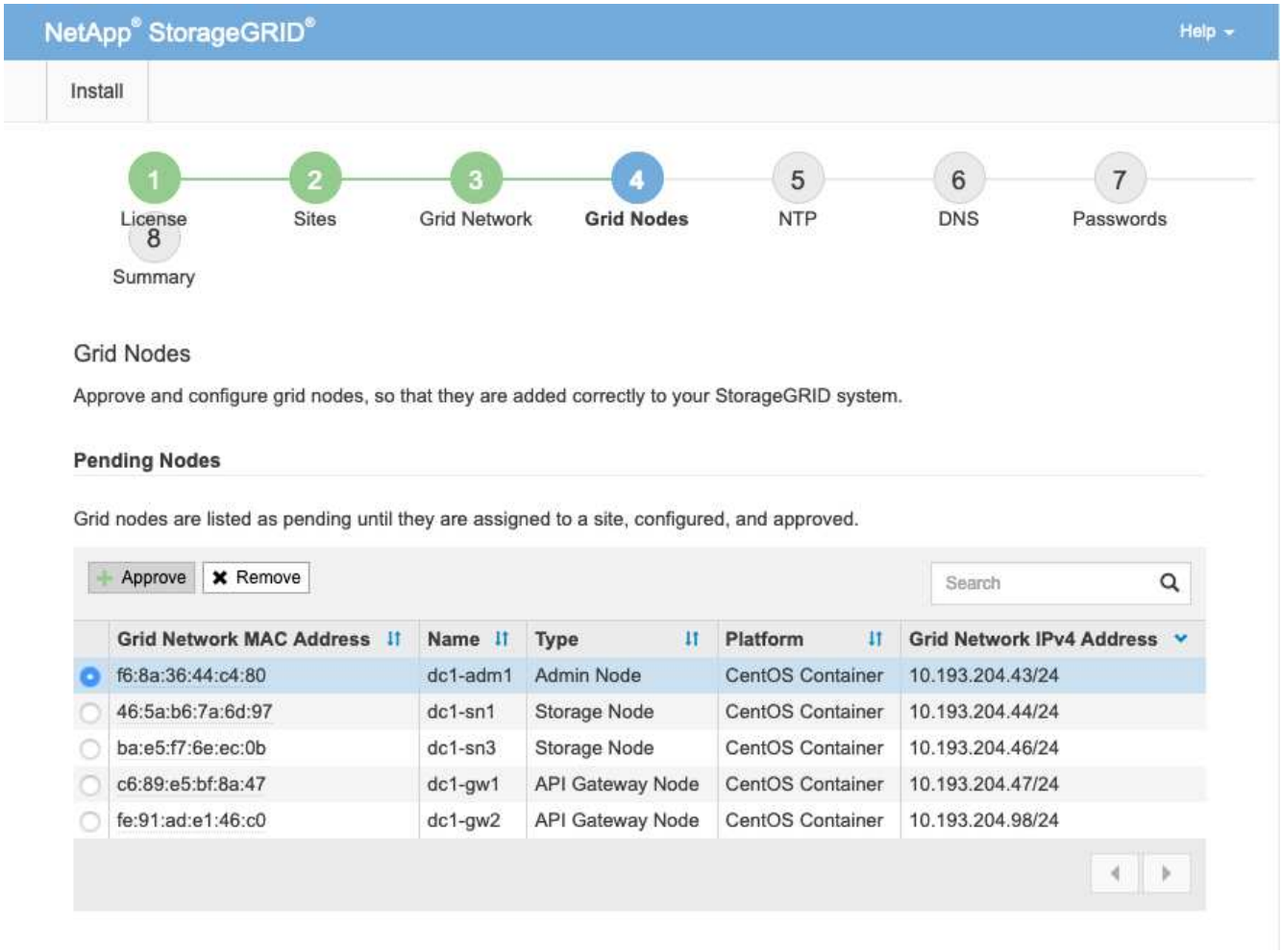
保留中のグリッドノードを承認するには、次の手順を実行します。

手順

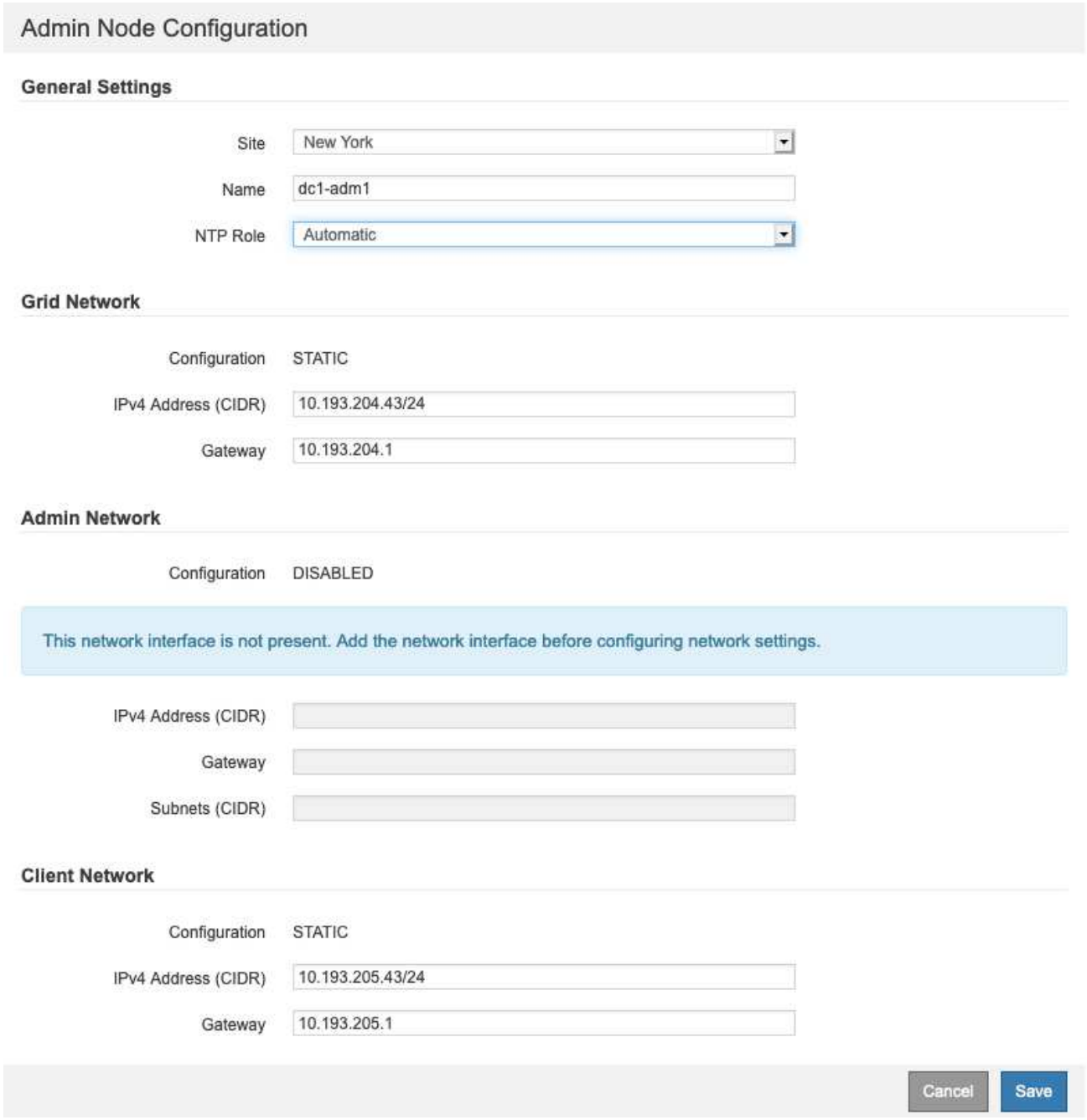
1. [Pending Nodes]リストで、導入したグリッドノードがすべて表示されていることを確認します。

   見つからないグリッドノードがある場合は、正常に導入されたことを確認します。

2. 承認する保留中のノードの横にあるラジオボタンをクリックします。



3. [承認]をクリックします。
4. [一般設定]で、必要に応じて次のプロパティの設定を変更します。



-* Site *：このグリッドノードのサイトのシステム名。

-* Name *：ノードに割り当てられるホスト名とGrid Managerに表示される名前。デフォルトでは、ノード導入時に指定した名前が使用されますが、必要に応じて名前を変更できます。

-* NTP role *：グリッドノードのNTPロール。オプションは、[Automatic]、[Primary]、および[Client]です。[Automatic]オプションを選択すると、管理ノード、Administrative Domain Controller（ADC）サービスを使用するストレージノード、ゲートウェイノード、および非静的IPアドレスが設定されたグリッドノードにPrimaryロールが割り当てられます。他のすべてのグリッドノードにはクライアントロールが割り当てられます。

各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

-* ADC service（ストレージノードのみ）*：このノードにADCサービスが必要かどうかをシステムで自動的に判断するには、[Automatic]を選択します。ADC サービスは、グリッドサービスの場所と可用性を追跡します。各サイトで少なくとも3つのストレージノードにADCサービスが含まれている必要があります。導入後のノードに ADC サービスを追加することはできません。

5. [Grid Network]で、次のプロパティの設定を必要に応じて変更します。

-* IPv4 address（CIDR）*：グリッドネットワークインターフェイスのCIDRネットワークアドレス（コンテナ内のeth0）。たとえば、 `192.168.1.234/24`です。

--ゲートウェイ：グリッドネットワークゲートウェイ。たとえば、 `192.168.0.1`です。

グリッドサブネットが複数ある場合は、ゲートウェイが必要です。

グリッドネットワーク設定でDHCPを選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。作成されたIPアドレスがDHCPアドレスプールに含まれていないことを確認します。

6. グリッドノードの管理ネットワークを設定するには、[Admin Network]セクションで必要に応じて設定を追加または更新します。

このインターフェイスの外部にあるルートのデスティネーションサブネットを、[Subnets（CIDR）]テキストボックスに入力します。管理サブネットが複数ある場合は、管理ゲートウェイが必要です。

管理ネットワーク設定でDHCPを選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。作成されたIPアドレスがDHCPアドレスプールに含まれていないことを確認します。

アプライアンス：StorageGRIDアプライアンスの場合、StorageGRIDアプライアンスインストーラを使用した初回インストール時に管理ネットワークが設定されていないと、この[Grid Manager]ダイアログボックスで設定できません。代わりに、次の手順を実行する必要があります。

a. アプライアンスをリブートします。アプライアンスインストーラで、メニューから[Advanced][Reboot]を選択します。リブートには数分かかることがあります。
b. メニュー：[Configure Networking][Link Configuration]を選択し、適切なネットワークを有効にします。
c. メニューから[Configure Networking][IP Configuration]を選択し、有効なネットワークを設定します。
d. のホームページに戻り、[Start Installation]をクリックします。
e. Grid Manager：ノードが[Approved Nodes]テーブルに表示されている場合は、ノードをリセットします。
f. Pending Nodes テーブルからノードを削除します。
g. ノードが Pending Nodes リストに再表示されるまで待ちます。

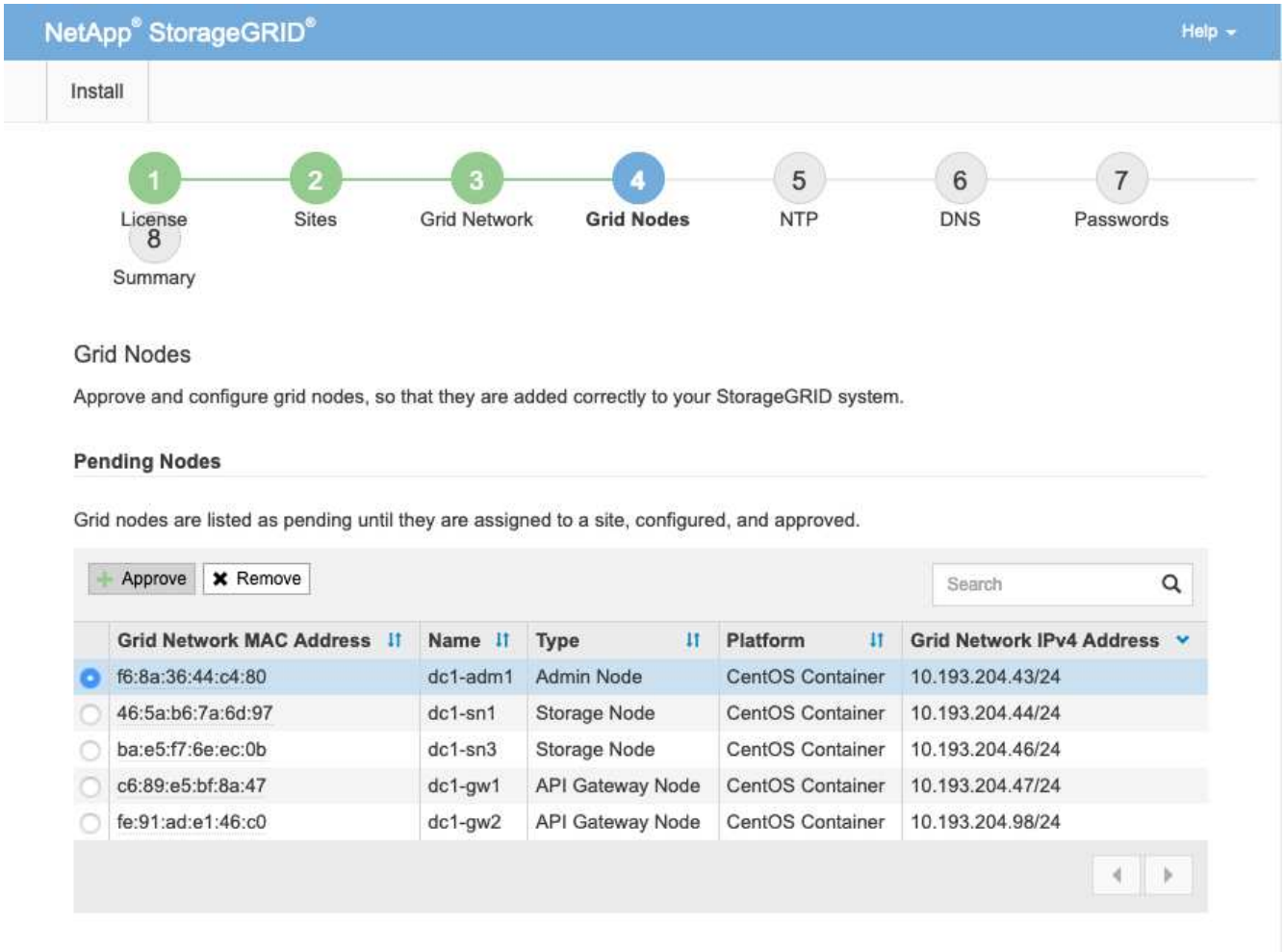
h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。追加情報 の場合は、使用しているアプライアンスモデルのインストールとメンテナンスの手順を参照してください。

7. グリッドノードのクライアントネットワークを設定する場合は、必要に応じてクライアントネットワークセクションで設定を追加または更新します。クライアントネットワークを設定する場合はゲートウェイが必要になります。これは、インストール後にノードのデフォルトゲートウェイになります。

   アプライアンス：StorageGRIDアプライアンスの場合、StorageGRIDアプライアンスインストーラを使用した初回インストール時にクライアントネットワークが設定されていないと、この[Grid Manager]ダイアログボックスで設定できません。代わりに、次の手順を実行する必要があります。

   a. アプライアンスをリブートします。アプライアンスインストーラで、メニューから[Advanced][Reboot]を選択します。リブートには数分かかることがあります。
   b. メニュー：[Configure Networking][Link Configuration]を選択し、適切なネットワークを有効にします。
   c. メニューから[Configure Networking][IP Configuration]を選択し、有効なネットワークを設定します。
   d. のホームページに戻り、[Start Installation]をクリックします。
   e. Grid Manager：ノードが[Approved Nodes]テーブルに表示されている場合は、ノードをリセットします。
   f. Pending Nodes テーブルからノードを削除します。
   g. ノードが Pending Nodes リストに再表示されるまで待ちます。
   h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。追加情報 の場合は、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

8. 保存をクリックします。グリッドノードエントリが [承認済みノード（ Approved Nodes ）] リストに移動します。



9. 承認する保留中のグリッドノードごとに手順1 ~ 8を繰り返します。

   グリッドに必要なすべてのノードを承認する必要があります。ただし、[Summary]ページで[Install]をクリックする前に、いつでもこのページに戻ることができます。承認したグリッドノードのプロパティを変更するには、ノードのラジオボタンをクリックし、[Edit]をクリックします。

10. グリッドノードの承認が完了したら、[Next]をクリックします。

StorageGRIDのNTPサーバの詳細の指定

別 々 のサーバで実行された処理の同期を維持できるように、StorageGRIDシステムのNTP設定情報を指定する方法について説明します。

時間のずれに関する問題を回避するには、Stratum 3以上の外部NTPサーバ参照を4つ指定する必要があります。

> 本番レベルの StorageGRID インストール環境で外部 NTP ソースを指定する場合は、 Windows Server 2016 より前のバージョンの Windows で Windows Time （ W32Time ）サービスを使用しないでください。以前のバージョンのWindowsのタイムサービスは十分に正確ではなく、StorageGRIDのような要求の厳しい環境での使用にはMicrosoftでサポートされていません。

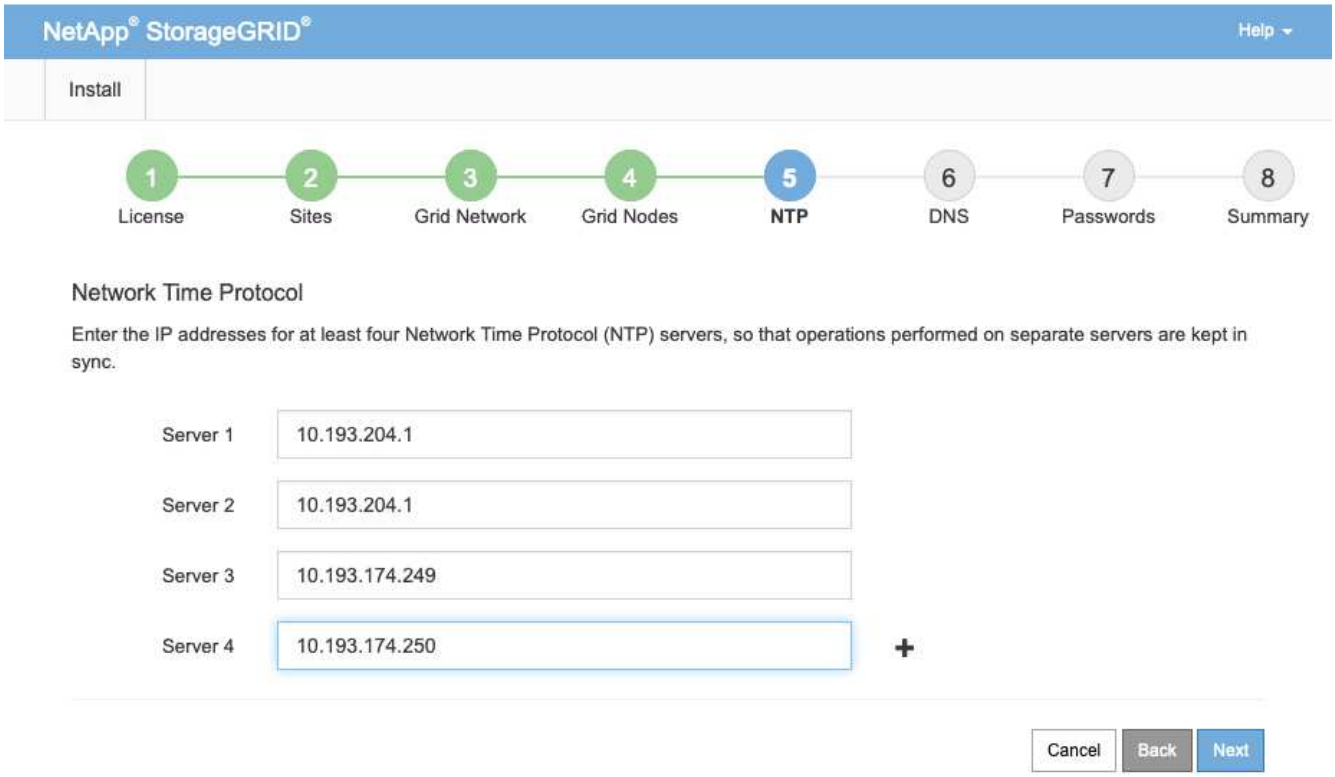
外部NTPサーバは、以前にプライマリNTPロールを割り当てたノードで使用されます。

クライアントネットワークをインストールプロセスの早い段階で有効にしないと、NTPサーバの唯一のソースになりません。少なくとも1つのNTPサーバにグリッドネットワークまたは管理ネットワーク経由でアクセスできることを確認してください。

NTPサーバ情報を指定するには、次の手順を実行します。

手順

1. [Server 1 to Server 4]テキストボックスで、少なくとも4つのNTPサーバのIPアドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号をクリックして、サーバエントリをさらに追加します。



3. [Next]をクリックします。

StorageGRIDのDNSサーバの詳細の指定

StorageGRID用にDNSサーバを設定する方法について説明します。

IPアドレスの代わりにホスト名を使用して外部サーバにアクセスできるように、StorageGRIDシステムのDNS情報を指定する必要があります。

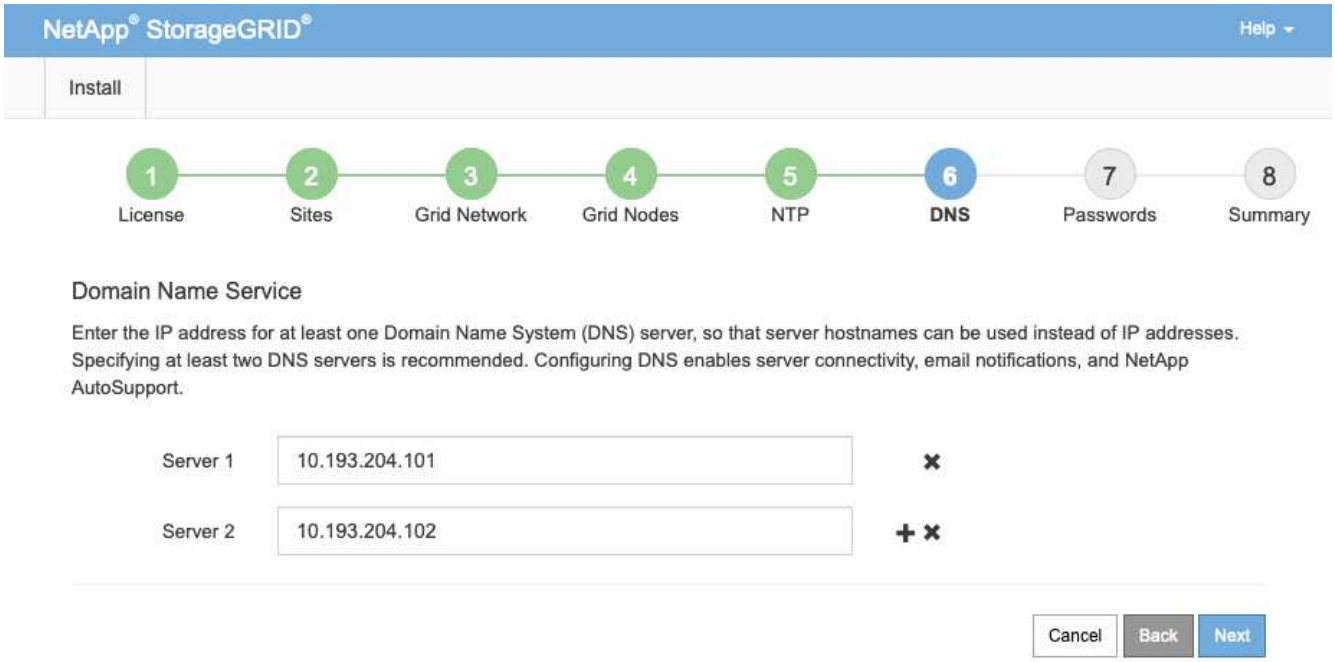
DNSサーバ情報を指定すると、Eメール通知やNetApp AutoSupport®メッセージに、IPアドレスではなく完全修飾ドメイン名（FQDN）ホスト名を使用できます。NetAppでは、少なくとも2つのDNSサーバを指定することを推奨します。

ネットワーク分離が発生した場合に各サイトがローカルにアクセスできる DNS サーバを選択する必要があります。

DNSサーバ情報を指定するには、次の手順を実行します。

手順

1. [Server 1]テキストボックスで、DNSサーバのIPアドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号をクリックしてサーバを追加します。



3. [Next]をクリックします。

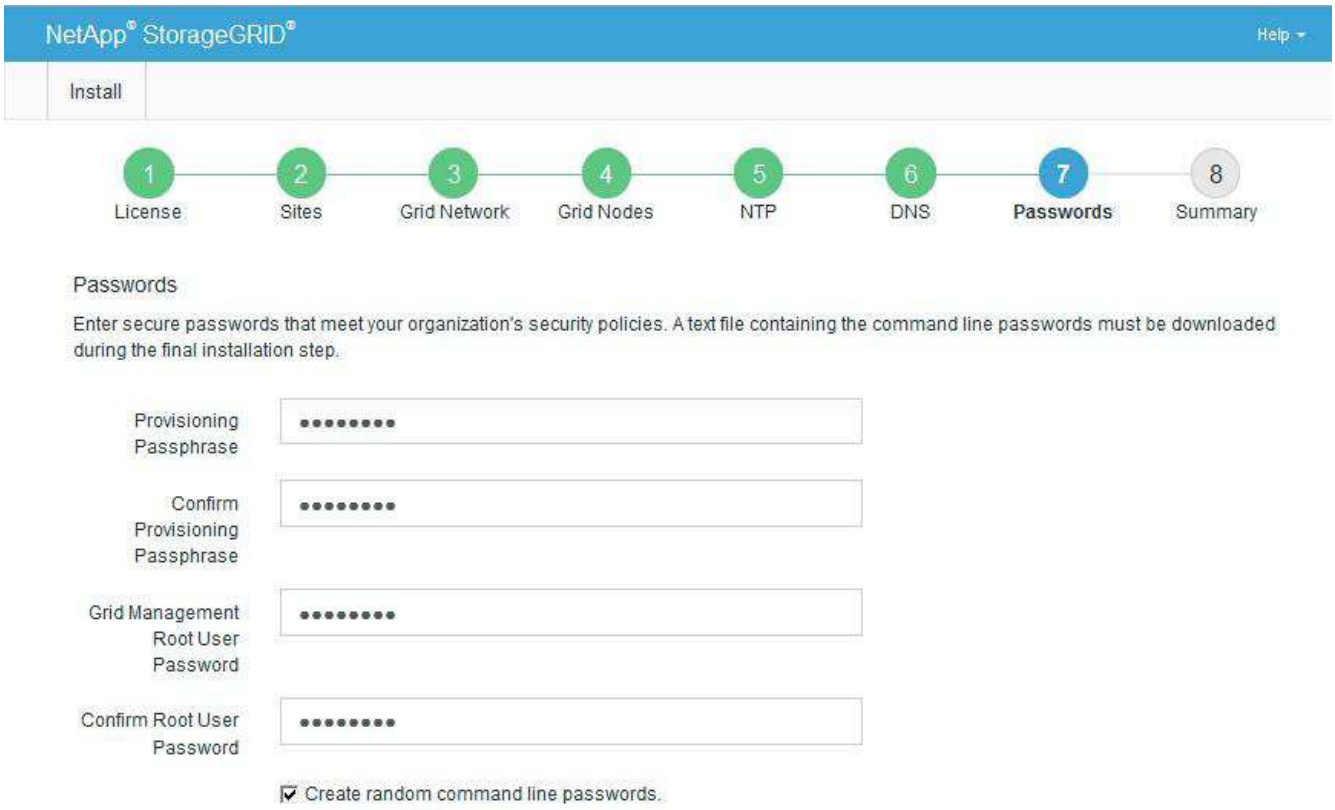
StorageGRIDのシステムパスワードの指定

プロビジョニングパスフレーズとグリッド管理rootユーザパスワードを設定して、StorageGRIDシステムを保護する方法について説明します。

StorageGRIDシステムを保護するために使用するパスワードを入力する手順は、次のとおりです。

手順

1. [Provisioning Passphrase]に、StorageGRIDシステムのグリッドトポロジを変更するために必要なプロビジョニングパスフレーズを入力します。このパスワードは安全な場所に記録してください。
2. [Confirm Provisioning Passphrase]にプロビジョニングパスフレーズを再入力します。
3. [Grid Management Root User Password]に、rootユーザとしてGrid Managerにアクセスする際に使用するパスワードを入力します。
4. [Confirm Root User Password]に、Grid Managerのパスワードを再入力します。



5. コンセプトの実証またはデモ用にグリッドをインストールする場合は、[Create Random Command Line Passwords]オプションの選択を解除します。

   本番環境では、セキュリティ上の理由から常にランダムパスワードを使用する必要があります。rootまたはadminアカウントを使用してコマンドラインからグリッドノードにアクセスする際にデフォルトのパスワードを使用する場合は、デモ用のグリッドでのみ[Create Random Command Line Passwords]オプションの選択を解除します。

   [Summary]ページで[Install]をクリックすると、リカバリパッケージファイルをダウンロードするように求められ (`sgws-recovery-packageid-revision.zip`ます）。インストールを完了するには、このファイルをダウンロードする必要があります。システムにアクセスするためのパスワードは、リカバリパッケージファイルに含まれているファイルに格納され `Passwords.txt` ています。

6. [Next]をクリックします。

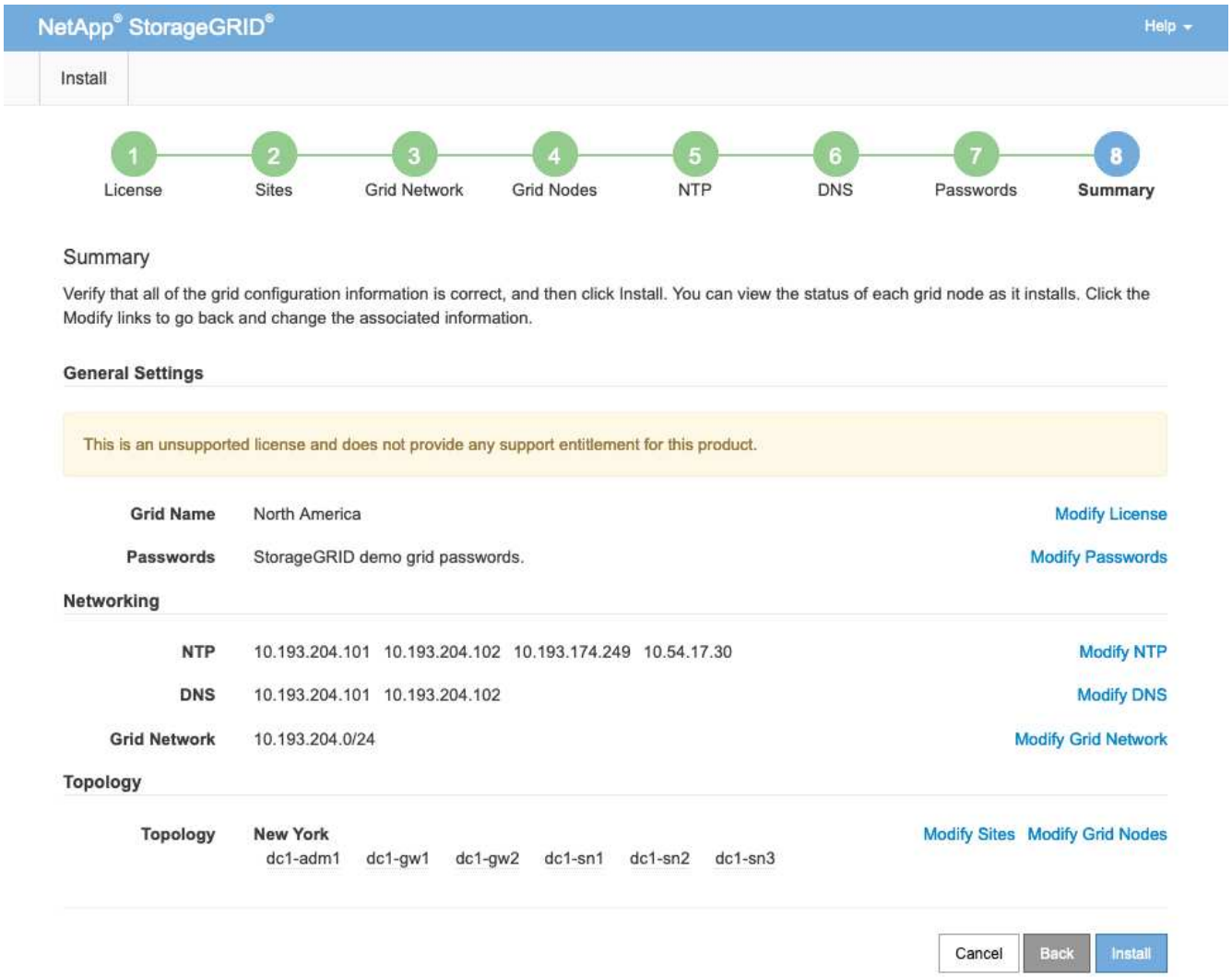
設定を確認して**StorageGRID**のインストールを完了

グリッド設定情報を検証し、StorageGRIDのインストールプロセスを完了する方法について説明します。

インストールが正常に完了したことを確認するには、入力した設定情報をよく確認してください。次の手順を実行します。

手順

1. [Summary]ページを表示します。



2. グリッドの設定情報がすべて正しいことを確認します。Summary （サマリ）ページの Modify （変更）リンクを使用して、戻ってエラーを修正します。
3. インストールをクリックします。

> クライアントネットワークを使用するようにノードが設定されている場合は、[Install]をクリックすると、そのノードのデフォルトゲートウェイがグリッドネットワークからクライアントネットワークに切り替わります。接続が失われた場合は、アクセス可能なサブネットを介してプライマリ管理ノードにアクセスしていることを確認してください。詳細については、「ネットワークのインストールとプロビジョニング」を参照してください。

4. [リカバリパッケージのダウンロード]をクリックします。

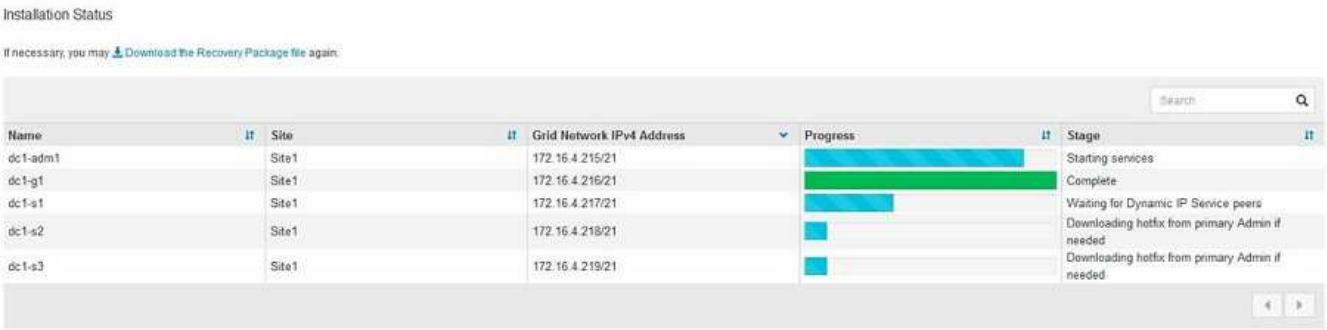
   グリッドトポロジを定義するポイントまでインストールが進むと、リカバリパッケージファイルをダウンロードするように求められます）、このファイルの内容にアクセスできることを確認するメッセージが表示され (`.zip`ます。リカバリパッケージファイルのダウンロードが必要になるのは、グリッドノードで障害が発生した場合にStorageGRIDシステムをリカバリできるようにするためです。

   ファイルの内容を展開できることを確認し `.zip` 、安全で安全な別 々 の場所に保存します。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

5. [I have successfully downloaded and verified the Recovery Package File]オプションを選択し、[Next]をクリックします。

インストールがまだ進行中の場合は、[Installation Status]ページが開きます。このページには、グリッドノードごとのインストールの進捗状況が表示されます。



すべてのグリッドノードがCompleteステージに達すると、Grid Managerのサインインページが開きます。

6. インストール時に指定したパスワードを使用して、Grid Managerにrootユーザとしてサインインします。

StorageGRIDでベアメタルノードをアップグレード

StorageGRIDでのベアメタルノードのアップグレードプロセスについて説明します。

ベアメタルノードのアップグレードプロセスは、アプライアンスまたはVMwareノードのアップグレードプロセスとは異なります。ベアメタルノードのアップグレードを実行する前に、GUIを使用してアップグレードを実行する前に、まずすべてのホストでRPMファイルをアップグレードする必要があります。

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

これで、GUIを使用してソフトウェアのアップグレードに進むことができます。

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

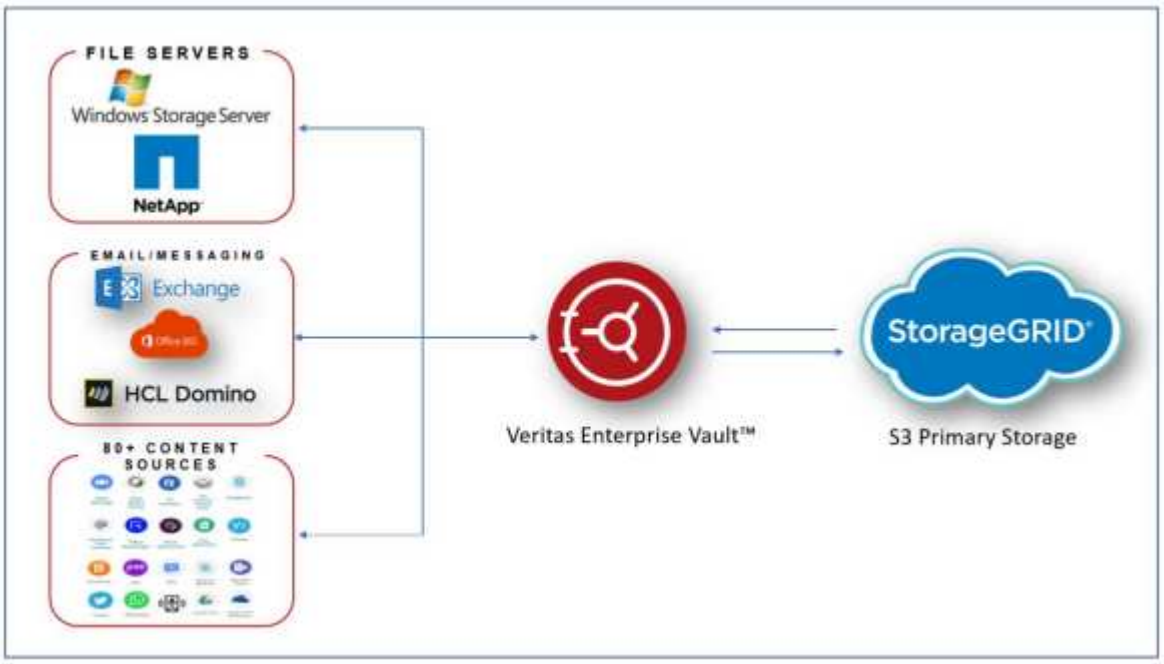
サイトフェイルオーバーのための**StorageGRID**の設定の概要

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/
- 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。

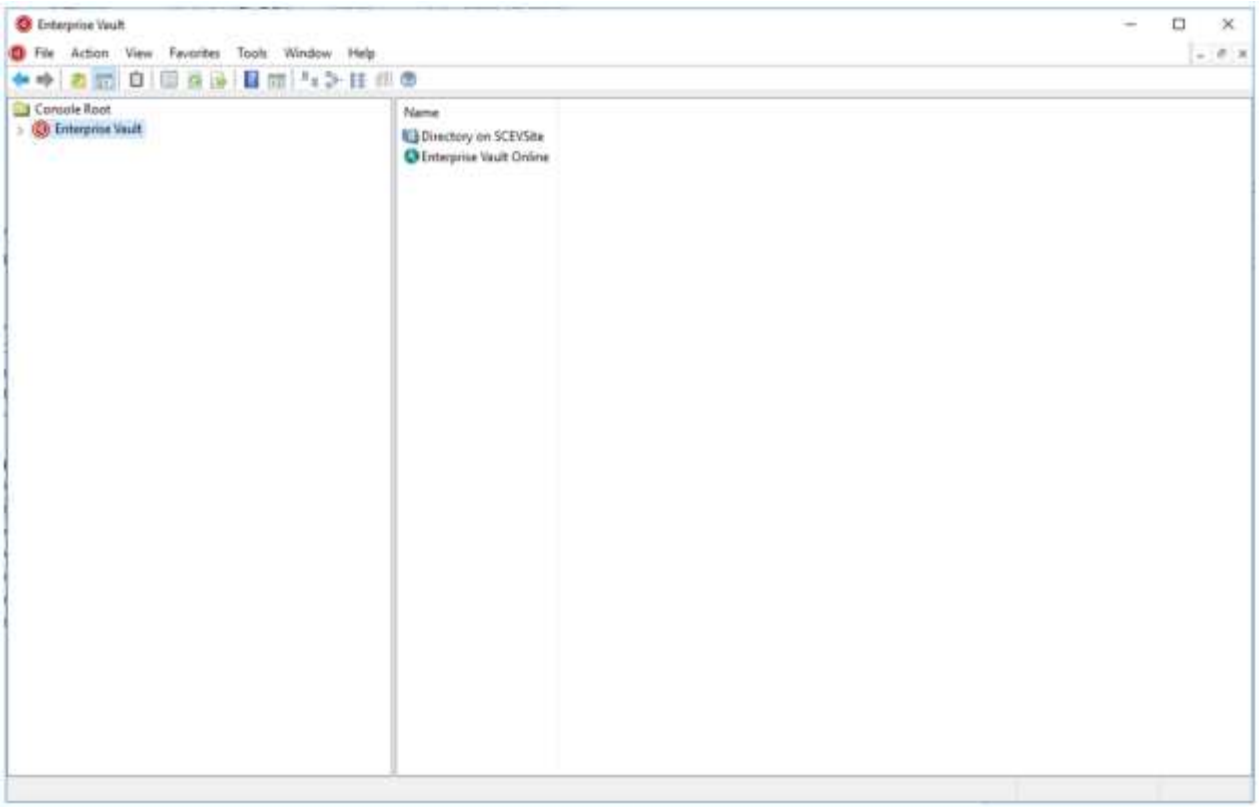
- ボールトストアグループとボールトストアが作成されました。詳細については、『Veritas Enterprise Vault Administration Guide』を参照してください。
- StorageGRIDテナント、アクセスキー、シークレットキー、およびバケットが作成されている。
- StorageGRIDロードバランサエンドポイント（HTTPまたはHTTPS）が作成されている。
- 自己署名証明書を使用する場合は、StorageGRID自己署名CA証明書をEnterprise Vaultサーバーに追加します。詳細については、こちらを参照して "Veritasナレッジベースの記事"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

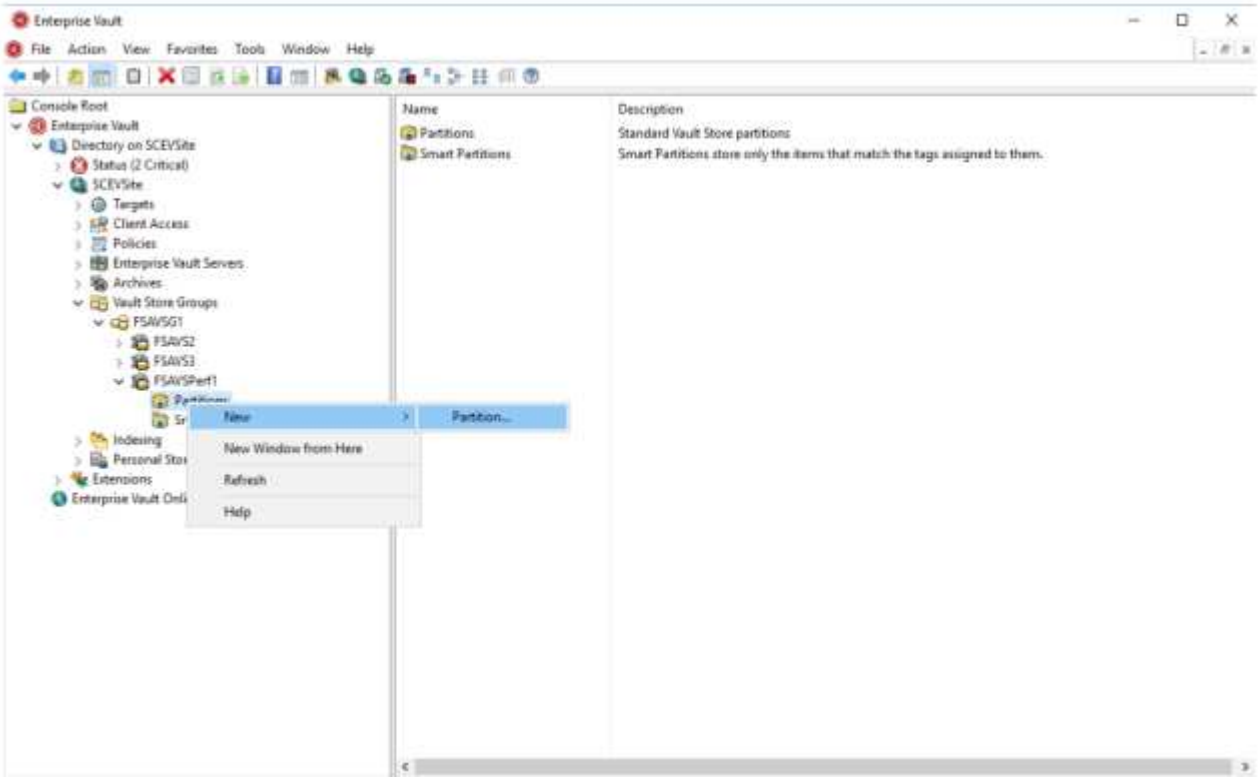
Veritas Enterprise Vaultを使用してStorageGRIDを設定するには、次の手順を実行します。

手順

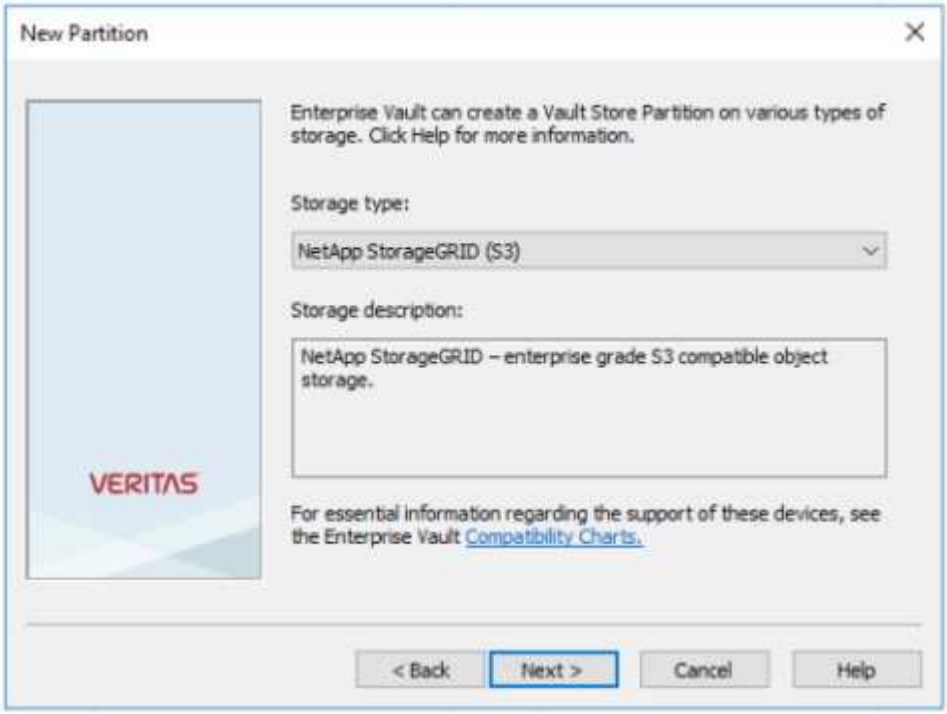
1. Enterprise Vault管理コンソールを起動します。



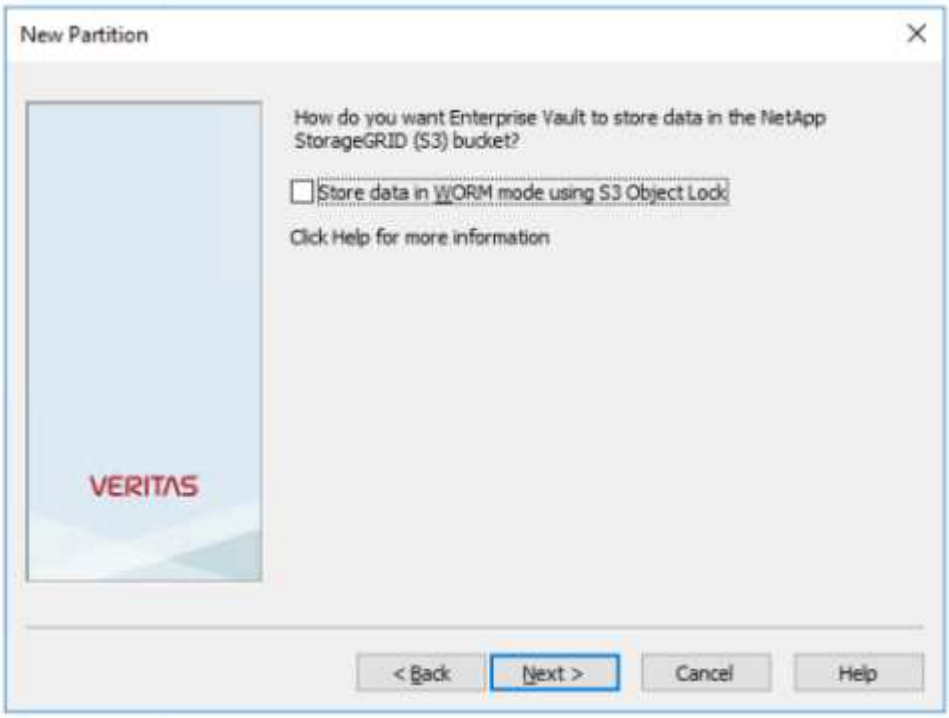
2. 適切なボールトストアに新しいボールトストアパーティションを作成します。ボールトストアグループ（Vault Store Groups）フォルダを展開し、適切なボールトストアを展開します。「パーティション」を右クリックし、メニュー「新規パーティション」を選択します。



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。

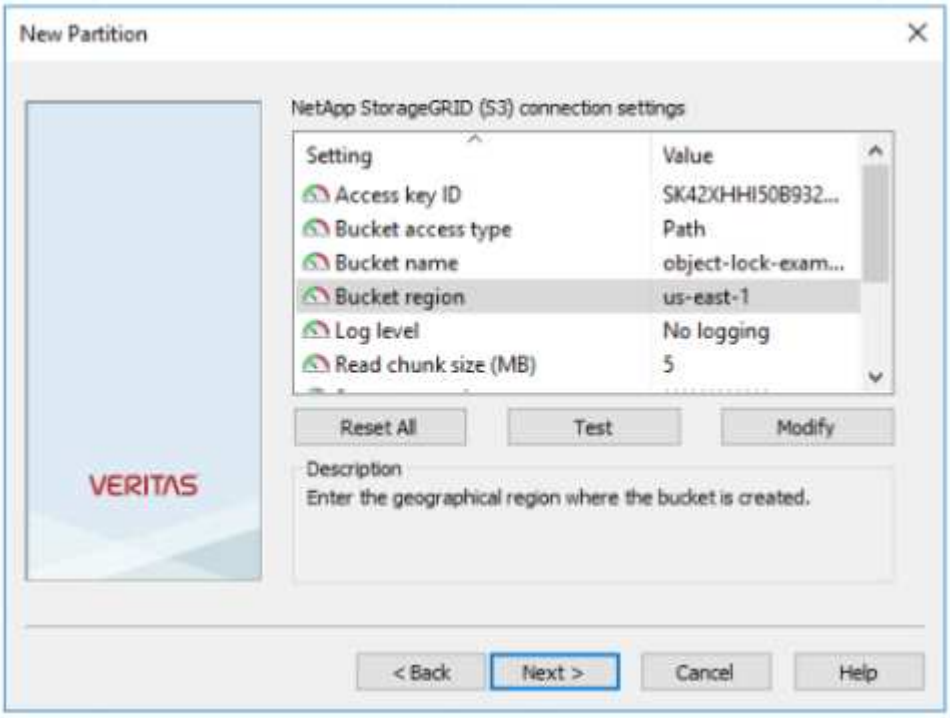


4. [Store Data in WORM Mode using S3 Object Lock]オプションはオフのままにします。[Next]をクリックします。

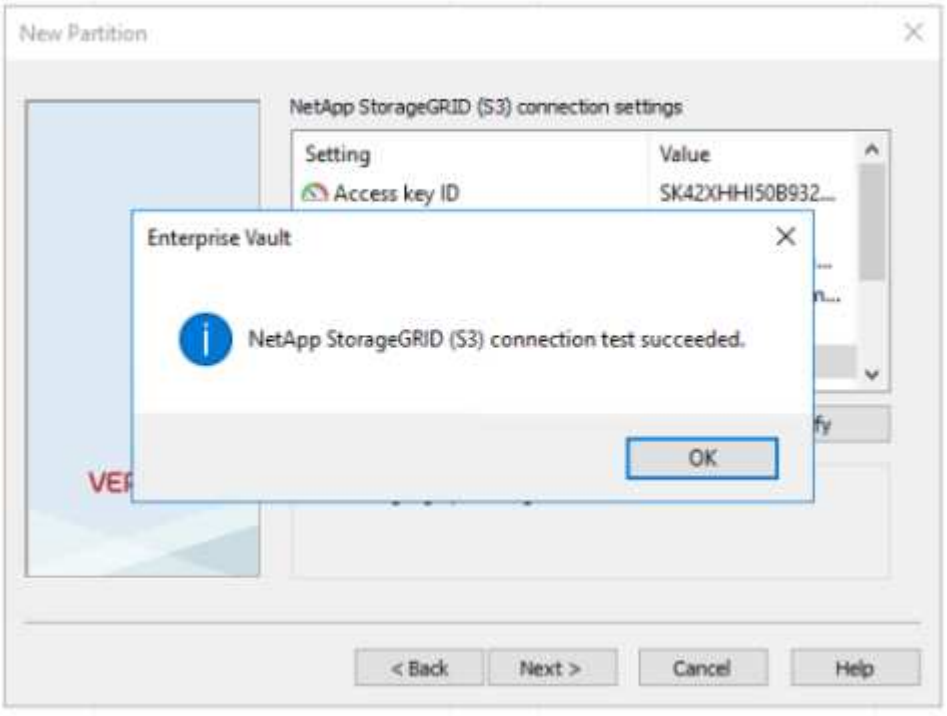


5. 接続設定ページで、次の情報を入力します。
   - アクセスキーID
   - シークレットアクセスキー
   - サービスホスト名：StorageGRIDで設定されたロードバランサエンドポイント（LBE）ポート（\https：//<hostname>：<LBE_port>など）を含めるようにしてください。

- 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ではバケットは作成されません。
- Bucket region： `us-east-1` デフォルト値。

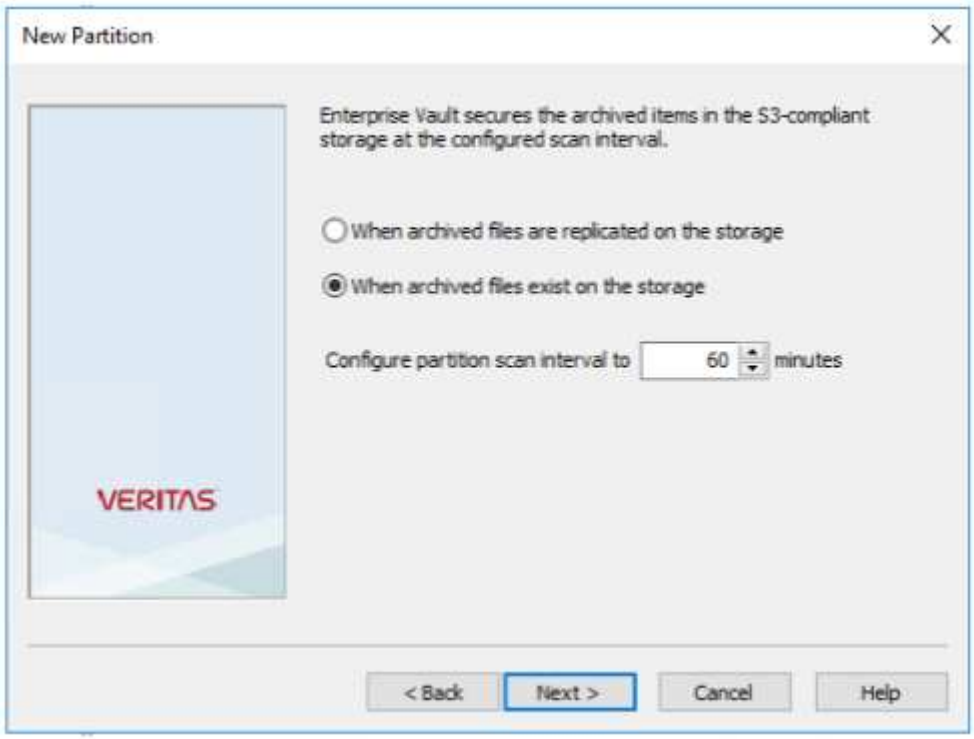


6. StorageGRIDバケットへの接続を確認するには、[Test]をクリックします。接続テストが成功したことを確認します。[OK]をクリックし、[Next]をクリックします。

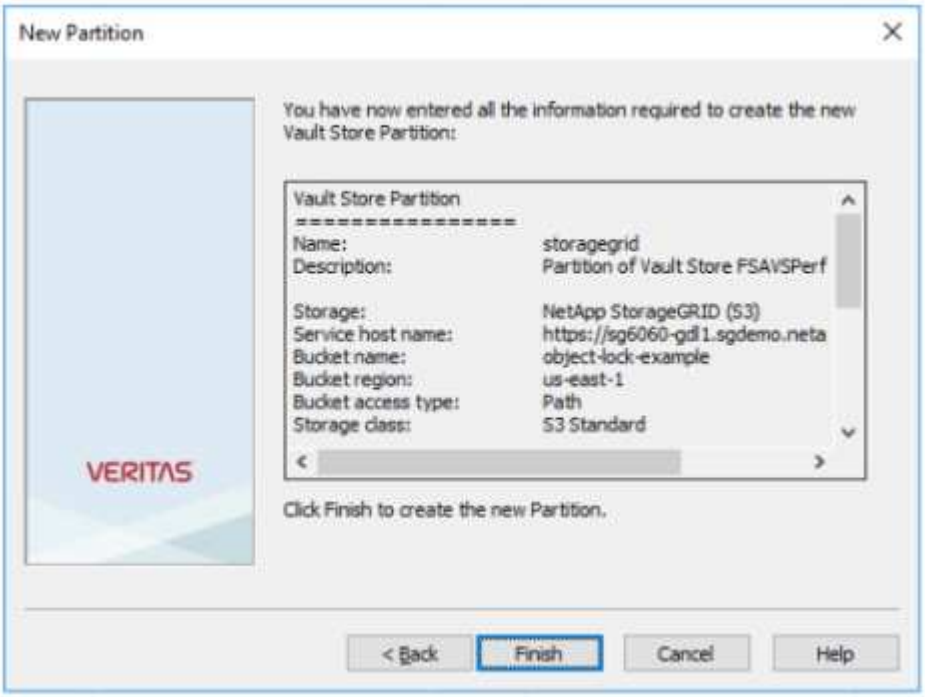


7. StorageGRIDでは、S3レプリケーションパラメータがサポートされません。StorageGRIDでは、オブジェクトを保護するために、情報ライフサイクル管理（ILM）ルールを使用してデータ保護スキーム（複数の

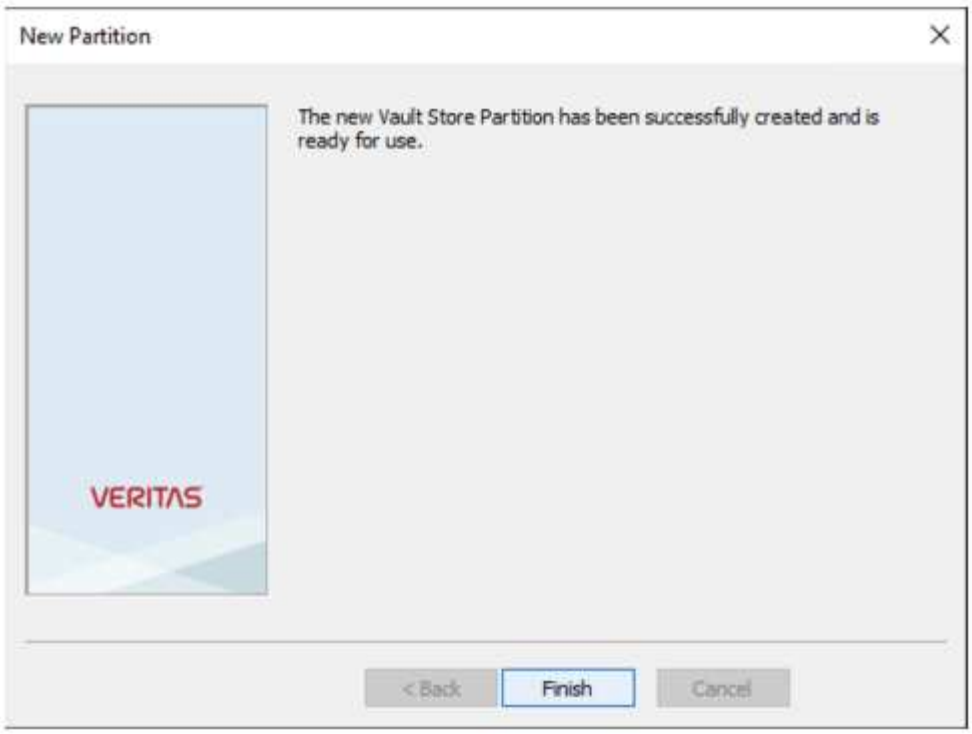
コピーまたはイレイジャーコーディング）を指定します。[When Archived Files Exist on the Storage]オプションを選択し、[Next]をクリックします。



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

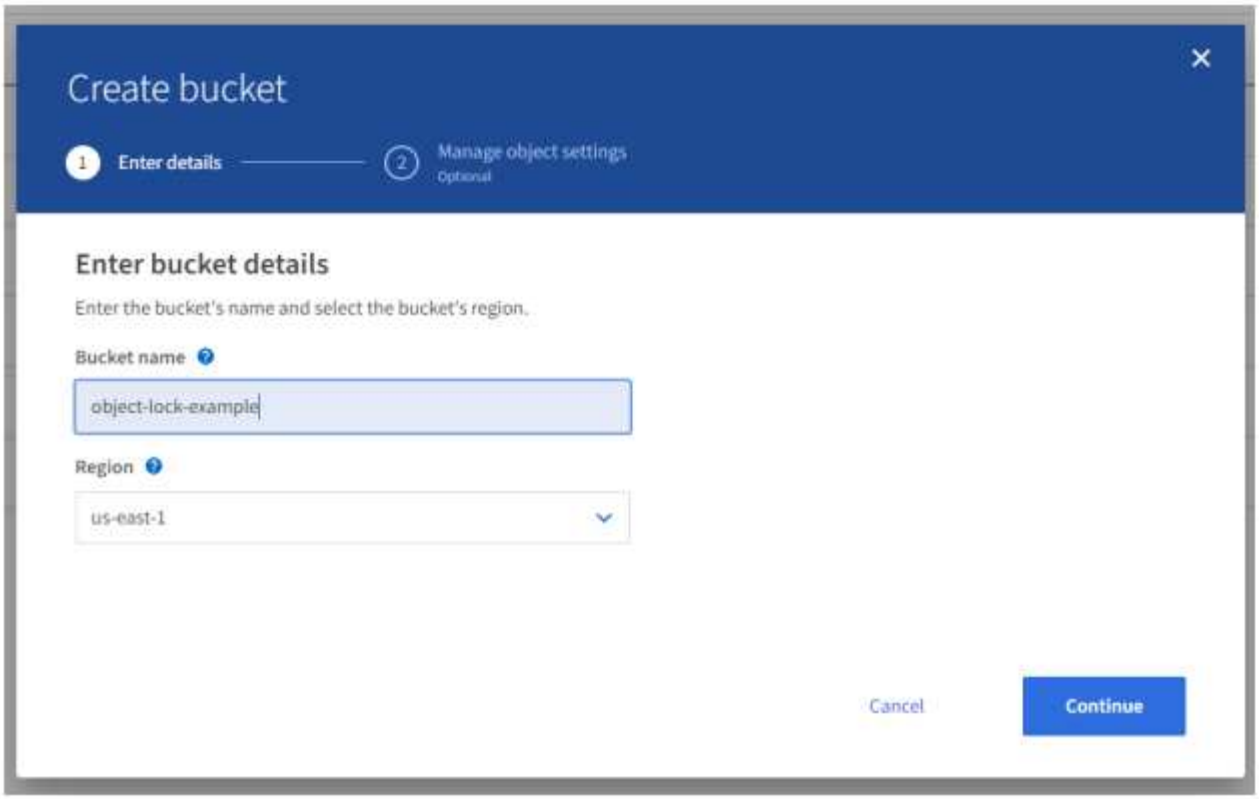
WORMストレージでは、StorageGRIDはS3オブジェクトロックを使用してオブジェクトを保持し、コンプライアンスを確保します。これには、S3オブジェクトロックのデフォルトバケット保持機能が導入されたStorageGRID 11.6以降が必要です。Enterprise Vaultにはバージョン14.2.2以降も必要です。

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

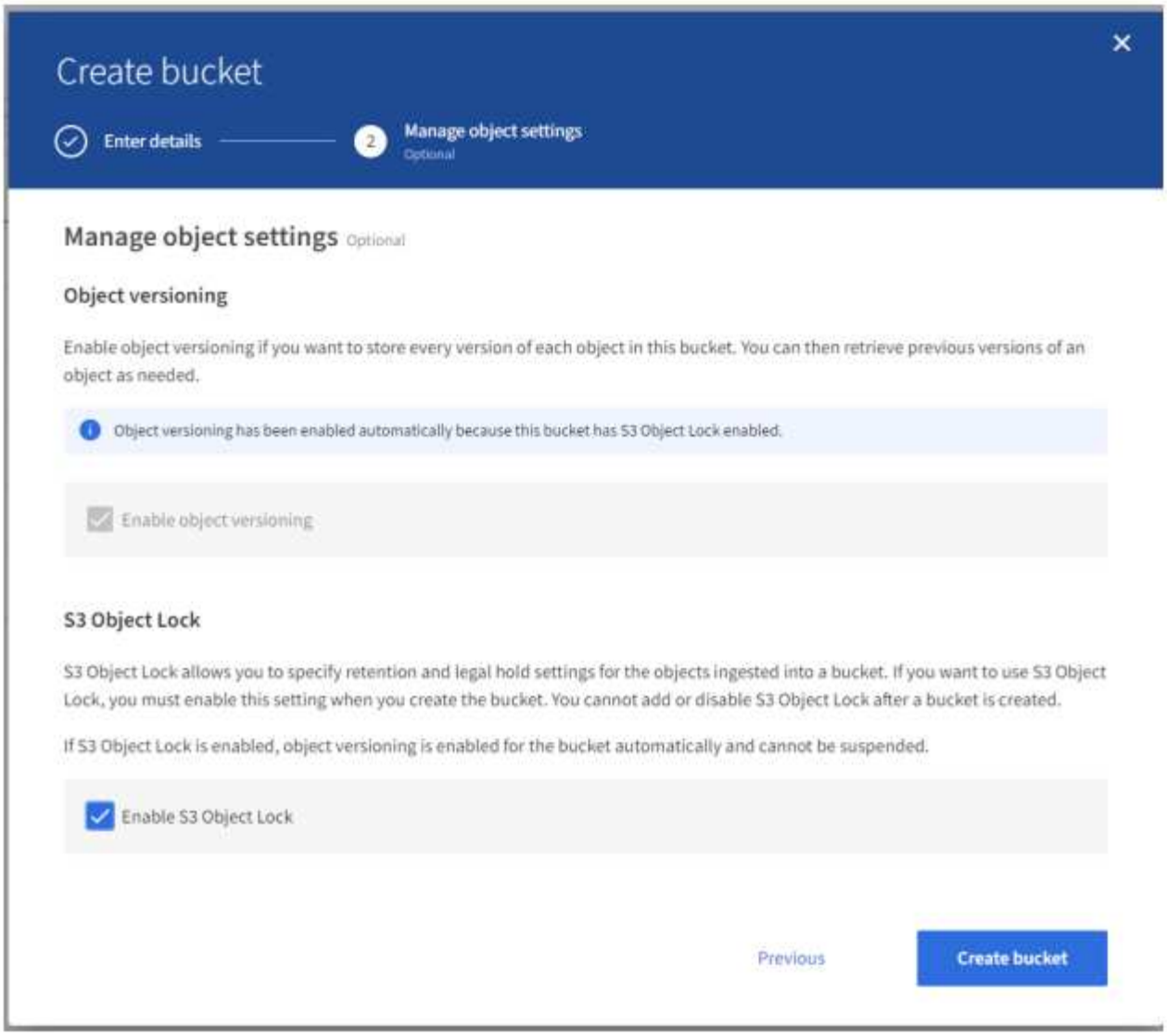
StorageGRID S3オブジェクトロックのデフォルトバケット保持を設定するには、次の手順を実行します。

手順

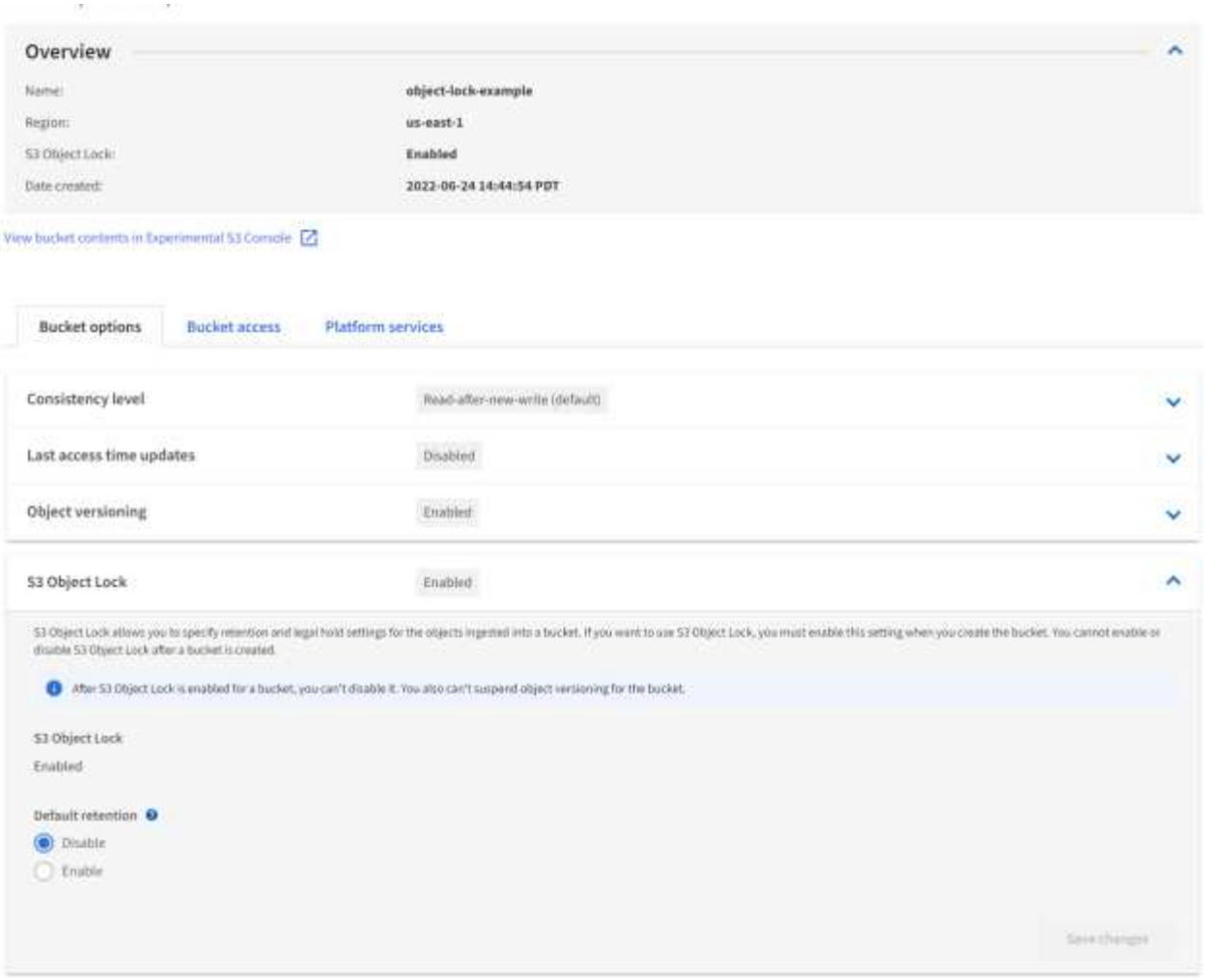
1. StorageGRIDテナントマネージャでバケットを作成し、[Continue]をクリックします。



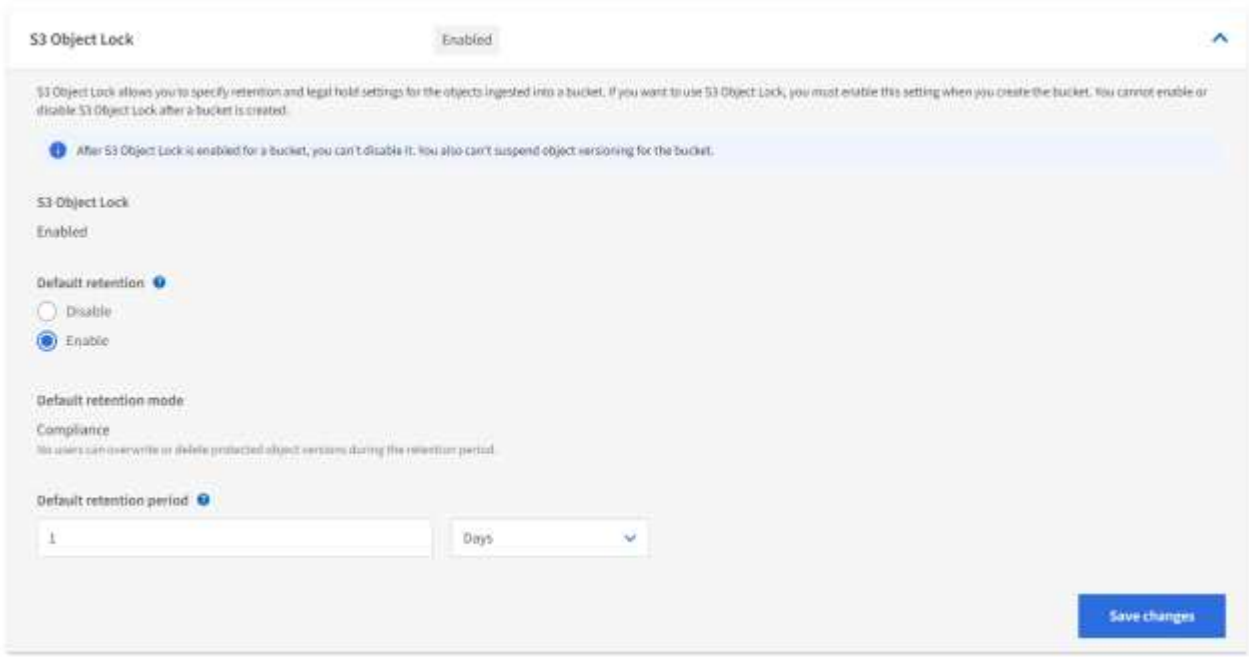
2. [Enable S3 Object Lock]オプションを選択し、[Create Bucket]をクリックします。



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。



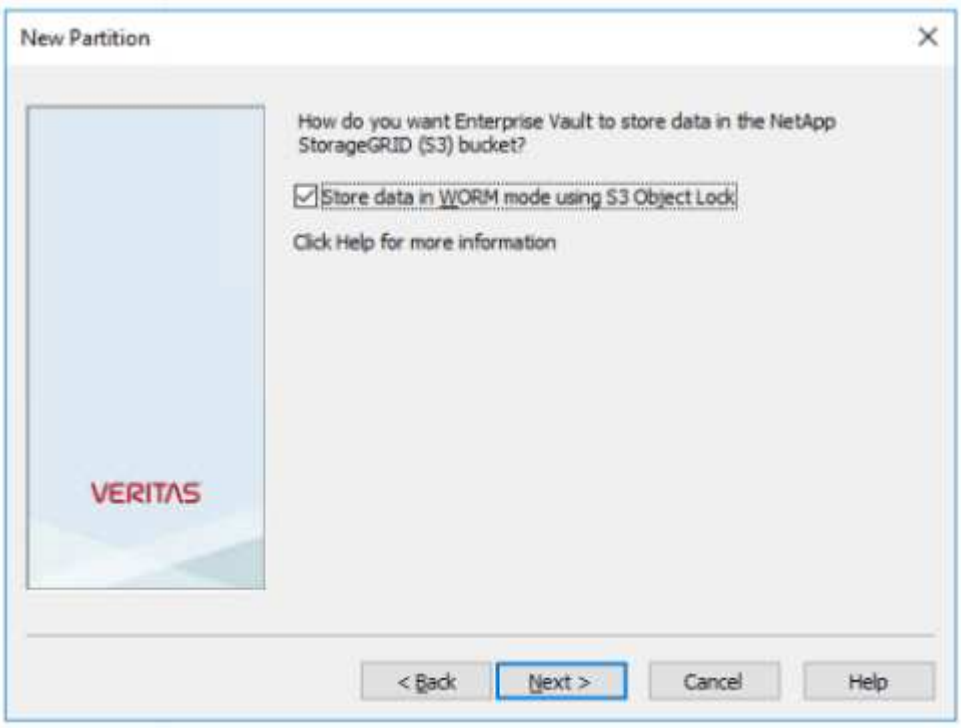
これで、バケットをEnterprise VaultでWORMデータの格納に使用できるようになりました。

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

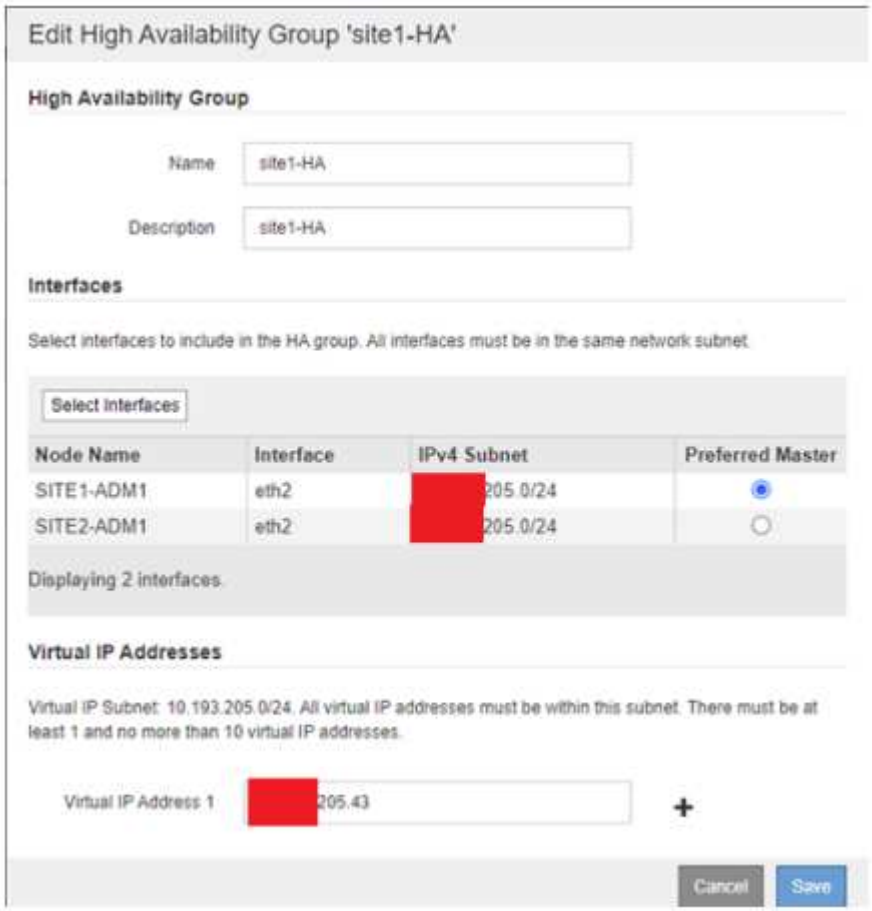
StorageGRIDサイトのフェールオーバーを設定するには、次の手順を実行します。

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。

   [Vertias / Veritas-create-high-availability-group]

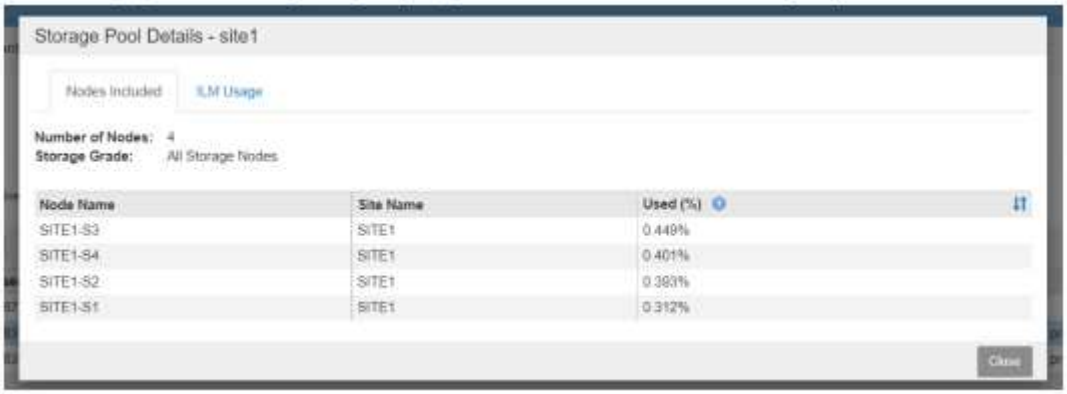
2. 必要な情報を入力します。[Select Interfaces]をクリックし、Site1（プライマリサイト）が優先マスターであるSite2のネットワークインターフェイスを含めます。同じサブネット内の仮想IPアドレスを割り当てます。保存をクリックします。

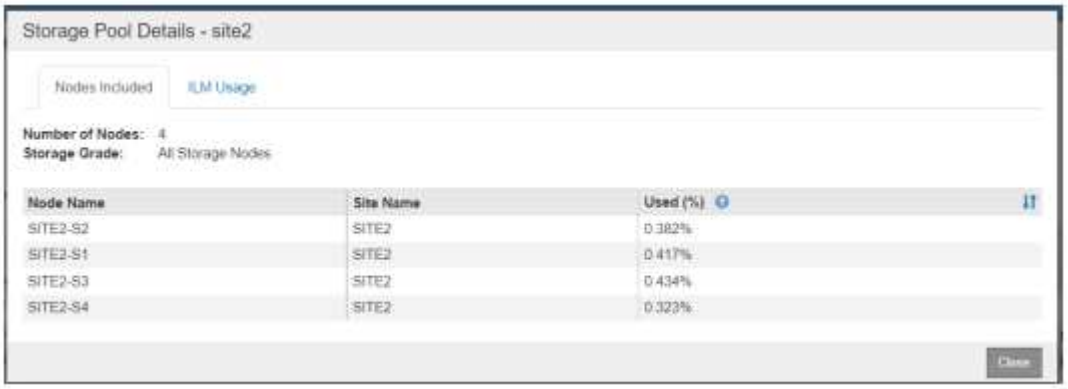


3. この仮想IP（VIP）アドレスは、Veritas Enterprise Vaultのパーティション設定時に使用されるS3ホスト名に関連付ける必要があります。VIPアドレスはトラフィックをSite1に解決します。Site1に障害が発生すると、VIPアドレスはトラフィックをSite2に透過的に再ルーティングします。
4. データがSite1とSite2の両方にレプリケートされていることを確認します。これにより、Site1に障害が発生しても、Site2からオブジェクトデータを引き続き使用できます。そのためには、まずストレージプールを構成します。

   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。

StorageGRID評価ソフトウェアへのアクセス手順

この手順は、NetAppと連携しているNetAppの営業担当者、パートナー様、見込み客を対象としています。

アカウントに登録します

1. お勤め先のEメールアドレスを使用して、でアカウントを登録し "NetAppサポートサイト" ます。
   a. 新しく作成したアカウントでサインインしていないことを確認します。
   b. すでにアカウントをお持ちの場合は、サインインしていないことを確認し、次の手順に進みます。
2. テクニカル以外のサポートケースを作成して、アクセスレベルを「見込み客」に引き上げます。これを行うには、Webサイトのフッターにある「リンク」をクリックして ""問題を報告する"ください。
3. フィードバックカテゴリとして「登録の問題」を選択します。
4. コメント欄に「私のアカウントのメールアドレスは_あなたの-メールアドレス_です。見込み顧客にStorageGRID評価ソフトウェアをダウンロードしてもらいたいのですが」
   a. 見込み客へのアクセスリクエストを提案したNetApp社内担当者の名前を記入します。

StorageGRIDのダウンロード

1. サポートケースの確認と承認が完了すると、NetAppサポートからお客様のアカウントに見込み客へのアクセス権が付与されたことがEメールで通知されます。
2. をダウンロードします "StorageGRID評価用ソフトウェア"。

Evalライセンスファイルはzipファイル内にあります。解凍した時点では、StorageGRID Webscale -<version>\ vsphere \ NLF000000.txtです。

ソフトウェアのダウンロードは、法的要件を遵守するための貿易コンプライアンス措置を含むプロセスです。コンプライアンスを確保するには、アクセスする前にアカウントを作成し、サポートケースをオープンする必要があります。このプロセスは、適切な管理と文書化を維持しながら、見込み客に必要な本番環境対応ソフトウェアを提供するのに役立ちます。

StorageGRIDの「本番環境対応」バージョンを提供しています。これは、オープンソースまたは代替バージョンではありません。お客様が本番環境のライセンスにアップグレードしない限り、サポートは提供されません。

上記の手順で問題が発生した場合は、StorageGRID.Feedback@netapp.comまでお問い合わせください。

ネットアップのStorageGRID ブログ

ネットアップのStorageGRID に関する優れたブログをいくつかご紹介します。

- 24年2月16日： "StorageGRID 11.8の紹介：セキュリティ、簡易性、ユーザエクスペリエンスの強化"
- 24年2月16日： "StorageGRID 11.8の概要"
- 24年2月2日： "StorageGRID + lakeFS解決策概要の発表"
- 23年12月12日： "StorageGRIDでのビッグデータ分析：DremioのパフォーマンスはApache Hiveの23倍"
- 23年11月7日： "Spectra Logic On-Prem GlacierとStorageGRID"
- 23年10月17日： "Hadoopからの移行：DremioとStorageGRIDによるデータ分析の刷新"
- 23年9月1日： "Fluent Bitを使用したCloud Insightsによるログの監視と収集"
- 23年8月30日： "Amazon S3ファイルシステムのマウントポイントの一般提供を開始"
- 23年5月16日： "StorageGRID 11.7と新しいオールフラッシュオブジェクトストレージアプライアンスSGF6112の概要"
- 23年5月16日： "StorageGRIDオブジェクトストレージファミリーの新機能"
- 23年3月30日： "StorageGRID を使用したAmazon S3 alphaリリースのマウントポイント"
- 23年3月30日： "BlueXPを使用して、3：2：1に準拠したバックアップポリシーでEpic EHRを保護"
- 23年3月14日： "3：2：1準拠のアーキテクチャで1つのコマンドでEpic SystemsのEHRデータベースをバックアップする方法"
- 23年2月14日： "チョコレート、スキー、時計、メインフレームにはどのような共通点がありますか？"
- 23年1月18日： "Veritas NetBackupでStorageGRID S3オブジェクトロックが検証されました"
- 23年1月16日： "StorageGRID はNF203およびISO/IEC 25051準拠認定を更新します"
- 22年12月6日： "StorageGRID はKPMGコンプライアンス認証を取得しています"
- 22年11月23日： "ネットアップとModzyを基盤とするMLOpsによる説明可能なAI"
- 22年11月7日： "StorageGRID とONTAP S3のサポート：相違点、類似点、統合"
- 22年10月5日： "NetApp Cloud Insights に、StorageGRID のギャラリーダッシュボードが追加されました"
- 22年10月5日： "StorageGRID for Snowflakeでデータを解凍します"
- 22年09月26日： "NetApp StorageGRID （サービスプロバイダ向け"
- 22年09月19日： "StorageGRID 向けのDataLockおよびランサムウェア対策サポート"
- 22年09月1日： "これらの指標を使用してグラフ化します"
- 22年08月23日： "StorageGRID 上にデータレイクを構築"
- 22年08月17日： "すべてはオブジェクトのロックから始まります。 重要なバックアップアプリケーション向けのS3ストレージエコシステムを構築"
- 22年08月16日： "StorageGRID とオープンソースのELKスタックを統合して、カスタマーエクスペリエンスを強化します"
- 22年08月5日： "NetApp StorageGRID は、Common Criteriaのセキュリティ認定を取得しています"

- 2022年7月26日： "StorageGRID向けの検証済みパートナーソリューションのリストが増え続けていますので、ぜひチェックしてください。"
- 2022年6月9日： "StorageGRID でCloudera Hadoop S3Aコネクタを使用します"
- 2022年5月26日： "StorageGRID：オンプレミスのバックアップデータとレプリケーションデータの格納と管理"
- 2022年5月24日： "ネットアップとAlluxioによる分析ワークロードの刷新"
- 2022年5月10日： "ラボオンデマンドはStorageGRIDに最適な営業ツール"

NetApp StorageGRID のドキュメント

NetApp StorageGRID の各リリースの完全なドキュメントは、次の場所にあります。

- "StorageGRIDアプライアンス"
- "StorageGRIDソフトウェア 11.5 - 12.0"

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

https://library.netapp.com/ecm/ecm_download_file/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511

著作権に関する情報

商標に関する情報